SonicWall® SonicOS 6.5 Connectivity

Administration

Contents

Part 1. Connectivity | VPN

Part 2. Connectivity | SSL VPN

Part 3. Connectivity | Access Points

Part 4. Connectivity | Wireless

Part 5. Connectivity | 3G/4G/Modem

Part 6. Connectivity | Appendixes

Part 1

Connectivity | VPN

VPN Overview

The VPN options provide the features for configuring and displaying your VPN policies. You can configure various types of IPsec VPN policies, such as site-to-site policies, including GroupVPN, and route-based Tunnel Interface policies. For specific details on the setting for these kinds of policies, go to the following sections:

- Site to Site VPNs
- VPN Auto Provisioning
- Tunnel Interface Route-based VPN

This section provides information on VPN types, discusses some of the security options you can select, and describes the interface for the **VPN > Base Settings** page on the **MANAGE** view. Subsequent sections describe how to configure site to site and route-based VPN, advanced settings, DHCP over VPN and L2TP servers.

> ⓘ **NOTE:** Functionality on the **VPN** pages is available when **Wireless Controller Mode** on the **MANAGE | System Setup | Appliance > Base Settings** page is set to either **Full-Feature-Gateway** or **Non-Wireless**. If **Wireless-Controller-Only** is enabled for **Wireless Controller Mode**, adding and managing VPN policies on the **VPN** pages is ***not*** available. See the *SonicOS 6.5 System Setup* administration documentation for more information.

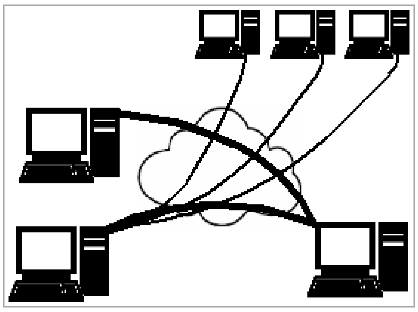
Topics:

- About Virtual Private Networks
- VPN Types
- VPN Security
- VPN Base Settings and Displays
- IPv6 VPN Configuration
- VPN Auto-Added Access Rule Control

About Virtual Private Networks

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public Internet. It provides authentication to ensure that the information is going to and from the correct parties. It also offers security to protect the data from viewing or tampering en route.

A VPN is created by establishing a secure tunnel through the Internet. This tunnel is a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. It is flexible in that you can change it at any time to add more nodes, change the nodes, or remove them altogether. VPN is less costly, because it uses the existing Internet infrastructure.



VPNs can support either remote access—connecting a user's computer to a corporate network—or site to site, which is connecting two networks. A VPN can also be used to interconnect two similar networks over a dissimilar middle network: for example, two IPv6 networks connecting over an IPv4 network.

VPN systems might be classified by:

- Protocols used to tunnel the traffic
- Tunnel's termination point location, for example, on the customer edge or network provider edge
- Type of topology of connections, such as site to site or network to network
- Levels of security provided
- OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
- Number of simultaneous connections

VPN Types

Several types of VPN protocols can be configured for use:

- IPsec VPN
- DHCP over VPN
- L2TP with IPsec
- SSL VPN

IPsec VPN

SonicOS supports the creation and management of IPsec VPNs. These VPNs are primarily configured on the **MANAGE** view at **VPN > Base Settings** and **VPN > Advanced Settings**.

IPsec (Internet Protocol Security) is a standards-based security protocol that was initially developed for IPv6, but it is also widely used with IPv4 and the Layer 2 Tunneling Protocol. Its design meets most security goals of authentication, integrity, and confidentiality. IPsec uses encryption and encapsulates an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.

An advantage of using IPsec is that security arrangements can be handled without requiring changes to individual user computers. It provides two types of security service:

- Authentication Header (AH), which essentially allows authentication of the sender of data

- Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data

You can use IPsec to develop policy-based VPN (site to site) or route-based VPN tunnels or Layer 2 Tunneling Protocol (L2TP).

DHCP over VPN

SonicOS allows you to configure a firewall to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, you want to have all VPN networks on one logical IP subnet and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.

The firewall at the remote and central sites are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The firewall at the remote site passes DHCP broadcast packets through its VPN tunnel. The firewall at the central site relays DHCP packets from the client on the remote network to the DHCP server on the central site.

L2TP with IPsec

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support VPNs or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself, and because of that lack of confidentiality in the L2TP protocol, it is often implemented along with IPsec. The general process for setting up an L2TP/IPsec VPN is:

1. Negotiate an IPsec security association (SA), typically through Internet key exchange (IKE). This is carried out over UDP port 500, and commonly uses either a shared password (also called *pre-shared keys*), public keys, or X.509 certificates on both ends, although other keying methods exist.
2. Establish Encapsulating Security Payload (ESP) communication in transport mode. The IP protocol number for ESP is 50 (compare TCP's 6 and UDP's 17). At this point, a secure channel has been established, but no tunneling is taking place.
3. Negotiate and establish L2TP tunnel between the SA endpoints. The actual negotiation of parameters takes place over the SA's secure channel, within the IPsec encryption. L2TP uses UDP port 1701.

When the process is complete, L2TP packets between the endpoints are encapsulated by IPsec. Because the L2TP packet itself is wrapped and hidden within the IPsec packet, no information about the internal private network can be garnered from the encrypted packet. Also, UDP port 1701 does not need to be opened on firewalls between the endpoints, because the inner packets are not acted upon until after IPsec data has been decrypted and stripped, which only takes place at the endpoints.

SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional IPsec VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It can be used to give remote users access to Web applications, client/server applications, and internal network connections.

An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) protocol. An SSL VPN offers versatility, ease of use and granular control for a range of users on a variety of computers, accessing resources from many locations. The two major types of SSL VPNs are:

- SSL Portal VPN
- SSL Tunnel VPN

The SSL Portal VPN allows single SSL connection to a Web site so the end user can securely access multiple network services. The site is called a portal because it is one door (a single page) that leads to many other resources. The remote user accesses the SSL VPN gateway using any modern Web browser, identifies himself or herself to the gateway using an authentication method supported by the gateway and is then presented with a Web page that acts as the portal to the other services.

The SSL tunnel VPN allows a Web browser to securely access multiple network services, including applications and protocols that are not Web-based, through a tunnel that is running under SSL. SSL tunnel VPNs require that the Web browser be able to handle active content, which allows them to provide functionality that is not accessible to SSL portal VPNs. Examples of active content include Java, JavaScript, Active X, or Flash applications or plug-ins.

SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. It also uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. An SRA/SMA appliance uses SSL to secure the VPN tunnel. One advantage of SSL VPN is that SSL is built into most web browsers. No special VPN client software or hardware is required.

> **NOTE:** SonicWall makes Secure Mobile Access (SMA) appliances you can use in concert with or independently of a SonicWall network security appliance running SonicOS. For information on SonicWall SMA appliances, refer to https://www.sonicwall.com/products/remote-access/remote-access-appliances.

VPN Security

IPsec VPN traffic is secured in two stages:

1. **Authentication**: The first phase establishes the authenticity of the sender and receiver of the traffic using an exchange of the public key portion of a public-private key pair. This phase must be successful before the VPN tunnel can be established.
2. **Encryption**: The traffic in the VPN tunnel is encrypted, using an encryption algorithm such as AES or 3DES.

Unless you use a manual key (which must be typed identically into each node in the VPN), the exchange of information to authenticate the members of the VPN and encrypt/decrypt the data uses the Internet Key Exchange (IKE) protocol for exchanging authentication information (keys) and establishing the VPN tunnel. SonicOS supports two versions of IKE:

IKE version 1 (IKEv1)	Uses a two phase process to secure the VPN tunnel. First, the two nodes authenticate each other and then they negotiate the methods of encryption.
	You can find more information about IKEv1 in the three specifications that initially define IKE: RFC 2407, RFC 2408, and RFC 2409. They are available on the web at: • http://www.faqs.org/rfcs/rfc2407.html – *The Internet IP Security Domain of Interpretation for ISAKMP* • http://www.faqs.org/rfcs/rfc2408.html – *RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)* • http://www.faqs.org/rfcs/rfc2409.html – *RFC 2409 - The Internet Key Exchange (IKE)*

IKE version 2 (IKEv2)	Is the default type for new VPN policies because of improved security, simplified architecture, and enhanced support for remote users. A VPN tunnel is initiated with a pair of message exchanges. The first pair of messages negotiate cryptographic algorithms, exchange nonces (random values generated and sent to guard against repeated messages), and perform a public key exchange. The second pair of messages authenticates the previous messages, exchange identities and certificates, and establish the first CHILD_SA (security association). Parts of these messages are encrypted and integrity protected with keys established through the first exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated.
	You can find more information about IKEv2 in the specification, RFC 4306, available on the Web at: http://www.ietf.org/rfc/rfc4306.txt.

ⓘ **IMPORTANT:** IKEv2 is not compatible with IKEv1. When using IKEv2, all nodes in the VPN must use IKEv2 to establish the tunnels.
DHCP over VPN is not supported in IKEv2.

For more VPN security information, see:

- About IKEv1
- About IKEv2
- Mobility and Multi-homing Protocol for IKEv2 (MOBIKE)
- About IPsec (Phase 2) Proposal
- About Suite B Cryptography

About IKEv1

In IKEv1, two modes are used to exchange authentication information:

- **Main Mode**: The node or gateway initiating the VPN queries the node or gateway on the receiving end, and they exchange authentication methods, public keys, and identity information. This usually requires six messages back and forth. The order of authentication messages in Main Mode is:
    1) The initiator sends a list of cryptographic algorithms the initiator supports.
    2) The responder replies with a list of supported cryptographic algorithms.
    3) The initiator send a public key (part of a Diffie-Hellman public/private key pair) for the first mutually supported cryptographic algorithm.
    4) The responder replies with the public key for the same cryptographic algorithm.
    5) The initiator sends identity information (usually a certificate).
    6) The responder replies with identity information.
- **Aggressive Mode**: To reduce the number of messages exchanged during authentication by half, the negotiation of which cryptographic algorithm to use is eliminated. The initiator proposes one algorithm and the responder replies if it supports that algorithm:
    1) The initiator proposes a cryptographic algorithm to use and sends its public key.
    2) The responder replies with a public key and identity proof.
    3) The initiator sends an identification proof. After authenticating, the VPN tunnel is established with two SAs, one from each node to the other.

About IKEv2

IKE version 2 (IKEv2) is a newer protocol for negotiating and establishing security associations. Secondary gateways are supported with IKEv2. IKEv2 is the default proposal type for new VPN policies.

> **NOTE:** IKEv2 is not compatible with IKEv1. When using IKEv2, all nodes in the VPN must use IKEv2 to establish the tunnels. DHCP over VPN is not supported in IKEv2.

IKEv2 has the following advantages over IKEv1:

- More secure
- More reliable
- Simpler
- Faster
- Extensible
- Fewer message exchanges to establish connections
- EAP Authentication support
- MOBIKE support
- Built-in NAT traversal
- Keep Alive is enabled as default

IKEv2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKEv2 greatly reduces the number of message exchanges needed to establish a Security Association over IKEv1 Main Mode, while being more secure and flexible than IKEv1 Aggressive Mode. This reduces the delays during re-keying. As VPNs grow to include more and more tunnels between multiple nodes or gateways, IKEv2 reduces the number of Security Associations required per tunnel, thus reducing required bandwidth and housekeeping overhead.

Security Associations (SAs) in IKEv2 are called Child SAs and can be created, modified, and deleted independently at any time during the life of the VPN tunnel.

Mobility and Multi-homing Protocol for IKEv2 (MOBIKE)

The Mobility and Multi-homing Protocol (MOBIKE) for IKEv2 provides the ability for maintaining a VPN session, when a user moves from one IP address to another, without the need for reestablishing IKE security associations with the gateway. For example, a user could establish a VPN tunnel while using a fixed Ethernet connection in the office. MOBIKE allows the user to disconnect the laptop and move to the office's wireless LAN without interrupting the VPN session.

MOBIKE operation is transparent and does not require any extra configuration by you or consideration by users.

About IPsec (Phase 2) Proposal

The IPsec (Phase 2) proposal occurs with both IKEv1 and IKEv2. In this phase, the two parties negotiate the type of security to use, which encryption methods to use for the traffic through the tunnel (if needed), and negotiate the lifetime of the tunnel before re-keying is needed.

The two types of security for individual packets are:

- **Encryption Secured Payload (ESP)**, in which the data portion of each packet is encrypted using a protocol negotiated between the parties.
- **Authentication Header (AH)**, in which the header of each packet contains authentication information to ensure the information is authenticated and has not been tampered with. No encryption is used for the data with AH.

SonicOS supports the following **Encryption** methods for traffic through the VPN:

- DES
- 3DES
- None
- AES-128
- AES-192
- AES-256
- AESGCM16-128
- AESGCM16-192
- AESGCM16-256
- AESGMAC-128
- AESGMAC-192
- AESGMAC-256

SonicOS supports the following **Authentication** methods:

- MD5
- SHA1
- SHA256
- SHA384
- SHA512
- AES-XCBC
- None

About Suite B Cryptography

SonicOS supports Suite B cryptography, which is a set of cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program. It serves as an interoperable cryptographic base for both classified and unclassified information. Suite B cryptography is approved by National Institute of Standards and Technology (NIST) for use by the U.S. Government.

Most of the Suite B components are adopted from the FIPS standard:

- Advanced Encryption Standard (AES) with key sizes of 128 to 256 bits (provides adequate protection for classified information up to the SECRET level).
- Elliptic Curve Digital Signature Algorithm (ECDSA) digital signatures (provides adequate protection for classified information up to the SECRET level).
- Elliptic Curve Diffie-Hellman (ECDH) key agreement (provides adequate protection for classified information up to the SECRET level).
- Secure Hash Algorithm 2 (SHA256, SHA384, SHA512) message digest (provides adequate protection for classified information up to the TOP SECRET level).

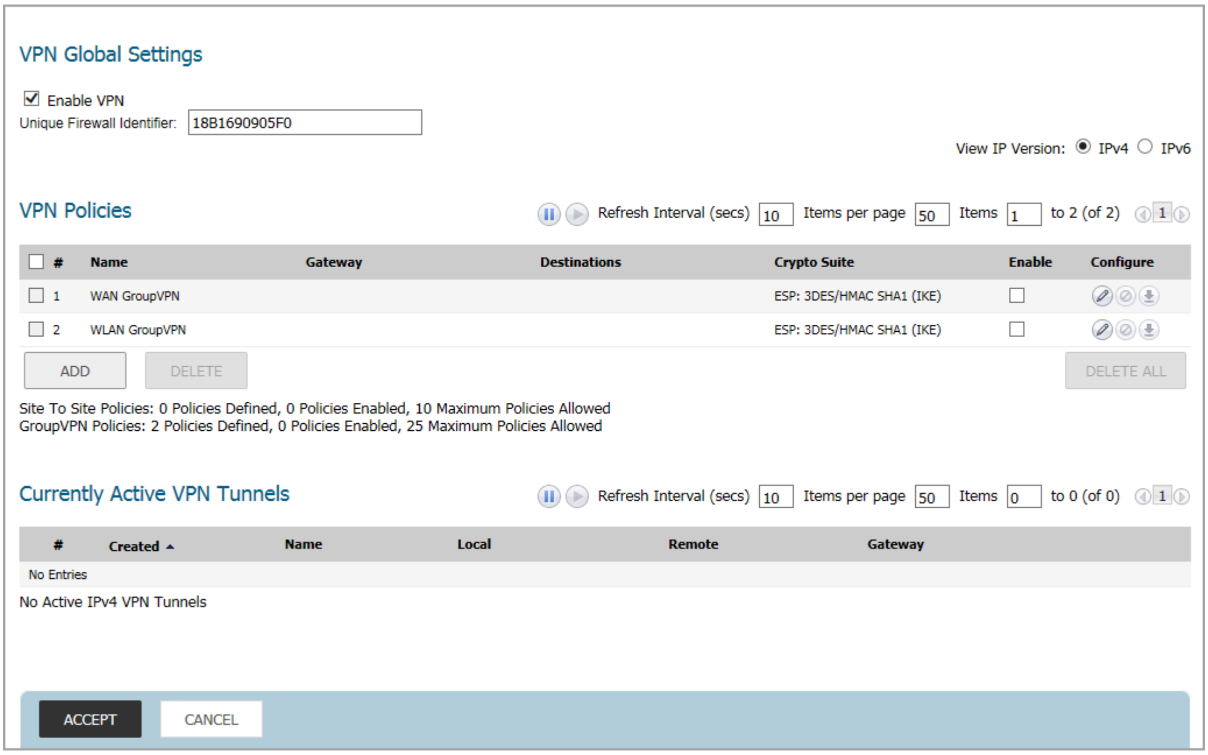
VPN Base Settings and Displays

The VPN pages offer a series of tables and settings, depending on the options selected. For information about how to navigate the tables and settings, refer to the *SonicOS 6.5 About SonicOS* administration documentation.

For details on the **VPN > Base Settings** page, refer to the following:

- VPN Global Settings
- VPN Policies
- Currently Active VPN Tunnels

VPN > Base Settings page



VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier: 18B1690905F0

View IP Version: ● IPv4 ○ IPv6

VPN Policies

Refresh Interval (secs) 10 Items per page 50 Items 1 to 2 (of 2)

☐ #	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
☐ 1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	☐	
☐ 2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	☐	

Site To Site Policies: 0 Policies Defined, 0 Policies Enabled, 10 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 25 Maximum Policies Allowed

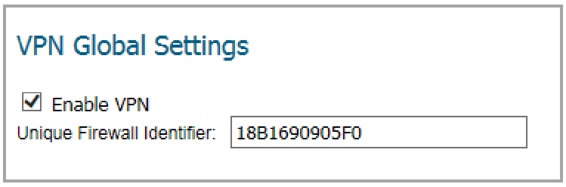
Currently Active VPN Tunnels

Refresh Interval (secs) 10 Items per page 50 Items 0 to 0 (of 0)

#	Created ▲	Name	Local	Remote	Gateway
No Entries					

No Active IPv4 VPN Tunnels

VPN Global Settings



VPN Global Settings

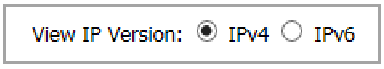
☑ Enable VPN

Unique Firewall Identifier: 18B1690905F0

The **Global VPN Settings** section of the **VPN > Base Settings** page displays the following information:

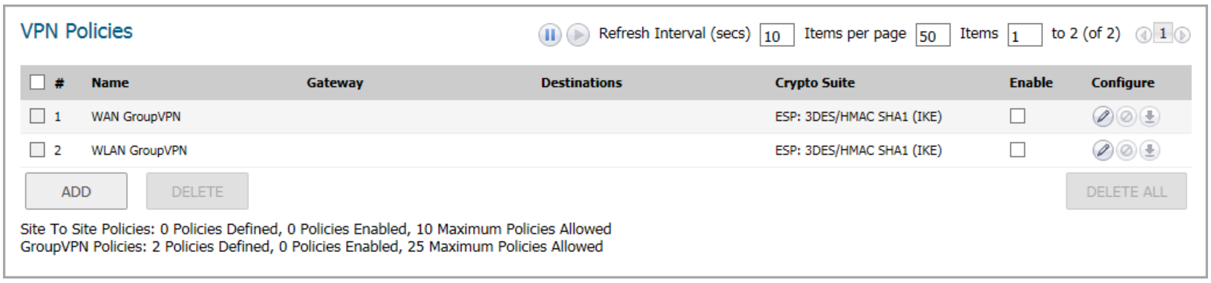
Enable VPN	Select to enable VPN policies through the SonicWall® security policies.
Unique Firewall Identifier	Identifies this SonicWall appliance when configuring VPN tunnels. The default value is the serial number of the appliance. You can change the identifier to something meaningful to you.
View IP Version	Sets IP version view. Options are **IPv4** or **IPv6**.

SonicWall VPN supports both IPv4 and IPv6 (Internet Protocol version 4 and Internet Protocol version 6). You can toggle between the versions by selecting the one you want in the upper right side of the window. The default view is for IPv4.



View IP Version: ● IPv4 ○ IPv6

VPN Policies



VPN Policies

Refresh Interval (secs) 10 Items per page 50 Items 1 to 2 (of 2)

□	#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
□	1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	□	✎ ⊘ ⤓
□	2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	□	✎ ⊘ ⤓

Site To Site Policies: 0 Policies Defined, 0 Policies Enabled, 10 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 25 Maximum Policies Allowed

All defined VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:

- **Name** – The default name or user-defined VPN policy name.
- **Gateway** – The IP address of the remote firewall. If the wildcard IP address, `0.0.0.0,` is used, it is displayed as the IP address.
- **Destinations** – The IP addresses of the destination networks.
- **Crypto Suite** – The type of encryption used for the VPN policy.
- **Enable** – Shows whether the policy is enabled. A checked box enables the VPN Policy. Clearing the box disables it.
- **Configure** – Options for managing the individual VPN policies:
  - **Edit** icon allows you to edit the VPN policy.
  - **Delete** icon deletes the policy on that line. The predefined GroupVPN policies cannot be deleted, so the **Delete** icons are dimmed.
  - **Export** icon exports the VPN policy configuration as a file for local installation by SonicWall Global VPN Clients.

The following buttons are shown below the VPN Policies table:

ADD	Accesses the **VPN Policy** window to configure site to site VPN policies.
DELETE	Deletes the selected (checked box before the VPN policy name in the **Name** column first). You cannot delete the GroupVPN policies.
DELETE ALL	Deletes all VPN policies in the VPN Policies table except the default GroupVPN policies.

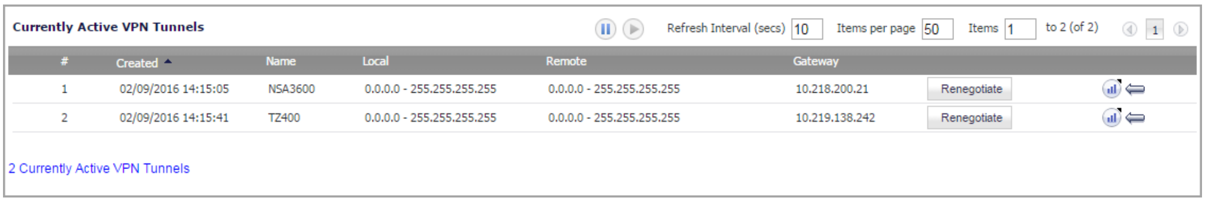
Some statistics about the VPN policies are also summarized below the table, for both site to site and GroupVPN policies:

- Number of policies defined
- Number of policies enabled
- Maximum number of policies allowed

You can define up to four GroupVPN policies, one for each zone. These GroupVPN policies are listed by default in the **VPN Policies** table as **WAN GroupVPN, LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. Clicking on the **Edit** icon in the **Configure** column for the GroupVPN displays the **Security Policy** window for configuring the GroupVPN policy.

NOTE: A VPN Policy cannot have two different WAN interfaces if the VPN Gateway IP is the same.

Currently Active VPN Tunnels



Currently Active VPN Tunnels

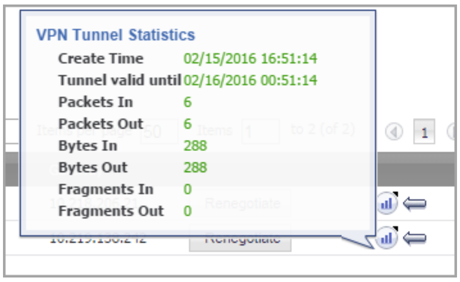
Refresh Interval (secs) 10 Items per page 50 Items 1 to 2 (of 2)

#	Created	Name	Local	Remote	Gateway		
1	02/09/2016 14:15:05	NSA3600	0.0.0.0 - 255.255.255.255	0.0.0.0 - 255.255.255.255	10.218.200.21	Renegotiate	
2	02/09/2016 14:15:41	TZ400	0.0.0.0 - 255.255.255.255	0.0.0.0 - 255.255.255.255	10.219.138.242	Renegotiate	

2 Currently Active VPN Tunnels

A list of currently active VPN tunnels is displayed in this section. The **Currently Active VPN Tunnels** table displays this information for each tunnel:

Created	Date and time the tunnel was created
Name	Name of the VPN Policy
Local	Local LAN IP address of the tunnel
Remote	Remote destination network IP address
Gateway	Peer gateway IP address
Renegotiate button	Forces the VPN Client to renegotiate the VPN tunnel when selected
Statistics icon	When the mouse hovers over the **Statistics** icon, **VPN Tunnel Statistics** are displayed:

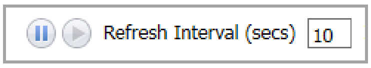


VPN Tunnel Statistics

Create Time	02/15/2016 16:51:14
Tunnel valid until	02/16/2016 00:51:14
Packets In	6
Packets Out	6
Bytes In	288
Bytes Out	288
Fragments In	0
Fragments Out	0

Left-arrow icon	When the mouse hovers over the **Left-arrow** icon, the respective VPN policy is displayed in the middle of the **VPN Policies** table

You can refresh the active tunnels by using the **Refresh Interval** options at the top of the **VPN Policies** and **Currently Active VPN Tunnels** tables:



Refresh Interval (secs) 10

You can set the **Refresh Interval** by specifying how often, in seconds, the tunnels refresh. Pause the refresh by clicking the **Pause** icon or start the refresh by clicking the **Start** icon.

IPv6 VPN Configuration

Site to Site VPNs can be configured for IPv6 in a similar manner to IPv4 VPNs after selecting the **IPv6** option in the **View IP Version** radio button on the **VPN > Base Settings** page.

There are certain VPN features that are currently not supported for IPv6, including:

- IKEv1 is not supported.
- GroupVPN is not supported.
- Tunnel Interface route-based VPN is not supported.

- DHCP Over VPN is not supported.
- L2TP Server is not supported.

When configuring an IPv6 VPN policy:

- On the **General** screen:
  - The **Gateways** must be configured using IPv6 addresses. FQDN is not supported.
  - Under **IKE Authentication**, IPV6 addresses can be used for the local and peer IKE IDs.
- On the **Network** screen:
  - IPV6 address objects (or address groups that contain only IPv6 address objects) must be selected for the **Local Network** and **Remote Network**.
  - **DHCP Over VPN** is not supported, thus the DHCP options for protected network are not available.
  - The **Any address** option for **Local Networks** and the **Tunnel All** option for **Remote Networks** are removed, but you can select an ***all zero*** IPv6 Network address object for the same functionality and behavior.
- On the **Proposals** screen, only **IKEv2 mode** is supported.
- On the **Advanced** screen, several options are disabled for IPv6 VPN policies:
  - **Suppress automatic Access Rules creation for VPN Policy** is disabled.
  - **Enable Windows Networking (NetBIOS) Broadcast** is disabled.
  - **Enable Multicast** is disabled.
  - **Apply NAT Policies** is disabled.

> **NOTE:** Because an interface might have multiple IPv6 address, sometimes the local address of the tunnel might vary periodically. If the user needs a consistent IP address, configure the **VPN policy bound to** option as an interface instead of a zone, and specify the address manually. The address must be one of the IPv6 addresses for that interface.

VPN Auto-Added Access Rule Control

When adding VPN Policies, SonicOS auto-creates non-editable Access Rules to allow the traffic to traverse the appropriate zones. Consider the following VPN Policy, where the Local Network is set to Firewalled Subnets (in this case comprising the LAN and DMZ) and the Destination Network is set to Subnet `192.168.169.0`.

While this is generally a tremendous convenience, you might want to suppress the auto-creation of Access Rules in support of a VPN Policy. One such instance would be the case of a large hub-and-spoke VPN deployment where all the spoke sites are addresses using address spaces that can easily be supernetted. For example, to provide access to/from the LAN and DMZ at the hub site to one subnet at each of 2,000 remote sites, addressed as follows:

remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)

Creating VPN Policies for each of these remote sites would result in having 2,000 VPN Policies, but would also create 8,000 Access Rules (LAN -> VPN, DMZ -> VPN, VPN -> LAN, and VPN -> DMZ for each site). However, all of these Access Rules could easily be handled with just four Access Rules to a supernetted or address range representation of the remote sites (more specific allow or deny Access Rules could be added as needed):

remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255) or
remoteRangeAll=Range 10.0.0.0-10.7.207.255

To enable this level of aggregation, the **Advanced** tab of the **VPN Policy** dialog offers the **Suppress automatic Access Rules creation for VPN Policy** option for site to site VPN policies. By default, the checkbox is not selected, meaning the accompanying Access Rules are created automatically, as they've always been. By selecting the checkbox when creating the VPN Policy, you have the ability and need to create custom Access Rules for the VPN traffic.

2

Site to Site VPNs

SonicWall VPN is based on the industry-standard IPsec VPN implementation. It provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners through the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dial-up Internet access can securely and easily access your network resources with the SonicWall Global VPN Client and GroupVPN on your firewall. Remote office networks can securely connect to your network using site to site VPN connections that enable network-to-network VPN connections.

The maximum number of policies you can add depends on which SonicWall model you have. The larger models allow more connections.

> ⓘ **NOTE:** Remote users must be explicitly granted access to network resources. Refer to *SonicOS 6.5 System Setup* for more information. Depending on how you define access, you can affect the ability of remote clients using GVC to connect to GroupVPN, but you can also affect remote users using NetExtender and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the allow list on the **VPN Access** window. To access this window, select the **MANAGE** view, and under **System Setup**, click **Users > Local Users & Groups > Local User > Add > VPN Access**.

This section describes site to site policies, including GroupVPN. Other sections describe auto provisioning and Tunnel Interface policies for route-based VPN. For specific details on the setting for these kinds of policies, go to the following sections:

- VPN Auto Provisioning
- Tunnel Interface Route-based VPN

Topics:

- Planning Site to Site Configurations
- General VPN Configuration
- Managing GroupVPN Policies
- Creating Site to Site VPN Policies

Planning Site to Site Configurations

You have many options when configuring site to site VPN and can include the following options:

Branch Office (Gateway to Gateway)	A SonicWall firewall is configured to connect to another SonicWall firewall through a VPN tunnel. Or, a SonicWall firewall is configured to connect through IPsec to another manufacturer’s firewall.

Hub and Spoke Design	All SonicWall VPN gateways are configured to connect to a central hub, such as a corporate firewall. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a SonicWall network security appliance.
Mesh Design	All sites connect to all other sites. All sites must have static IP addresses.

SonicWall has video clips and knowledge base articles that can help you with some of those decisions.

ⓘ **VIDEO:** Informational videos with site to site VPN configuration examples are available online. For example, see How to Create a Site to Site VPN in Main Mode using Preshared Secret or How to Create Aggressive Mode Site to Site VPN using Preshared Secret.

Additional videos are available at: https://www.sonicwall.com/support/video-tutorials.

ⓘ **TIP:** See the knowledge base articles for information about Site to Site VPNs:

- *VPN: Types of Site to Site VPN Scenarios and Configurations (SW12884)*
- *Troubleshooting articles of Site to Site VPN (SW7570)*

When designing your VPN configurations, be sure to document all pertinent IP addressing information. You might want to create a network diagram to use as a reference. A few other things to note:

- The firewall must have a routable WAN IP address whether it is dynamic or static.
- In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

General VPN Configuration

This section reviews the general process for site to site configurations. Specific scenarios might be different and some are described in subsequent sections. Note that configuring IPsec VPNs for IPv4 and IPv6 are very similar; however, certain VPN features are currently not supported in IPv6. See IPv6 VPN Configuration on page 21 for information.

To configure a VPN:

1. Navigate to the **MANAGE | Connectivity | VPN > Base Settings** page.
2. Make the appropriate selection in **View IP Version** field: either **IPv4** or **IPv6**.
3. In the **VPN Policies** section, click **ADD**.
4. Complete **General**, **Network**, **Proposals**, and **Advanced** sections on the **VPN Policy** dialog. The following sections provide additional information for each of those pages.

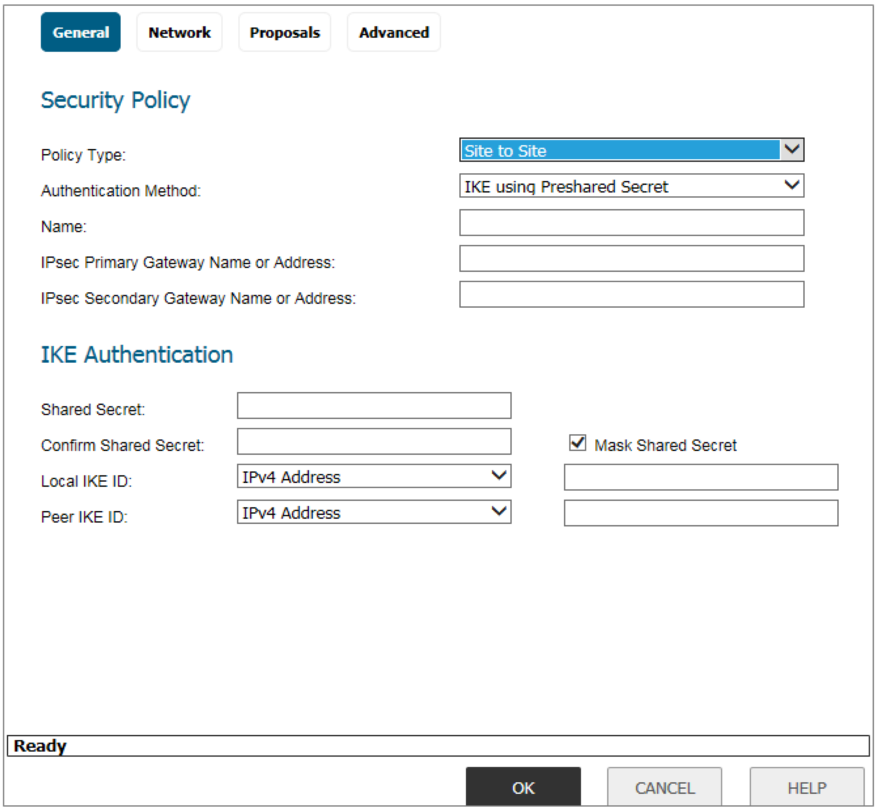
Topics:

- Configuring Settings on the General Screen
- Configuring Settings on the Network Screen
- Configuring Settings on the Proposals Screen
- Configuring Settings on the Advanced Screen

Configuring Settings on the General Screen

On the **General** screen, you begin defining the site to site VPN policy. There are some slight differences between IPv4 and IPv6 networks, which are noted.

IPv4 ADD VPN Policy: General



Security Policy

Policy Type: Site to Site

Authentication Method: IKE using Preshared Secret

Name:

IPsec Primary Gateway Name or Address:

IPsec Secondary Gateway Name or Address:

IKE Authentication

Shared Secret:

Confirm Shared Secret: ☑ Mask Shared Secret

Local IKE ID: IPv4 Address

Peer IKE ID: IPv4 Address

Ready

1 If configuring an IPv4 VPN, select **Policy Type** from the drop-down menu.

> **NOTE:** The **Policy Type** field is not available for IPv6.

2 Select the authentication method from the **Authentication Method** drop-down menu. The remaining fields in the **General** screen change depending on which option you select. The following options are available.

IPv4	IPv6
Manual Key	Manual Key
IKE using Preshared Secret (default)	IKE using Preshared Secret (default)
IKE using 3rd Party Certificates	IKE using 3rd Party Certificates
SonicWall Auto Provisioning Client	
SonicWall Auto Provisioning Server	

3 Type in a **Name** for the policy.

4 For **IPsec Primary Gateway Name or Address**, type in the gateway name or address.

5 For **IPsec Secondary Gateway Name or Address**, type in the gateway name or address.

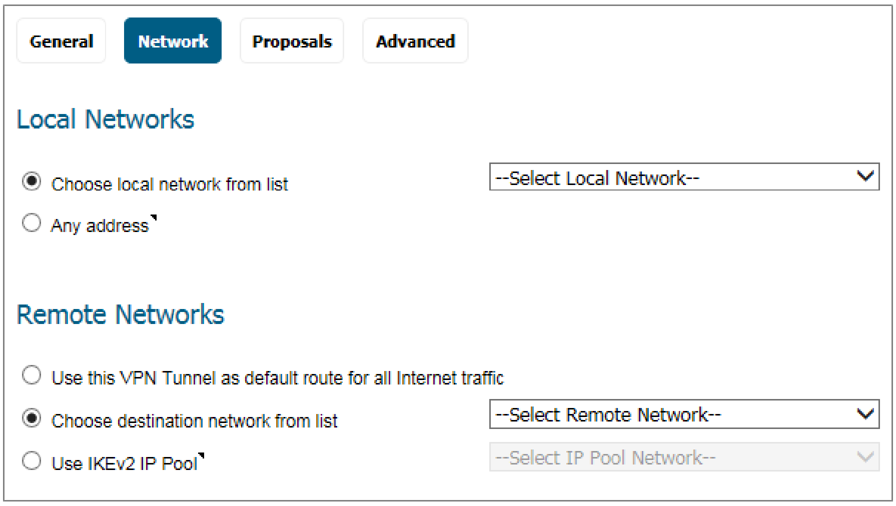
6 Under **IKE Authentication**, provide the required authentication information.

> ⓘ **NOTE:** When configuring IKE authentication, IPv6 addresses can be used for the local and peer IKE IDs.

Configuring Settings on the Network Screen

On the **Network** screen, define the networks that comprise the site to site VPN policy.

IPv4 ADD VPN Policy: Network



Local Networks

● Choose local network from list — --Select Local Network--

○ Any address

Remote Networks

○ Use this VPN Tunnel as default route for all Internet traffic

● Choose destination network from list — --Select Remote Network--

○ Use IKEv2 IP Pool — --Select IP Pool Network--

On the **Network** screen of the VPN policy, select the local and remote networks from the **Local Network** and **Remote Network** options.

For IPv6, the drop-down menus are the only option provided and only address objects that can be used by IPv6 are listed. Because DHCP is not supported, those options are not available. Also the **Any address** option for **Local Networks** and the **Tunnel All** option for **Remote Networks** are removed. An all-zero IPv6 Network address object could be selected for the same functionality and behavior.

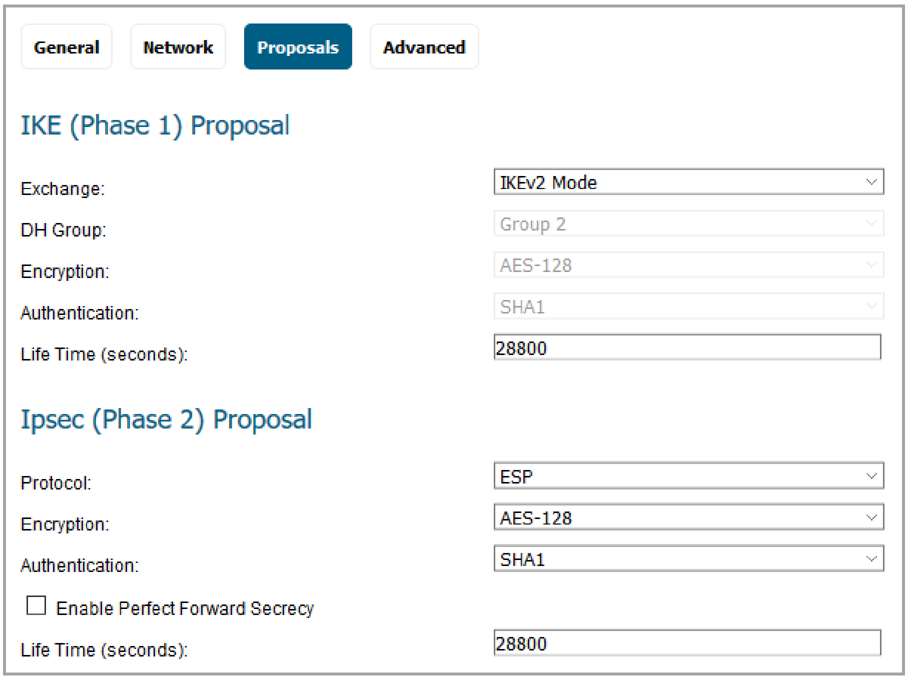
For IPv4, additional options are provided. Under **Local Networks**, you can **Choose local network from list** or choose **Any address**. If **Any address** is selected, auto-added rules are created between Trusted Zones and the VPN zone.

For IPv4 under **Remote Networks**, you can chose one of the following:

- **Use this VPN tunnel as default route for all Internet traffic.**
- **Choose destination network from list**. If none are listed you can create a new address object or address group.
- **Use IKEv2 IP Pool**. Select this to support IKEv2 Config Payload.

Configuring Settings on the Proposals Screen

On the **Proposals** screen, you define the security parameters for your VPN policy. The page is same for IPv4 and IPv6, but the options are different depending on what you selected. IPv4 offers both IKEv1 and IKEv2 options in the **Exchange** field, whereas IPv6 only has IKEv2.



IKE (Phase 1) Proposal

Exchange: IKEv2 Mode

DH Group: Group 2

Encryption: AES-128

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: AES-128

Authentication: SHA1

□ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Configuring Settings on the Advanced Screen

The **Advanced** screens for IPv4 and IPv6 are similar, but some options are available only for one version or the other, as shown in Advanced Settings: Option Availability. Options also change depending on the authentication method selected.

Advanced Settings: Option Availability

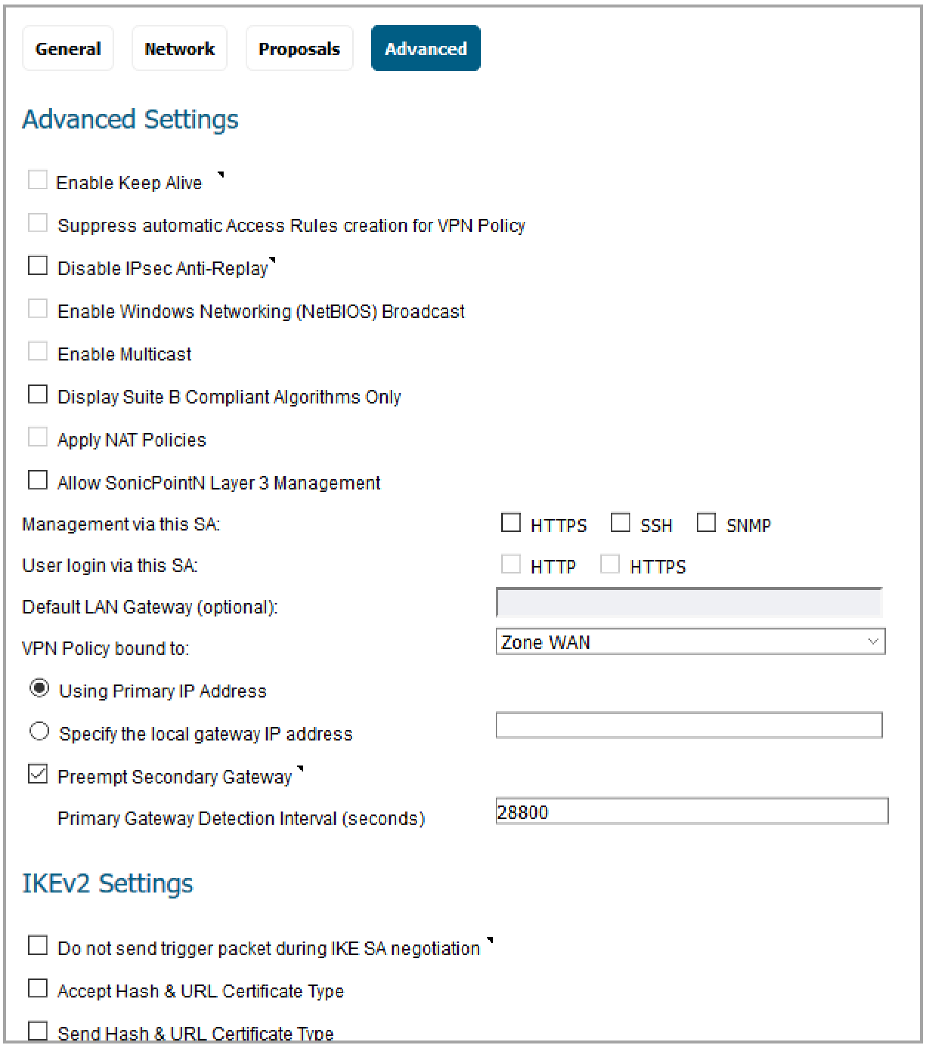
Option	IP Version	
	IPv4	IPv6
Enable Keep Alive	Supported	Supported
Suppress automatic Access Rules creation for VPN Policy	Supported	–
Disable IPsec Anti-Replay	Supported	Supported
Enable Windows Networking (NetBIOS) Broadcast	Supported	–
Enable Multicast	Supported	–
Display Suite B Compliant Algorithms Only	Supported	Supported
Apply NAT Policies	Supported	–
Allow SonicPointN Layer 3 Management	Supported	Supported
Using Primary IP Address	–	Supported
Specify the local gateway IP address	–	Supported
Preempt Secondary Gateway	Supported	Supported
Primary Gateway Detection Interval (seconds)	Supported	Supported

Advanced Settings: Option Availability (Continued)

Option	IP Version	
	IPv4	IPv6
Do not send trigger packet during IKE SA negotiation	Supported	Supported
Accept Hash & URL Certificate Type	Supported	Supported
Send Hash & URL Certificate Type	Supported	Supported

> **NOTE:** Because an interface might have multiple IPv6 addresses, sometimes the local address of the tunnel might vary periodically. If a user needs a consistent IP address, select either the **Using Primary IP Address** or **Specify the local gateway IP address** option, or configure the VPN policy to be bound to an interface instead of a Zone. With **Specify the local gateway IP address**, specify the address manually. The address must be one of the IPv6 addresses for that interface.

IPv6 ADD VPN Policy: Advanced



Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Disable IPsec Anti-Replay

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

□ Display Suite B Compliant Algorithms Only

□ Apply NAT Policies

□ Allow SonicPointN Layer 3 Management

Management via this SA: □ HTTPS □ SSH □ SNMP

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

● Using Primary IP Address

○ Specify the local gateway IP address

☑ Preempt Secondary Gateway

Primary Gateway Detection Interval (seconds) 28800

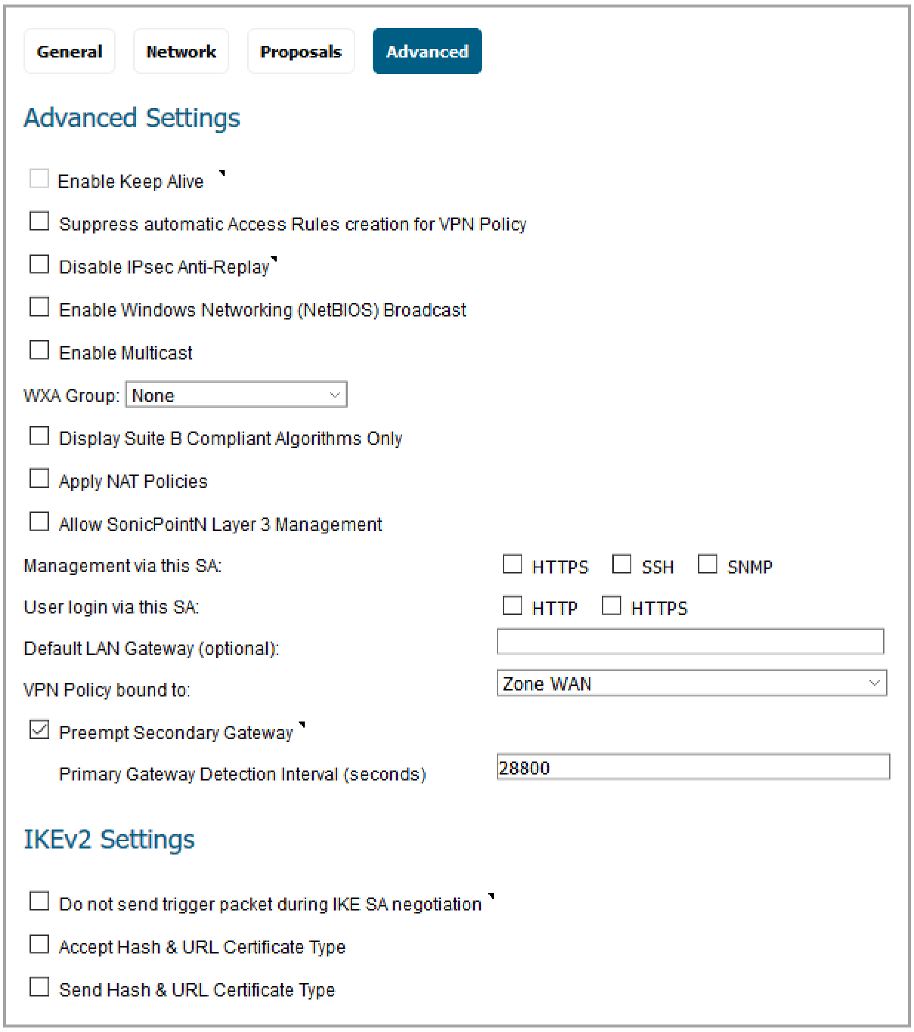
IKEv2 Settings

□ Do not send trigger packet during IKE SA negotiation

□ Accept Hash & URL Certificate Type

□ Send Hash & URL Certificate Type

IPv4 ADD VPN Policy: Advanced



Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Disable IPsec Anti-Replay

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

WXA Group: None

□ Display Suite B Compliant Algorithms Only

□ Apply NAT Policies

□ Allow SonicPointN Layer 3 Management

Management via this SA:	□ HTTPS □ SSH □ SNMP
User login via this SA:	□ HTTP □ HTTPS
Default LAN Gateway (optional):	
VPN Policy bound to:	Zone WAN

☑ Preempt Secondary Gateway

Primary Gateway Detection Interval (seconds) 28800

IKEv2 Settings

□ Do not send trigger packet during IKE SA negotiation

□ Accept Hash & URL Certificate Type

□ Send Hash & URL Certificate Type

Managing GroupVPN Policies

The GroupVPN feature provides automatic VPN policy provisioning for Global VPN Clients (GVC). The GroupVPN feature on the SonicWall network security appliance and GVC streamlines VPN deployment and management. Using the Client Policy Provisioning technology, you define the VPN policies for GVC users. This policy information downloads automatically from the firewall (VPN Gateway) to GVC, saving remote users the burden of provisioning VPN connections.

GroupVPN policies facilitate the set up and deployment of multiple Global VPN Clients by the firewall administrator. **GroupVPN** is only available for GVC and you should use XAUTH/RADIUS or third-party certificates in conjunction with it for added security. For more information on how to create GroupVPN policies for any zones, refer to *SonicOS 6.5 System Setup*, or navigate to the **MANAGE** view, under **System Setup**, and select **Network > Zones > Add**.

SonicOS provides default GroupVPN policies for the WAN zone and the WLAN zone, as these are generally the less trusted zones. These default GroupVPN policies are listed in the **VPN Policies** table on the **VPN > Base Settings** page and can be customized:

- WAN GroupVPN
- WLAN GroupVPN

> **NOTE:** GroupVPN policies are not automatically created in SonicOS 6.5.4 with factory default settings. However, these policies remain unchanged on appliances that are upgraded from an earlier version of SonicOS. For information about Group VPN and Global VPN Client, refer to *Types of Group VPN/Global VPN Client Scenarios and Configurations* (SW7411).

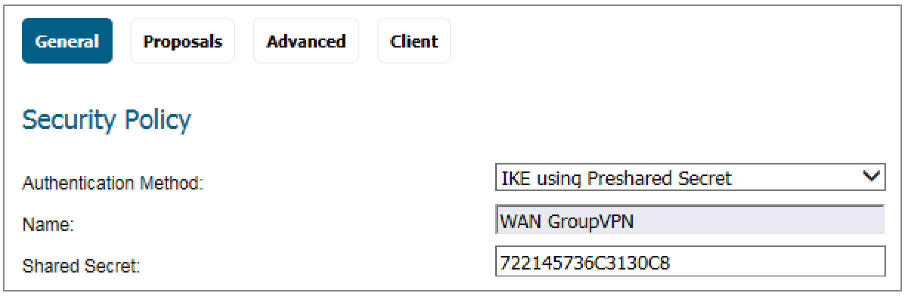
Topics:

- Configuring IKE Using a Preshared Secret Key
- Configuring IKE Using 3rd Party Certificates
- Exporting a GroupVPN Client Policy

Configuring IKE Using a Preshared Secret Key

To configure the WAN GroupVPN using a preshared secret key:

1. Navigate to **MANAGE | Connectivity | VPN > Base Settings**.
2. Click the **Edit** icon for the **WAN GroupVPN** policy.



Security Policy

Authentication Method: IKE using Preshared Secret

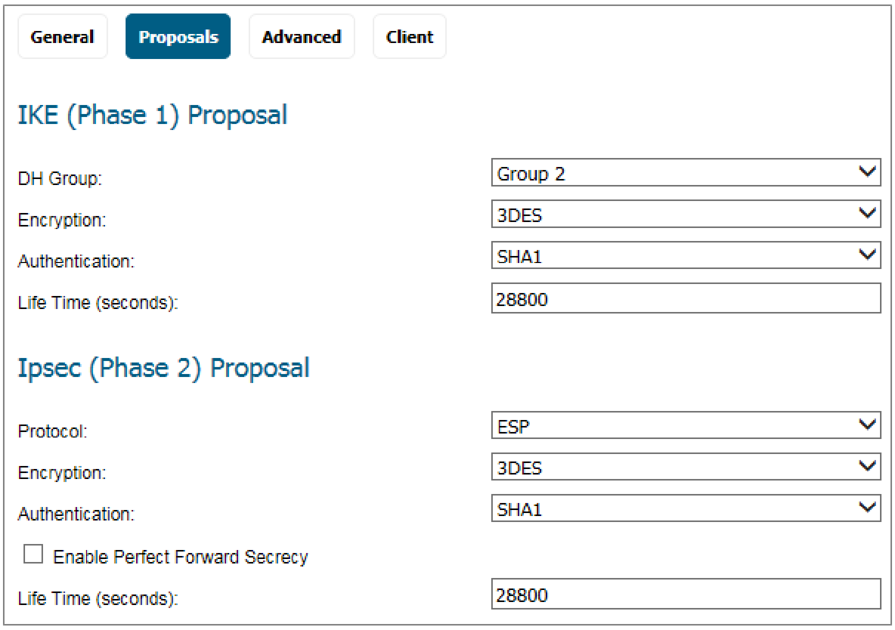
Name: WAN GroupVPN

Shared Secret: 722145736C3130C8

On the **General** screen, **IKE using Preshared Secret** is the default setting for **Authentication Method**. A shared secret code is automatically generated by the firewall and written in the **Shared Secret** field. You can generate your own shared secret. A self-defined shared secret code must be a minimum of four characters.

> **NOTE:** You cannot change the name of any GroupVPN policy.

3 Click **Proposals** to continue the configuration process.



IKE (Phase 1) Proposal

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

□ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

4 In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select **Group 2** (default) from the **DH Group** drop-down menu.

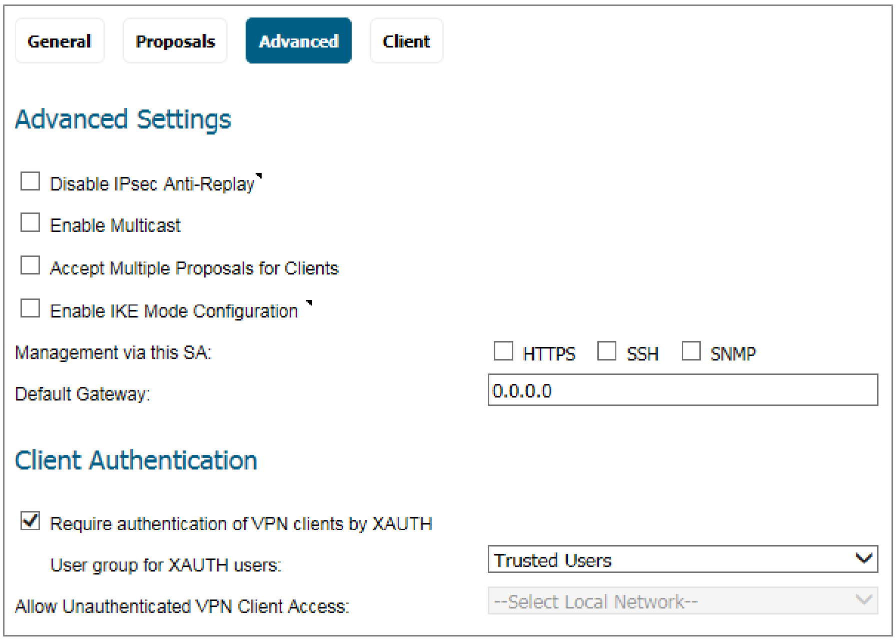
  > **NOTE:** The Windows XP L2TP client only works with DH Group 2.

- In the **Encryption** drop-down menu, select **DES**, **3DES** (default), **AES-128**, **AES-192**, or **AES-256**.
- From the **Authentication** drop-down menu, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, or **SHA512**.
- In the **Life Time (seconds)** field, enter a value. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

5 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- From the **Protocol** drop-down menu, select **ESP** (default).
- In the **Encryption** drop-down menu, select **3DES** (default), **AES-128**, **AES-192**, or **AES-256**.
- In the **Authentication** drop-down menu, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, **SHA512**, **AES-XCBC**, or **None**.
- Check **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

6 Click **Advanced**.



Advanced Settings

☐ Disable IPsec Anti-Replay

☐ Enable Multicast

☐ Accept Multiple Proposals for Clients

☐ Enable IKE Mode Configuration

Management via this SA: ☐ HTTPS ☐ SSH ☐ SNMP

Default Gateway: 0.0.0.0

Client Authentication

☑ Require authentication of VPN clients by XAUTH

User group for XAUTH users: Trusted Users

Allow Unauthenticated VPN Client Access: --Select Local Network--

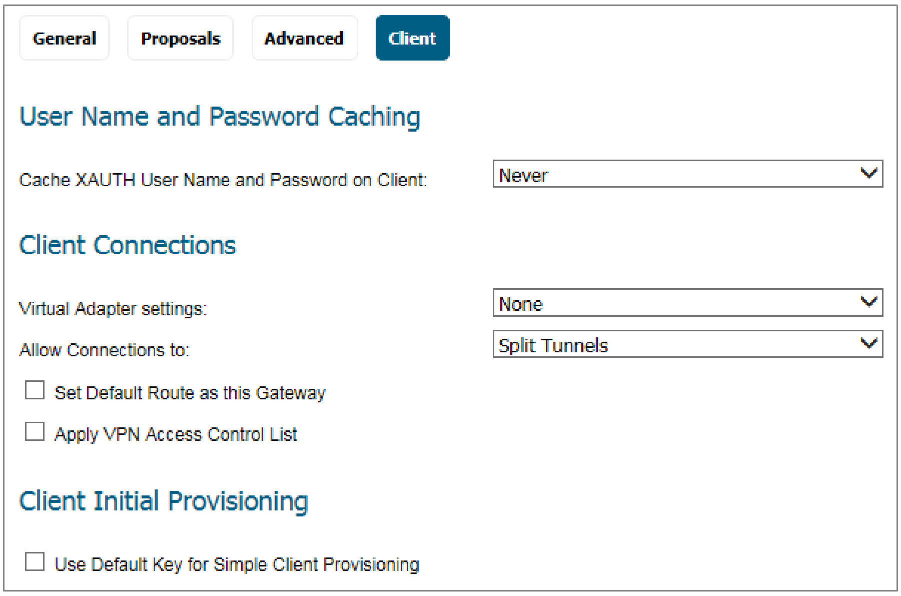
7 Select any of the following optional settings you want to apply to your GroupVPN policy:

Advanced Settings	
Disable IPsec Anti-Replay	Stops packets with duplicate sequence numbers from being dropped.
Enable Multicast	Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
Accept Multiple Proposals for Clients	Allows multiple proposals for clients, such as the IKE (Phase 1) Proposal or the IKE (Phase 2) Proposal, to be accepted.
Enable IKE Mode Configuration	Allows SonicOS to assign internal IP address, DNS Server, or WINS Server to third-party clients, like iOS devices or Avaya IP phones.
Management via this SA:	If using the VPN policy to manage the firewall, select the management method, either **HTTP**, **SSH**, or **HTTPS**. **NOTE:** SSH is valid for IPv4 only.
Default Gateway	Allows you to specify the IP address of the default network route for incoming IPsec packets for this VPN policy. Incoming packets are decoded by the firewall and compared to static routes configured in the firewall. As packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received through an IPsec tunnel, the firewall looks up a route. If no route is found, the security appliance checks for a Default Gateway. If a Default Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

Client Authentication

Require Authentication of VPN Clients via XAUTH	Requires that all inbound traffic on this VPN tunnel is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel. The **Trusted users** group is selected by default. You can select another user group or **Everyone from User Group for XAUTH users** from the **User group for XAUTH** users menu.
Allow Unauthenticated VPN Client Access	Allows you to enable unauthenticated VPN client access. If you clear **Require Authentication of VPN Clients via XAUTH**, the **Allow Unauthenticated VPN Client Access** menu is activated. Select an Address Object or Address Group from menu of predefined options, or select **Create new address object** or **Create new address group** to create a new one.

8 Click **Client**.



User Name and Password Caching

Cache XAUTH User Name and Password on Client: Never

Client Connections

Virtual Adapter settings: None

Allow Connections to: Split Tunnels

☐ Set Default Route as this Gateway

☐ Apply VPN Access Control List

Client Initial Provisioning

☐ Use Default Key for Simple Client Provisioning

9 Select any of the following settings you want to apply to your GroupVPN policy.

User Name and Password Caching

Cache XAUTH User Name and Password on Client	Allows the Global VPN Client to cache the user name and password: • If **Never** is selected, the Global VPN Client is not allowed to cache the username and password. The user is prompted for a username and password when the connection is enabled and also every time there is an IKE Phase 1 rekey. This is the default. • If **Single Session** is selected, the Global VPN Client user is prompted for username and password each time the connection is enabled and is valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey. • If **Always** is selected Global VPN Client user prompted for username and password only once when the connection is enabled. When prompted, the user is given the option of caching the username and password.

Client Connections

Virtual Adapter Settings	The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing is a requirement, obtain the MAC address of the Virtual Adapter and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. **NOTE:** This feature requires the use of SonicWall GVC. Select one of the following: • Choose **None** if a Virtual Adapter is not used by this GroupVPN connection. This is the default. • Choose **DHCP Lease** if the Virtual Adapter obtains its IP configuration from the DHCP Server only, as configured in the **VPN > DHCP over VPN** page. • Choose **DHCP Lease or Manual Configuration** when the GVC connects to the firewall, the policy from the firewall instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the firewall so it can proxy ARP for the manually assigned IP address. By design, the Virtual Adapter currently has no limitations on IP address assignments. Only duplicate static addresses are not permitted.
Allow Connections to	Client network traffic that matches the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. Select one of the following: • **This Gateway Only** allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected with **Set Default Route as this Gateway**, then the Internet traffic is also sent through the VPN tunnel. If selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked. • **All Secured Gateways** allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, Internet traffic is also sent through the VPN tunnel. If this option is selected along without **Set Default Route as this Gateway,** the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled. • **Split Tunnels** allows the VPN user to have both local Internet connectivity and VPN connectivity. This is the default.
Set Default Route as this Gateway	Select this checkbox if all remote VPN connections access the Internet through this VPN tunnel. You can only configure one VPN policy to use this setting. By default, this option is not enabled.
Apply VPN Access Control List	Select this checkbox to apply the VPN access control list. When this option is enabled, specified users can access only those networks configured for them (for more information, refer to **System Setup Users > Local Users & Groups** in the *SonicOS 6.5 System Setup*). This option is not enabled by default.

Client Initial Provisioning	
Use Default Key for Simple Client Provisioning	Uses Aggressive mode for the initial exchange with the gateway, and VPN clients uses a default Preshared Key for authentication. This option is not enabled by default.

10 Click **OK**.

11 Click **ACCEPT** on the **VPN > Base Settings** page to update the VPN Policies.

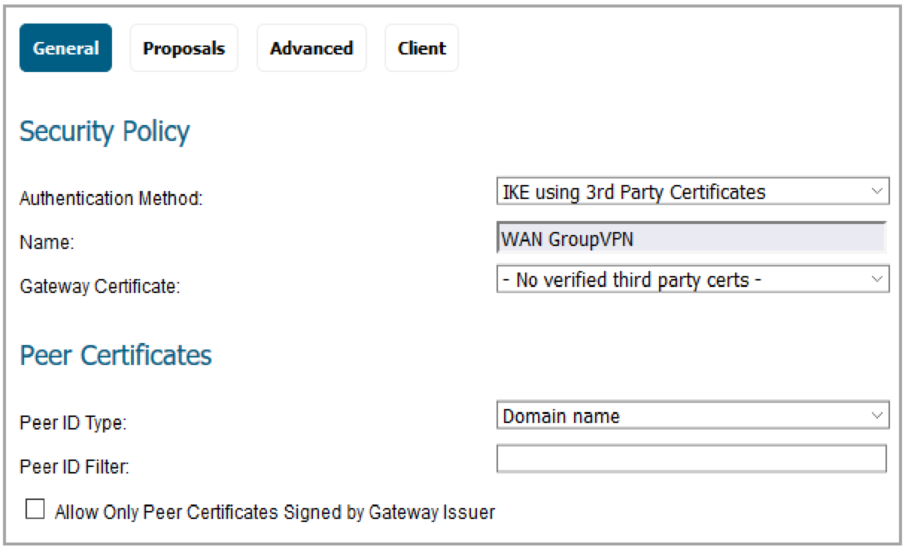
Configuring IKE Using 3rd Party Certificates

ⓘ **IMPORTANT:** Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the firewall.

To configure GroupVPN with IKE using 3rd Party Certificates

1 Navigate to **MANAGE | Connectivity | VPN > Base Settings**.

2 Click the **Edit** icon for the **WAN GroupVPN** policy.



Security Policy

Authentication Method: IKE using 3rd Party Certificates

Name: WAN GroupVPN

Gateway Certificate: - No verified third party certs -

Peer Certificates

Peer ID Type: Domain name

Peer ID Filter:

□ Allow Only Peer Certificates Signed by Gateway Issuer

3 In the **Security Policy** section, select **IKE using 3rd Party Certificates** from the **Authentication Method** drop-down menu.

ⓘ **NOTE:** The VPN policy name is GroupVPN by default and cannot be changed.

4 Select a certificate for the firewall from the **Gateway Certificate** drop-down menu.

If you did not download your third-party certificates before starting this procedure, the **Gateway Certificates** field shows **- No verified third-party certs -**.

5 In the **Peer Certificates** section, select one of the following from the **Peer ID Type** drop-down menu:

Distinguished Name

Based on the certificate's Subject Distinguished Name field, which is contained on all certificates by default and is set by the issuing Certificate Authority.

The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: `/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub`.

Up to three organizational units can be specified. The usage is `c=*;o=*;ou=*;ou=*;ou=*;cn=*`. The final entry does not need to contain a semi-colon. You must enter at least one entry, for example, *c=us*.

E-mail ID

Domain ID

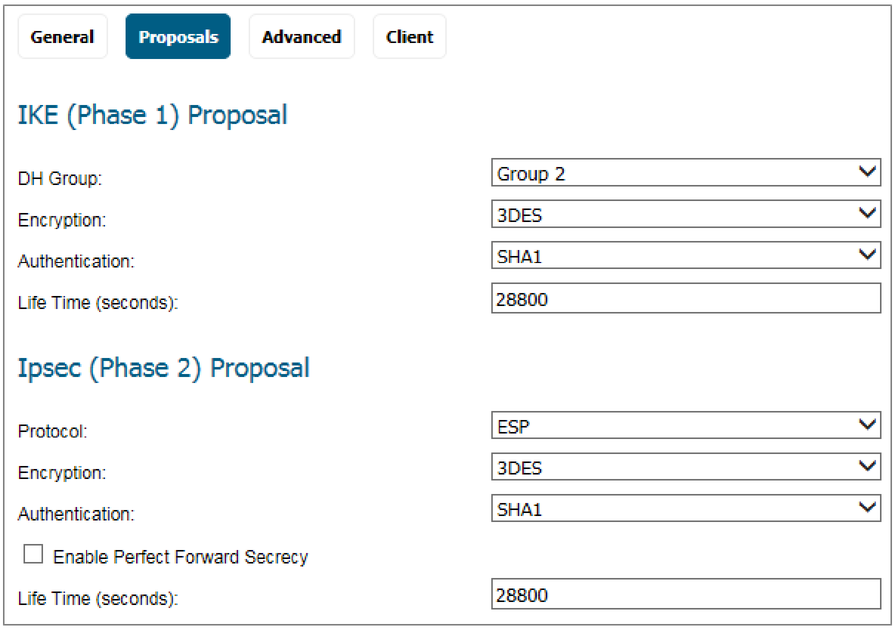
E-mail ID and **Domain ID** are based on the certificate's Subject Alternative Name field, which is not contained on all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter does not work.

6 Enter the Peer ID filter in the **Peer ID Filter** field.

The **Email ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters * (for more than 1 character) and? (for a single character). For example, when **Email ID** is selected, the string `*@sonicwall.com` allows anyone with an email address that ended in `@sonicwall.com` to have access; when **Domain Name** is selected, the string `*sv.us.sonicwall.com` allows anyone with a domain name that ended in `sv.us.sonicwall.com` to have access.

7 Select **Allow Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the **Gateway Certificate** menu.

8 Click **Proposals**.



IKE (Phase 1) Proposal

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

9 In the **IKE (Phase 1)** section, select the following settings:

a For **DH Group**, select **Group 1**, **Group 2** (default), **Group 5**, or **Group 14**.

ⓘ **NOTE:** The Windows XP L2TP client only works with DH Group 2.

b For **Encryption**, select **DES**, **3DES** (default), **AES-128**, **AES-192**, or **AES-256**.

c For **Authentication**, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**,**SHA512, AES-XCBC**, or **None**.

d In the **Life Time (seconds)** field, enter a value. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

10 In the **IPsec (Phase 2)** section, select the following settings:

a For **Protocol**, select **ESP** (default).

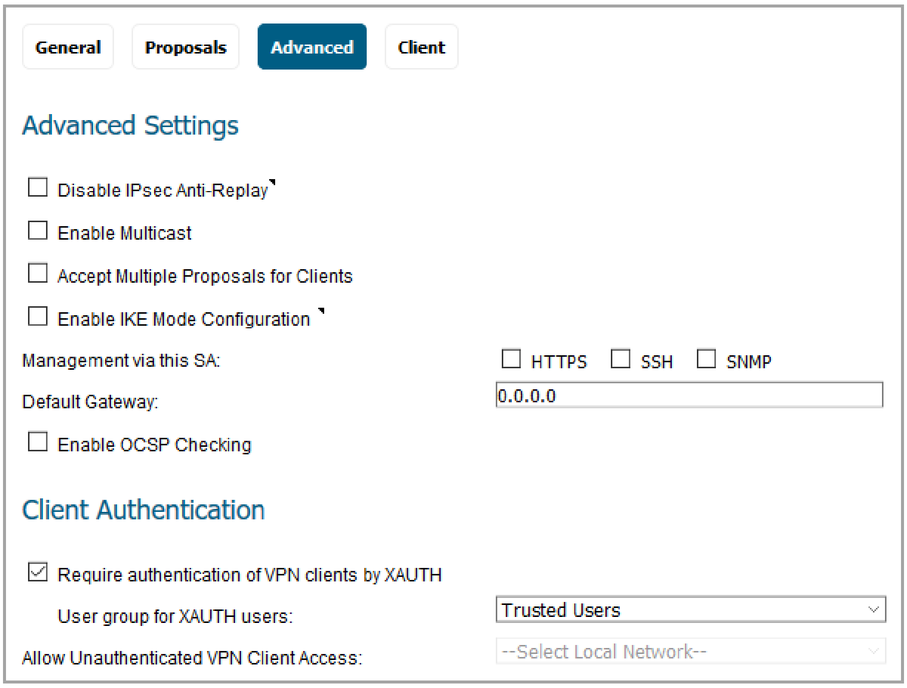
b For **Encryption**, select **3DES** (default), **AES-128**, **AES-192**, or **AES-256**.

c For **Authentication**, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, **SHA512**, **AES-XCBC**, or **None**.

d Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security.

e Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

11 Click **Advanced**.



Advanced Settings

☐ Disable IPsec Anti-Replay

☐ Enable Multicast

☐ Accept Multiple Proposals for Clients

☐ Enable IKE Mode Configuration

Management via this SA: ☐ HTTPS ☐ SSH ☐ SNMP

Default Gateway: 0.0.0.0

☐ Enable OCSP Checking

Client Authentication

☑ Require authentication of VPN clients by XAUTH

User group for XAUTH users: Trusted Users

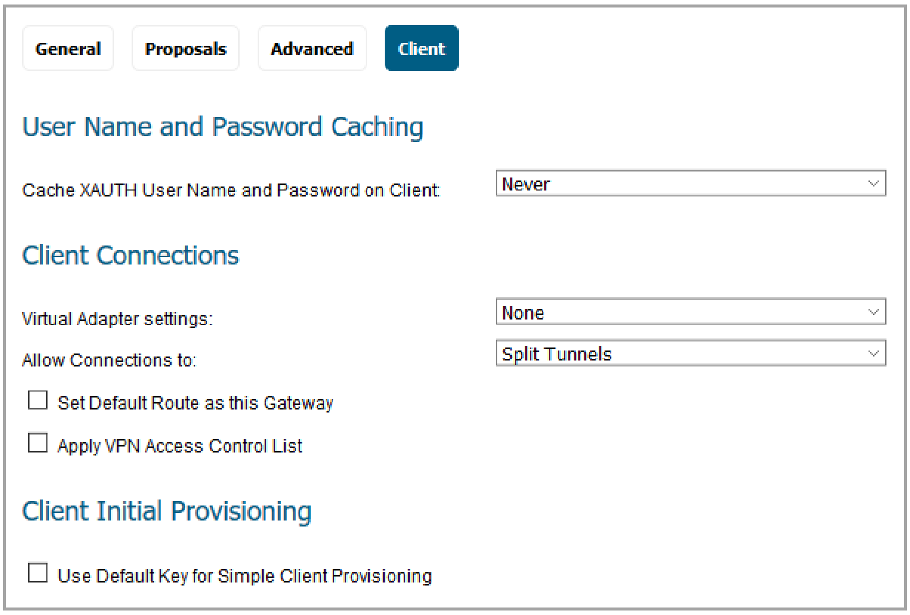
Allow Unauthenticated VPN Client Access: --Select Local Network--

12 Select any of the following optional settings that you want to apply to your GroupVPN Policy:

Disable IPsec Anti-Replay	Anti-Replay is a form of partial sequence integrity and it detects arrival of duplicated I datagrams (within a constrained window).
Enable Multicast	Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
Accept Multiple Proposal fro Clients	Allows multiple proposals for clients, such as the IKE (Phase 1) Proposal or the IKE (Phase 2) Proposal, to be accepted.
Enable IKE Mode Configuration	Allows SonicOS to assign internal IP address, DNS Server or WINS Server to Third-Party Clients like iOS devices or Avaya IP Phones.

Management via this SA	If using the VPN policy to manage the firewall, select one or more management methods, **HTTP**, **SSH**, or **HTTPS**. **NOTE:** SSH is valid for IPv4 only.
Default Gateway	Used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** checkbox. Default LAN Gateway allows you to specify the IP address of the default LAN route for incoming IPsec packets for this SA. Incoming packets are decoded by the firewall and compared to static routes configured in the firewall. Because packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received through an IPsec tunnel, the firewall looks up a route for the LAN. If no route is found, the firewall checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
Enable OCSP Checking and **OCSP Responder URL**	Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status.
Require Authentication of VPN Clients via XAUTH	Requires that all inbound traffic on this VPN policy is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.
User group for XAUTH users	Allows you to select a defined user group for authentication.
Allow Unauthenticated VPN Client Access	Allows you to specify network segments for unauthenticated Global VPN Client access.

13 Click **Client**.



User Name and Password Caching

Cache XAUTH User Name and Password on Client: Never

Client Connections

Virtual Adapter settings: None

Allow Connections to: Split Tunnels

□ Set Default Route as this Gateway

□ Apply VPN Access Control List

Client Initial Provisioning

□ Use Default Key for Simple Client Provisioning

14 Select any of the following boxes that you want to apply to Global VPN Client provisioning:

Cache XAUTH User Name and Password	Allows the Global VPN Client to cache the user name and password: • Choose **Never** to prohibit the Global VPN Client from caching the username and password. The user is prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey. • Choose **Single Session** to prompt the user for username and password each time the connection is enabled, which is valid until the connection is disabled. This username and password is used through IKE phase 1 rekey. • Choose **Always** to prompt the user for username and password only once when the connection is enabled. When prompted, the user is given the option of caching the username and password.
Virtual Adapter Settings	The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing is a requirement, obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of SonicWall GVC. • Choose **None** to not use the Virtual Adapter by this GroupVPN connection. • Choose **DHCP Lease** to have the Virtual Adapter obtain its IP configuration from the DHCP Server only, as configured in the **VPN > DHCP over VPN** page. • Choose **DHCP Lease or Manual Configuration** and when the GVC connects to the firewall, the policy from the firewall instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the firewall so that it can proxy ARP for the manually assigned IP address. By design, IP address assignments currently has no limitations on for the Virtual Adapter. Only duplicate static addresses are not permitted.

Allow Connections to	Client network traffic that matches the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. Select one of the following options: • **This Gateway Only** allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected with **Set Default Route as this Gateway**, then the Internet traffic is also sent through the VPN tunnel. If selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked. • **All Secured Gateways** allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, Internet traffic is also sent through the VPN tunnel. If this option is selected along without **Set Default Route as this Gateway,** the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled. **NOTE:** Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled. • **Split Tunnels** allows the VPN user to have both local Internet connectivity and VPN connectivity. This is the default.
Set Default Route as this Gateway	Enable this checkbox if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting.
Apply VPN Access Control List	Enable this option to control client connections with an access control list.
Use Default Key for Simple Client Provisioning	Uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

15 Click **OK**.

16 Click **ACCEPT** on the **VPN > Base Settings** page to update the VPN Policies.

Exporting a GroupVPN Client Policy

You can provide a file to your end users that contains configuration settings for their Global VPN clients. Simply export the GroupVPN client policy from the firewall.

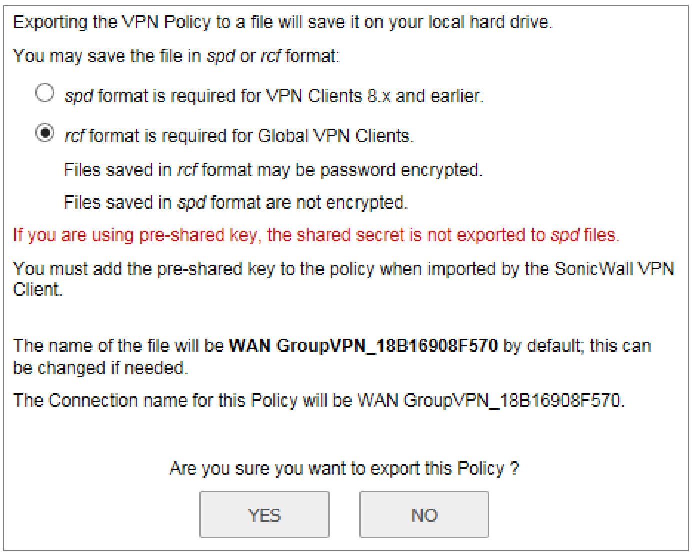
IMPORTANT: The GroupVPN SA (Secure Association) must be enabled on the firewall to export a configuration file.

To export the Global VPN Client configuration settings:

1 Navigate to **MANAGE | Connectivity | VPN > Base Settings**.

2 Be sure the policy you want to export is enabled.

3 Click the **Export** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table.



Exporting the VPN Policy to a file will save it on your local hard drive.

You may save the file in *spd* or *rcf* format:

○ *spd* format is required for VPN Clients 8.x and earlier.

● *rcf* format is required for Global VPN Clients.

Files saved in *rcf* format may be password encrypted.

Files saved in *spd* format are not encrypted.

If you are using pre-shared key, the shared secret is not exported to *spd* files.

You must add the pre-shared key to the policy when imported by the SonicWall VPN Client.

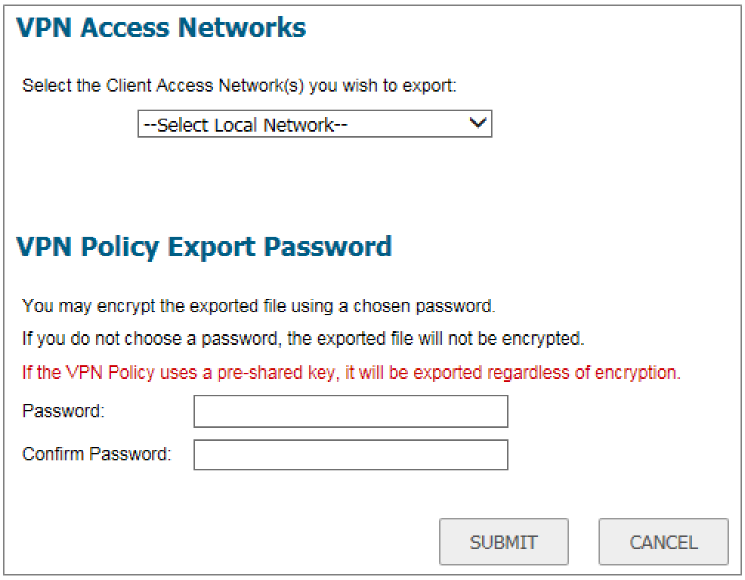
The name of the file will be **WAN GroupVPN_18B16908F570** by default; this can be changed if needed.

The Connection name for this Policy will be WAN GroupVPN_18B16908F570.

Are you sure you want to export this Policy ?

rcf format is required for SonicWall Global VPN Clients is the default. Files saved in the rcf format can be password encrypted. The firewall provides a default file name for the configuration file, which you can change.

4 Click **Yes**.



VPN Access Networks

Select the Client Access Network(s) you wish to export:

--Select Local Network--

VPN Policy Export Password

You may encrypt the exported file using a chosen password.

If you do not choose a password, the exported file will not be encrypted.

If the VPN Policy uses a pre-shared key, it will be exported regardless of encryption.

Password:

Confirm Password:

5 In the drop-down menu for **Select the client Access Network(s) you wish to export**, select **VPN Access Network**.

6 Type a password in the **Password** field and reenter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.

7 Click **SUBMIT**. If you did not enter a password, a message appears confirming your choice.

8 Click **OK**. You can change the configuration file before saving.

9 Save the file.

10 Click **Close**.

The file can be saved or sent electronically to remote users to configure their Global VPN Clients.

Creating Site to Site VPN Policies

A site to site VPN allows offices in multiple locations to establish secure connections with each other over a public network. It extends the company's network, making computer resources from one location available to employees at other locations.

You can create or modify existing site to site VPN policies. To add a policy, click **ADD** under the **VPN Policies** table; to modify an existing policy click the **Edit** icon for that policy. The following options can be set up when configuring a site to site VPN:

- Configuring with a Preshared Secret Key
- Configuring with a Manual Key
- Configuring with a Third-Party Certificate
- **SonicWall Auto Provisioning Client** or **SonicWall Auto Provisioning Server**. For information about these options, see VPN Auto Provisioning on page 69.

This section also contains information on how to configure the remote SonicWall firewall and how to configure a static route to act as a failover in case the VPN tunnel failure.

- Configuring the Remote SonicWall Network Security Appliance
- Configuring VPN Failover to a Static Route

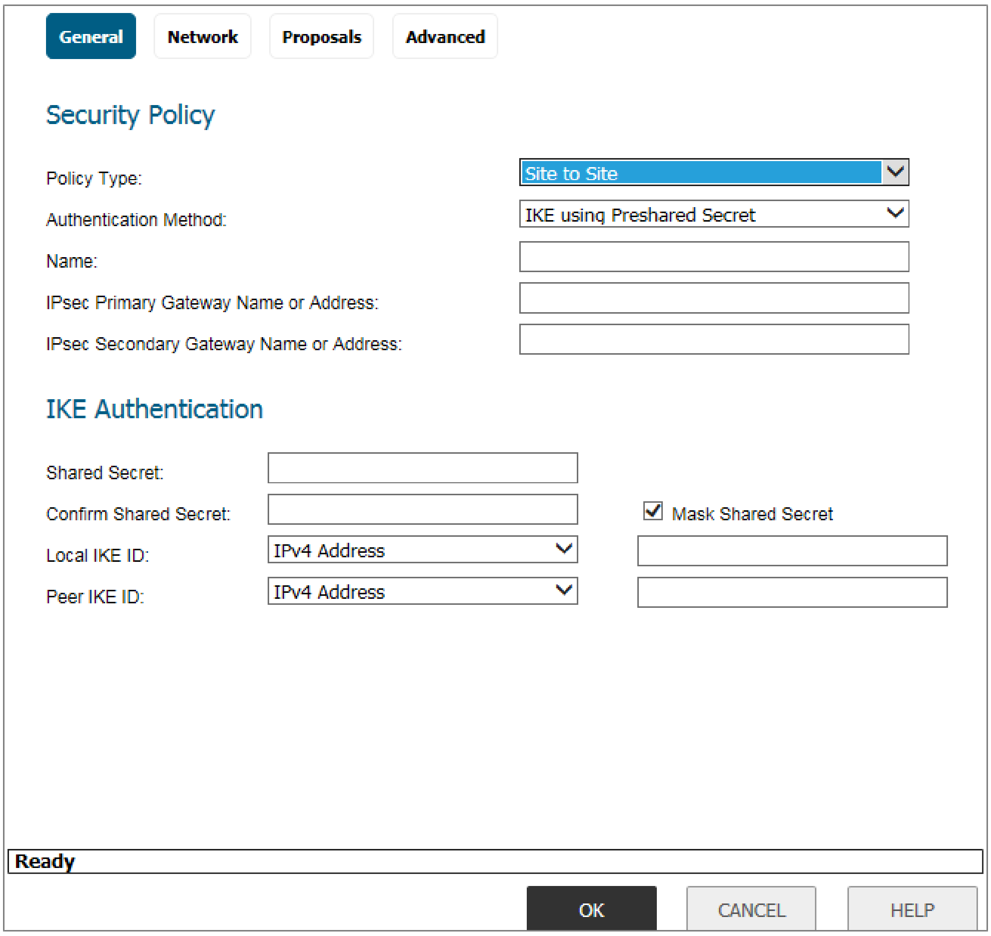
> ⓘ **VIDEO:** Informational videos with site to site VPN configuration examples are available online. For example, see How to Create a Site to Site VPN in Main Mode using Preshared Secret or How to Create Aggressive Mode Site to Site VPN using Preshared Secret.
>
> Additional videos are available at: https://www.sonicwall.com/support/video-tutorials.

Configuring with a Preshared Secret Key

To configure a VPN Policy using Internet Key Exchange (IKE) with a preshared secret key:

1 Navigate to **MANAGE | Connectivity | VPN > Base Settings**.

2 Click **ADD** to create a new policy or click the **Edit** icon if you are updating an existing policy.



Security Policy

Policy Type: Site to Site

Authentication Method: IKE using Preshared Secret

Name:

IPsec Primary Gateway Name or Address:

IPsec Secondary Gateway Name or Address:

IKE Authentication

Shared Secret:

Confirm Shared Secret: ☑ Mask Shared Secret

Local IKE ID: IPv4 Address

Peer IKE ID: IPv4 Address

Ready

3 From **Policy Type** on the **General** screen, select **Site to Site**.

4 From **Authentication Method**, select **IKE using Preshared Secret**.

5 Enter a name for the policy in the **Name** field.

6 Enter the host name or IP address of the remote connection in the **IPsec Primary Gateway Name or Address** field.

7 If the Remote VPN device supports more than one endpoint, enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field (optional).

8 In the **IKE Authentication** section, in the **Shared Secret** and **Confirm Shared Secret** fields, enter a Shared Secret password. This is used to set up the SA (Security Association). The Shared Secret password must be at least four characters long, and should include both numbers and letters.

9 To see the shared secret key in both fields, clear the checkbox for **Mask Shared Secret**. By default, **Mask Shared Secret** is selected, which causes the shared secret key to be displayed as black circles.

10 Optionally, specify a **Local IKE ID** and **Peer IKE ID** for this Policy.

You can select from the following IDs from the drop-down menu:

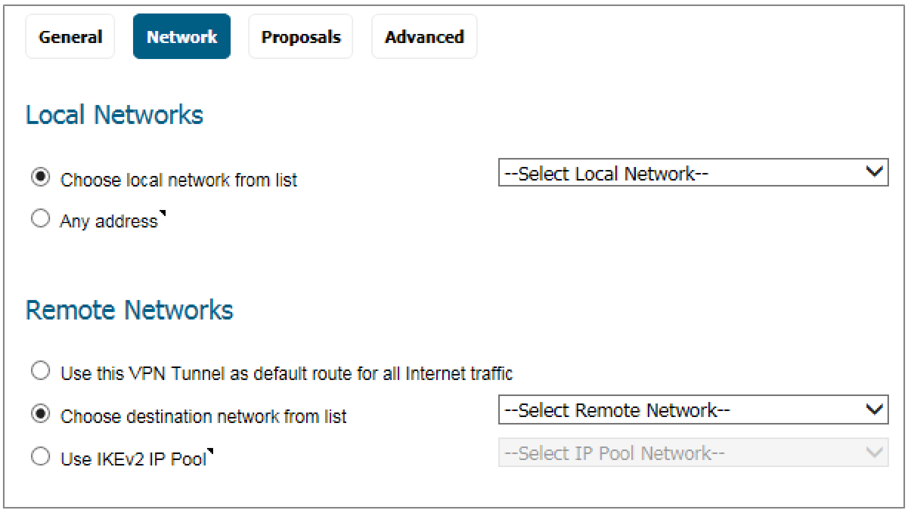
- **IPv4 Address**
- **Domain Name**
- **E-mail Address**
- **Firewall Identifier**

- **Key Identifier**

By default, the **IP Address** (ID_IPv4_ADDR) is used for Main Mode negotiations, and the firewall Identifier (ID_USER_FQDN) is used for Aggressive Mode.

11 Enter the address, name, or ID in the **Local IKE ID** and **Peer IKE ID** fields.

12 Click **Network**.



Local Networks

● Choose local network from list --Select Local Network--

○ Any address

Remote Networks

○ Use this VPN Tunnel as default route for all Internet traffic

● Choose destination network from list --Select Remote Network--

○ Use IKEv2 IP Pool --Select IP Pool Network--

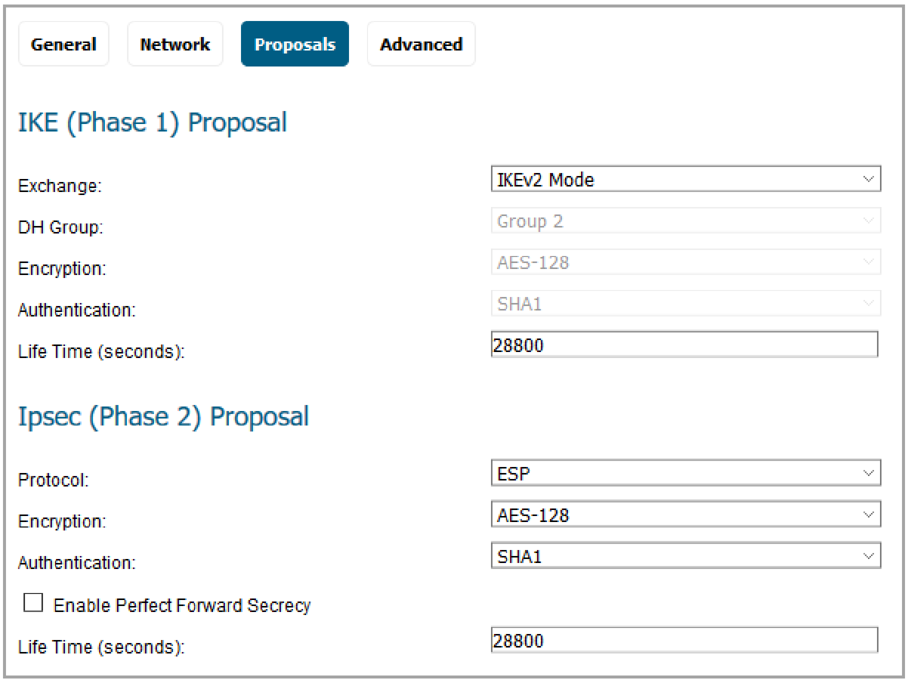
13 Under **Local Networks**, select one of the following:

Choose local network from list	Select a local network from the drop-down menu if a specific network can access the VPN tunnel.
Any address	Use this option if traffic can originate from any local network or if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules are created between Trusted Zones and the VPN Zone. **NOTE:** DHCP over VPN is not supported with IKEv2.

14 Under **Remote Networks**, select one of the following:

Use this VPN Tunnel as default route for all Internet traffic	Select this option if traffic from any local user cannot leave the firewall unless it is encrypted. **NOTE:** You can only configure one SA to use this setting.
Destination network obtains IP addresses using DHCP through this VPN Tunnel	Select this option if the remote network requests IP addresses from a DHCP Server in the local network. **NOTE:** This option is only available if **Main Mode** or **Aggressive Mode** is selected on the **Proposals** screen.
Choose Destination network from list	Select a remote network from the drop-down menu.
Use IKEv2 IP Pool	Select this option to support IKEv2 Config Payload. **NOTE:** This option is only available if **IKEv2 Mode** is selected on the **Proposals** screen.

15 Click **Proposals**.



IKE (Phase 1) Proposal

Exchange:	IKEv2 Mode
DH Group:	Group 2
Encryption:	AES-128
Authentication:	SHA1
Life Time (seconds):	28800

Ipsec (Phase 2) Proposal

Protocol:	ESP
Encryption:	AES-128
Authentication:	SHA1
□ Enable Perfect Forward Secrecy	
Life Time (seconds):	28800

16 Under **IKE (Phase 1) Proposal**, choose one of the following options from the **Exchange** drop-down menu:

Main Mode	Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
Aggressive Mode	Generally used when WAN addressing is dynamically assigned. Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
IKEv2 Mode	Causes all negotiation to happen through IKEv2 protocols, rather than using IKEv1 phase 1. **NOTE:** If you select **IKE v2 Mode**, both ends of the VPN tunnel must use IKE v2. When selected, the **DH Group**, **Encryption**, and **Authentication** fields are dimmed and cannot be defined.

17 Under **IKE (Phase 1) Proposal**, set the values for the remaining options. The default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations.

> **NOTE:** If **IKEv2 Mode** is selected for the **Exchange** field, the **DH Group**, **Encryption**, and **Authentication** fields are dimmed and no selection can be made for those options.

> **NOTE:** Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.

a For the **DH Group**, when in **Main Mode** or **Aggressive Mode**, you can select from several Diffie-Hellman exchanges:

Diffie-Hellman Groups Included in Suite B Cryptography	**Other Diffie-Hellman Options**
256-bit Random ECP Group	Group 1

384-bit Random ECP Group	Group 2
521-bit Random ECP Group	Group 5
192-bit Random ECP Group	Group 14
224-bit Random ECP Group	

b For the **Encryption** field, if **Main Mode** or **Aggressive Mode** was selected, choose **3DES**, **DES**, **AES-128** (default), **AES-192**, or **AES-256** from the drop-down menu.

c For the **Authentication** field, if **Main Mode** or **Aggressive Mode** was selected, choose **SHA-1** (default), **MD5**, **SHA256**, **SHA384**, or **SHA512** for enhanced authentication security.

d For all **Exchange** modes, enter a value for **Life Time (seconds)**. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

18 Set the options in the **IPsec (Phase 2) Proposal** section. The default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, and **Life Time (seconds)** are acceptable for most VPN SA configurations.

> ⓘ **NOTE:** Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

- If you selected **ESP** in the **Protocol** field, then in the **Encryption** field you can select from six encryption algorithms that are included in Suite B cryptography:

Suite B Cryptography Options	Other Options
AESGCM16-128	**DES**
AESGCM16-192	**3DES**
AESGCM16-256	**AES-128**
AESGMAC-128	**AES-192**
AESGMAC-192	**AES-256**
AESGMAC-256	**None**

- If you selected **AH** in the **Protocol** field, the **Encryption** field is dimmed and you cannot select any options.

19 Click **Advanced**.

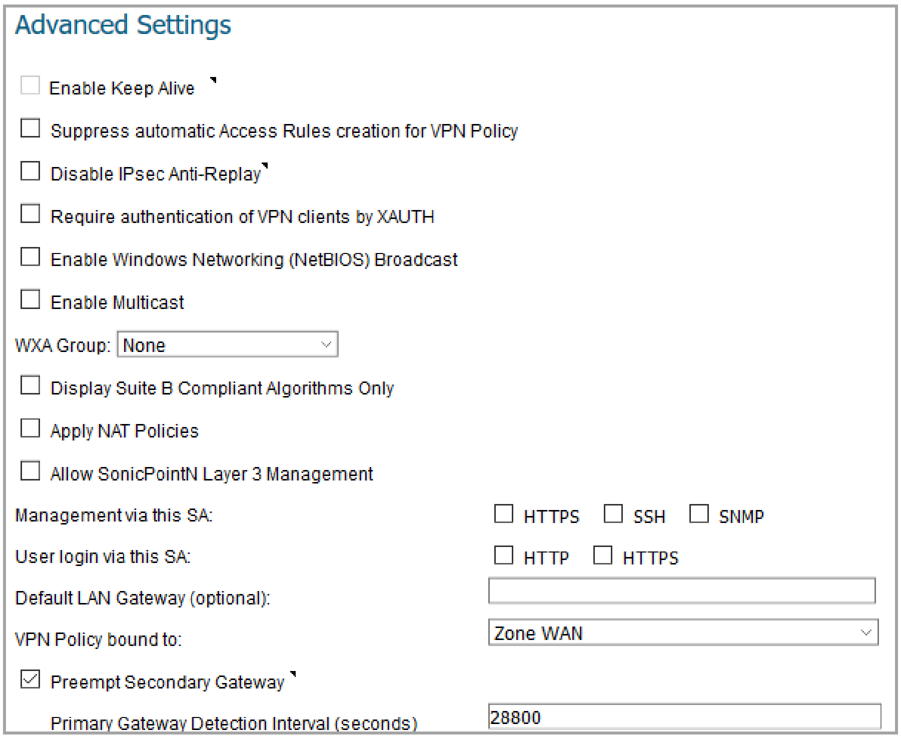
20 Select any of the optional settings you want to apply to your VPN policy. The options change depending on options you selected in the **Proposals** screen.

Options	**Main Mode or Aggressive Mode** (See figure Advanced Settings for Main and Aggressive Modes below)	**IKEv2 Mode** (See figure Advanced Settings for IKEv2 Mode below)
Advanced Settings		
Enable Keep Alive	Select to use heartbeat messages between peers on this VPN tunnel if one end of the tunnel fails, using a keep-alive heartbeat allows automatic renegotiation of the tunnel after both sides are available again without having to wait for the proposed Life Time to expire. **NOTE:** The Keep Alive option is disabled when the VPN policy is configured as a central gateway for DHCP over VPN or with a primary gateway name or address 0.0.0.0.	Cannot be selected for IKEv2 mode.
Suppress automatic Access Rules creation for VPN Policy	When *not* selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control on page 22 for more information.	When *not* selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control on page 22 for more information.
Disable IPsec Anti-Replay	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window).	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window).
Require authentication of VPN clients by XAUTH	Requires that all inbound traffic on this VPN policy is from a user authenticated by XAUTH/RADIUS. Unauthenticated traffic is not allowed on the VPN tunnel.	Not available in IKEv2 Mode.
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.
Enable Multicast	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.
WXA Group	Select **None** (default) or **Group One.**	Select **None** (default) or **Group One**.
Display Suite B Compliant Algorithms Only	Select if you want to show only the Suite B compliant algorithms.	Select if you want to show only the Suite B compliant algorithms.

Options	Main Mode or Aggressive Mode (See figure Advanced Settings for Main and Aggressive Modes below)	IKEv2 Mode (See figure Advanced Settings for IKEv2 Mode below)
Apply NAT Policies	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
Allow SonicPointN Layer 3 Management	Select if you want to allow Layer 3 management.	Select if you want to allow Layer 3 management.
Management via this SA	Select any of **HTTPS**, **SSH**, or **SNMP** for this option to manage the local SonicWall firewall through the VPN tunnel.	Select any of **HTTPS**, **SSH**, or **SNMP** for this option to manage the local SonicWall firewall through the VPN tunnel.
User login via this SA	Select **HTTP**, **HTTPS**, or both to allow users to login using the SA. **NOTE:** HTTP user login is not allowed with remote authentication.	Select **HTTP**, **HTTPS**, or both to allow users to login using the SA. **NOTE:** HTTP user login is not allowed with remote authentication.
Default LAN Gateway (optional)	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected **Use this VPN Tunnel as a default route for all Internet traffic** (on the **Network** screen, under **Remote Networks**) enter the router address.	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected **Use this VPN Tunnel as a default route for all Internet traffic** (on the **Network** screen, under **Remote Networks**) enter the router address.
VPN Policy bound to	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. **Important:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. **Important:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.

Options	**Main Mode or Aggressive Mode** (See figure Advanced Settings for Main and Aggressive Modes below)	**IKEv2 Mode** (See figure Advanced Settings for IKEv2 Mode below)
Preempt Secondary Gateway	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the **Primary Gateway Detection Interval (seconds)** option. The default time is 28800 seconds, or 8 hours.	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the **Primary Gateway Detection Interval (seconds)** option. The default time is 28800 seconds, or 8 hours.
IKEv2 Settings		
Do not send trigger packet during IKE SA negotiation	Not available in Main or Aggressive modes.	Is *not* selected (default). Should only be selected when required for interoperability if the peer cannot handle trigger packets. The recommended practice is to include trigger packets to help the IKEv2 Responder select the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it might be appropriate to disable the inclusion of trigger packets to some IKE peers.
Accept Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, sends a message to the peer device saying that HTTP certification look-up is supported.
Send Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, responds to the message from the peer device and confirms HTTP certification look-up is supported.

Advanced Settings for Main and Aggressive Modes



Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Disable IPsec Anti-Replay

□ Require authentication of VPN clients by XAUTH

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

WXA Group: None

□ Display Suite B Compliant Algorithms Only

□ Apply NAT Policies

□ Allow SonicPointN Layer 3 Management

Management via this SA: □ HTTPS □ SSH □ SNMP

User login via this SA: □ HTTP □ HTTPS

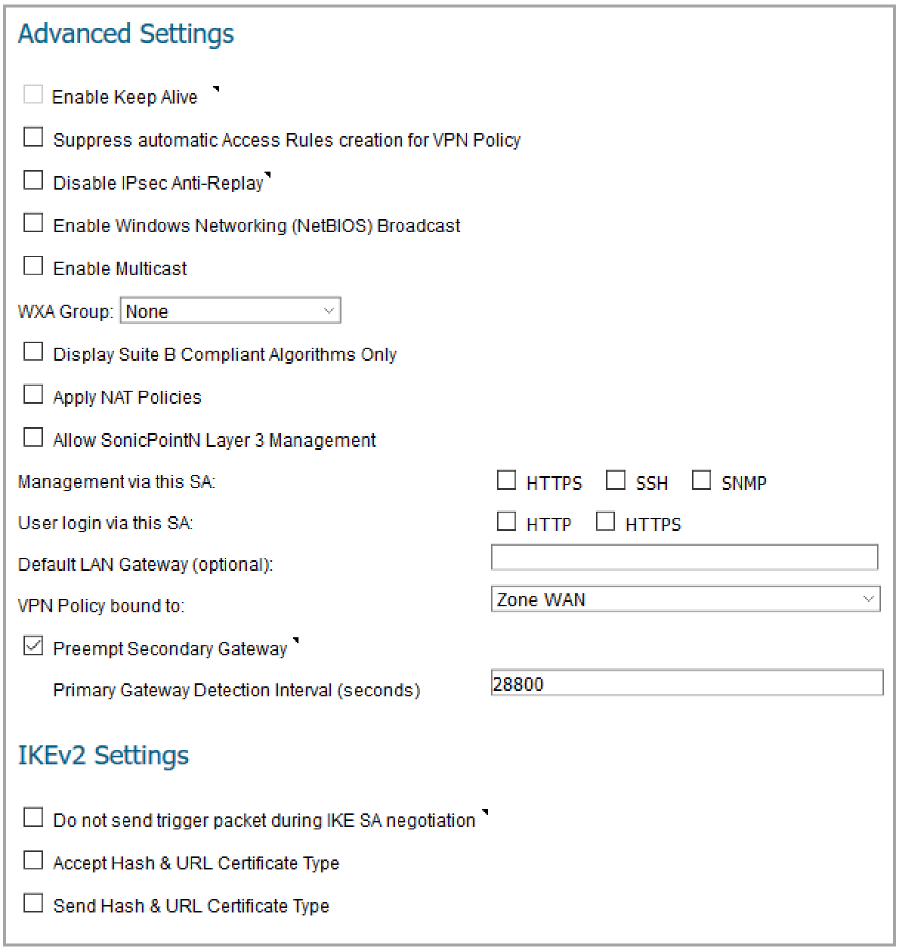
Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

☑ Preempt Secondary Gateway

Primary Gateway Detection Interval (seconds) 28800

Advanced Settings for IKEv2 Mode



Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Disable IPsec Anti-Replay

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

WXA Group: None

□ Display Suite B Compliant Algorithms Only

□ Apply NAT Policies

□ Allow SonicPointN Layer 3 Management

Management via this SA: □ HTTPS □ SSH □ SNMP

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

☑ Preempt Secondary Gateway

Primary Gateway Detection Interval (seconds) 28800

IKEv2 Settings

□ Do not send trigger packet during IKE SA negotiation

□ Accept Hash & URL Certificate Type

□ Send Hash & URL Certificate Type

21 Click **OK**.

22 Click **ACCEPT** on the **VPN > Base Settings** page to update the VPN Policies.

Configuring with a Manual Key

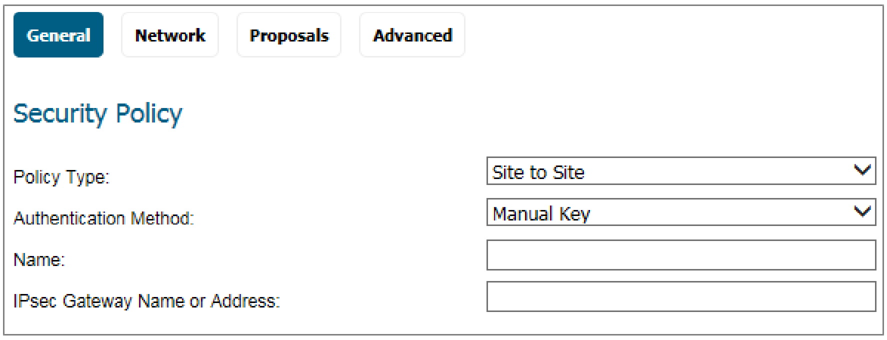
You can manually define encryption keys for establishing an IPsec VPN tunnel. You define manual keys when you need to specify what the encryption or authentication key is (for example, when one of the VPN peers requires a specific key) or when you need to disable encryption and authentication.

To configure a VPN policy using Manual Key:

1 Navigate to **MANAGE | Connectivity | VPN > Base Settings**.

2 Click **ADD** to create a new policy or click the **Edit** icon if you are updating an existing policy.

3 In the **Authentication Method** field, select **Manual Key** from drop-down menu. The window shows only the Manual Key options.



Security Policy

Policy Type: Site to Site

Authentication Method: Manual Key

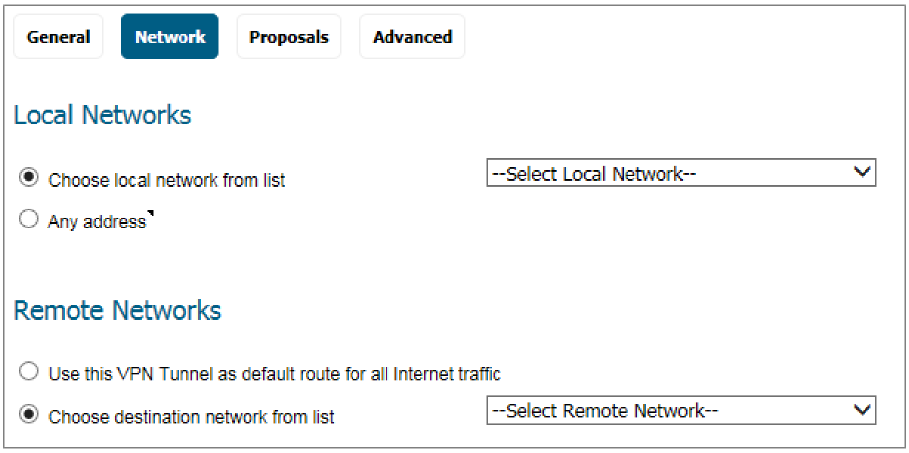
Name:

IPsec Gateway Name or Address:

4 Enter a name for the policy in the **Name** field.

5 Enter the host name or IP address of the remote connection in the **IPsec Gateway Name or Address** field.

6 Click **Network**.



Local Networks

● Choose local network from list --Select Local Network--

○ Any address

Remote Networks

○ Use this VPN Tunnel as default route for all Internet traffic

● Choose destination network from list --Select Remote Network--

7 Under **Local Networks**, select one of these options:

- If a specific local network can access the VPN tunnel, select a that local network from the **Choose local network from list** drop-down menu.
- If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules are created between Trusted Zones and the VPN Zone.

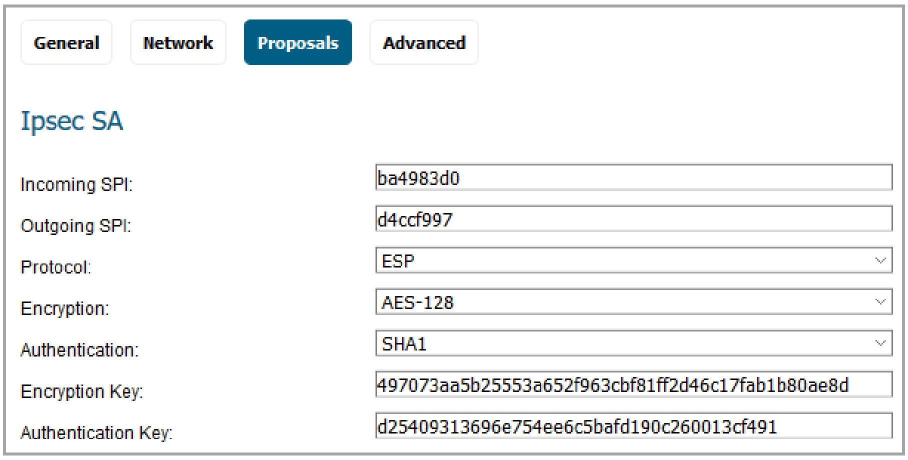
8 Under **Destination Networks**, select one of these:

- If traffic from any local user cannot leave the firewall unless it is encrypted, select **Use this VPN Tunnel as default route for all Internet traffic**.

  NOTE: You can only configure one SA to use this setting.

- Alternatively, select **Choose Destination network from list**, and select the address object or group.

9 Click **Proposals**.



Ipsec SA

Incoming SPI:	ba4983d0
Outgoing SPI:	d4ccf997
Protocol:	ESP
Encryption:	AES-128
Authentication:	SHA1
Encryption Key:	497073aa5b25553a652f963cbf81ff2d46c17fab1b80ae8d
Authentication Key:	d25409313696e754ee6c5bafd190c260013cf491

10 Define an **Incoming SPI** and an **Outgoing SPI**. A Security Parameter Index (SPI) is hexadecimal and can range from 3 to 8 characters in length.

> **IMPORTANT:** Each Security Association (SA) must have unique SPIs; no two SAs can share the same SPIs. However, each SA Incoming SPI can be the same as the Outgoing SPI.

11 The default values for **Protocol, Encryption**, and **Authentication** are acceptable for most VPN SA configurations; otherwise, select values from the drop-down menu.

> **NOTE:** The values for **Protocol, Encryption**, and **Authentication** must match the values on the remote firewall.

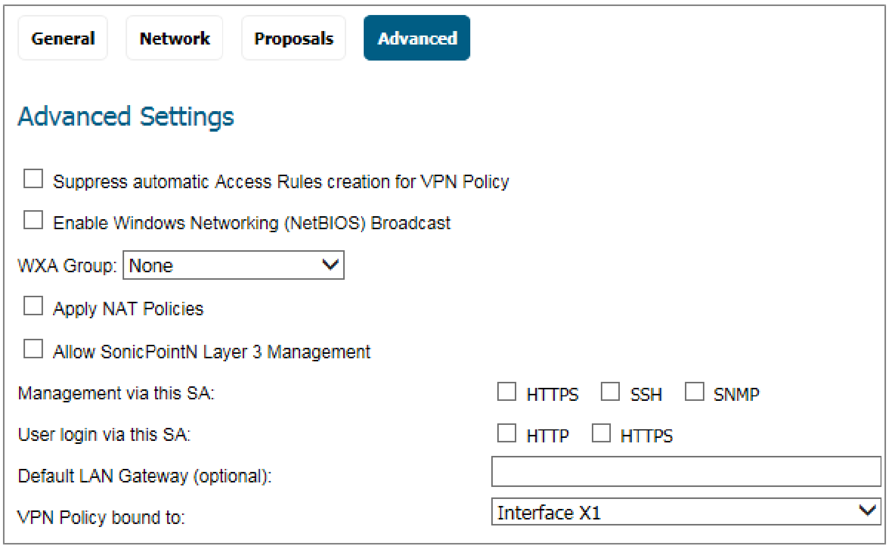
- If you selected **ESP** in the **Protocol** field, then in the **Encryption** field you can select from six encryption algorithms that are included in Suite B cryptography:
  - **DES**
  - **3DES**
  - **AES-128** (default)
  - **AES-192**
  - **AES-256**
  - **None**
- If you selected **AH** in the **Protocol** field, the **Encryption** field is grayed out, and you cannot select any options.

12 In the **Encryption Key** field, enter a 48-character hexadecimal encryption key or use the default value. This encryption key is used to configure the remote SonicWall encryption key, so write it down to use when configuring the remote firewall.

> **TIP:** Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption or authentication key, an error message is displayed at the bottom of the browser window.

13 In the **Authentication Key** field, enter a 40-character hexadecimal authentication key or use the default value. Write down the key to use while configuring the firewall settings.

14 Click **Advanced**.



Advanced Settings

□ Suppress automatic Access Rules creation for VPN Policy

□ Enable Windows Networking (NetBIOS) Broadcast

WXA Group: None

□ Apply NAT Policies

□ Allow SonicPointN Layer 3 Management

Management via this SA: □ HTTPS □ SSH □ SNMP

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Interface X1

15 Select any of the following optional settings you want to apply to your VPN policy.

Option	Definition
Suppress automatic Access Rules creation for VPN Policy	When *not* selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control on page 22 for more information.
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.
WXA Group	Select **None** (default) or **Group One**
Apply NAT Policies	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both side of a tunnel use either the same or overlapping subnets. **Tip:** Informational videos with interface configuration examples are available online. For example, see How to Configure NAT over VPN in a Site to Site VPN with Overlapping Networks. Additional videos are available at: https://www.sonicwall.com/support/video-tutorials.
Allow SonicPointN Layer 3 Management	Select if you want to allow Layer 3 management.
Management via this SA	Select **HTTPS**, **SSH**, **SNMP** or any combination of these three to manage the local SonicWall firewall through the VPN tunnel.
User login via this SA	Select **HTTP**, **HTTPS**, or both to allow users to log in using the SA. **NOTE:** HTTP user login is not allowed with remote authentication.

Option	Definition
Default LAN Gateway (optional)	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected **Use this VPN Tunnel as a default route for all Internet traffic** (on the **Network** screen under **Remote Networks**) enter the router address.
VPN Policy bound to	Select an interface or zone from the drop-down menu. **Important:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.

16 Click **OK**.

17 Click **ACCEPT** on the **VPN > Base Settings** page to update the VPN Policies.

Configuring with a Third-Party Certificate

> ⓘ **NOTE:** You must have a valid certificate from a third-party certificate authority installed on your SonicWall firewall before you can configure your VPN policy using a third-party IKE certificate.

With SonicWall firewalls, you can opt to use third-party certificates for authentication instead of the SonicWall Authentication Service. Using certificates from a third-party provider or using local certificates is a more manual process; therefore, experience with implementing Public Key Infrastructure (PKI) is necessary to understand the key components of digital certificates.

SonicWall supports the following two certificate providers:

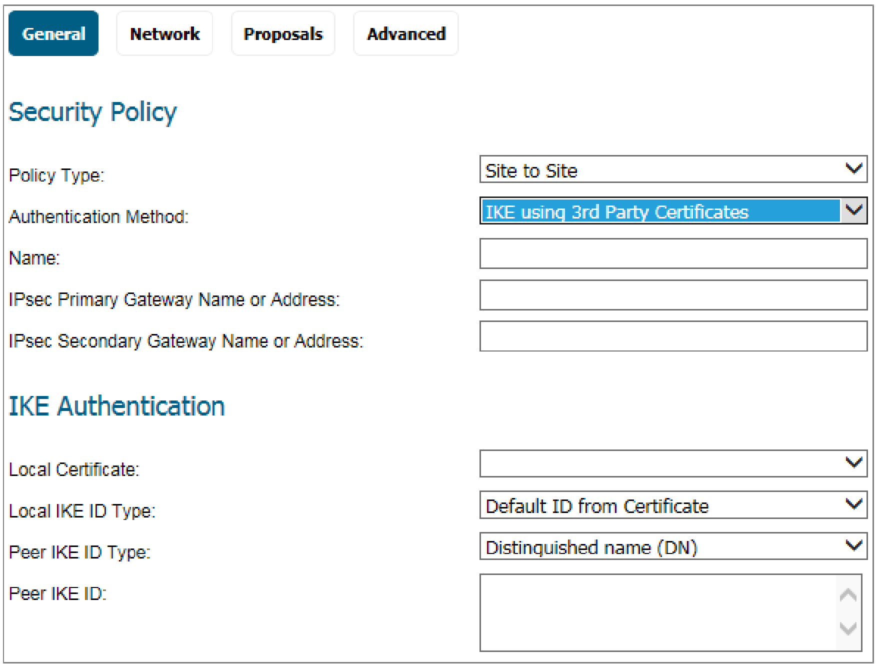
- VeriSign
- Entrust

To create a VPN SA using IKE and third-party certificates:

1 Navigate to **MANAGE | Connectivity | VPN > Base Settings**.

2 Click **ADD** to create a new policy or click the **Edit** icon if you are updating an existing policy.

3 In the **Authentication Method** field, select **IKE using 3rd Party Certificates**. The **VPN Policy** window displays the third-party certificate options in the **IKE Authentication** section.



Security Policy

Policy Type: Site to Site

Authentication Method: IKE using 3rd Party Certificates

Name:

IPsec Primary Gateway Name or Address:

IPsec Secondary Gateway Name or Address:

IKE Authentication

Local Certificate:

Local IKE ID Type: Default ID from Certificate

Peer IKE ID Type: Distinguished name (DN)

Peer IKE ID:

4 Type a name for the Security Association in the **Name** field.

5 Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWall in the **IPsec Primary Gateway Name or Address** field.

6 If you have a secondary remote SonicWall, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPsec Secondary Gateway Name or Address** field.

7 Under **IKE Authentication**, select a third-party certificate from the **Local Certificate** list. You must have imported local certificates before selecting this option.

8 For **Local IKE ID Type**, the default is **Default ID from Certificate**. Or, choose one of the following:

- **Distinguished Name (DN)**
- **Email ID (UserFQDN)**
- **Domain Name (FQDN)**
- **IP Address (IPV4)**

These alternate selections are the same as those for **Peer IKE ID Type**, described in the next step.

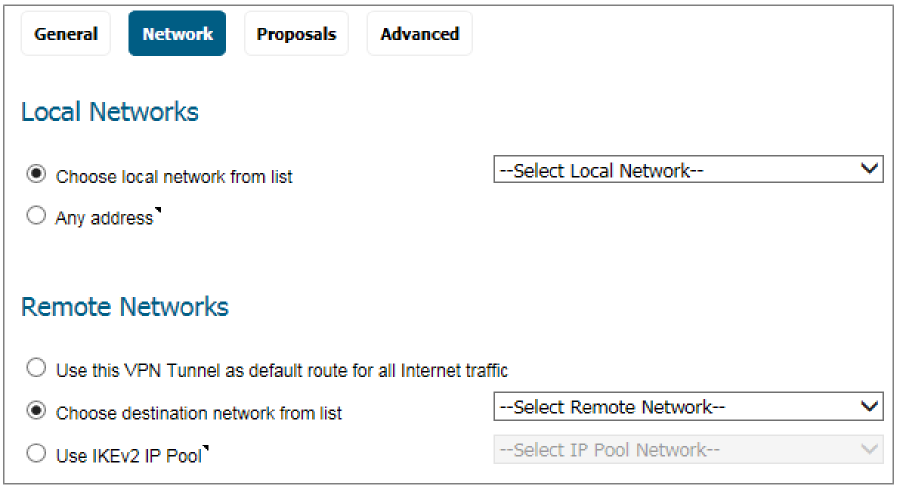
9 From the **Peer IKE ID Type** drop-down menu, select one of the following Peer ID types:

Peer IKE ID Type Option	Definition
Default ID from Certificate	Authentication is taken from the default ID on the certificate.
Distinguished Name (DN)	Authentication is based on the certificate's Subject Distinguished Name field, which is contained in all certificates by default. The entire Distinguished Name field must be entered for site to site VPNs. Wild card characters are not supported. The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: **/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub**.
Email ID (UserFQDN)	Authentication based on the **Email ID (UserFQDN)** types are based on the certificate's Subject Alternative Name field, which is *not* contained in all certificates by default. If the certificate contains a Subject Alternative Name, that value must be used. For site to site VPNs, wild card characters cannot be used. The full value of the Email ID must be entered. This is because site to site VPNs are expected to connect to a single peer, whereas Group VPNs expect to connect to multiple peers.
Domain Name (FQDN)	Authentication based on the **Domain Name (FQDN)** types are based on the certificate's Subject Alternative Name field, which is *not* contained in all certificates by default. If the certificate contains a Subject Alternative Name, that value must be used. For site to site VPNs, wild card characters cannot be used. The full value of the Domain Name must be entered because site to site VPNs are expected to connect to a single peer, whereas Group VPNs expect to connect to multiple peers.
IP Address (IPV4)	Based on the IPv4 IP address.

ⓘ **NOTE:** To find the certificate details (Subject Alternative Name, Distinguished Name, and so on), navigate to the **MANAGE | System Setup | Appliance > Certificates** page.

10 Type an ID string in the **Peer IKE ID** field.

11 Click **Network**.



Local Networks

● Choose local network from list — --Select Local Network--

○ Any address

Remote Networks

○ Use this VPN Tunnel as default route for all Internet traffic

● Choose destination network from list — --Select Remote Network--

○ Use IKEv2 IP Pool — --Select IP Pool Network--

12 Under **Local Networks**, select one of these options:

- Select a local network from the **Choose local network from list** drop-down menu if a specific local network can access the VPN tunnel.
- Select **Any Address** if traffic can originate from any local network. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules are created between Trusted Zones and the VPN Zone.

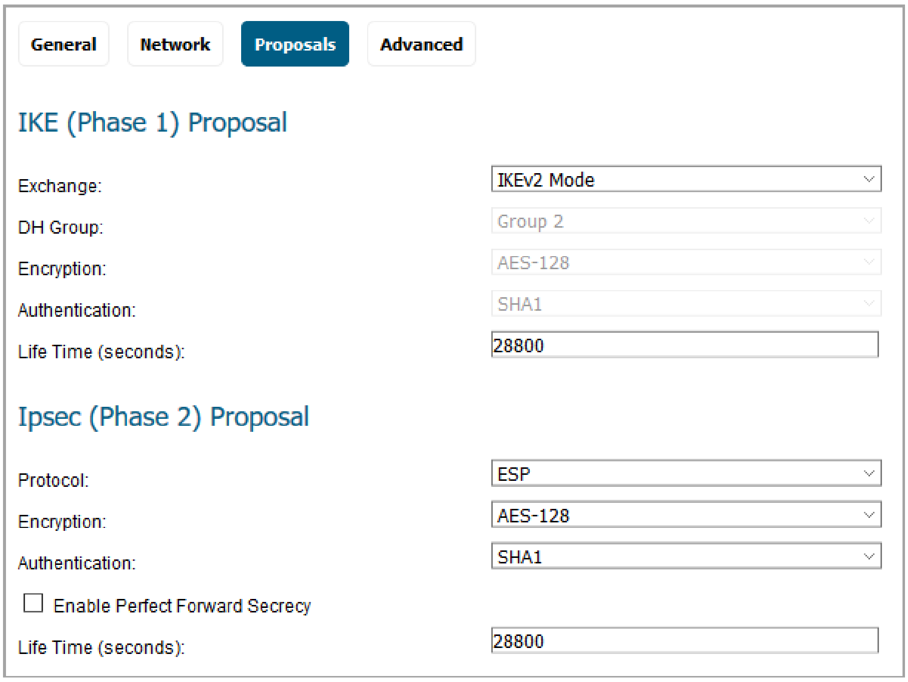
13 Under **Remote Networks**, select one of these options:

- Select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the firewall unless it is encrypted,

  NOTE: You can only configure one SA to use this setting.

- Alternatively, select **Choose Destination network from list,** and select the address object or group from the drop-down menu.
- Select **Use IKEv2 IP Pool** if you want to support IKEv2 Config payload, and select the address object or IP Pool Network from the drop-down menu.

14 Click **Proposals**.



IKE (Phase 1) Proposal

Exchange:	IKEv2 Mode
DH Group:	Group 2
Encryption:	AES-128
Authentication:	SHA1
Life Time (seconds):	28800

Ipsec (Phase 2) Proposal

Protocol:	ESP
Encryption:	AES-128
Authentication:	SHA1
☐ Enable Perfect Forward Secrecy	
Life Time (seconds):	28800

15 In the **IKE (Phase 1) Proposal** section, select the following settings:

Main Mode	Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
Aggressive Mode	Generally used when WAN addressing is dynamically assigned. Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
IKEv2 Mode	Causes all negotiation to happen through IKEv2 protocols, rather than using IKEv1 phases. **NOTE:** If you select **IKE v2 Mode**, both ends of the VPN tunnel must use IKE v2. When selected, the **DH Group**, **Encryption**, and **Authentication** fields are dimmed and cannot be defined.

16 Under **IKE (Phase 1) Proposal**, set the values for the remaining options. The default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations.

> ⓘ **NOTE:** If **IKEv2 Mode** is selected for the **Exchange** field, the **DH Group**, **Encryption**, and **Authentication** fields are dimmed and no selection can be made for those options.

> ⓘ **NOTE:** Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.

a For the **DH Group**, when in **Main Mode** or **Aggressive Mode**, you can select from several Diffie-Hellman exchanges:

Diffie-Hellman Groups Included in Suite B Cryptography	Other Diffie-Hellman Options
256-bit Random ECP Group	Group 1

384-bit Random ECP Group	Group 2
521-bit Random ECP Group	Group 5
192-bit Random ECP Group	Group 14
224-bit Random ECP Group	

b For the **Encryption** field, if **Main Mode** or **Aggressive Mode** was selected, choose **DES**, **3DES**, **AES-128** (default), **AES-192**, or **AES-256** from the drop-down menu.

c For the **Authentication** field, if **Main Mode** or **Aggressive Mode** was selected, choose **MD5**, **SHA-1** (default), **SHA256**, **SHA384**, or **SHA512** for enhanced authentication security.

17 For all **Exchange** modes, enter a value for **Life Time (seconds)**. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

18 Set the options in the **IPsec (Phase 2) Proposal** section. The default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, and **Life Time (seconds)** are acceptable for most VPN SA configurations.

> **NOTE:** Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

a Select the desired protocol for **Protocol**.

If you selected **ESP** in the **Protocol** field, then in the **Encryption** field you can select from six encryption algorithms that are included in Suite B cryptography:

Suite B Cryptography Options	Other Options
AESGCM16-128	**DES**
AESGCM16-192	**3DES**
AESGCM16-256	**AES-128**
AESGMAC-128	**AES-192**
AESGMAC-192	**AES-256**
AESGMAC-256	**None**

If you selected **AH** in the **Protocol** field, the **Encryption** field is dimmed and you cannot select any options.

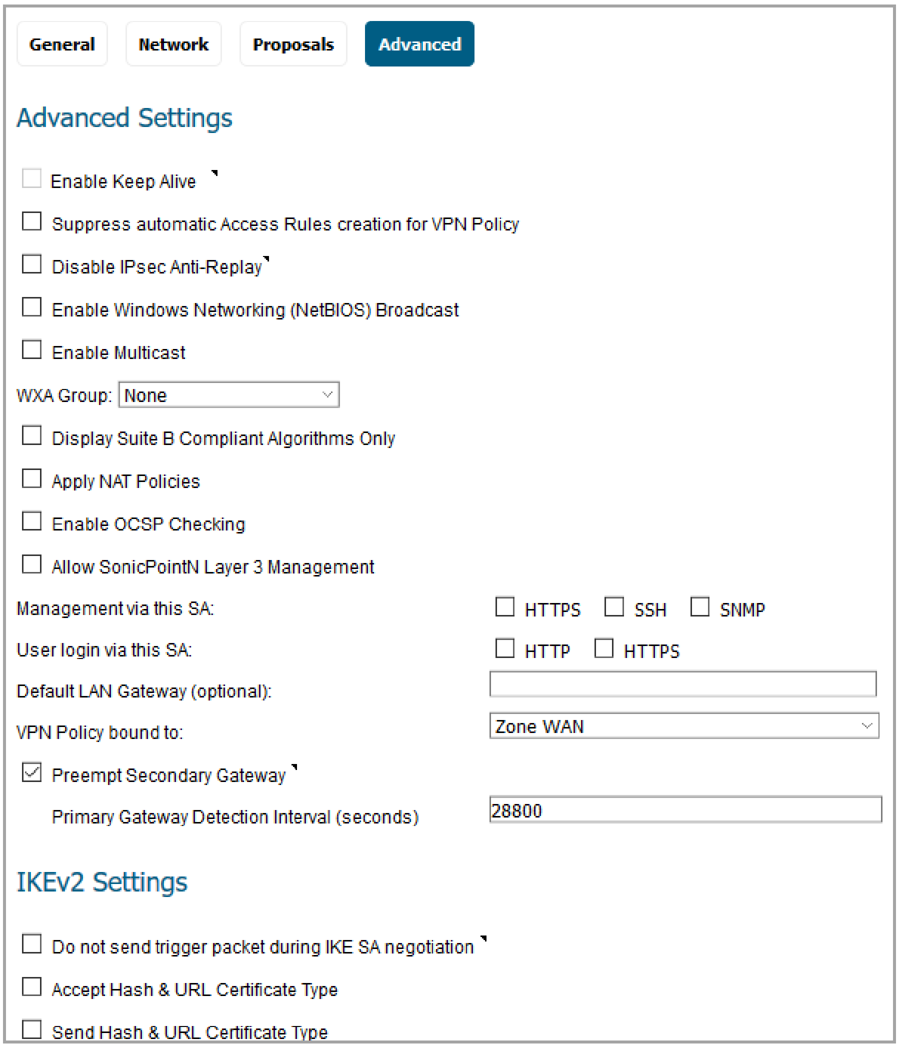
b For **Authentication**, select the desired authentication method: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, **SHA512**, **AES-XCBC**, or **None**.

c Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security and select **Group 2** from the **DH Group** menu.

d Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

19 Click **Advanced**.

Advanced for 3rd Party Certificates with IKEv2 Mode



General | Network | Proposals | Advanced

Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Disable IPsec Anti-Replay

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

WXA Group: None

□ Display Suite B Compliant Algorithms Only

□ Apply NAT Policies

□ Enable OCSP Checking

□ Allow SonicPointN Layer 3 Management

Management via this SA: □ HTTPS □ SSH □ SNMP

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

☑ Preempt Secondary Gateway

Primary Gateway Detection Interval (seconds) 28800

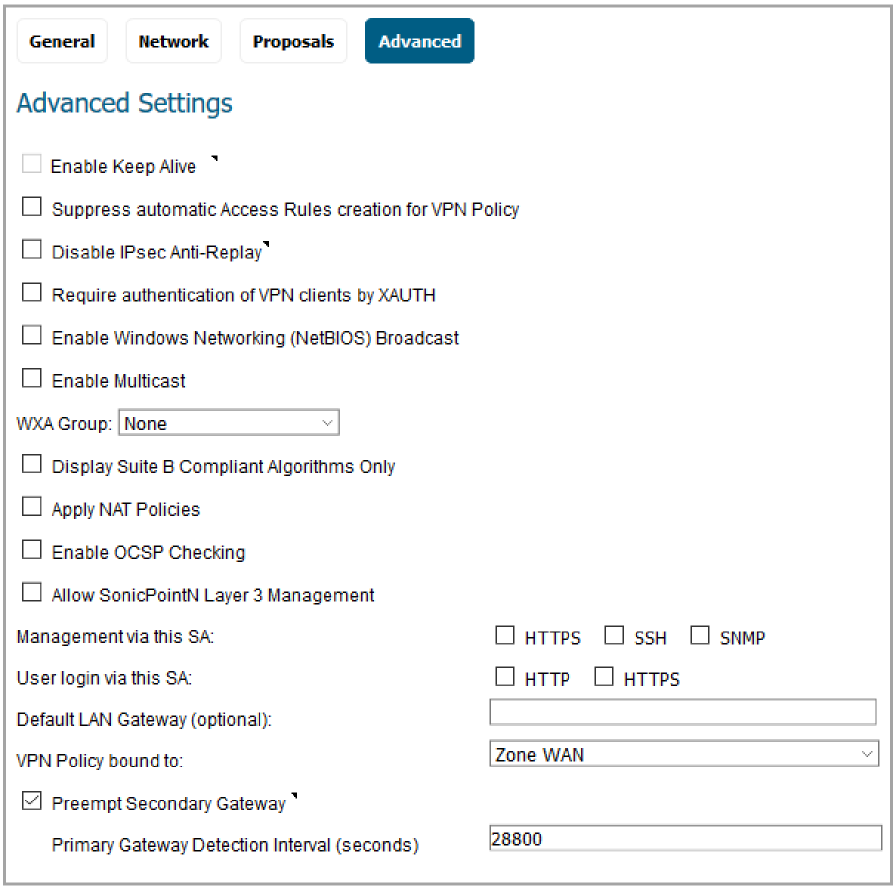
IKEv2 Settings

□ Do not send trigger packet during IKE SA negotiation

□ Accept Hash & URL Certificate Type

□ Send Hash & URL Certificate Type

Advanced for 3rd Party Certificates with Main or Aggressive Mode



Advanced Settings

□ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Disable IPsec Anti-Replay

□ Require authentication of VPN clients by XAUTH

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

WXA Group: None

□ Display Suite B Compliant Algorithms Only

□ Apply NAT Policies

□ Enable OCSP Checking

□ Allow SonicPointN Layer 3 Management

Management via this SA: □ HTTPS □ SSH □ SNMP

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

☑ Preempt Secondary Gateway

Primary Gateway Detection Interval (seconds) 28800

20 Select any configuration options you want to apply to your VPN policy:

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Advanced Settings		
Enable Keep Alive	Select to use heartbeat messages between peers on this VPN tunnel if one end of the tunnel fails, using a keep-alive heartbeat allows automatic renegotiation of the tunnel after both sides are available again without having to wait for the proposed Life Time to expire. **NOTE:** The Keep Alive option is disabled when the VPN policy is configured as a central gateway for DHCP over VPN or with a primary gateway name or address 0.0.0.0.	Cannot be selected for IKEv2 mode.
Suppress automatic Access Rules creation for VPN Policy	When *not* selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control on page 22 for more information.	When *not* selected (default), accompanying Access Rules are created automatically. See VPN Auto-Added Access Rule Control on page 22 for more information.

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Disable IPsec Anti-Replay	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window).	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window).
Require authentication of VPN clients by XAUTH	Requires that all inbound traffic on this VPN policy is from a user authenticated by XAUTH/RADIUS. Unauthenticated traffic is not allowed on the VPN tunnel.	Not available in IKEv2 Mode.
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.
Enable Multicast	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.
WXA Group	Select **None** (default) or **Group One**.	Select **None** (default) or **Group One**.
Display Suite B Compliant Algorithms Only	Select if you want to show only the Suite B compliant algorithms.	Select if you want to show only the Suite B compliant algorithms.
Apply NAT Policies	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
Enable OCSP Checking	Select if you want to check VPN certificate status and provide the **OCSP Responder URL** in the field provided.	Select if you want to check VPN certificate status and provide the **OCSP Responder URL** in the field provided.
Allow SonicPointN Layer 3 Management	Allows Layer 3 management of the access point.	Allows Layer 3 management of the access point.
Management via this SA	Select **HTTPS**, **SSH**, **SNMP** or any combination of these three to manage the local SonicWall firewall through the VPN tunnel.	Select **HTTPS**, **SSH**, **SNMP** or any combination of these three to manage the local SonicWall firewall through the VPN tunnel.

Options	Main Mode or Aggressive Mode	IKEv2 Mode
User login via this SA	Select **HTTP**, **HTTPS**, or both to allow users to log in using the SA. **NOTE:** HTTP user login is not allowed with remote authentication.	Select **HTTP**, **HTTPS**, or both to allow users to log in using the SA. **NOTE:** HTTP user login is not allowed with remote authentication.
Default LAN Gateway (optional)	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected **Use this VPN Tunnel as a default route for all Internet traffic** (on the **Network** view of this page, under **Remote Networks**) enter the router address.	If you want to route traffic that is destined for an unknown subnet through a LAN before entering this tunnel, select this option. For example, if you selected **Use this VPN Tunnel as a default route for all Internet traffic** (on the **Network** view of this page, under **Remote Networks**) enter the router address.
VPN Policy bound to	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. **Important:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.	Select an interface or zone from the drop-down menu. Zone WAN is the preferred setting if you are using WAN load balancing and you want the VPN to use either WAN interface. **Important:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.
Preempt Secondary Gateway	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the **Primary Gateway Detection Interval (seconds)** option. The default time is 28800 seconds, or 8 hours.	To preempt a second gateway after a specified time, select this checkbox and configure the desired time in the **Primary Gateway Detection Interval (seconds)** option. The default time is 28800 seconds, or 8 hours.
IKEv2 Settings		
Do not send trigger packet during IKE SA negotiation	Not available in Main or Aggressive modes.	Is *not* selected (default). Should only be selected when required for interoperability if the peer cannot handle trigger packets. The recommended practice is to include trigger packets to help the IKEv2 Responder select the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it might be appropriate to disable the inclusion of trigger packets to some IKE peers.

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Accept Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, sends a message to the peer device saying that HTTP certification look-up is supported.
Send Hash & URL Certificate Type	Not available in Main or Aggressive modes.	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, responds to the message from the peer device and confirms HTTP certification look-up is supported.

21 Click **OK**.

22 Click **ACCEPT** on the **VPN > Base Settings** page to update the VPN Policies.

Configuring the Remote SonicWall Network Security Appliance

1 Navigate to **MANAGE | Connectivity | VPN > Base Settings**.

2 Click **ADD**. The **VPN Policy** dialog displays.

3 In the **General** screen, select **Manual Key** from the **Authentication Method** drop-down menu.

4 Enter a name for the SA in the **Name** field.

5 Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address** field.

6 Click **Network**.

7 Under **Local Networks**, select one of these:

- If a specific local network can access the VPN tunnel, select a local network from the **Choose local network from list** drop-down menu.
- If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto-added rules are created between Trusted Zones and the VPN Zone.

8 Under **Remote Networks**, select one of these:

- If traffic from any local user cannot leave the firewall unless it is encrypted, select **Use this VPN Tunnel as default route for all Internet traffic**.

  ⓘ **NOTE:** You can only configure one SA to use this setting.

- Alternatively, select **Choose Destination network from list,** and select the address object or group.

9 Click **Proposals**.

10 Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

> ⓘ **NOTE:** Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

11 The default values for **Protocol**, **Encryption**, and **Authentication** are acceptable for most VPN SA configurations.

> ⓘ **NOTE:** The values for **Protocol, Encryption**, and **Authentication** must match the values on the opposite side of the tunnel.

12 Enter a 48-character hexadecimal encryption key in the **Encryption Key** field. Use the same value as used on the firewall on the opposite side of the tunnel.

13 Enter a 40-character hexadecimal authentication key in the **Authentication Key** field. Use the same value as used on the firewall on the opposite side of the tunnel.

> ⓘ **TIP:** Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

14 Click **Advanced.**

15 Select any of the following optional settings you want to apply to your VPN policy:

- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- For **WXA Group**, select **None** or **Group One**.
- Select **Apply NAT Policies** if you want the firewall to translate the Local, Remote or both networks communicating through this VPN tunnel. Two drop-down menus display:
    - To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu.
    - To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

    > ⓘ **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- To manage the remote SonicWall through the VPN tunnel, select **HTTP**, **SSH**, **SNMP**, or any combination of these three from **Management via this SA.**
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.

    > ⓘ **NOTE:** HTTP user login is not allowed with remote authentication.

- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** menu.

    > ⓘ **IMPORTANT:** Two different WAN interfaces cannot be selected from the **VPN Policy bound to** drop-down menu if the VPN Gateway IP address is the same for both.

16 Click **OK**.

17 Click **ACCEPT** on the **VPN > Base Settings** page to update the VPN Policies.

TIP: If Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.

Configuring VPN Failover to a Static Route

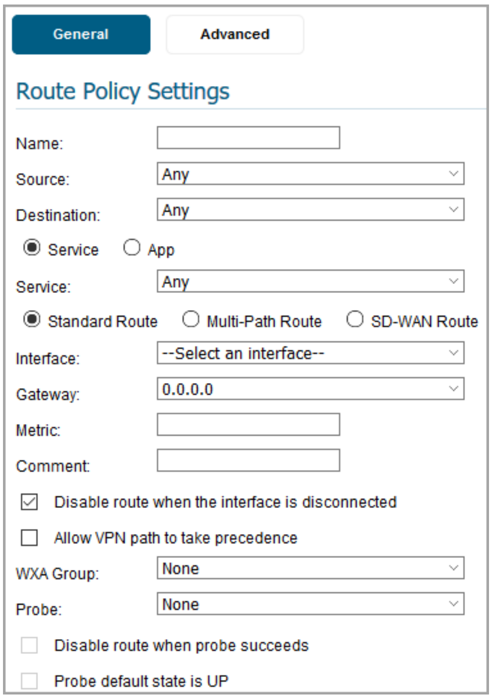
You can configure a static route as a secondary route in case the VPN tunnel goes down. When defining the route policies, the **Allow VPN path to take precedence** option allows you to create a secondary route for a VPN tunnel and gives precedence to VPN traffic having the same destination address object. This results in the following behavior:

- When a VPN tunnel is active: static routes matching the destination address object of the VPN tunnel are automatically disabled if the **Allow VPN path to take precedence** option is enabled. All traffic is routed over the VPN tunnel to the destination address object.
- When a VPN tunnel goes down: static routes matching the destination address object of the VPN tunnel are automatically enabled. All traffic to the destination address object is routed over the static routes.

More information on how to set up network routing policies is provided in *SonicOS 6.5 System Setup*.

To configure a static route as a VPN failover:

1. Navigate to **MANAGE | System Setup | Network > Routing**.
2. Click **Route Policies > Add**.



Route Policy Settings

Name:

Source: Any

Destination: Any

● Service ○ App

Service: Any

● Standard Route ○ Multi-Path Route ○ SD-WAN Route

Interface: --Select an interface--

Gateway: 0.0.0.0

Metric:

Comment:

☑ Disable route when the interface is disconnected

□ Allow VPN path to take precedence

WXA Group: None

Probe: None

□ Disable route when probe succeeds

□ Probe default state is UP

3. Type a descriptive name for the policy into the **Name** field.
4. Select the appropriate **Source**, **Destination**, **Service**, **Gateway**, and **Interface**.
5. Define **Metric** as **1**.
6. Select **Allow VPN path to take precedence**.
7. Click **OK**.

VPN Auto Provisioning

You can configure various types of IPsec VPN policies, such as site-to-site policies, including GroupVPN, and route-based policies. For specific details on the setting for these kinds of policies, go to the following sections:

- Site to Site VPNs
- Tunnel Interface Route-based VPN

Topics in this section include:

- About VPN Auto Provisioning
- Configuring a VPN AP Server
- Configuring a VPN AP Client

About VPN Auto Provisioning

The SonicOS VPN Auto Provisioning feature simplifies the provisioning of site to site VPNs between two SonicWall firewalls. This section provides conceptual information and describes how to configure and use the VPN Auto Provisioning feature.

Topics:

- Defining VPN Auto Provisioning
- Benefits of VPN Auto Provisioning
- How VPN Auto Provisioning Works

Defining VPN Auto Provisioning

The VPN Auto Provisioning feature simplifies the VPN provisioning of SonicWall firewalls. This is especially useful in large scale VPN deployments. In a classic hub-and-spoke site-to-site VPN configuration, there are many complex configuration tasks needed on the spoke side, such as configuring the Security Association and configuring the Protected Networks. In a large deployment with many remote gateways, or spokes, this can be a challenge. VPN Auto Provisioning provides a simplified configuration process to eliminate many configuration steps on the remote VPN peers.

ⓘ **NOTE:** The ***Hub*** in a hub-and-spoke site-to-site VPN configuration can be referred to using various names, such as Server, Hub Gateway, Primary Gateway, Central Gateway. In the context of the VPN Auto Provisioning feature, the term ***VPN AP Server*** is used for the Hub. Similarly, the term ***VPN AP Client*** is used to refer to a Spoke, Client, Remote Gateway, Remote Firewall, or Peer Firewall.

Benefits of VPN Auto Provisioning

The obvious benefit of the VPN Auto Provisioning feature is ease of use. This is accomplished by hiding the complexity of initial configuration from the SonicOS administrator, similar to the provisioning process of the SonicWall Global VPN Client (GVC).

When using SonicWall GVC, a user merely points the GVC at a gateway; security and connection configuration occur automatically. VPN Auto Provisioning provides a similar solution for provisioning site-to-site hub-and-spoke configurations, simplifying large scale deployment to a trivial effort.

An added advantage is that after the initial VPN auto-provisioning, policy changes can be controlled at the central gateway and automatically updated at the spoke end. This solution is especially appealing in Enterprise and Managed Service deployments where central management is a top priority.

How VPN Auto Provisioning Works

There are two steps involved in VPN Auto Provisioning:

- SonicWall Auto Provisioning Server configuration for the central gateway, or VPN AP Server
- SonicWall Auto Provisioning Client configuration for the remote firewall, or VPN AP Client

Both are configured by adding a VPN policy on the **VPN > Base Settings** page in SonicOS.

In Server mode, you configure the Security Association (SA), Protected Networks, and other configuration fields as in a classic site-to-site VPN policy. In Client mode, limited configuration is needed. In most cases the remote firewall administrator simply needs to configure the IP address to connect to the peer server (central gateway), and then the VPN can be established.

ⓘ **NOTE:** SonicWall does not recommend configuring a single appliance as both an AP Server and an AP Client at the same time.

VPN Auto Provisioning is simple on the client side while still providing the essential elements of IP security:

Access control	Network access control is provided by the VPN AP Server. From the VPN AP Client perspective, destination networks are entirely under the control of the VPN AP Server administrator. However, a mechanism is provided to control access to VPN AP Client local networks.
Authentication	Authentication is provided with machine authentication credentials. In Phase 1 of the IPsec proposal, the Internet Key Exchange (IKE) protocol provides machine-level authentication with *preshared keys* or *digital signatures*. You can select one of these authentication methods when configuring the VPN policy. For the preshared key authentication method, the administrator enters the VPN Auto Provisioning client ID and the key, or secret. For the digital signatures authentication method, the administrator selects the X.509 certificate which contains the client ID from the firewall’s local certificate store. The certificate must have been previously stored on the firewall.

To increase security, user level credentials through XAUTH are supported. The user credentials are entered when adding the VPN policy. XAUTH extracts them as authorization records by using a key or magic cookie, rather than using a challenge/response mechanism in which a user dynamically enters a username and password. Besides providing additional authentication, the user credentials provide further access control to remote resources and/or a local proxy address used by the VPN AP Client. User credentials allow sharing of a single VPN AP Server policy among multiple VPN AP Client devices by differentiating the subsequent network provisioning.

Data confidentiality and integrity Data confidentiality and integrity are provided by Encapsulated Security Payload (ESP) crypto suite in Phase 2 of the IPsec proposal.

When policy changes occur at the VPN AP Server that affect a VPN AP Client configuration, the VPN AP Server uses IKE re-key mechanisms to ensure that a new Security Association with the appropriate parameters is established.

About Establishing the IKE Phase 1 Security Association

Because the goal of the VPN AP Client is ease of use, many IKE and IPsec parameters are defaulted or auto-negotiated. The VPN AP Client initiates Security Association establishment, but does not know the configuration of the VPN AP Server at initiation.

To allow IKE Phase 1 to be established, the set of possible choices is restricted; the VPN AP Client proposes multiple transforms (combined security parameters) from which the VPN AP Server can select its configured values. A Phase 1 transform contains the following parameters:

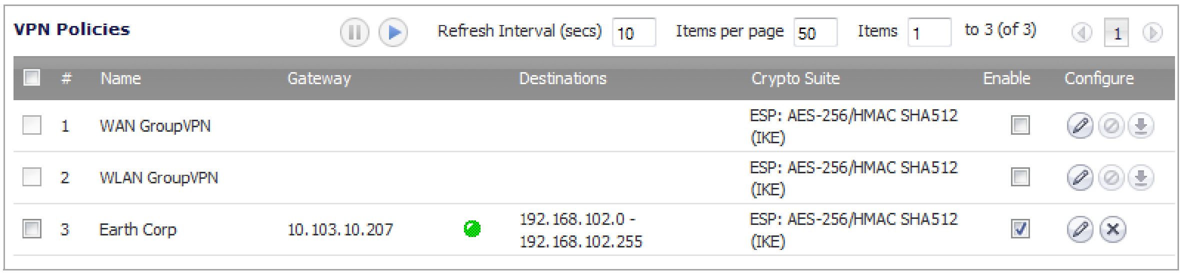
- Authentication – One of the following:
    - PRESHRD – Uses the preshared secret.
    - RSA_SIG – Use an X.509 certificate.
    - SW_DEFAULT_PSK – Uses the Default Provisioning Key.
    - XAUTH_INIT_PRESHARED – Uses the preshared secret combined with XAUTH user credentials.
    - XAUTH_INIT_RSA – Uses an X.509 certificate combined with XAUTH user credentials.
    - SW_XAUTH_DEFAULT_PSK – Uses the Default Provisioning Key combined with XAUTH user credentials.

  All the previously mentioned transforms contain the restricted or default values for the Phase 1 proposal settings:

    - Exchange - Aggressive Mode
    - Encryption – AES-256
    - Hash – SHA1
    - DH Group – Diffie-Hellman Group 5
    - Life Time (seconds) – 28800

The VPN AP Server responds by selecting a single transform from those contained in the VPN AP Client proposal. If the VPN AP Server selects a transform which uses an XAUTH Authentication Method, the VPN AP Client awaits an XAUTH challenge following Phase 1 completion. If a non-XAUTH transform is chosen, the provisioning phase begins. The VPN AP Server provisions the VPN AP Client with the appropriate policy values including the Shared Secret, if one was configured on the VPN AP Server, and the VPN AP Client ID that was configured on the VPN AP Server.

After the Phase 1 SA is established and policy provisioning has completed, the Destination Networks appear in the **VPN Policies** section of the **VPN > Settings** page.



VPN Policies Refresh Interval (secs) 10 Items per page 50 Items 1 to 3 (of 3) 1

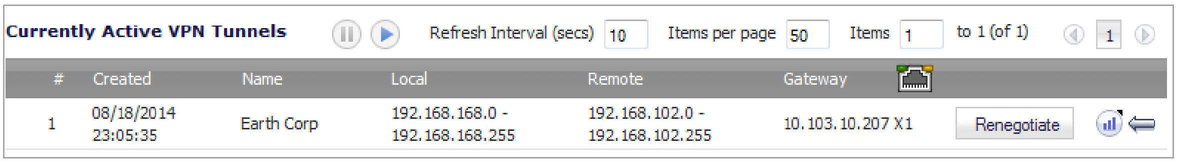
□	#	Name	Gateway		Destinations	Crypto Suite	Enable	Configure
□	1	WAN GroupVPN				ESP: AES-256/HMAC SHA512 (IKE)	□	
□	2	WLAN GroupVPN				ESP: AES-256/HMAC SHA512 (IKE)	□	
□	3	Earth Corp	10.103.10.207	●	192.168.102.0 - 192.168.102.255	ESP: AES-256/HMAC SHA512 (IKE)	☑	

About Establishing IKE Phase 2 using a Provisioned Policy

The values received during the VPN AP provisioning transaction are used to establish any subsequent Phase 2 Security Associations. A separate Phase 2 SA is initiated for each Destination Network. Traffic must be initiated from behind the remote side in order to trigger the Phase 2 SA negotiation. The SA is built based on the address object specified when configuring the VPN AP server policy settings on the **Network** screen (see Configuring VPN AP Server Settings on Network on page 76).

> **NOTE:** If the same VPN policy on the AP Server is shared with multiple remote AP Clients, each remote network must be specifically listed as a unique address object. The individual address objects can be summarized in an Address Group when added to the **Remote Networks** section during configuration of the VPN AP server policy settings on the **Network** screen. A single address object cannot be used to summarize multiple remote networks as the SA is built based on the *specific* address object.

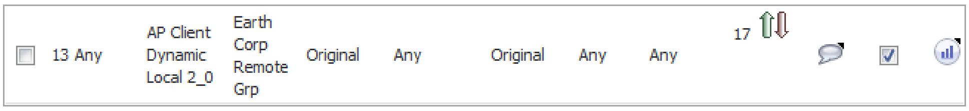
Upon success, the resulting tunnel appears in the **Currently Active VPN Tunnels** list.



Currently Active VPN Tunnels Refresh Interval (secs) 10 Items per page 50 Items 1 to 1 (of 1) 1

#	Created	Name	Local	Remote	Gateway	
1	08/18/2014 23:05:35	Earth Corp	192.168.168.0 - 192.168.168.255	192.168.102.0 - 192.168.102.255	10.103.10.207 X1	Renegotiate

A NAT rule is also added to the **Network > NAT Policies** table.



□	13	Any	AP Client Dynamic Local 2_0	Earth Corp Remote Grp	Original	Any	Original	Any	Any	17	☑

As Phase 2 parameters are provisioned by the VPN AP Server, there is no chance of a configuration mismatch. If Phase 2 parameters change at the VPN AP Server, all Phase 1 and Phase 2 Security Associations are deleted and renegotiated, ensuring policy synchronization.

Configuring a VPN AP Server

VPN AP Server settings are configured on the server (hub) firewall by adding a VPN policy on the **VPN > Settings** page in SonicOS.

Because of the number of settings being described, the configuration is presented in multiple sections:

- Starting the VPN AP Server Configuration
- Configuring VPN AP Server Settings on General

- Configuring VPN AP Server Settings on Network
- Configuring Advanced Settings on Proposals
- Configuring Advanced Settings on Advanced

Starting the VPN AP Server Configuration

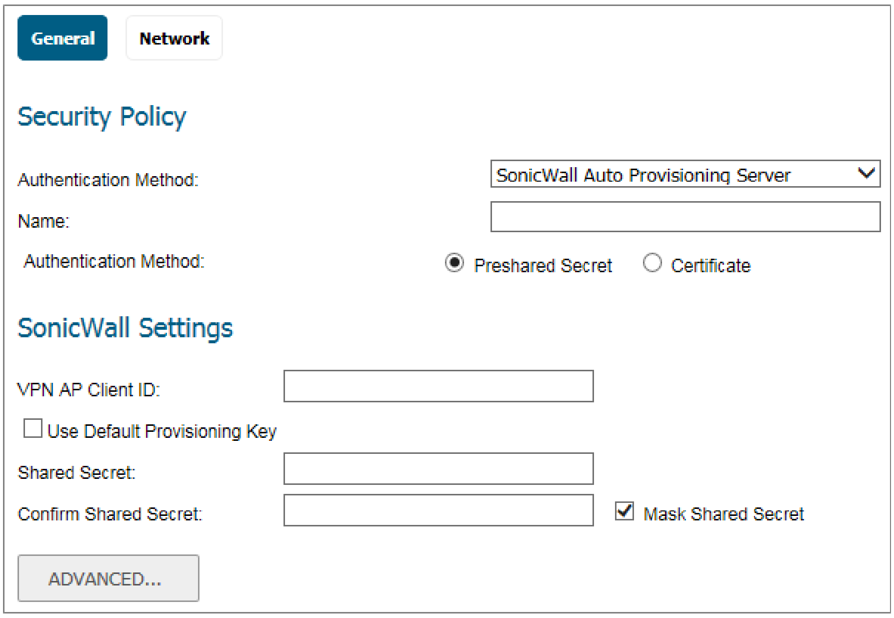
To begin configuration of VPN AP Server firewall settings using VPN Auto Provisioning:

1 Navigate to the **VPN > Settings** page.

2 Select **IPv4** for **View IP Version**.

3 Below the **VPN Policies** table, click **ADD**. The **VPN Policy** dialog displays.

4 In the **Authentication Method** drop-down menu, select **SonicWall Auto Provisioning Server**. The display changes.



Authentication Method: SonicWall Auto Provisioning Server

Name:

Authentication Method: ● Preshared Secret ○ Certificate

VPN AP Client ID:

□ Use Default Provisioning Key

Shared Secret:

Confirm Shared Secret: ☑ Mask Shared Secret

NOTE: The **ADVANCED.../HIDE** button at the bottom of the page toggles between showing or hiding the **Proposals** and **Advanced** options. The settings on these two options contain default values that might be changed at your discretion.

Configuring VPN AP Server Settings on General

To configure VPN AP server settings on the General screen:

1 In the **Name** field, type in a descriptive name for the VPN policy.

2 For **Authentication Method**, select either:

- **Preshared Secret** – Uses the VPN Auto Provisioning client ID and shared secret that you enter next. This option is selected by default. Proceed to Step 3.

- **Certificate** – Uses the X.509 certificate that you select next (the certificate must have been previously stored on the appliance). Skip to Step 9.

  ⓘ **NOTE:** If VPN AP Server policies are to be shared (as in hub-and-spoke deployments), SonicWall recommends using X.509 certificates to provide true authentication and prevent man-in-the-middle attacks.

3 If you selected **Preshared Secret** for the **Authentication Method**, then under **SonicWall Settings**, type the VPN Auto Provisioning client ID into the **VPN AP Client ID** field.This field is automatically populated with the value you entered into the **Name** field, but it can be changed.

ⓘ **NOTE:** This VPN policy value has to match at both the AP Server and AP Client side. A single AP Server policy can also be used to terminate multiple AP Clients.

4 Check the box for **Use Default Provisioning Key** to allow VPN AP Clients to use the default key known to all SonicWall appliances for the *initial* Security Association. After the SA is established, the **Preshared Secret** configured on the VPN AP Server is provisioned to the VPN AP Client for future use.

If this checkbox is cleared, VPN AP Clients must use the configured Shared Secret. This allows the administrator to modify the configured Shared Secret on the VPN AP Server only and then briefly allow Default Provisioning Key use to update the VPN AP Clients with the new Shared Secret value.

ⓘ **NOTE:** For best security, SonicWall recommends that the Default Provisioning Key option is only enabled for a short time during which the VPN AP Client can be provisioned with the Shared Secret while under administrative scrutiny.

5 If you want, clear the **Mask Shared Secret** checkbox before typing anything into the **Shared Secret** field. This checkbox is selected by default, which hides typed characters. If this checkbox is reselected, then the values from the **Shared Secret** field are automatically copied to the **Confirm Shared Secret** field.

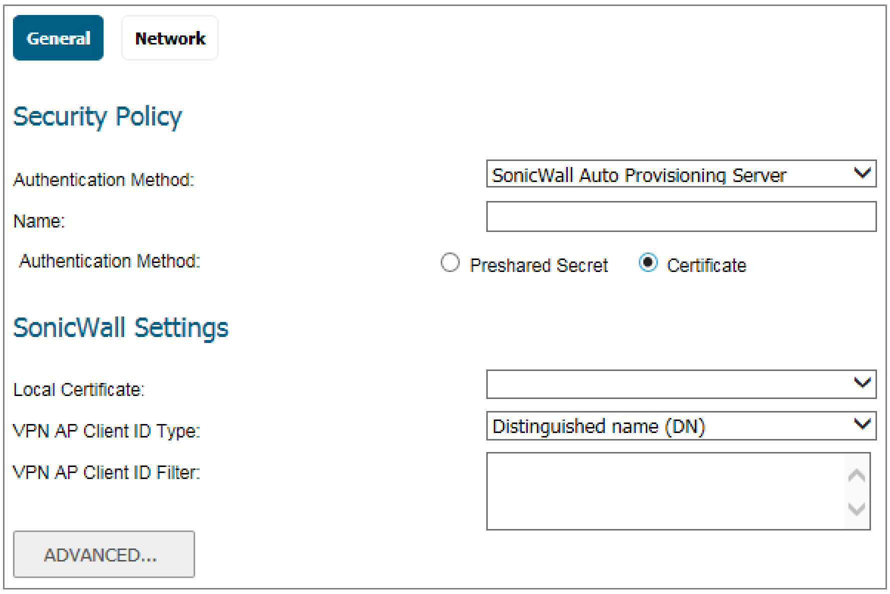
6 In the **Shared Secret** field, type in the shared secret key. A minimum of four characters is required.

If **Use Default Provisioning Key** is checked, the **Preshared Secret** configured on the VPN AP Server is provisioned to the VPN AP Clients. If **Use Default Provisioning Key** is cleared, then this shared secret must also be configured on the VPN AP Clients.

7 In the **Confirm Shared Secret** field, type in the shared secret again. It must match the value entered in the **Shared Secret** field.

8 Go to Step 12.

9 If you selected **Certificate** for the **Authentication Method**, then under **SonicWall Settings** select the desired certificate from the **Local Certificate** drop-down menu.



Security Policy

Authentication Method: SonicWall Auto Provisioning Server

Name:

Authentication Method: ○ Preshared Secret ● Certificate

SonicWall Settings

Local Certificate:

VPN AP Client ID Type: Distinguished name (DN)

VPN AP Client ID Filter:

10 Select one of the following from the **VPN AP Client ID Type** drop-down menu:

- **Distinguished name (DN)**
- **E-Mail ID (UserFQDN)**
- **Domain name (FQDN)**
- **IP Address (IPV4)**

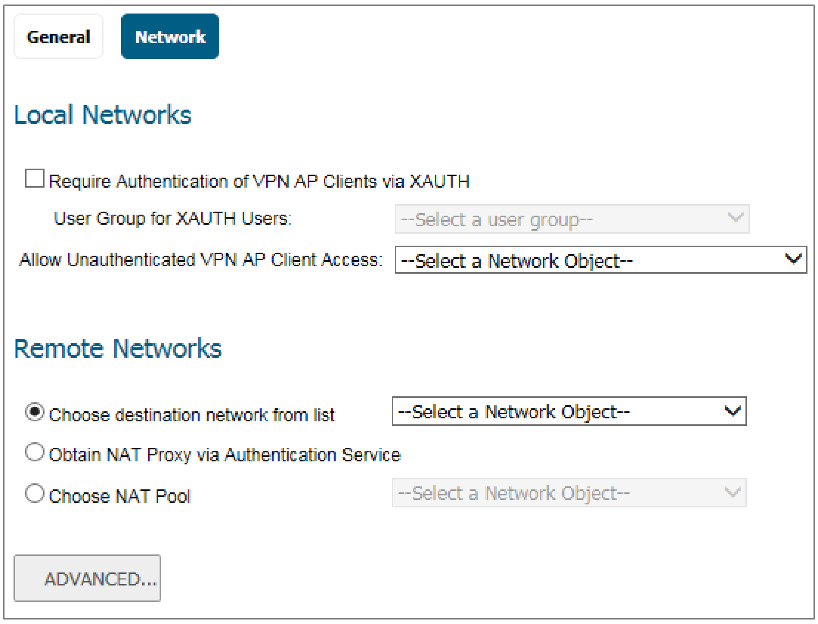
11 In the **VPN AP Client ID Filter**, type in a matching string or filter to be applied to the Certificate ID presented during IKE negotiation.

12 Continue to Configuring VPN AP Server Settings on Network.

Configuring VPN AP Server Settings on Network

To configure VPN AP server settings on the Network screen:

1 Click **Network**.



Local Networks

□ Require Authentication of VPN AP Clients via XAUTH

User Group for XAUTH Users: --Select a user group--

Allow Unauthenticated VPN AP Client Access: --Select a Network Object--

Remote Networks

● Choose destination network from list --Select a Network Object--

○ Obtain NAT Proxy via Authentication Service

○ Choose NAT Pool --Select a Network Object--

2 Under **Local Networks**, select **Require Authentication of VPN AP Clients via XAUTH** to force the use of user credentials for added security when establishing the SA.

3 If the XAUTH option is enabled, select the user group for the allowed users from the **User Group for XAUTH Users** drop-down menu. You can select an existing group such as *Trusted Users* or another standard group, or select **Create a new user group** to create a custom group.

For each authenticated user, the authentication service returns one or more network addresses which are sent to the VPN AP Client during the provisioning exchange.

If XAUTH is enabled and a user group is selected, the user on the VPN AP Client side must meet the following conditions for authentication to succeed:

- The user must belong to the selected user group.
- The user can pass the authentication method configured in **MANAGE | System Setup | Users > Settings > User Authentication Method**.
- The user has VPN access privileges.

4 If the XAUTH option is disabled, select a network address object or group from the **Allow Unauthenticated VPN AP Client Access** drop-down menu, or select **Create a new address object/group** to create a custom object or group. The selected object defines the list of addresses and domains that can be accessed through this VPN connection. It is sent to the VPN AP Client during the provisioning exchange and then used as the VPN AP Client's remote proxy ID.

5 Under **Remote Networks**, select one of the following radio buttons and choose from the associated list, if applicable:

- **Choose destination network from list** – Select a network object from the drop-down menu of remote address objects that are actual routable networks at the VPN AP Client side, or create a custom object.

  ⓘ **NOTE:** VPN Auto Provisioning does not support using a "super network" that includes all the AP Clients' protected subnets. To allow multiple AP Clients with different protected subnets to connect to the same AP Server, configure an Address Group that includes all of the AP Clients' protected subnets and use that in the **Choose destination network from list** field. This Address Group must be kept up to date as new AP Clients are added.

- **Obtain NAT Proxy via Authentication Service** – Select this option to have the RADIUS server return a Framed-IP Address attribute for the user, which is used by the VPN AP Client to NAT its internal addresses before sending traffic down the IPsec tunnel.
- **Choose NAT Pool** – Select a network object from the drop-down menu, or create a custom object. The chosen object specifies a pool of addresses to be assigned to the VPN AP Client for use with NAT. The client translates its internal address to an address in the NAT pool before sending traffic down the IPsec tunnel.

  ⓘ **NOTE:** When deploying VPN Auto Provisioning, you should allocate a large enough NAT IP address pool for all the existing and expected VPN AP Clients. Otherwise, additional VPN AP Clients cannot work properly if all the IP addresses in the pool have already been allocated.

  NOTE: Configuring a large IP pool does not consume more memory than a small pool, so it is safe and a best practice to allocate a large enough pool to provide redundancy.

6 Continue to Configuring Advanced Settings on Proposals.

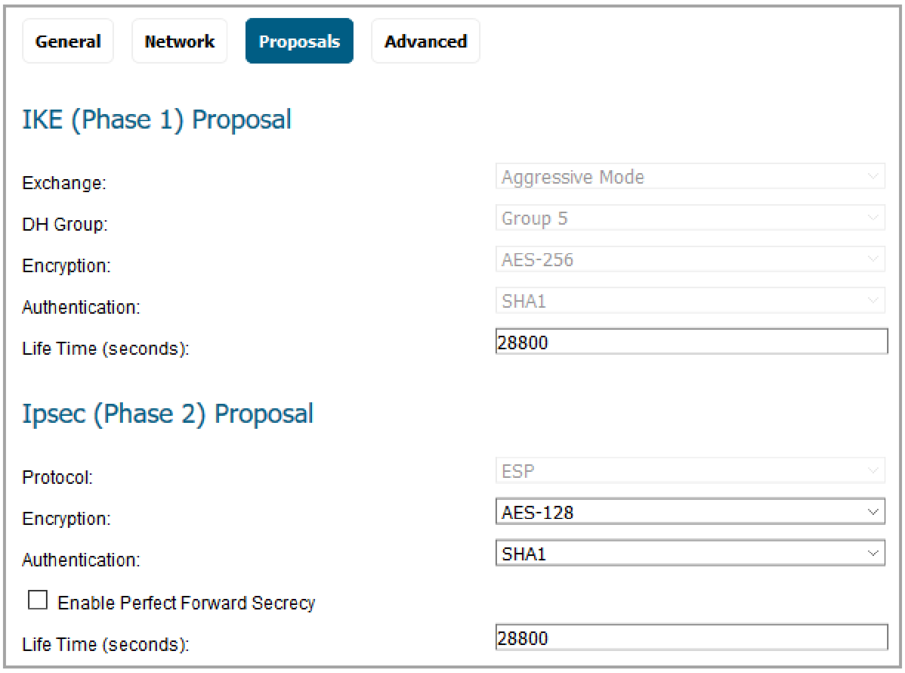
Configuring Advanced Settings on Proposals

The configured parameters are automatically provisioned to the VPN AP Client prior to Phase 2 establishment, so there is no chance of configuration discrepancies between the VPN AP Server and VPN AP Client.

To configure VPN AP Server settings on the Proposals screen:

1 On the **General** or **Network** screen, click **Advanced** to display **Proposals**.

2 Click **Proposals**.



IKE (Phase 1) Proposal

Exchange: Aggressive Mode

DH Group: Group 5

Encryption: AES-256

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: AES-128

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

3 Under **IKE (Phase 1) Proposal**, enter the phase 1 proposal lifetime in seconds. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

To simplify auto-provisioning, the other fields in this section are dimmed and preset to:

- **Exchange: Aggressive Mode**
- **DH Group: Group 5**
- **Encryption: AES-256**
- **Authentication: SHA1**

4 Under **Ipsec (Phase 2) Proposal**, select the desired encryption algorithm from the **Encryption** drop-down menu. The default is **AES-128**.

The **Protocol** field is dimmed and preset to **ESP** to use the Encapsulated Security Payload (ESP) crypto suite.

5 Select the desired authentication encryption method from the **Authentication** drop-down menu. The default is **SHA1**.

6 Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. If selected, the **DH Group** drop-down menu is displayed. Select the desired group from the list. The default is Group 2.

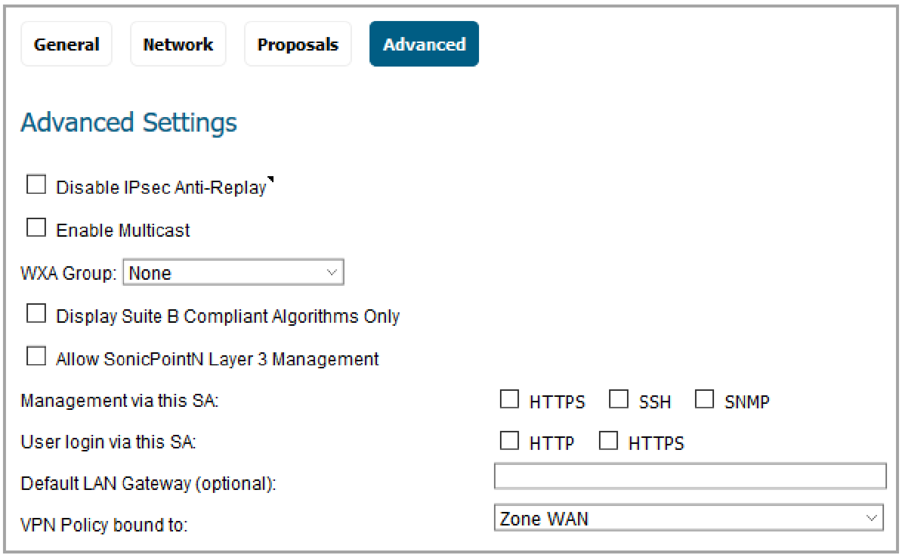
7 Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every eight hours.

8 Continue to Configuring Advanced Settings on Advanced.

Configuring Advanced Settings on Advanced

To configure VPN AP Server settings on the Advanced screen:

1 Click **Advanced**.



Advanced Settings

□ Disable IPsec Anti-Replay

□ Enable Multicast

WXA Group: None

□ Display Suite B Compliant Algorithms Only

□ Allow SonicPointN Layer 3 Management

Management via this SA: □ HTTPS □ SSH □ SNMP

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Zone WAN

2 Select **Disable IPsec Anti-Replay** to prevent packets with duplicate sequence numbers from being dropped.

3 Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass from the VPN AP Server over any VPN AP Client SA established using this policy.

4 If you are using SonicWall WAN Acceleration, select a value from the **WXA Group** drop-down menu.

5 Optionally select **Display Suite B Compliant Algorithms Only**.

6 Select **Allow SonicPointN Layer 3 Management** to allow management of SonicWall SonicPoint wireless access devices through the VPN tunnel.

7 For **Management via this SA**, select one or more of the checkboxes to allow remote users to manage the VPN AP Server through the VPN tunnel using **HTTPS**, **SSH**, or **SNMP**.

8 For **User login via this SA**, select one or more of the checkboxes to allow remote users to log in through the VPN tunnel using **HTTP** or **HTTPS**.

9 In the **Default LAN Gateway (optional)** field, optionally enter the default LAN gateway IP address of the VPN AP Server. If a static route cannot be found for certain traffic, the VPN AP Server forwards the traffic out the configured default LAN gateway.

ⓘ | **NOTE:** This option might not work in some versions of SonicOS.

10 Select an interface or zone in the **VPN Policy bound to** drop-down menu to bind this VPN policy to a specific interface or zone. **Zone WAN** is the default.

11 When finished, click **OK**.

Configuring a VPN AP Client

VPN AP Client settings are configured on the client firewall by adding a VPN policy on the **VPN > Settings** page in SonicOS.

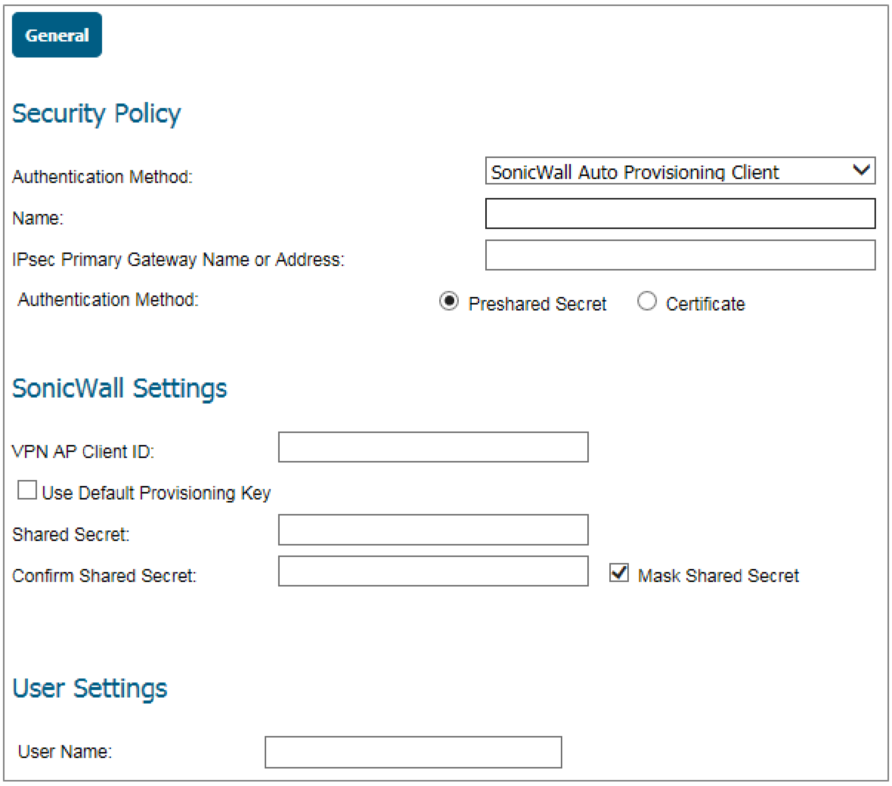
To configure remote client firewall settings using VPN Auto Provisioning:

1 Navigate to the **VPN > Settings** page.

2 Select **IPv4** for **View IP Version**.

3 Below the **VPN Policies** table, click **Add**. The **VPN Policy** dialog displays.

4 In the **Authentication Method** drop-down menu, select **SonicWall Auto Provisioning Client**. The page refreshes with different fields.



General

Security Policy

Authentication Method: SonicWall Auto Provisioning Client

Name:

IPsec Primary Gateway Name or Address:

Authentication Method: ● Preshared Secret ○ Certificate

SonicWall Settings

VPN AP Client ID:

□ Use Default Provisioning Key

Shared Secret:

Confirm Shared Secret: ☑ Mask Shared Secret

User Settings

User Name:

5 In the **Name** field, type in a descriptive name for the VPN policy.

6 In the **IPsec Primary Gateway Name or Address** field, enter the Fully Qualified Domain Name (FQDN) or the IPv4 address of the VPN AP Server.

7 For **Authentication Method**, select either:

- **Preshared Secret** – Uses the VPN Auto Provisioning client ID and shared secret that you enter next. This option is selected by default. Proceed to Step 8.
- **Certificate** – Uses the X.509 certificate that you select next (the certificate must have been previously stored on the appliance). Skip to Step 14.

8 If you selected **Preshared Secret** for the **Authentication Method**, then under **SonicWall Settings**, type the VPN Auto Provisioning client ID into the **VPN AP Client ID** field.

The client ID is determined by the configuration of the VPN AP Server (the SonicWall firewall configured as the **SonicWall Auto Provisioning Server**).

> ⓘ **NOTE:** This VPN policy value has to match at both the AP Server and AP Client side. A single AP Server policy can also be used to terminate multiple AP Clients.

9 Optionally, select **Use Default Provisioning Key** to use the default key known to all SonicWall appliances for the *initial* Security Association. After the SA is established, the **Preshared Secret** configured on the VPN AP Server is provisioned to the VPN AP Client for future use.

> ⓘ **NOTE:** The VPN AP Server must be configured to accept the Default Provisioning Key. If it is not, SA establishment fails.

If you selected **Use Default Provisioning Key**, skip to Step 13.

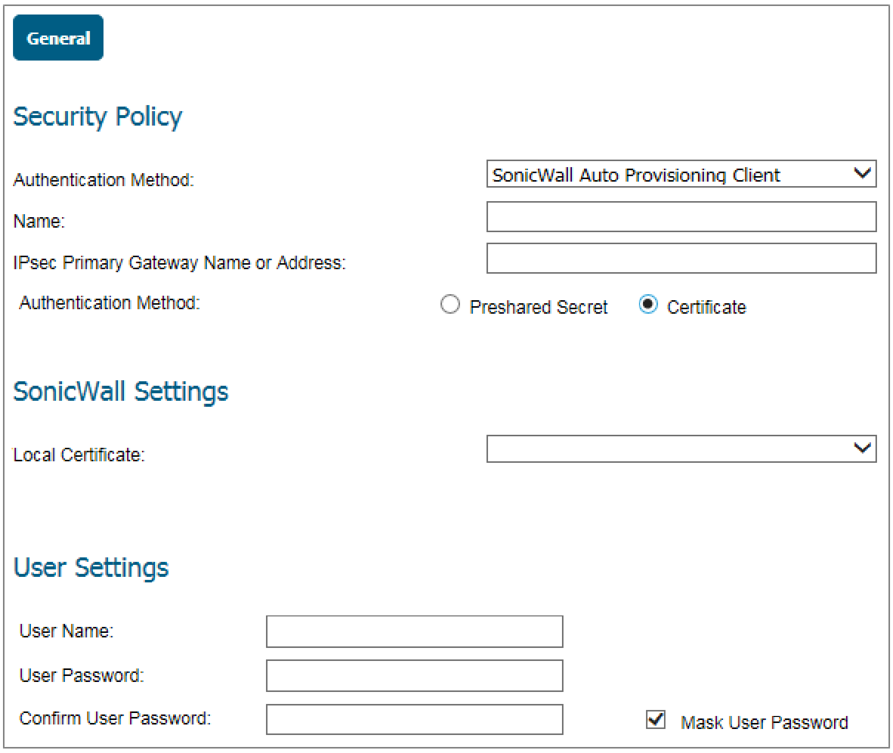
10 If you did not select **Use Default Provisioning Key**, then optionally clear the **Mask Shared Secret** checkbox before typing anything into the **Shared Secret** field. This checkbox is selected by default, which hides typed characters. If this checkbox is reselected, then the values from the **Shared Secret** field are automatically copied to the **Confirm Shared Secret** field.

11 In the **Shared Secret** field, type in the shared secret. This must be the same as the shared secret configured on the VPN AP Server, and must be a minimum of four characters.

12 In the **Confirm Shared Secret** field, type in the shared secret again. It must match the value entered in the **Shared Secret** field.

13 Skip to Step 15 for information about entering the user credentials under **User Settings**. User credentials are optional.

14 If you selected **Certificate** for the **Authentication Method**, then under **SonicWall Settings** select the desired certificate from the **Local Certificate** drop-down menu.



General

Security Policy

Authentication Method: SonicWall Auto Provisioning Client

Name:

IPsec Primary Gateway Name or Address:

Authentication Method: ○ Preshared Secret ● Certificate

SonicWall Settings

Local Certificate:

User Settings

User Name:

User Password:

Confirm User Password: ☑ Mask User Password

15 Under **User Settings**, type the user name to be used for the optional user credentials into the **User Name** field. This user name is sent through XAUTH for user-level authentication.

16 Optionally clear the **Mask User Password** checkbox before typing anything into the **User Password** field. This checkbox is selected by default. If selected, the typed characters are represented as dots. Clearing this checkbox displays the values in plain text and automatically copies the value entered in the **User Password** field to the **Confirm User Password** field.

17 In the **User Password** field, type in the user password.

18 In the **Confirm User Password** field, type in the user password again.

19 When ready, click **OK** to add the VPN policy.

4

Tunnel Interface Route-based VPN

This section describes how to configure Tunnel Interface VPN policies, which provide a route-based VPN solution. Tunnel Interface VPN policies differ from site to site VPN policies, which force the VPN policy configuration to include the network topology configuration. This makes it difficult to configure and maintain the VPN policy with a constantly changing network topology. Refer to Site to Site VPNs on page 24 for details.

With the route-based VPN approach, network topology configuration is removed from the VPN policy configuration. The VPN policy configuration creates an ***unnumbered Tunnel Interface*** between two end points. Static or dynamic routes can then be added to the Tunnel Interface. The route-based VPN approach moves network configuration from the VPN policy configuration to static or dynamic route configuration.

Route-based VPN makes configuring and maintaining the VPN policy easier, and provides flexibility on how traffic is routed. You can define multiple paths for overlapping networks over a clear or redundant VPN.

For auto provisioning of VPN networks, refer to VPN Auto Provisioning for details.

Topics:

- Terminology
- Adding a Tunnel Interface
- Route Entries for Different Network Segments
- Redundant Static Routes for a Network

Terminology

The following terms are used throughout this section:

VPN Tunnel Policy	A policy configured without a local/remote protected network. When sending a packet out, SonicOS does not need to look up any tunnel policy.
VPN Tunnel Interface	A numbered tunnel interface created on the **Network > Interfaces** page and bound to a tunnel policy. The interface is configured as the egress interface of a route entry or a SonicOS feature that actively sends out packets such as Net Monitor Policy or Syslog policy. When SonicOS sends a packet out over the VPN Tunnel, logically it is the same as sending the packet over a physical interface, except the packet is encrypted.

Numbered Tunnel Interface	A numbered tunnel interface has an IP address. A numbered tunnel interface is created on the **Network > Interfaces** page by adding a VPN Tunnel Interface. Functionally, the numbered tunnel interface is a superset of the unnumbered tunnel interface. You can configure a numbered tunnel interface in the same way as a standard interface, including settings for HTTPS, Ping, SNMP, and SSH management, HTTP and HTTPS user login, and fragmentation handling. You can use a numbered tunnel interface when configuring NAT policies, firewall access control lists, and routing policies including all types of dynamic routing (RIP, OSPF, BGP).
Unnumbered Tunnel Interface	An unnumbered tunnel interface has no IP address. An unnumbered tunnel interface is created when you configure a VPN policy with a **Policy Type** of **Tunnel Interface**. By default, it is used for simple, route-based VPN and does not require an IP address. If the **Allow Advanced Routing** option is enabled in the Advanced screen of the policy configuration dialog, an unnumbered tunnel interface can be used with RIP and OSPF dynamic routing. When configuring RIP or OSPF using an unnumbered tunnel interface, an IP address is borrowed for it from either a physical or logical (VLAN) interface.

Adding a Tunnel Interface

Route-based VPN configuration is a two-step process:

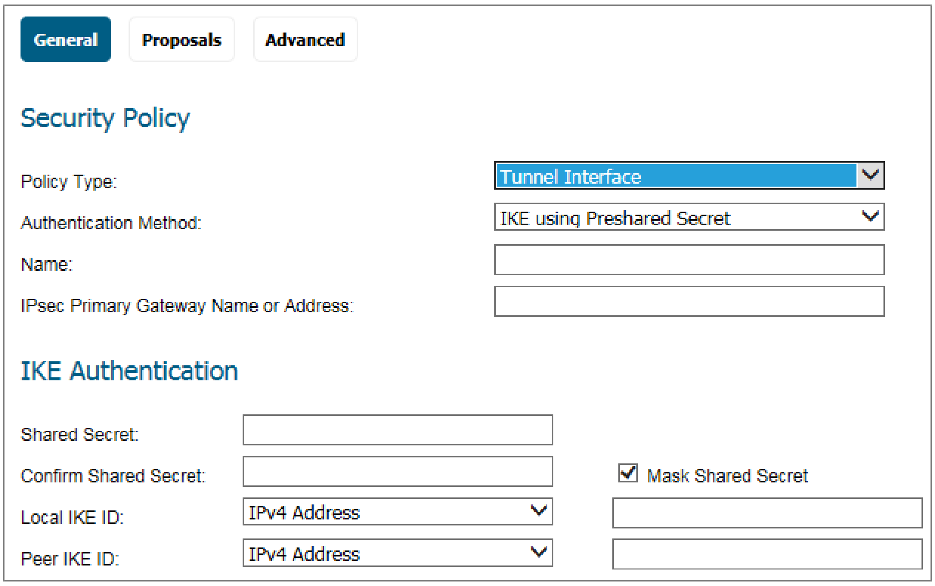
1. Create a Tunnel Interface. The cryptography suites used to secure the traffic between two end-points are defined in the Tunnel Interface.
2. Create a static or dynamic route using Tunnel Interface.

The Tunnel Interface is created when a Policy of type **Tunnel Interface** is added for the remote gateway. The Tunnel Interface must be bound to a physical interface and the IP address of that physical interface is used as the source address of the tunneled packet.

To add a Tunnel Interface:

1. Navigate to **MANAGE | Connectivity | VPN > Base Settings**.
2. Select **IPv4** or **IPv6** for the **View IP Version** option.

3 Click **ADD**.



Security Policy

Policy Type:	Tunnel Interface
Authentication Method:	IKE using Preshared Secret
Name:	
IPsec Primary Gateway Name or Address:	

IKE Authentication

Shared Secret:		
Confirm Shared Secret:		☑ Mask Shared Secret
Local IKE ID:	IPv4 Address	
Peer IKE ID:	IPv4 Address	

4 On the **General** screen, select **Tunnel Interface** as the **Policy Type**.

5 Select one the following for **Authentication Method**:

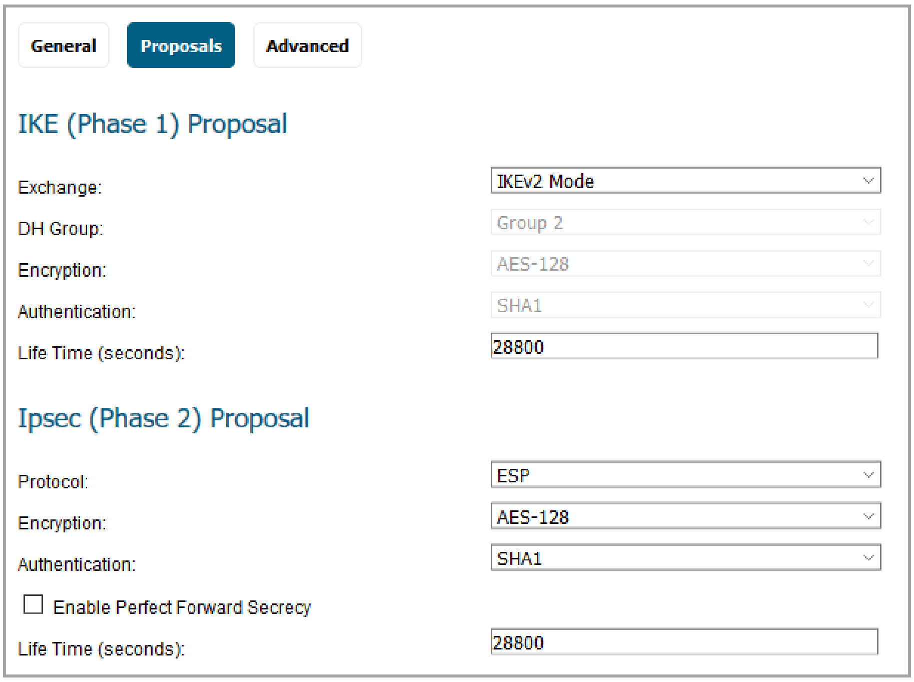
- **Manual Key**
- **IKE using Preshared Secret** (default)
- **IKE using 3rd Party Certificates**
- **SonicWall Auto Provisioning Client**
- **SonicWall Auto Provisioning Server**

The remaining fields in the **General** screen change depending on which option you select.

For more information about the available selections, see:

- Configuring with a Manual Key on page 52
- Configuring with a Preshared Secret Key on page 43
- Configuring with a Third-Party Certificate on page 56
- Configuring a VPN AP Client on page 80
- Configuring a VPN AP Server on page 72

6 Click **Proposals**.



IKE (Phase 1) Proposal

Exchange: IKEv2 Mode

DH Group: Group 2

Encryption: AES-128

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: AES-128

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

7 Under **IKE (Phase 1) Proposal**, choose one of the following options from the **Exchange** drop-down menu:

Main Mode	Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
Aggressive Mode	Generally used when WAN addressing is dynamically assigned. Uses IKEv1 Phase 1 proposals with IPsec Phase 2 proposals. Suite B cryptography options are available for the DH Group in IKE Phase 1 settings, and for Encryption in the IPsec Phase 2 settings.
IKEv2 Mode	Causes all negotiation to happen through IKEv2 protocols, rather than using IKEv1 phases. **NOTE:** If you select **IKE v2 Mode**, both ends of the VPN tunnel must use IKE v2. When selected, the **DH Group**, **Encryption**, and **Authentication** fields are disabled and cannot be defined.

8 Under **IKE (Phase 1) Proposal**, set the values for the remaining options. The default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations.

NOTE: Be sure the Phase 1 values on the opposite side of the tunnel are configured to match.

a For the **DH Group**, when in **Main Mode** or **Aggressive Mode**, you can select from several Diffie-Hellman exchanges:

Diffie-Hellman Groups Included in Suite B Cryptography	Other Diffie-Hellman Options
256-bit Random ECP Group	Group 1
384-bit Random ECP Group	Group 2
521-bit Random ECP Group	Group 5

192-bit Random ECP Group	Group 14
224-bit Random ECP Group	

b For the **Encryption** field, if **Main Mode** or **Aggressive Mode** was selected, choose **DES**, **3DES**, **AES-128** (default), **AES-192**, or **AES-256** from the drop-down menu.

c For the **Authentication** field, if **Main Mode** or **Aggressive Mode** was selected, choose **SHA-1** (default), **MD5**, **SHA256**, **SHA384**, or **SHA512** for enhanced authentication security.

d For all **Exchange** modes, enter a value for **Life Time (seconds)**. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every eight hours.

9 Set the options in the **IPsec (Phase 2) Proposal** section. The default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, and **Life Time (seconds)** are acceptable for most VPN SA configurations.

NOTE: Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

a In the **Protocol** field, select **ESP** or **AH**.

b In the **Encryption** field, if you selected **ESP** in the **Protocol** field, you can select from six encryption algorithms that are included in Suite B cryptography:

Suite B Cryptography Options	Other Options
AESGCM16-128	**DES**
AESGCM16-192	**3DES**
AESGCM16-256	**AES-128**
AESGMAC-128	**AES-192**
AESGMAC-192	**AES-256**
AESGMAC-256	**None**

NOTE: If you selected **AH** in the **Protocol** field, the **Encryption** field is disabled, and you cannot select any options.

c In the **Authentication** field, select the authentication method from the drop-down menu:

- **MD5**
- **SHA1** (default)
- **SHA256**
- **SHA384**
- **SHA512**
- **AES-XCBC**

d Select **Enable Perfect Forward Secrecy** if you want added security.

e Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

10 Click **Advanced**.

11 The following advanced options can be configured; by default, none are selected:

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Advanced Settings		
Enable Keep Alive	Cannot be selected for a route-based interface.	Cannot be selected for a route-based interface.
Disable IPsec Anti-Replay	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window)	Anti-replay is a form of partial sequence integrity and it detects arrival of duplicate IP datagrams (within a constrained window)
Allow Advanced Routing	Adds this Tunnel Interface to the list of interfaces in the **Routing Protocols** table on the **Network > Routing** page.	Adds this Tunnel Interface to the list of interfaces in the **Routing Protocols** table on the **Network > Routing** page.
	NOTE: This option must be selected if the Tunnel Interface is to be used for advanced routing (RIP, OSPF). Making this an optional setting avoids adding all Tunnel Interfaces to the **Routing Protocols** table, which helps streamline the routing configuration.	
Enable Transport Mode	This option is used to protect packets that are already encapsulated by another tunneling protocol such as Generic Routing Encapsulation (GRE). It encrypts only the payload and ESP trailer, so the IP header of the original packet is not encrypted.	Not available for **IKEv2 Mode**.
Enable Windows Networking (NetBIOS) Broadcast	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.	Select to allow access to remote network resources by browsing the Windows Network Neighborhood.
Enable Multicast	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.	Select to allow multicasting traffic, such as streaming audio (including VoIP) and video application, to pass through the VPN tunnel.
WXA Group	Select None (default) or Group One	Select None (default) or Group One
Display Suite B Compliant Algorithms Only	Select if you want to show only the Suite B compliant algorithms.	Select if you want to show only the Suite B compliant algorithms.

Options	Main Mode or Aggressive Mode	IKEv2 Mode
Apply NAT Policies	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.	Select if you want the firewall to translate traffic going over the Local network, Remote network, or both networks that are communicating through the VPN tunnel. When selected, choose a **Translated Local Network** or a **Translated Remote Network** or one of each from the two drop-down menus. **NOTE:** Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
Allow SonicPointN Layer 3 Management	Allows Layer-3 management for SonicPointN and SonicWave.	Allows Layer-3 management for SonicPointN and SonicWave.
Management via this SA	Select any of **HTTPS**, **SSH**, or **SNMP** for this option to manage the local SonicWall firewall through the VPN tunnel.	Select any of **HTTPS**, **SSH**, or **SNMP** for this option to manage the local SonicWall firewall through the VPN tunnel.
User login via this SA	Select **HTTP**, **HTTPS**, or both to allow users to login using the SA. **NOTE:** HTTP user login is not allowed with remote authentication.	Select **HTTP**, **HTTPS**, or both to allow users to login using the SA. **NOTE:** HTTP user login is not allowed with remote authentication.
VPN Policy bound to	Select an interface from the drop-down menu. **Important:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.	Select an interface from the drop-down menu. **Important:** Two different WAN interfaces cannot be selected from the drop-down menu if the VPN Gateway IP address is the same for both.

Options	Main Mode or Aggressive Mode	IKEv2 Mode
IKEv2 Settings		
Do not send trigger packet during IKE SA negotiation	Not available	Is *not* selected (default). It should only be selected when required for interoperability if the peer cannot handle trigger packets. The recommended practice is to include trigger packets to help the IKEv2 Responder select the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it might be appropriate to disable the inclusion of trigger packets to some IKE peers.
Accept Hash & URL Certificate Type	Not available	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, sends a message to the peer device saying that HTTP certification look-up is supported.
Send Hash & URL Certificate Type	Not available	Select if your devices can send and process hash and certificate URLs instead of the certificate itself. If selected, responds to the message from the peer device and confirms HTTP certification look-up is supported.

12 Click **OK**.

13 Click **Accept** on the **VPN > Base Settings** page to update the VPN Policies.

Creating a Static Route for the Tunnel Interface

After you have successfully added a Tunnel Interface, you can then create a Static Route to go with it.

To create a Static Route for a Tunnel Interface:

1 Navigate to **MANAGE | System Setup | Network > Routing > Route Policies**.

2 Click **Add** to display the **Add Route Policy** dialog.

3 Select the Tunnel Interface from the **Interface** drop-down menu that lists all available tunnel interfaces.

> **NOTE:** If the **Auto-add Access Rule** option is selected, firewall rules are automatically added and traffic is allowed between the configured networks using the tunnel interface.

4 Configure the rest of the settings as necessary. Refer to the Network Routing section of *SonicOS 6.5 System Setup* for detailed information.

5 Click **OK**.

Route Entries for Different Network Segments

After a tunnel interface is created, multiple route entries can be configured to use the same tunnel interface for different networks. This provides a mechanism to modify the network topology without making any changes to the tunnel interface.

Redundant Static Routes for a Network

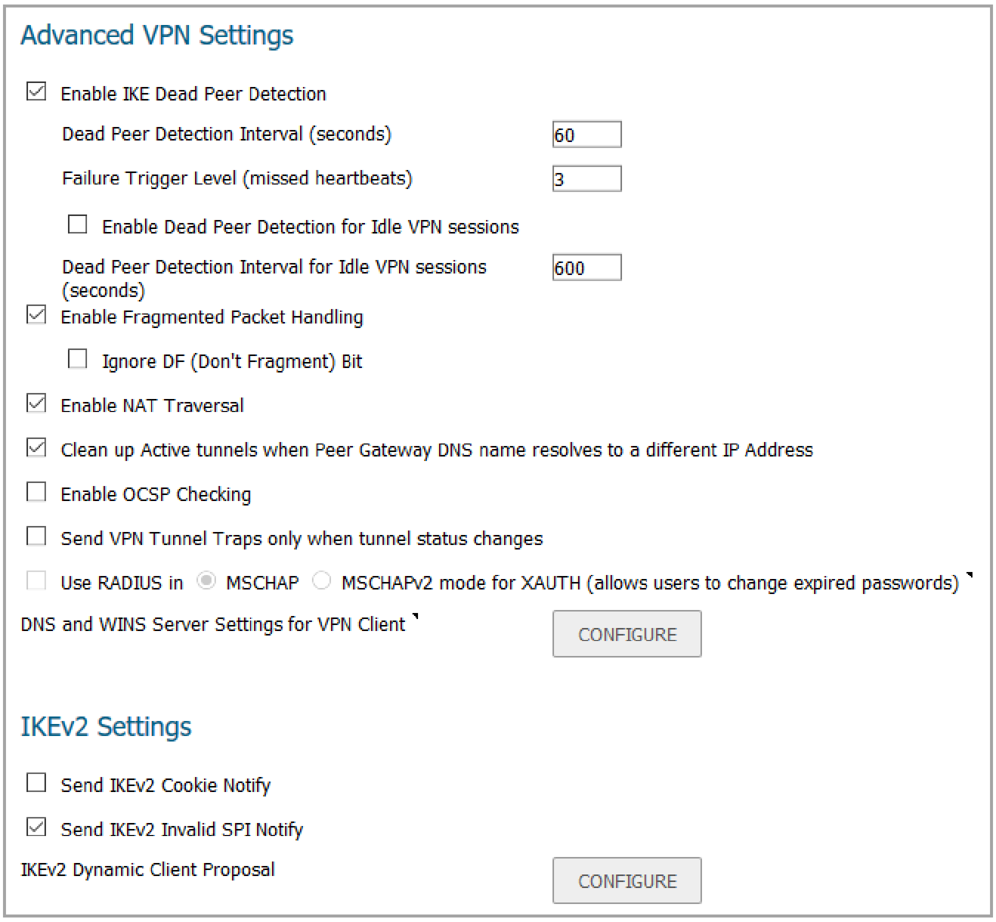
After more than one tunnel interface is configured, you can add multiple overlapping static routes; each static route uses a different tunnel interface to route the traffic. This provides routing redundancy for the traffic to reach the destination. If no redundant routes are available, you can add a static route to a drop tunnel interface to prevent VPN traffic from being sent out the default route. For more information, refer to the Network Interfaces section of *SonicOS 6.5 System Setup*.

5

Configuring Advanced VPN Settings

The **VPN > Advanced** page has two sections:

- **Advanced VPN Settings**
- **IKEv2 Settings**



Advanced VPN Settings

☑ Enable IKE Dead Peer Detection

Dead Peer Detection Interval (seconds) 60

Failure Trigger Level (missed heartbeats) 3

□ Enable Dead Peer Detection for Idle VPN sessions

Dead Peer Detection Interval for Idle VPN sessions (seconds) 600

☑ Enable Fragmented Packet Handling

□ Ignore DF (Don't Fragment) Bit

☑ Enable NAT Traversal

☑ Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address

□ Enable OCSP Checking

□ Send VPN Tunnel Traps only when tunnel status changes

□ Use RADIUS in ● MSCHAP ○ MSCHAPv2 mode for XAUTH (allows users to change expired passwords)

DNS and WINS Server Settings for VPN Client

IKEv2 Settings

□ Send IKEv2 Cookie Notify

☑ Send IKEv2 Invalid SPI Notify

IKEv2 Dynamic Client Proposal

Topics:

- Configuring Advanced VPN Settings
- Configuring IKEv2 Settings

Configuring Advanced VPN Settings

Advanced VPN Settings globally affect all VPN policies. This section also provides solutions for Online Certificate Status Protocol (OCSP). OCSP allows you to check VPN certificate status without Certificate Revocation Lists (CRLs). This allows timely updates regarding the status of the certificates used on your firewall.

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the firewall.
    - **Dead Peer Detection Interval** - Enter the number of seconds between “heartbeats.” The default value is 60 seconds.
    - **Failure Trigger Level (missed heartbeats)** - Enter the number of missed heartbeats. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the firewall. The firewall uses a UDP packet protected by Phase 1 Encryption as the heartbeat.
    - **Enable Dead Peer Detection for Idle VPN Sessions** - Select this setting if you want idle VPN connections to be dropped by the firewall after the time value defined in the **Dead Peer Detection Interval for Idle VPN Sessions (seconds)** field. The default value is 600 seconds (10 minutes).
- **Enable Fragmented Packet Handling** - If the VPN log report shows the log message `Fragmented IPsec packet dropped`, select this feature. Do not select it until the VPN tunnel is established and in operation.
    - **Ignore DF (Don't Fragment) Bit** - Select this checkbox to ignore the DF bit in the packet header. Some applications can explicitly set the ‘Don’t Fragment’ option in a packet, which tells all security appliances to not fragment the packet. This option, when enabled, causes the firewall to ignore the option and fragment the packet regardless.
- **Enable NAT Traversal** - Select this setting if a NAT device is located between your VPN endpoints. IPsec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPsec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPsec peer.
- **Clean up Active Tunnels when Peer Gateway DNS name resolves to a different IP address** - Breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
- **Enable OCSP Checking and OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See Using OCSP with SonicWall Network Security Appliances.
- **Send VPN Tunnel Traps only when tunnel status changes** - Reduces the number of VPN tunnel traps that are sent by only sending traps when the tunnel status changes.
- **Use RADIUS in** - The primary reason for choosing this option is so that VPN client users can make use of the MSCHAP feature to allow them to change expired passwords at login time. When using RADUIS to authenticate VPN client users, select whether RADIUS is used in one of these modes:
    - **MSCHAP**
    - **MSCHAPv2** mode for XAUTH (allows users to change expired passwords)

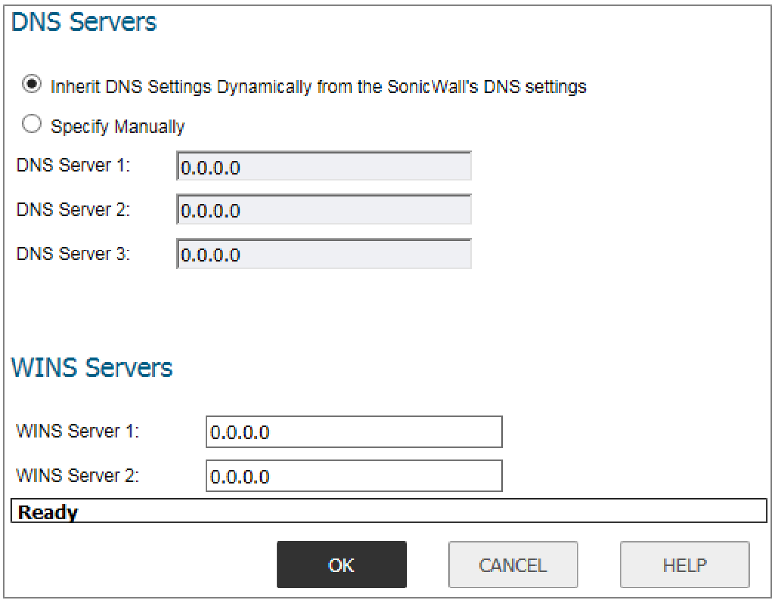
    Also, if this is set and LDAP is selected as the **Authentication method for login** on the **Users > Settings** page, but LDAP is not configured in a way that allows password updates, then password updates for VPN client users are done using MSCHAP-mode RADIUS after using LDAP to authenticate the user.

    NOTE: Password updates can only be done by LDAP when using either:

    - Active Directory with TLS and binding to it using an administrative account
    - Novell eDirectory.

- **DNS and WINS Server Settings for VPN Client** – To configure DNS and WINS server settings for Client, such as a third-party VPN Client through GroupVPN, or a Mobile IKEv2 Client, click **Configure**. The **Add VPN DNS And WINS Server** dialog displays.

  ⓘ | **NOTE:** This option appears only for TZ appliances.



DNS Servers

● Inherit DNS Settings Dynamically from the SonicWall's DNS settings

○ Specify Manually

DNS Server 1:	0.0.0.0
DNS Server 2:	0.0.0.0
DNS Server 3:	0.0.0.0

WINS Servers

WINS Server 1:	0.0.0.0
WINS Server 2:	0.0.0.0

Ready

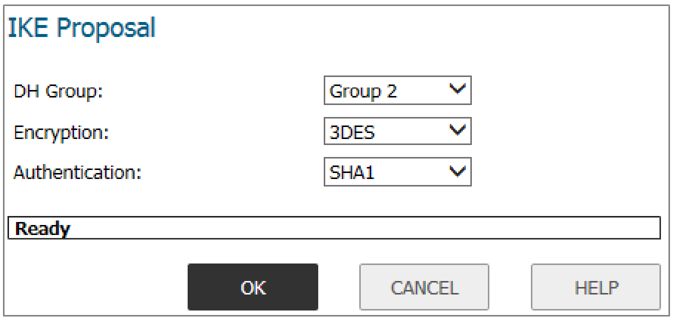
  - **DNS Servers** – Select whether to specify the DNS servers dynamically or manually:
    - **Inherit DNS Settings Dynamically from the SonicWall’s DNS settings** – The SonicWall appliance obtains the DNS server IP addresses automatically.
    - **Specify Manually** – Enter up to three DNS server IP addresses in the **DNS Server 1/3** fields.
  - **WINS Servers** – Enter up to two WINS server IP address in the **WINS Server 1/2** fields.

Configuring IKEv2 Settings

IKEv2 Settings affect IKE notifications and allow you to configure dynamic client support.

- **Send IKEv2 Cookie Notify** - Sends cookies to IKEv2 peers as an authentication tool.
- **Send IKEv2 Invalid SPI Notify** – Sends an invalid Security Parameter Index (SPI) notification to IKEv2 peers when an active IKE security association (SA) exists. This option is selected by default.
- **IKEv2 Dynamic Client Proposal** - SonicOS provides IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings.

  Clicking **Configure** launches the **Configure IKEv2 Dynamic Client Proposal** dialog.


IKE Proposal

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Ready

SonicOS supports these **IKE Proposal** settings:

- **DH Group**: **Group 1**, **Group 2** (default), **Group 5**, **Group 14**, and the following five Diffie-Hellman groups that are included in Suite B cryptography:
  - **256-bit Random ECP Group**
  - **384-bit Random ECP Group**
  - **521-bit Random ECP Group**
  - **192-bit Random ECP Group**
  - **224-bit Random ECP Group**
- **Encryption**: **DES**, **3DES** (default), **AES-128**, **AES-192**, **AES-256**
- **Authentication**: **MD5**, **SHA1** (default), **SHA256**, **SHA384**, or **SHA512**

If a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPSec gateway is defined, however, you cannot configure these IKE Proposal settings on an individual policy basis.

ⓘ **NOTE:** The VPN policy on the remote gateway must also be configured with the same settings.

Using OCSP with SonicWall Network Security Appliances

OCSP is designed to augment or replace CRL in your Public Key Infrastructure (PKI) or digital certificate system. The CRL is used to validate the digital certificates comprised by the PKI. This allows the Certificate Authority (CA) to revoke certificates before their scheduled expiration date and is useful in protecting the PKI system against stolen or invalid certificates.

The main disadvantage of Certificate Revocation Lists is the need for frequent updates to keep the CRL of every client current. These frequent updates greatly increase network traffic when the complete CRL is downloaded by every client. Depending on the frequency of the CRL updates, a period of time can exist when a certificate is revoked by the CRL but the client has not received the CRL update and permits the certificate to be used.

Online Certificate Status Protocol determines the current status of a digital certificate without using a CRL. OCSP enables the client or application to directly determine the status of an identified digital certificate. This provides more timely information about the certificate than is possible with CRLs. In addition, each client typically only checks a few certificates and does not incur the overhead of downloading an entire CRL for only a few entries. This greatly reduces the network traffic associated with certificate validation.

OCSP transports messages over HTTP for maximum compatibility with existing networks. This requires careful configuration of any caching servers in the network to avoid receiving a cached copy of an OCSP response that might be out of date.

The OCSP client communicates with an OCSP responder. The OCSP responder can be a CA server or another server that communicates with the CA server to determine the certificate status. The OCSP client issues a status request to an OCSP responder and suspends the acceptance of the certificate until the responder provides a response. The client request includes data such as protocol version, service request, target certificate identification and optional extensions. These optional extensions might or might not be acknowledged by the OCSP responder.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN. If both the OCSP client and responder support the optional extensions, other responses are possible. The GOOD state is the desired response as it indicates the certificate has not been revoked. The REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

OCSP servers typically work with a CA server in push or pull setup. The CA server can be configured to push a CRL list (revocation list) to the OCSP server. Additionally the OCSP server can be configured to periodically download (pull) the CRL from the CA server. The OCSP server must also be configured with an OCSP response signing certificate issued by the CA server. The signing certificate must be properly formatted or the OCSP client cannot accept the response from the OSCP server.

OpenCA OCSP Responder

Using OCSP requires the OpenCA (OpenSource Certificate Authority) OpenCA OCSP Responder as it is the only supported OCSP responder. OpenCA OCSP Responder is available at http://www.openca.org. The OpenCA OCSP Responder is an rfc2560 compliant OCSP responder that runs on a default port of 2560 in homage to being based on rfc2560.

Loading Certificates to Use with OCSP

For SonicOS to act as an OCSP client to a responder, the CA certificate must be loaded onto the firewall.

1 On the **System** -> **Certificates** page, click **Import**. This brings up the **Import Certificate** page.

2 Select the **Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file** option and specify the location of the certificate.

Using OCSP with VPN Policies

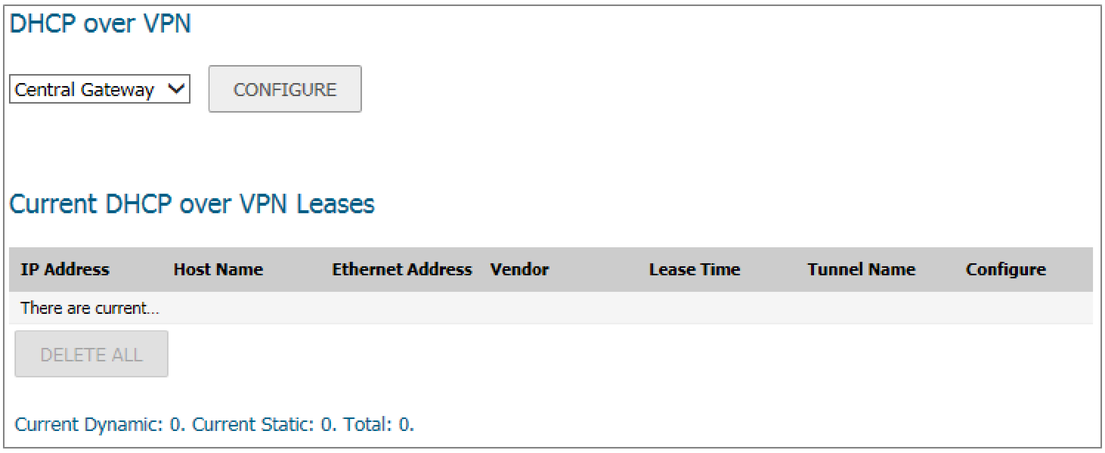
The firewall OCSP settings can be configured on a policy level or globally. To configure OCSP checking for individual VPN policies, use the Advanced tab of the VPN Policy configuration page.

1 Select **Enable OCSP Checking**.

2 Specify the **OCSP Responder URL** of the OCSP server, for example http://192.168.168.220:2560 where 192.168.168.220 is the IP address of your OCSP server and 2560 is the default port of operation for the OpenCA OCSP responder service.

Configuring DHCP over VPN

The **VPN > DHCP over VPN** page allows you to configure a firewall to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.



DHCP over VPN

Current DHCP over VPN Leases

IP Address	Host Name	Ethernet Address	Vendor	Lease Time	Tunnel Name	Configure
There are current...						

Current Dynamic: 0. Current Static: 0. Total: 0.

Topics:

- DHCP Relay Mode
- Configuring the Central Gateway for DHCP Over VPN
- Configuring DHCP over VPN Remote Gateway
- Current DHCP over VPN Leases

DHCP Relay Mode

The firewall at the remote and central sites are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The firewall at the remote site (**Remote Gateway**) passes DHCP broadcast packets through its VPN tunnel. The firewall at the central site (**Central Gateway**) relays DHCP packets from the client on the remote network to the DHCP server on the central site.

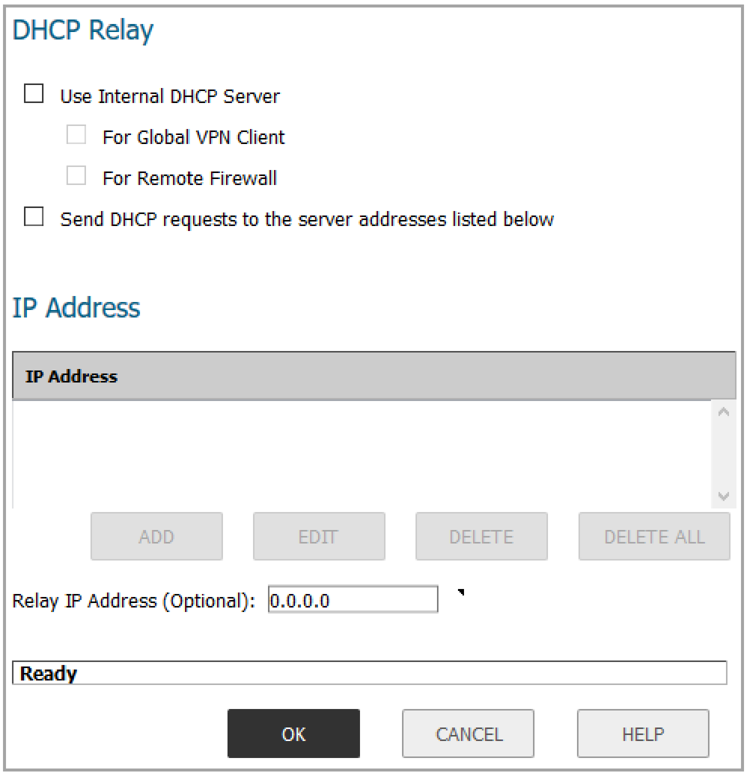
Configuring the Central Gateway for DHCP Over VPN

To configure DHCP over VPN for the Central Gateway:

1 Select **VPN > DHCP over VPN**.

2 Select **Central Gateway** from the **DHCP over VPN** drop-down menu.

3 Click **CONFIGURE**.



DHCP Relay

□ Use Internal DHCP Server

□ For Global VPN Client

□ For Remote Firewall

□ Send DHCP requests to the server addresses listed below

IP Address

IP Address

Relay IP Address (Optional): 0.0.0.0

Ready

4 Select one of the following:

- If you want to use the DHCP Server for global VPN clients or for a remote firewall or for both, select the **Use Internal DHCP Server** option.
    - To use the DHCP Server for global VPN clients, select the **For Global VPN Clients** option.
    - To use the DHCP Server for a remote firewall, select the **Remote Firewall** option.
- If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.
    a) Click **ADD**.
    b) Type the IP addresses of DHCP servers in the **IP Address** field.
    c) Click **OK**. The firewall now directs DHCP requests to the specified servers.

5 Type the IP address of a relay server in the **Relay IP Address (Optional)** field.

When set, this IP address is used as the DHCP Relay Agent IP address (giaddr) in place of this SonicWall's LAN IP address. This address is only used when no Relay IP Address has been set on the Remote Gateway, and must be reserved in the DHCP scope on the DHCP server.

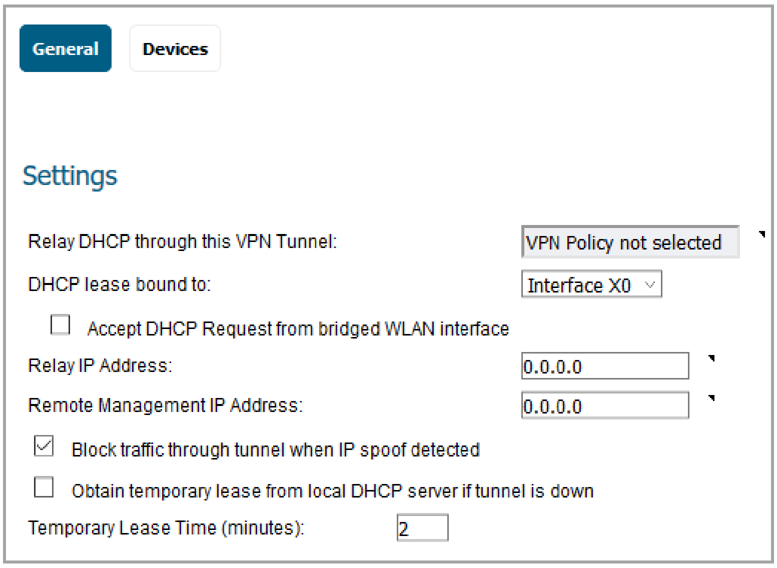
6 Click **OK**.

Configuring DHCP over VPN Remote Gateway

To configure DHCP over VPN Remote Gateway:

1 Select **Remote Gateway** from the **DHCP over VPN** drop-down menu.

2 Click **CONFIGURE**.



Settings

Relay DHCP through this VPN Tunnel: VPN Policy not selected

DHCP lease bound to: Interface X0

□ Accept DHCP Request from bridged WLAN interface

Relay IP Address: 0.0.0.0

Remote Management IP Address: 0.0.0.0

☑ Block traffic through tunnel when IP spoof detected

□ Obtain temporary lease from local DHCP server if tunnel is down

Temporary Lease Time (minutes): 2

3 On the **General** screen, the VPN policy name is automatically displayed in the **Relay DHCP through this VPN Tunnel** field if the VPN policy has the setting **Local network obtains IP addresses using DHCP through this VPN Tunnel** enabled.

> **NOTE:** Only VPN policies using IKE can be used as VPN tunnels for DHCP. The VPN tunnel must use IKE and the local network must be set appropriately. The local network obtains IP addresses using DHCP through this VPN Tunnel.

4 Select the interface the DHCP lease is bound from the **DHCP lease bound to** menu.

5 To accept DJCP requests from bridged WLAN interfaces, enable **Accept DJCP Request from bridged WLA interface**.

6 If you enter an IP address in the **Relay IP Address** field, this IP address is used as the DHCP Relay Agent IP address (giaddr) in place of the Central Gateway's address and must be reserved in the DHCP scope on the DHCP server. This address can also be used to manage this firewall remotely through the VPN tunnel from behind the Central Gateway.

> **NOTE:** The Relay IP address and Remote Management IP Address fields cannot be zero if management through the tunnel is required.

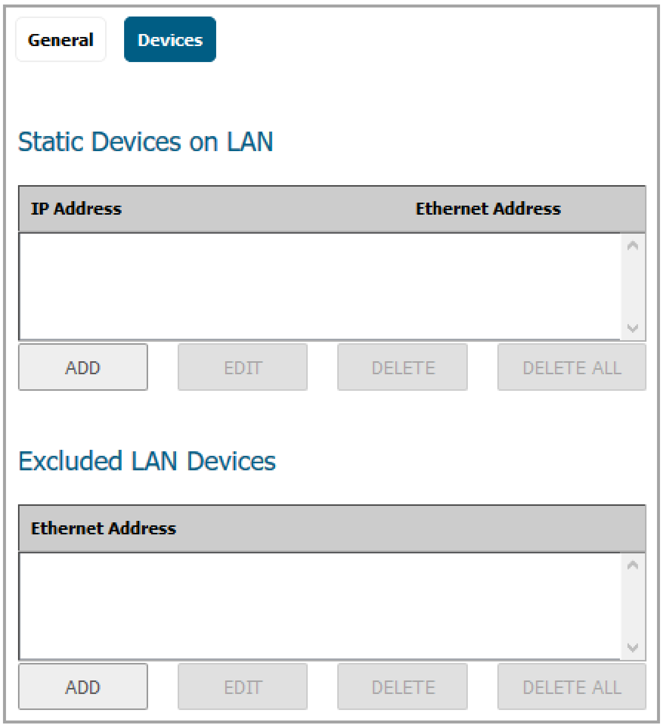
7 If you enter an IP address in the **Remote Management IP Address** field, this IP address is used to manage the firewall from behind the Central Gateway, and must be reserved in the DHCP scope on the DHCP server.

8 If you enable **Block traffic through tunnel when IP spoof detected**, the firewall blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is typed for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the firewall to respond to IP spoofs.

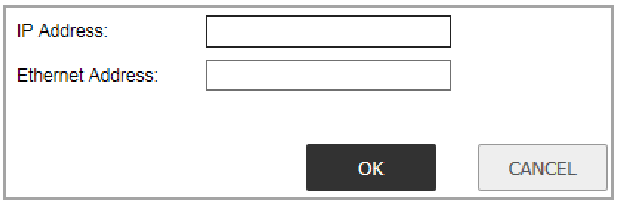
9 If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. After the tunnel is again active, the local DHCP server stops issuing leases. Enable **Obtain temporary lease from local DHCP server if tunnel is down**. By enabling this checkbox, you have a failover option in case the tunnel ceases to function.

10 If you want to allow temporary leases for a certain time period, type the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is **2** minutes.

11 To configure devices on your LAN, click **Devices**.



12 To configure **Static Devices on the LAN**, click **ADD** to display the **Add LAN Device Entry** dialog.



13 Type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field.

An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to type the Ethernet address of a device. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses.

14 Click **OK**.

15 To exclude devices on your LAN, click **Add** to display the **Add Excluded LAN Entry** dialog.

16 Enter the MAC address of the device in the **Ethernet Address** field.

17 Click **OK**.

18 Click **OK** to exit the **DHCP over VPN Configuration** dialog.

> **NOTE:** You must configure the local DHCP server on the remote firewall to assign IP leases to these computers.

> **NOTE:** If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.

> **TIP:** If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, that is, two LANs.

> **NOTE:** Wireless clients are assigned an IP address in this subnet. The IP address and a DHCP server are automatically created and assign DHCP addresses.

Current DHCP over VPN Leases

The **Current DHCP over VPN Leases** table shows the details on the current bindings: **IP Address**, **Host Name**, **Ethernet Address**, **Lease Time**, and **Tunnel Name**. The last column in the table, **Configure**, enables you to configure or delete a table entry (binding) to:

- Edit a binding, click **Edit**.
- Delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the **Delete** icon. The operation takes a few seconds to complete. When completed, a message confirming the update is displayed at the bottom of the Web browser window.
- Delete all VPN leases, click **Delete All**.

Configuring L2TP Servers and VPN Client Access

The SonicWall network security appliance can terminate L2TP-over-IPsec connections from incoming Microsoft Windows or Google Android clients. In situations where running the Global VPN Client (GVC) is not possible, you can use the SonicWall L2TP Server to provide secure access to resources behind the firewall.

You can use Layer 2 Tunneling Protocol (L2TP) to create a VPN over public networks. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them.

L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPsec to provide a secure, encrypted VPN solution.

Topics:

- Configuring the L2TP Server
- Viewing Currently Active L2TP Sessions
- Configuring Microsoft Windows L2TP VPN Client Access
- Configuring Google Android L2TP VPN Client Access

> ⓘ **NOTE:** For more complete information on configuring the L2TP Server, see the technote **Configuring the L2TP Server on SonicOS** located on the SonicWall support site: https://www.sonicwall.com/support.

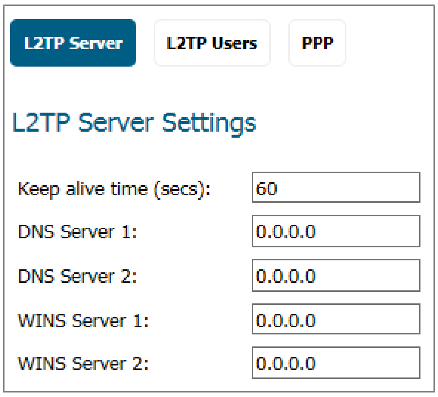
Configuring the L2TP Server

The **MANAGE | Connectivity | VPN > L2TP Server** page provides the settings for configuring the SonicWall network security appliance as a L2TP Server.

To configure the L2TP Server:

1. Navigate to the **MANAGE | Connectivity | VPN > L2TP Server** page.
2. Select **Enable L2TP Server**. **CONFIGURE** becomes available.

3 Click **CONFIGURE** to display the **L2TP Server Configuration** dialog.



L2TP Server Settings

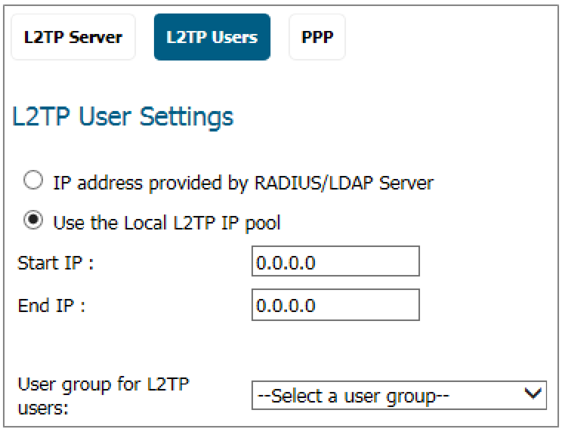
Keep alive time (secs):	60
DNS Server 1:	0.0.0.0
DNS Server 2:	0.0.0.0
WINS Server 1:	0.0.0.0
WINS Server 2:	0.0.0.0

4 On the **L2TP Server** screen, enter a value, in seconds, in the **Keep alive time (secs)** field. This specifies how often special packets are sent to keep the connection open. The default is **60** seconds.

5 Enter the IP address of your first DNS server in the **DNS Server 1** field. If you have a second DNS server, type the IP address in the **DNS Server 2** field.

6 Enter the IP address of your first WINS server in the **WINS Server 1** field. If you have a second WINS server, type the IP address in the **WINS Server 2** field.

7 Click **L2TP Users**.



L2TP User Settings

○ IP address provided by RADIUS/LDAP Server

● Use the Local L2TP IP pool

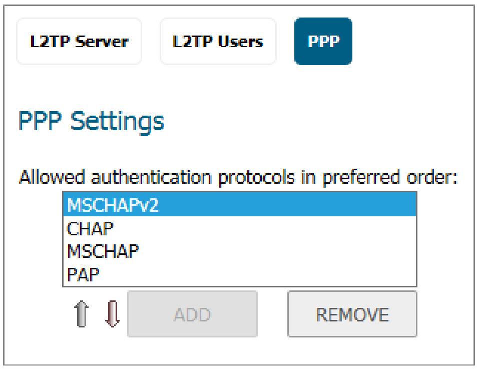
Start IP :	0.0.0.0
End IP :	0.0.0.0
User group for L2TP users:	--Select a user group--

8 Select one of the following radio buttons for IP address settings:

IP address provided by RADIUS/LDAP Server	By default, this option is not selected. Choose it if a RADIUS/LDAP server provides IP addressing information to the L2TP clients. The **Start IP** and **End IP** fields are no longer active. **NOTE:** To use this option RADIUS or LDAP authentication must be selected on the **MANAGE | System Setup | Users > Settings** page. If this option is selected, an informational message to this effect is displayed. click **OK.**
Use the Local L2TP IP Pool	This is the default IP address setting. Choose it if the L2TP Server provides IP addresses. Enter the range of private IP addresses on the LAN in the **Start IP** and **End IP** fields.

9 If you have configured a specific user group defined for using L2TP, select it from the **User Group for L2TP users** menu or use **Everyone**.

10 Click **PPP**.

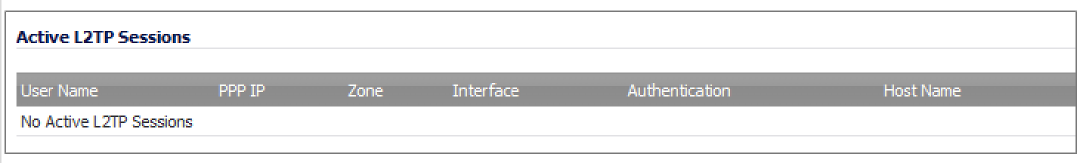


11 Select an authentication protocol and click **ADD** to add it. You can also remove authentication protocols or rearrange the order of authentication.

12 Click **OK**.

Viewing Currently Active L2TP Sessions

The **Active L2TP Sessions** section displays the currently active L2TP sessions.



Active L2TP Sessions

User Name	PPP IP	Zone	Interface	Authentication	Host Name
No Active L2TP Sessions					

The following information is displayed.

User Name	The user name assigned in the local user database or the RADIUS user database.
PPP IP	The source IP address of the connection.
Zone	The zone used by the L2TP client.
Interface	The interface used to access the L2TP Server, whether it is a VPN client or another firewall.
Authentication	Type of authentication used by the L2TP client.
Host Name	The name of the L2TP client connecting to the L2TP Server.

Configuring Microsoft Windows L2TP VPN Client Access

This section provides an example for configuring L2TP client access to the WAN GroupVPN SA using the built-in L2TP Server and Microsoft's L2TP VPN Client.

ⓘ **NOTE:** SonicOS supports only X.509 certificates for L2TP clients; PKCS #7 encoded X.509 certificates are not supported in SonicOS for L2TP connections.

To enable Microsoft L2TP VPN Client access to the WAN GroupVPN SA:

1 Navigate to the **MANAGE | Connectivity | VPN > Base Settings** page.

2 For the WAN GroupVPN policy, click the **Edit** icon in the **Configure** column.

3 On the **General** screen, select **IKE using Preshared Secret** for the **Authentication Method**.

4 Enter a shared secret passphrase in the **Shared Secret** field to complete the client policy configuration.

5 Click **OK**.

6 Navigate to the **MANAGE | Connectivity | VPN > L2TP Server** page.

7 In the **L2TP Server Settings** section, select **Enable L2TP Server**.

8 Click **CONFIGURE**.

9 Provide the following L2TP server settings:

- **Keep alive time (secs)**: *60*
- **DNS Server 1**: *199.2.252.10* (or use your ISP's DNS)
- **DNS Server 2**: *4.2.2.2* (or use your ISP's DNS)
- **DNS Server 3**: *0.0.0.0* (or use your ISP's DNS)
- **WINS Server 1**: *0.0.0.0* (or use your WINS IP)
- **WINS Server 2**: *0.0.0.0* (or use your WINS IP)

10 Click **L2TP Users**.

11 Set the following options:

- **Use the Local L2TP IP pool**: Enabled (selected; the default)
- **Start IP**: *10.20.0.1* (use your own IP)
- **End IP**: *10.20.0.20* (use your own IP)

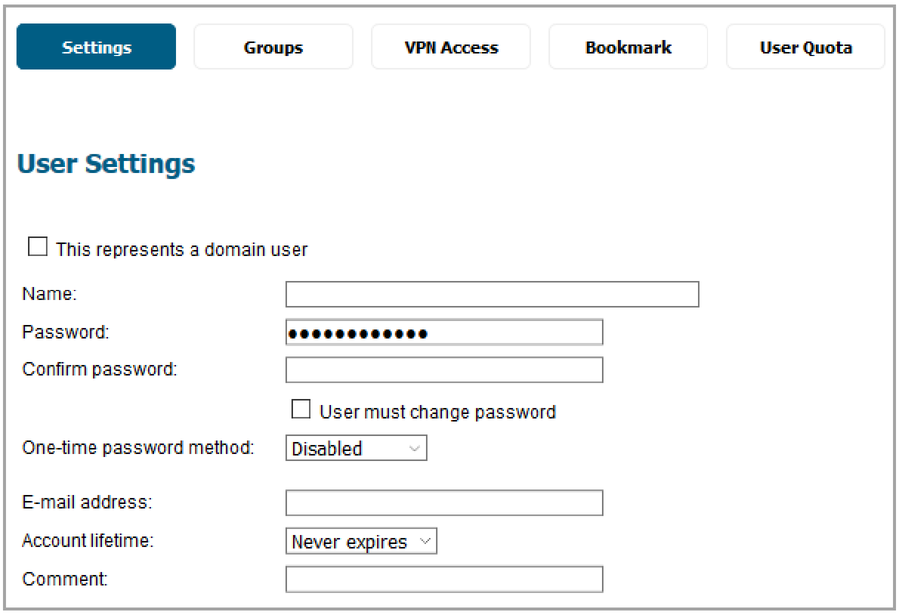
12 Select **Trusted Users** from the **User group for L2TP users** drop-down menu.

13 Click **OK**.

14 Navigate to the **MANAGE | System Setup | Users > Local Users & Groups** page.

15 Click **Local Users**.

16 Click **Add** to display the **Add User** dialog.



User Settings

□ This represents a domain user

Name:	
Password:	●●●●●●●●●●●●
Confirm password:	
	□ User must change password
One-time password method:	Disabled
E-mail address:	
Account lifetime:	Never expires
Comment:	

17 Specify a user name and password in the **Name**, **Password**, and **Confirm Password** fields.

18 Click **OK**.

> **NOTE:** By editing the VPN > LAN access rule or another VPN access rule (under **MANAGE | Policies | Rules > Access Rules**), you can restrict network access for L2TP clients. To locate a rule to edit, select the **All Types** view on the **Access Rules** table and look at the Source column for **L2TP IP Pool**.

19 On your Microsoft Windows computer, complete the following L2TP VPN Client configuration to enable secure access:

a Navigate to the **Start > Control Panel > Network and Sharing Center**.

b Open the New Connection Wizard.

c Choose **Connect to a workplace**.

d Click **Next**.

e Choose **Virtual Private Network Connection**. Click **Next**.

f Enter a name for your VPN connection. Click **Next**.

g Enter the Public (WAN) IP address of the firewall. Alternatively, you can use a domain name that points to the firewall.

h Click **Next**, and then click **Finish**.

i In the Connection window, click **Properties**.

j Click **Security**.

k Click on **IPSec Settings.**

l Enable **Use preshared key for authentication**.

m Enter your preshared secret key and click **OK**.

n Click **Networking**.

o Change **Type of VPN** from **Automatic** to **L2TP IPSec VPN**.

p Click **OK**.

q Enter your XAUTH username and password.

r Click **Connect**.

20 Verify your Microsoft Windows L2TP VPN device is connected by navigating to the **MANAGE | Connectivity | VPN > Base Settings** page. The VPN client is displayed in the **Currently Active VPN Tunnels** section.

Configuring Google Android L2TP VPN Client Access

This section provides an example for configuring L2TP client access to WAN GroupVPN SA using the built-in L2TP Server and Google Android's L2TP VPN Client.

To enable Google Android L2TP VPN Client access to WAN GroupVPN SA, perform the following steps:

1 Navigate to the **MANAGE | Connectivity | VPN > Base Settings** page.

2 For the WAN GroupVPN policy, click the **Edit** icon.

3 Select **IKE using Preshared Secret** (default) from the **Authentication Method** drop-down menu.

4 Enter a shared secret passphrase in the **Shared Secret** field to complete the client policy configuration.

5 Click **Proposals**.

6 Provide the following settings for **IKE (Phase 1) Proposal**:

- DH Group: **Group 2**
- Encryption: **3DES**
- Authentication: **SHA1**
- Life Time (seconds): **28800**

7 Provide the following settings for **IPsec (Phase 2) Proposal**:

- Protocol: **ESP**
- Encryption: **DES**
- Authentication: **SHA1**
- Enable Perfect Forward Secrecy: **Enabled**
- Life Time (seconds): **28800**

8 Click **Advanced**.

9 Set the following options:

- **Enable Multicast**: Disabled
- **Management via this SA**: Disabled all
- **Default Gateway**: 0.0.0.0
- **Require authentication of VPN clients by XAUTH**: Enabled
- **User group for XAUTH users**: Trusted Users

10 Click **Client**.

11 Set the following options:

- **Cache XAUTH User Name and Password on Client**: Single Session or Always
- **Virtual Adapter setting**: DHCP Lease
- **Allow Connections to**: Split Tunnels
- **Set Default Route as this Gateway**: Disabled
- **Apply VPN Access Control List**: Disabled
- **Use Default Key for Simple Client Provisioning**: Enabled

12 Click **OK**.

13 Navigate to the **MANAGE | Connectivity | VPN > L2TP Server** page.

14 Select **Enable the L2TP Server**.

15 Click **CONFIGURE**.

16 Provide the following L2TP server settings:

- **Keep alive time (secs)**: 60
- **DNS Server 1**: 199.2.252.10 (or use your ISPs DNS)
- **DNS Server 2**: 4.2.2.2 (or use your ISPs DNS)
- **DNS Server 3**: 0.0.0.0 (or use your ISPs DNS)
- **WINS Server 1**: 0.0.0.0 (or use your WINS IP)
- **WINS Server 2**: 0.0.0.0 (or use your WINS IP)

17 Click **L2TP Users**.

18 Set the following options:

- **IP address provided by RADIUS/LDAP Server**: Disabled
- **Use the Local L2TP IP Pool**: Enabled
- **Start IP**: 10.20.0.1 (or use your own)
- **End IP**: 10.20.0.20 (or use your own)

19 In the **User Group for L2TP Users** drop-down menu, select **Trusted Users**.

20 Click **OK**.

21 Navigate to the **MANAGE | System Setup | Users > Local Users and Groups** page.

22 Click **Local Users**.

23 Click **Add**.

24 Navigate to the **MANAGE | System Setup | Users > Local Users** page. Click **Add User**.

25 In the **Settings** screen, specify a user name and password.

26 In the VPN Access screen, add the desired network address object(s) that the L2TP clients to the access list networks.

> **NOTE:** At the minimum add the LAN Subnets, LAN Primary Subnet, and L2TP IP Pool address objects to the access list.

> **NOTE:** You have now completed the SonicOS configuration.

27 On your Google Android device, complete the following L2TP VPN Client configuration to enable secure access:

   a Navigate to the APP page, and select the **Settings** icon. From the Settings menu, select **Wireless & networks**.

   b Select **VPN Settings**, and click **Add VPN**.

   c Select **Add L2TP/IPSec PSK VPN**.

   d Under VPN Name, enter a VPN friendly name.

   e Set **VPN Server**.

   f Enter the public IP address of firewall.

   g Set **IPSec preshared key**: enter the passphrase for your WAN GroupVPN policy.

   h Leave **L2TP secret** blank.

   i If you want set LAN domain setting. They are optional.

   j Enter your XAUTH username and password. Click **Connect**.

28 Verify your Google Android device is connected by navigating to the **MANAGE | Connectivity | VPN > Settings** page. The VPN client is displayed in the Currently Active VPN Tunnels section.

8

AWS VPN

The AWS VPN page makes it easy to create VPN connection from the SonicWall firewall to Virtual Private Clouds (VPCs) on Amazon Web Services (AWS). For more information about Amazon Virtual Private Cloud, refer to https://aws.amazon.com/vpc/.

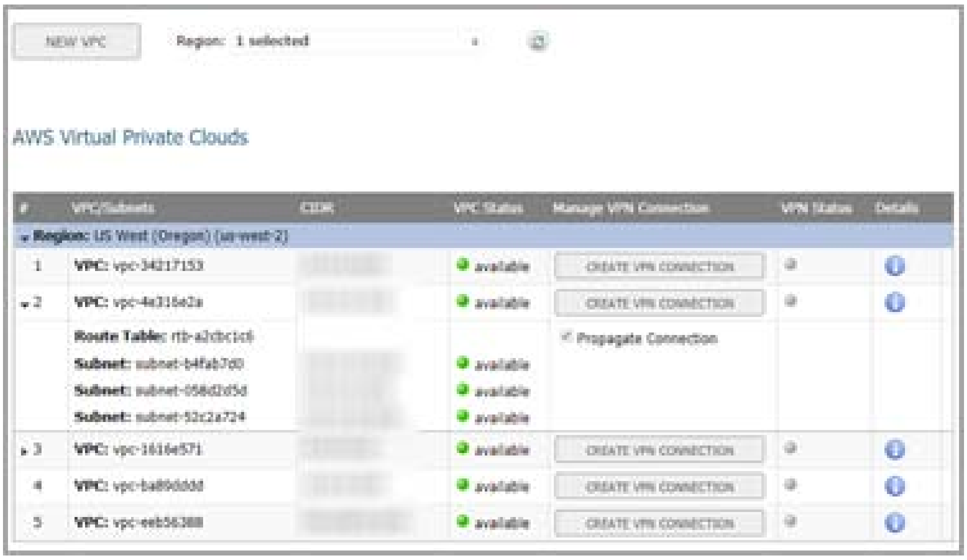
> ⓘ **IMPORTANT:** Before setting up AWS VPN, be sure to configure the firewall with the AWS credentials that it needs to use. Navigate to **System Setup | Network > AWS Configuration** on the **MANAGE** view to do this. In addition, click **Test Configuration** to validate the settings before proceeding.

Topics:

- Overview
- Creating a New VPN Connection
- Reviewing the VPN Connection
- Route Propagation
- AWS Regions
- Deleting VPN Connections

Overview

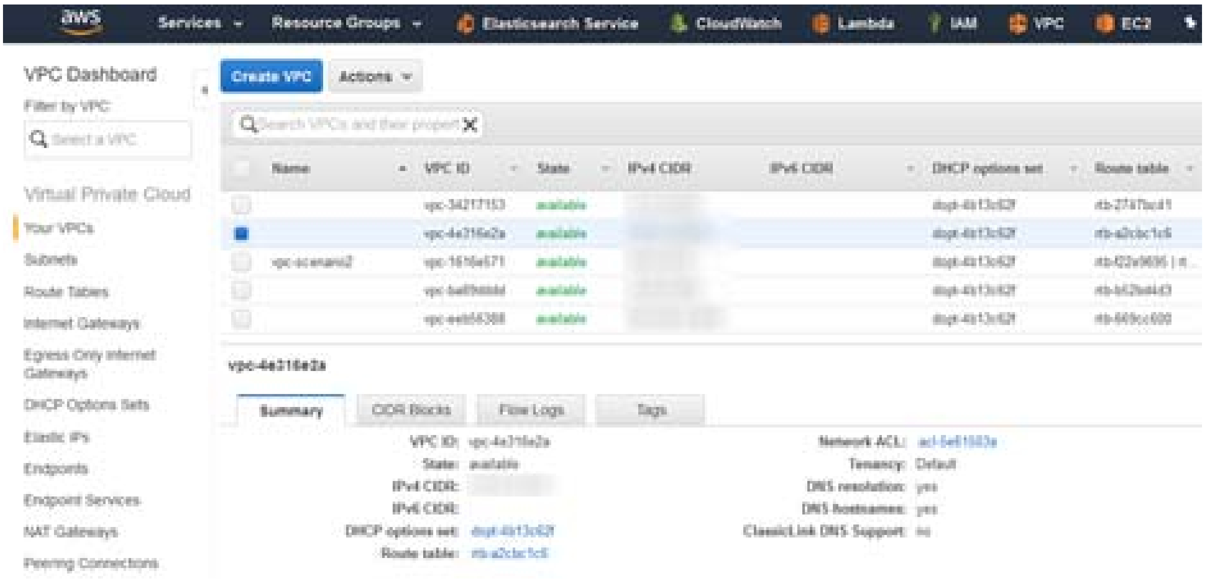
To get to AWS VPN, navigate to **MANAGE | Connectivity > VPN > AWS VPN**. The AWS VPN page is dominated by a table showing the VPCs in the AWS regions of interest. Each row in the table can be expanded to show the subnets, organized by route table, for the VPC. Other columns in the table show status information, and the buttons can be used to create and delete VPN connections to the corresponding VPC.



AWS Virtual Private Clouds

#	VPC/Subnets	CIDR	VPC Status	Manage VPN Connection	VPN Status	Details
▾ **Region:** US West (Oregon) (us-west-2)						
1	**VPC:** vpc-34217153	[redacted]	● available	CREATE VPN CONNECTION	●	ⓘ
▾ 2	**VPC:** vpc-4e316e2a	[redacted]	● available	CREATE VPN CONNECTION	●	ⓘ
	Route Table: rtb-a2cbc1c6			✓ Propagate Connection		
	Subnet: subnet-b4fab7d0	[redacted]	● available			
	Subnet: subnet-058d2d5d	[redacted]	● available			
	Subnet: subnet-52c2a724	[redacted]	● available			
▸ 3	**VPC:** vpc-1616e571	[redacted]	● available	CREATE VPN CONNECTION	●	ⓘ
4	**VPC:** vpc-ba89dddd	[redacted]	● available	CREATE VPN CONNECTION	●	ⓘ
5	**VPC:** vpc-eeb56388	[redacted]	● available	CREATE VPN CONNECTION	●	ⓘ

The table on the firewall's AWS VPN page reflects the VPC information that is available on the AWS Console under the VPC Dashboard (shown below).



Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table
	vpc-34217153	available	[redacted]		dopt-4b13c62f	rtb-27d7bcd1
	vpc-4e216e2a	available	[redacted]		dopt-4b13c62f	rtb-a2cbc1c6
vpc-scenario2	vpc-1616e571	available	[redacted]		dopt-4b13c62f	rtb-622e9695 | rt...
	vpc-ba89dddd	available	[redacted]		dopt-4b13c62f	rtb-b62bd4d3
	vpc-ee656388	available	[redacted]		dopt-4b13c62f	rtb-669cc600

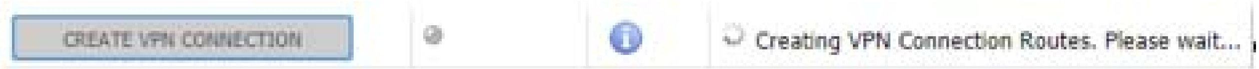
vpc-4e216e2a

VPC ID: vpc-4e216e2a
State: available
IPv4 CIDR: [redacted]
IPv6 CIDR:
DHCP options set: dopt-4b13c62f
Route table: rtb-a2cbc1c6

Network ACL: acl-5e81503a
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

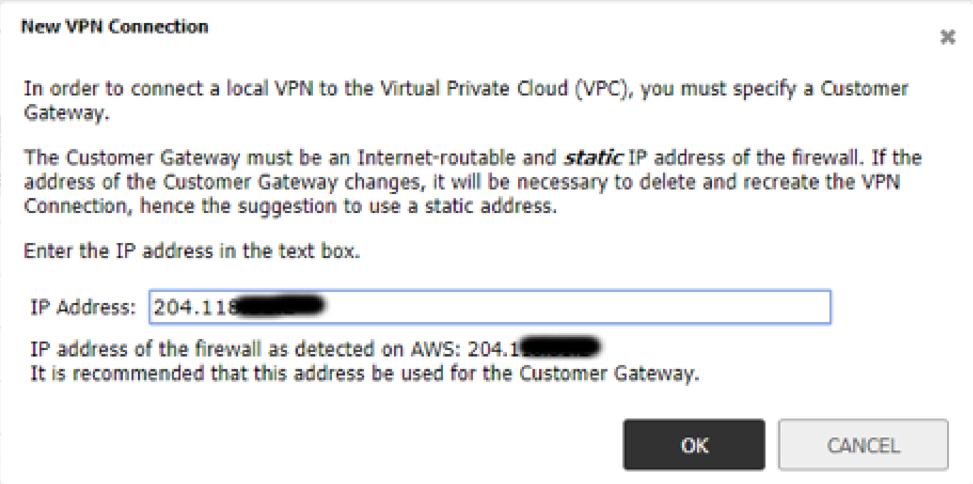
Creating a New VPN Connection

Creating a new VPN Connection from the firewall is relatively simple. To start the process, simply click **CREATE VPN CONNECTION** on the appropriate row for the Amazon VPC that you wish to connect to the firewall.



Creating VPN Connection Routes. Please wait...

The **New VPN Connection** window appears. Provide the public IP address of the firewall as seen from AWS. Code running on AWS attempts to detect the address and prepopulate the text input field. Verify that the address is reachable from outside the local network. If the firewall is behind a router or some other proxy, NAT rules should be put in place to ensure VPN traffic initiated from the AWS side can route back to the firewall.



New VPN Connection

In order to connect a local VPN to the Virtual Private Cloud (VPC), you must specify a Customer Gateway.

The Customer Gateway must be an Internet-routable and ***static*** IP address of the firewall. If the address of the Customer Gateway changes, it will be necessary to delete and recreate the VPN Connection, hence the suggestion to use a static address.

Enter the IP address in the text box.

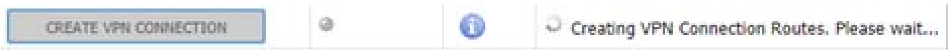
IP Address: 204.11[redacted]

IP address of the firewall as detected on AWS: 204.1[redacted]
It is recommended that this address be used for the Customer Gateway.

NOTE: in some circumstances, you might be asked whether to enable Route Propagation. Refer to Route Propagation for more information.

The IP address you entered is used as the Customer Gateway. Click **OK** to close the dialog and initiate a series of processes that configure both the firewall and AWS in order to establish a VPN Connection between them.

Messages appear in the table row for the VPC that is the subject of the new VPN Connection, keeping you informed of the progress at the different stages.



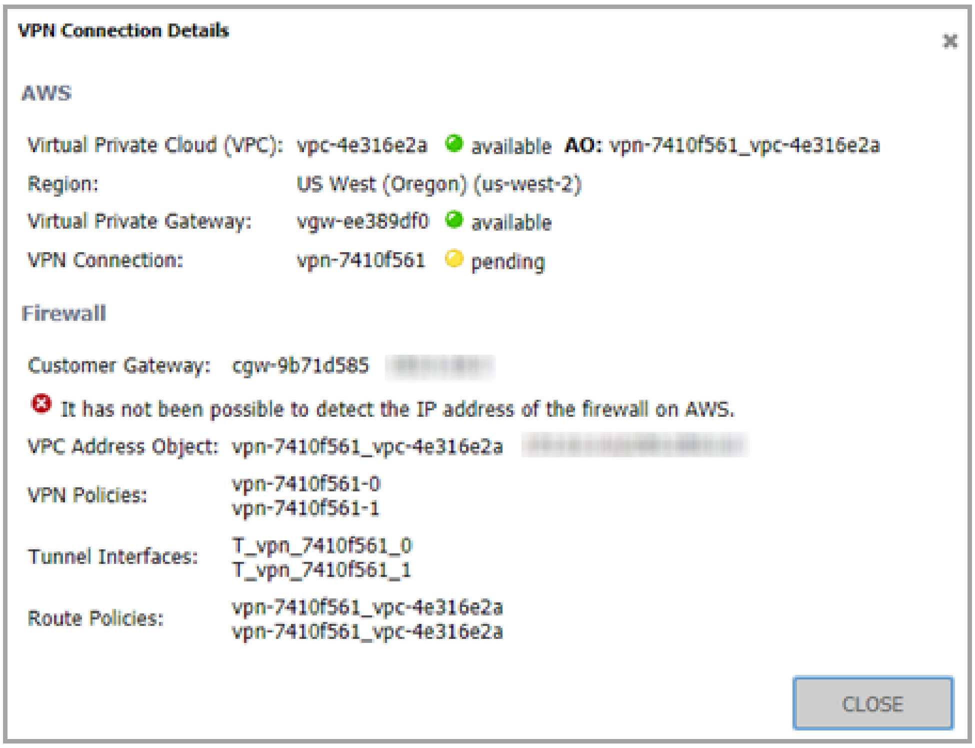
Creating VPN Connection Routes. Please wait...

If an error occurs at any stage, a message appears with details of the problem and all the changes that have been made are reversed. This should allow you to correct any issues and try again.

Reviewing the VPN Connection

After creating a new VPN connection between the firewall and a VPC on AWS, you can view details of how the process changed their respective configurations.

On the firewall, navigate to **MANAGE | Connectivity > VPN > AWS VPN**. Find the row in the VPC table corresponding to the AWS VPC in question and click **Information**. Details of the VPN connection are shown.



VPN Connection Details

AWS

Virtual Private Cloud (VPC): vpc-4e316e2a ● available **AO:** vpn-7410f561_vpc-4e316e2a

Region: US West (Oregon) (us-west-2)

Virtual Private Gateway: vgw-ee389df0 ● available

VPN Connection: vpn-7410f561 ● pending

Firewall

Customer Gateway: cgw-9b71d585 [redacted]

It has not been possible to detect the IP address of the firewall on AWS.

VPC Address Object: vpn-7410f561_vpc-4e316e2a [redacted]

VPN Policies: vpn-7410f561-0
vpn-7410f561-1

Tunnel Interfaces: T_vpn_7410f561_0
T_vpn_7410f561_1

Route Policies: vpn-7410f561_vpc-4e316e2a
vpn-7410f561_vpc-4e316e2a

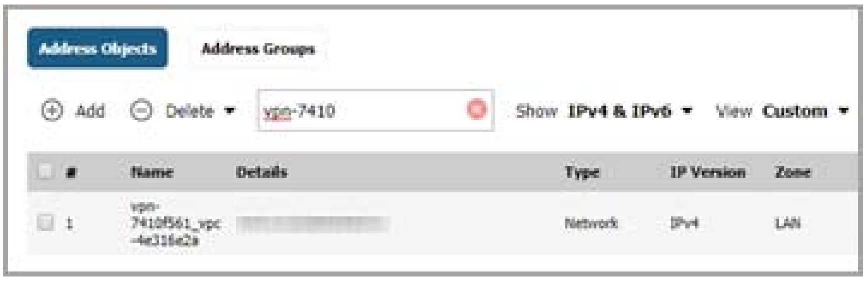
NOTE: Because the VPN connection has only just been created, the status is reported as still **pending**. Use **Refresh** on the AWS VPN page to reload the data in the table and on the associated VPN Connection Details window.

The following sections describe the configuration on the firewall and on AWS.

- Configuration on the Firewall
- Configuration on Amazon Web Services

Configuration on the Firewall

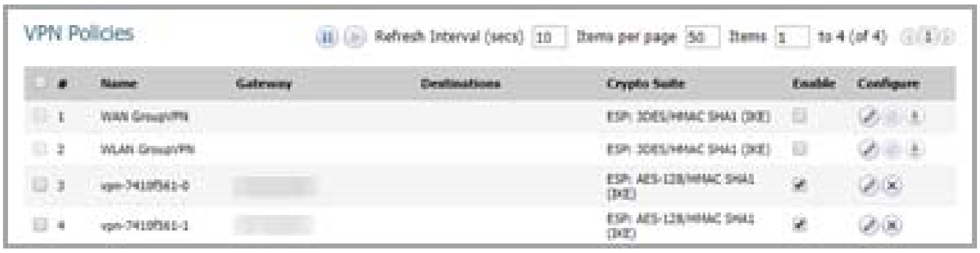
As part of the process to create a new VPN connection, an Address Object representing the VPC is added and can be viewed in SonicOS on the **Address Objects** page. Navigate to **MANAGE | Policies | Objects > Address Objects**. The convention used to name the object combines the AWS IDs of the VPN connection and the VPC itself. The Address Object is a network type, with the network being that of the remote VPC.



vpn-7410

☐	#	Name	Details	Type	IP Version	Zone
☐	1	vpn-7410f561_vpc-4e316e2a	[redacted]	Network	IPv4	LAN

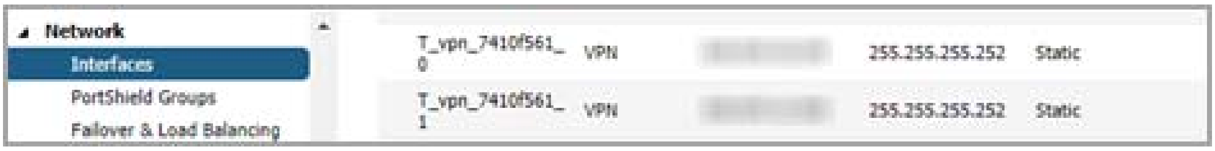
Two VPN policies are also created, showing that AWS uses two VPNs per VPN connection to provide redundancy for a failover mechanism. Navigate to **MANAGE | Connectivity | VPN > Base Settings**. The VPN policy names used on the firewall are based on the AWS ID for the connection along with a suffix to differentiate between the two policies.



Refresh Interval (secs) 10 Items per page 50 Items 1 to 4 (of 4)

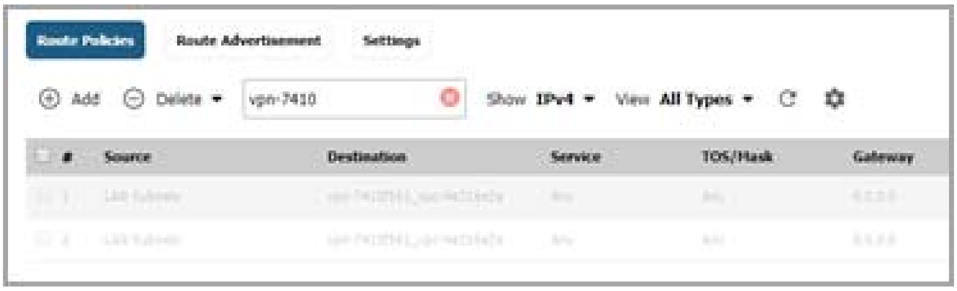
☐	#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
☐	1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	☐	
☐	2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	☐	
☐	3	vpn-7410f561-0	[redacted]		ESP: AES-128/HMAC SHA1 (IKE)	☑	
☐	4	vpn-7410f561-1	[redacted]		ESP: AES-128/HMAC SHA1 (IKE)	☑	

Matching the two VPN policies, two tunnel interfaces are created. Navigate to **MANAGE | System Setup | Network > Interfaces**. They also use a naming convention based on the ID of the VPN Connection.



T_vpn_7410f561_0	VPN	[redacted]	255.255.255.252	Static
T_vpn_7410f561_1	VPN	[redacted]	255.255.255.252	Static

Similarly, two route policies are created, both using the Address Object representing the VPC as their destination. Navigate to **MANAGE | System Setup | Network > Routing**. Each one uses a different tunnel interface.

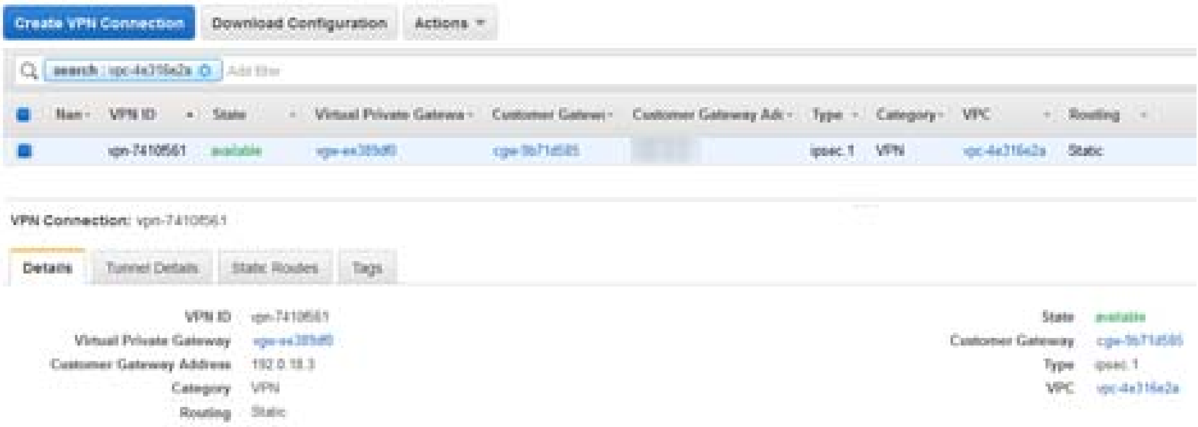


vpn-7410

☐	#	Source	Destination	Service	TOS/Mask	Gateway
☐	1	LAN Subnets	vpn-7410f561_vpc-4e316e2a	Any	Any	0.0.0.0
☐	2	LAN Subnets	vpn-7410f561_vpc-4e316e2a	Any	Any	0.0.0.0

Configuration on Amazon Web Services

The process of creating a VPN Connection from the AWS VPN page in the firewall GUI also makes changes to the configuration on AWS. Using the AWS Console, under the VPC Dashboard, view VPN connections. Using the VPC ID as a filter, find the VPN connection that was created.



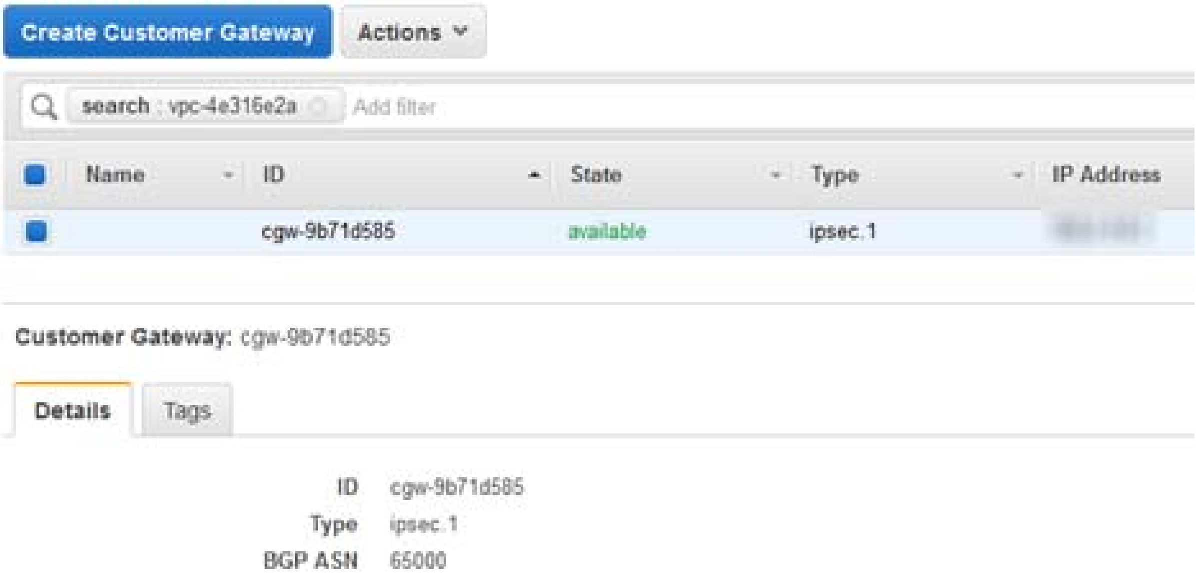
Nan	VPN ID	State	Virtual Private Gatewa	Customer Gatewa	Customer Gateway Ad	Type	Category	VPC	Routing
	vpn-7410f561	available	vgw-ee385df0	cgw-9b71d585	[redacted]	ipsec.1	VPN	vpc-4e316e2a	Static

VPN Connection: vpn-7410f561

VPN ID vpn-7410f561
Virtual Private Gateway vgw-ee385df0
Customer Gateway Address 192.0.18.3
Category VPN
Routing Static

State available
Customer Gateway cgw-9b71d585
Type ipsec.1
VPC vpc-4e316e2a

The customer gateway, the endpoint at the firewall, and the IP address specified when first creating the VPN connection can also be viewed on the AWS Console. Navigate to the Customer Gateways page, under the VPC Dashboard.



Name	ID	State	Type	IP Address
	cgw-9b71d585	available	ipsec.1	[redacted]

Customer Gateway: cgw-9b71d585

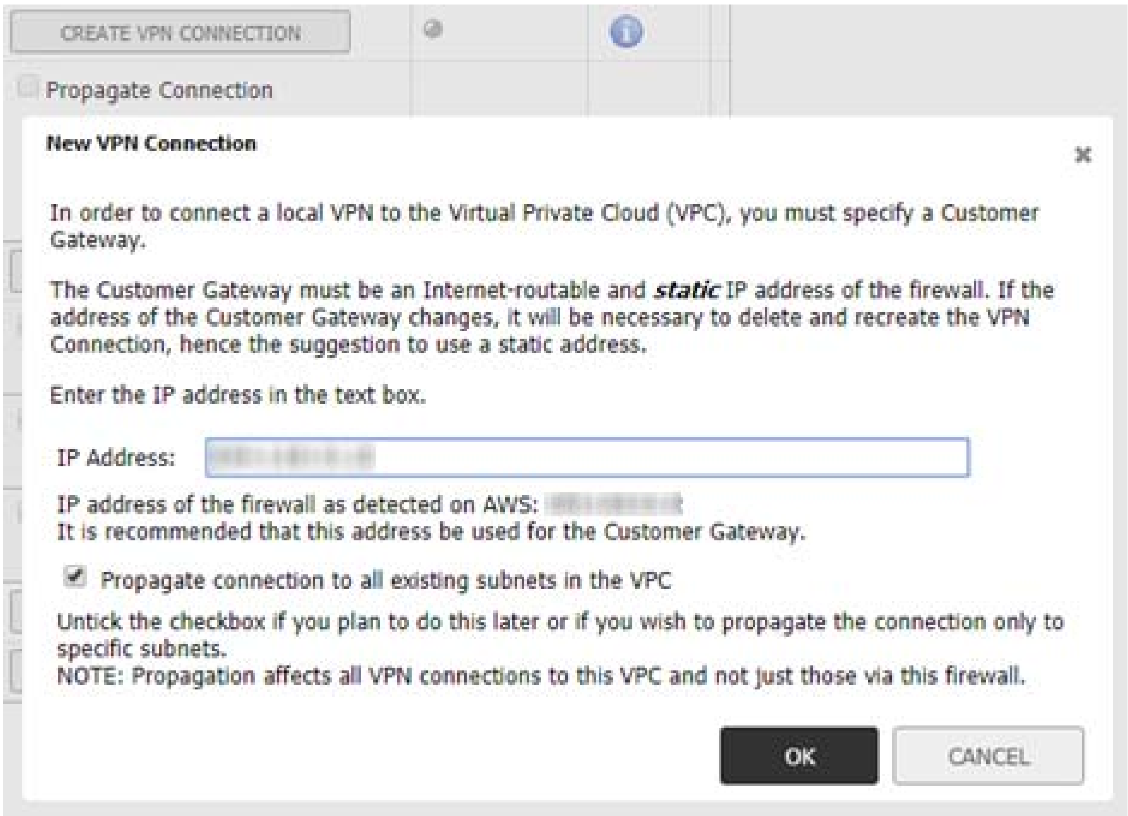
ID cgw-9b71d585
Type ipsec.1
BGP ASN 65000

Route Propagation

Additional steps need to be taken to ensure connections can be made to and from resources on subnets within a particular VPC. You must also propagate the connections to the route table that is used for the subnet of interest. Three ways can be used to enable propagation to the route tables in a VPC.

- When Creating the VPN Connection

  If the firewall detects that route propagation is disabled for one or more route tables within a VPC, the popup dialog includes a checkbox allowing you to specify that Route Propagation should be enabled for all route tables within that VPC. However, this is not a a consistent approach; it does allows propagation for some route tables and not others.



New VPN Connection

In order to connect a local VPN to the Virtual Private Cloud (VPC), you must specify a Customer Gateway.

The Customer Gateway must be an Internet-routable and ***static*** IP address of the firewall. If the address of the Customer Gateway changes, it will be necessary to delete and recreate the VPN Connection, hence the suggestion to use a static address.

Enter the IP address in the text box.

IP Address:

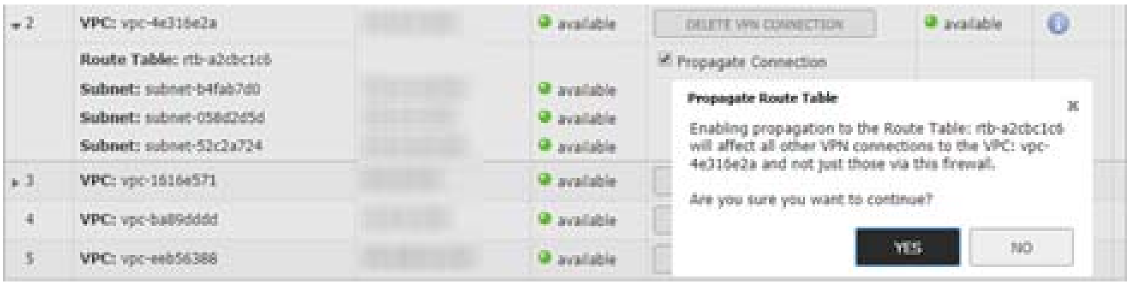
IP address of the firewall as detected on AWS:
It is recommended that this address be used for the Customer Gateway.

☑ Propagate connection to all existing subnets in the VPC

Untick the checkbox if you plan to do this later or if you wish to propagate the connection only to specific subnets.
NOTE: Propagation affects all VPN connections to this VPC and not just those via this firewall.

- Using checkboxes for each route table

  After a VPN connection has been established, expanding a row in the VPC table on the AWS VPN page reveals all of the subnets in that VPC, organized by route table. Each route table row includes a checkbox that can be used to enable or disable propagation for that particular route table and the subnets it governs.



▾ 2	**VPC:** vpc-4e316e2a	● available
	Route Table: rtb-a2cbc1c6	
	Subnet: subnet-b4fab7d0	● available
	Subnet: subnet-058d2d5d	● available
	Subnet: subnet-52c2a724	● available
▸ 3	**VPC:** vpc-1616e571	● available
4	**VPC:** vpc-ba89dddd	● available
5	**VPC:** vpc-eeb56388	● available

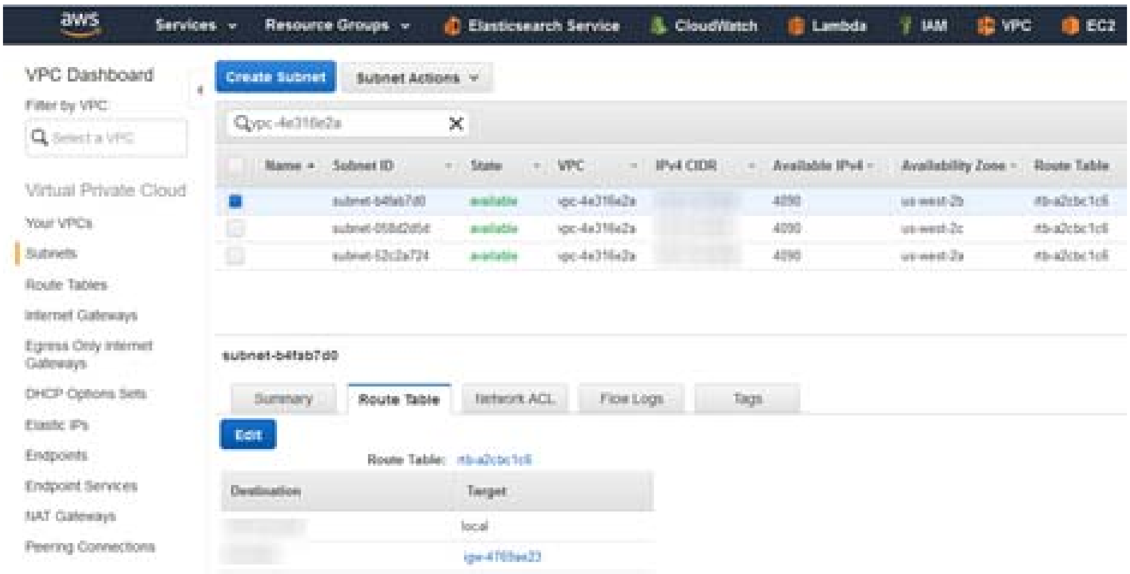
Propagate Route Table

Enabling propagation to the Route Table: rtb-a2cbc1c6 will affect all other VPN connections to the VPC: vpc-4e316e2a and not just those via this firewall.

Are you sure you want to continue?

- On the AWS Console

  The subnets for each VPC can be viewed on the subnets page under the VPC Dashboard on the AWS Console. Selecting a subnet identifies the governing route table and provides a hyperlink so that you can jump to the relevant page.



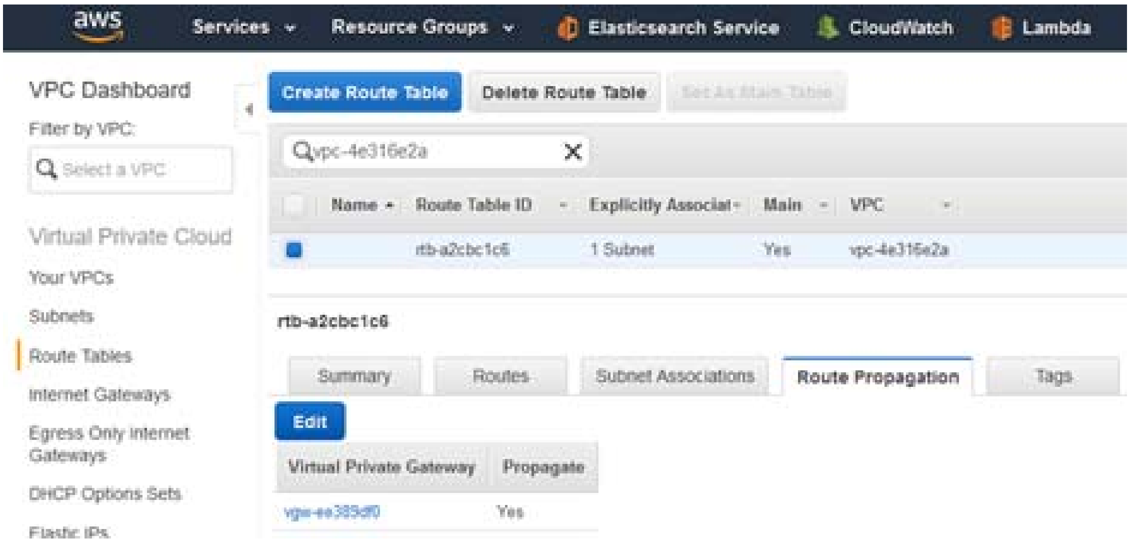
	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	Availability Zone	Route Table
■		subnet-b4fab7d0	available	vpc-4e316e2a	[redacted]	4090	us-west-2b	rtb-a2cbc1c6
□		subnet-058d2d5d	available	vpc-4e316e2a	[redacted]	4090	us-west-2c	rtb-a2cbc1c6
□		subnet-52c2a724	available	vpc-4e316e2a	[redacted]	4090	us-west-2a	rtb-a2cbc1c6

subnet-b4fab7d0

Route Table: rtb-a2cbc1c6

Destination	Target
[redacted]	local
[redacted]	igw-4769ae23

Otherwise, you can navigate to the Route Table page and use the filter to narrow the search by VPC or subnet.



	Name	Route Table ID	Explicitly Associat	Main	VPC
■		rtb-a2cbc1c6	1 Subnet	Yes	vpc-4e316e2a

rtb-a2cbc1c6

Virtual Private Gateway	Propagate
vgw-ee385df0	Yes

To enable or disable route propagation to a specific route table:

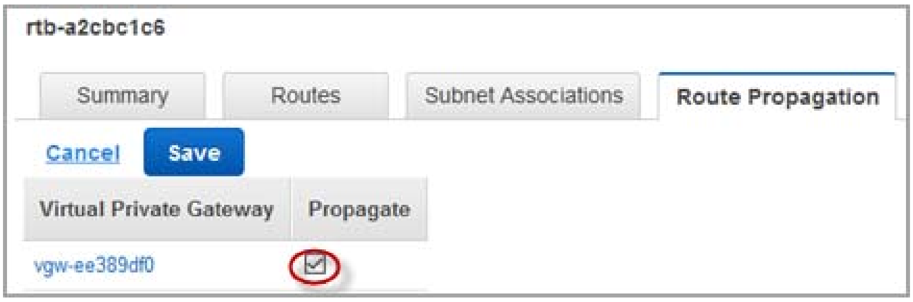
1 Select the route table in question.

2 Click on the **Route Propagation** tab.

3 Click ***Edit***.

4 Check or uncheck the **Propagate** box as appropriate.

5 Click **Save** to commit your changes.

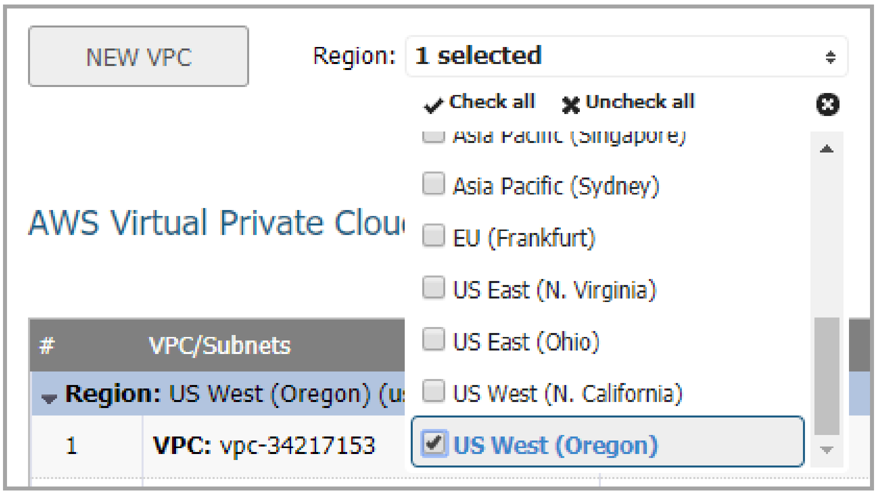


Virtual Private Gateway: vgw-ee389df0, Propagate: ☑

AWS Regions

Resources on Amazon Web Services are distributed across a number of AWS regions. A customer can have VPCs in any or all regions. The AWS VPN page includes a drop-down control allowing you to select one or more regions of interest. The VPCs from all selected regions are displayed in the table and new VPN connections can be made to any of those VPCs.

The region selection control is initialized with the default region as specified on the AWS configuration and is used to send firewall logs to AWS CloudWatch Logs on the AWS Logs page. Regardless of the initial selection, you can choose which regions from which to show the associated VPCs in the table.



Region: 1 selected

□ Asia Pacific (Singapore)
□ Asia Pacific (Sydney)
□ EU (Frankfurt)
□ US East (N. Virginia)
□ US East (Ohio)
□ US West (N. California)
☑ US West (Oregon)

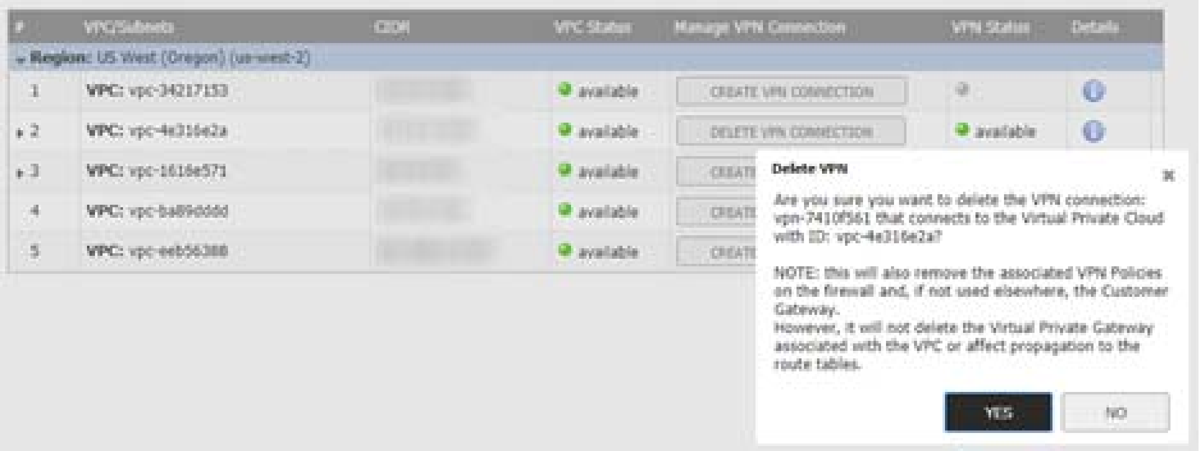
Region: US West (Oregon) (u

1 VPC: vpc-34217153

Deleting VPN Connections

The AWS VPN page includes a facility for removing unwanted VPN Connections.

For VPCs that have a corresponding VPN Connection, the button in the related table row in the VPC table changes from a **Create VPN Connection** function to **Delete VPN Connection**. After clicking the button, the system asks for confirmation and then initiates a process that deletes as many configuration settings as it safe to do without affecting other VPN connections from this or other firewalls. It removes the associated VPN and route policies, and the tunnel interfaces on the firewall. On AWS, it removes the Customer Gateway, but only if it is not being used elsewhere (perhaps on other VPN Connections from the same firewall but to other VPCs). It does not delete the VPN gateway or change the route propagation settings.



#	VPC/Subnets	CIDR	VPC Status	Manage VPN Connection	VPN Status	Details
Region: US West (Oregon) (us-west-2)						
1	**VPC:** vpc-34217153	[redacted]	● available	CREATE VPN CONNECTION	●	ⓘ
▸ 2	**VPC:** vpc-4e316e2a	[redacted]	● available	DELETE VPN CONNECTION	● available	ⓘ
▸ 3	**VPC:** vpc-1616e571	[redacted]	● available	CREATE		
4	**VPC:** vpc-ba89dddd	[redacted]	● available	CREATE		
5	**VPC:** vpc-eeb56388	[redacted]	● available	CREATE		

Delete VPN

Are you sure you want to delete the VPN connection: vpn-7410f561 that connects to the Virtual Private Cloud with ID: vpc-4e316e2a?

NOTE: this will also remove the associated VPN Policies on the firewall and, if not used elsewhere, the Customer Gateway.
However, it will not delete the Virtual Private Gateway associated with the VPC or affect propagation to the route tables.

Part 2

Connectivity | SSL VPN

- About SSL VPN
- Configuring SSL VPN Server Behavior
- Configuring SSL VPN Client Settings
- Configuring the SSL VPN Web Portal
- Configuring Virtual Office

9

About SSL VPN

This section provides information on how to configure the SSL VPN features on the SonicWall network security appliance. SonicWall's SSL VPN features provide secure remote access to the network using the NetExtender client.

NetExtender is an SSL VPN client for Windows, Mac, or Linux users that is downloaded transparently. It allows you to run any application securely on the network and uses Point-to-Point Protocol (PPP). NetExtender allows remote clients seamless access to resources on your local network. Users can access NetExtender two ways:

- Logging in to the Virtual Office web portal provided by the SonicWall network security appliance
- Launching the standalone NetExtender client

Each SonicWall appliance supports a maximum number of concurrent remote users. Refer to the the Maximum number of concurrent SSL VPN users table for details.

Maximum number of concurrent SSL VPN users

SonicWall appliance model	Maximum concurrent SSL VPN connections	SonicWall appliance model	Maximum concurrent SSL VPN connections	SonicWall appliance model	Maximum concurrent SSL VPN connections
NS*a* 9650	3000	SM 9600	3000	TZ600/TZ600P	200
NS*a* 9450	3000	SM 9400	3000		
NS*a* 9250	3000	SM 9200	3000	TZ500/TZ500 W	150
NS*a* 6650	2000	NSA 6600	1500	TZ400/TZ400 W	100
NS*a* 5650	1500	NSA 5600	1000	TZ300/TZ300 W/TZ300P	50
NS*a* 4650	1000	NSA 4600	500		
NS*a* 3650	500	NSA 3600	350	SOHO W	10
NS*a* 2650	350	NSA 2600	250		
SOHO 250	25				
SOHO 250W	25				
TZ350	75				
TZ350W	75				

SonicOS supports NetExtender connections for users with IPv6 addresses. The address objects drop-down menu includes all the predefined IPv6 address objects.

ⓘ **NOTE:** IPv6 Wins Server is *not* supported. IPv6 FQDN *is* supported.

ⓘ **NOTE:** In SonicOS 6.5.3 and higher, **SSL VPN** connectivity is available when **Wireless Controller Mode** on the **MANAGE | System Setup | Appliance > Base Settings** page is set to either **Full-Feature-Gateway** or **Non-Wireless**. If **Wireless-Controller-Only** is enabled for **Wireless Controller Mode**, **SSL VPN** interfaces are ***not*** available, **SSL VPN > Server Settings > SSL VPN Status on Zones** displays inactive status for all zones, and **SSL VPN** zones are not editable. See the *SonicOS 6.5 System Setup* administration documentation for more information.

Topics:

- About NetExtender
- Configuring Users for SSL VPN Access
- Biometric Authentication

About NetExtender

SonicWall's SSL VPN NetExtender is a transparent software application for Windows, Mac, and Linux users that enables remote users to securely connect to the company network. With NetExtender, remote users can securely run any application on the company network. Users can upload and download files, mount network drives, and access resources as if they were on the local network.

NetExtender provides remote users with full access to your protected internal network. The experience is virtually identical to that of using a traditional IPsec VPN client, but the NetExtender Windows client is automatically installed on a remote user's PC using the XPCOM plugin when using Firefox. On MacOS systems, supported browsers use Java controls to automatically install NetExtender from the Virtual Office portal. Linux systems can also install and use the NetExtender client. Windows users need to download the client from the portal, and those with mobile devices need to download Mobile Connect from the application store.

The NetExtender standalone client can be installed the first time the user launches NetExtender. Thereafter, it can be accessed directly from the **Start** menu on Windows systems and from the **Application** folder or dock on MacOS systems or by he path name or from the shortcut bar on Linux systems.

After installation, NetExtender automatically launches and connects a virtual adapter for secure SSL VPN, point-to-point access to permitted hosts and subnets on the internal network.

Topics:

- Creating an Address Object for the NetExtender Range
- Setting Up Access
- Configuring Proxies
- Installing the Stand-Alone Client

Creating an Address Object for the NetExtender Range

As a part of the NetExtender configuration, you need to create an address object for the NetExtender IP address range. This address object is then used when configuring the Device Profiles.

You can create address objects for both an IPv4 address range and an IPv6 address range to be used in the **SSL VPN > Client Settings** configuration. The address range configured in the address object defines the IP address pool from which addresses are assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you intend to support. You might want to allow for a few extra addresses for growth, but it is not required.

ⓘ **NOTE:** In cases where other hosts are on the same segment as the appliance, the address range must not overlap or collide with any assigned addresses.

Details for how to configure an address object is provided in *SonicOS 6.5 Policies*, in the **Address Objects** section. Refer to the quick reference that follows for the settings needed to define an SSL address object.

To create an address object for the NetExtender IP address range:

1 Navigate to **MANAGE | Policies | Objects > Address Objects**.

2 Click **Add**.

3 Type a descriptive name in the **Name** field.

4 For **Zone Assignment**, select **SSLVPN**.

5 For **Type**, select **Range**.

6 In the **Starting IP Address** field, type in the lowest IP address in the range you want to use.

> ⓘ **NOTE:** The IP address range must be on the same subnet as the interface used for SSL VPN services.

7 In the **Ending IP Address** field, type in the highest IP address in the range you want to use.

8 Click **ADD**.

9 Click **CLOSE**.

Setting Up Access

NetExtender client routes are used to allow and deny access for SSL VPN users to various network resources. Address objects are used to easily and dynamically configure access to network resources. **Tunnel All** mode routes all traffic to and from the remote user over the SSL VPN NetExtender tunnel—including traffic destined for the remote user’s local network. This is done by adding the following routes to the remote client’s route table:

Routes to be Added to Remote Client’s Route Table

IP Address	Subnet mask
`0.0.0.0`	`0.0.0.0`
`0.0.0.0`	`128.0.0.0`
`128.0.0.0`	`128.0.0.0`

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user is has the IP address `10.0.67.64` on the `10.0.*.*` network, the route `10.0.0.0/255.255.0.0` is added to route traffic through the SSL VPN tunnel.

ⓘ **NOTE:** To configure **Tunnel All** mode, you must also configure an address object for `0.0.0.0`, and assign SSL VPN NetExtender users and groups to have access to this address object.

Administrators also have the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or Web sites. NetExtender Connection Scripts can support any valid batch file commands.

Configuring Proxies

SonicWall SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal and if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings. The proxy settings can also be manually configured in the NetExtender client preferences. NetExtender can automatically detect proxy settings for proxy servers that support the Web Proxy Auto Discovery (WPAD) Protocol.

NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, you can select this option and provide the URL of the script.
- **Use proxy server** - You can use this option to specify the IP address and port of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses and bypass the proxy server. If required, you can enter a user name and password for the proxy server. If the proxy server requires a username and password, but you do not specify them, a NetExtender pop-up window prompts you to enter them when you first connect.

When NetExtender connects using proxy settings, it establishes an HTTPS connection to the proxy server instead of connecting to the firewall server directly. The proxy server then forwards traffic to the SSL VPN server. All traffic is encrypted by SSL with the certificate negotiated by NetExtender, of which the proxy server has no knowledge. The connecting process is identical for proxy and non-proxy users.

Installing the Stand-Alone Client

The first time a user launches NetExtender, the NetExtender stand-alone client is automatically installed on the user’s PC or Mac, or the installer can be downloaded and run on the user’s system. The installer creates a profile based on the user’s login information. The installer window then closes and automatically launches NetExtender. If the user has a legacy version of NetExtender installed, the installer uninstalls or requests the user to uninstall the old NetExtender first and then can install the new version.

After the NetExtender stand-alone client has been installed, Windows users can launch NetExtender from their PC’s **Start > Programs** menu or system tray and can configure NetExtender to launch when Windows boots. Mac users can launch NetExtender from their system **Applications** folder, or drag the icon to the dock for quick access. On Linux systems, the installer creates a desktop shortcut in **/usr/share/NetExtender**. This can be dragged to the shortcut bar in environments like Gnome and KDE.

Configuring Users for SSL VPN Access

For users to be able to access SSL VPN services, they must be assigned to the **SSLVPN Services** group. Users attempting to login through the Virtual Office and who do not belong to the **SSLVPN Services** group are denied access.

Topics:

- For Local Users
- For RADIUS and LDAP Users
- For Tunnel All Mode Access

For Local Users

The detailed process for adding and configuring local users and groups is described in *SonicOS 6.5 System Setup*, in the **Users** section. The following is a quick reference, listing the User settings needed to enable SSLVPN Services.

To configure SSL VPN access for local users:

1. Navigate to **MANAGE | System Setup | Users > Local Users & Groups**.
2. Click the **Edit** icon for the user you want to set up, or click **Add User** to create a new user.
3. Select **Groups**.
4. In the **User Groups** column, select **SSLVPN Services** and click the **Right Arrow** to move it to the **Member Of** column.
5. Select **VPN Access** and move the appropriate network resources VPN users (GVC, NetExtender, or Virtual Office bookmarks) to the **Access List**.

   ⓘ **NOTE:** The **VPN Access** settings affect the ability of remote clients using GVC, NetExtender, or SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the **Access List** on **VPN Access**.

6. Click **OK**.

For RADIUS and LDAP Users

The procedure for configuring RADIUS user and LDAP users is similar. You need to add the users to the SSLVPN Services user group.

The detailed process for configuring user groups is described in *SonicOS 6.5 System Setup*, in the **Users** section. The following is a quick reference, listing the User settings needed to add users to the right group.

To configure SSL VPN access for RADIUS and LDAP users:

Common Steps	Setting Up RADIUS Users	Setting Up LDAP Users
1 Select the **MANAGE** view.		
2 Navigate to **Users > Settings**.		
3 Select **Authentication**.		
4 In the **User authentication method** field:	Select **RADIUS** or **RADIUS + Local Users**.	Select **LDAP** or **LDAP + Local Users**.
5 Select:	**CONFIGURE RADIUS**	**CONFIGURE LDAP**
6 Select:	**RADIUS Users**	**Users & Groups**

Common Steps	Setting Up RADIUS Users	Setting Up LDAP Users
7 Select **SSLVPN Services** in the appropriate field:	**Default user group to which all RADIUS users belong**	**Default LDAP User Group**
8 Click **OK**.		

For Tunnel All Mode Access

The detailed process for adding and configuring local users and groups is described in *SonicOS 6.5 System Setup*, in the **Users** section. The following is a quick reference, listing the User settings needed to set up users and groups for **Tunnel All** mode.

To configure SSL VPN NetExtender users and groups for Tunnel All Mode:

1. Navigate to **MANAGE | System Setup | Users > Local Users & Groups**.
2. Click the **Configure** icon for an SSL VPN NetExtender user or group.
3. Select **VPN Access**.
4. Select the **WAN RemoteAccess Networks** address object and click **Right Arrow** to move it to the **Access List**.
5. Click **OK**.
6. Repeat the processes for all local users and groups that use SSL VPN NetExtender.

Biometric Authentication

ⓘ **IMPORTANT:** To use biometric authentication, Mobile Connect 4.0 or higher must be installed on the mobile device and configured to connect with the firewall.

SonicOS supports biometric authentication in conjunction with SonicWall Mobile Connect. Mobile Connect is an application that allows users to securely access private networks from a mobile device. With Mobile Connect 4.0 you can use finger-touch for authentication as a substitute for username and password.

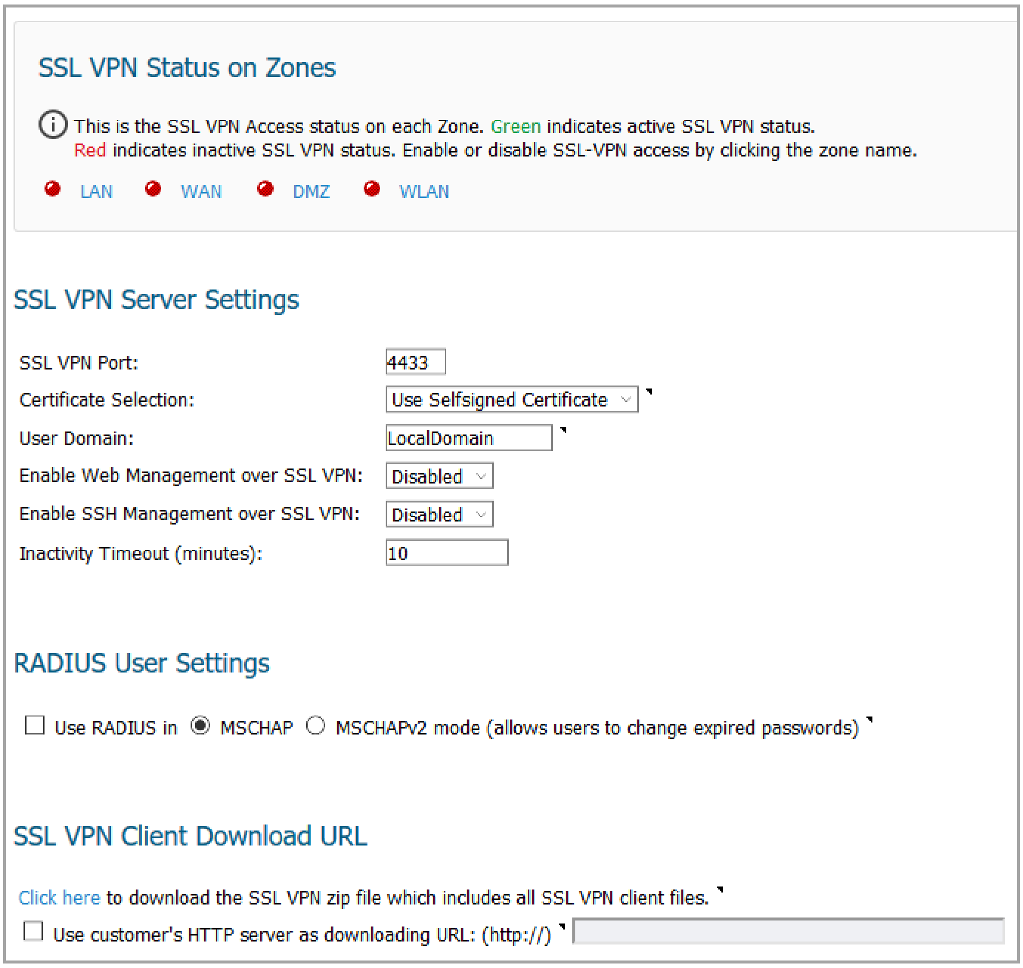
The configuration settings to allow this method of authentication are on the **SSL VPN > Client Settings** page. These options only show when Mobile Connect is used to connect to the firewall.

After configuring biometric authentication on the **SSL VPN > Client Settings** page, Touch ID (iOS) or Fingerprint Authentication (Android) need to be enabled on the user’s smart phone or other mobile device.

10

Configuring SSL VPN Server Behavior

The **SSL VPN > Server Settings** page configures firewall to act as an SSL VPN server.



SSL VPN Status on Zones

ⓘ This is the SSL VPN Access status on each Zone. Green indicates active SSL VPN status.
Red indicates inactive SSL VPN status. Enable or disable SSL-VPN access by clicking the zone name.

● LAN ● WAN ● DMZ ● WLAN

SSL VPN Server Settings

SSL VPN Port:	4433
Certificate Selection:	Use Selfsigned Certificate
User Domain:	LocalDomain
Enable Web Management over SSL VPN:	Disabled
Enable SSH Management over SSL VPN:	Disabled
Inactivity Timeout (minutes):	10

RADIUS User Settings

□ Use RADIUS in ● MSCHAP ○ MSCHAPv2 mode (allows users to change expired passwords)

SSL VPN Client Download URL

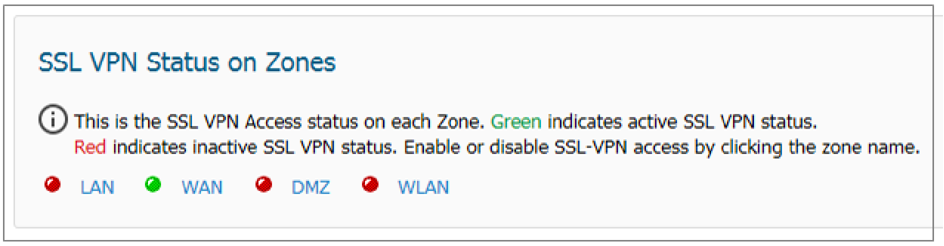
Click here to download the SSL VPN zip file which includes all SSL VPN client files.

□ Use customer's HTTP server as downloading URL: (http://)

Topics:

- SSL VPN Status on Zones
- SSL VPN Server Settings
- RADIUS User Settings
- SSL VPN Client Download URL

SSL VPN Status on Zones



SSL VPN Status on Zones

ⓘ This is the SSL VPN Access status on each Zone. Green indicates active SSL VPN status. Red indicates inactive SSL VPN status. Enable or disable SSL-VPN access by clicking the zone name.

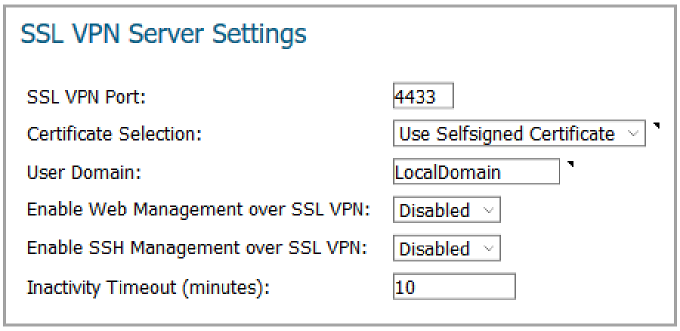
🔴 LAN 🟢 WAN 🔴 DMZ 🔴 WLAN

This section displays the SSL VPN Access status on each zone:

- Green indicates active SSL VPN status.
- Red indicates inactive SSL VPN status.

Enable or disable SSL VPN access by clicking the zone name.

SSL VPN Server Settings



SSL VPN Server Settings

SSL VPN Port:	4433
Certificate Selection:	Use Selfsigned Certificate
User Domain:	LocalDomain
Enable Web Management over SSL VPN:	Disabled
Enable SSH Management over SSL VPN:	Disabled
Inactivity Timeout (minutes):	10

To configure the SSL VPN server settings:

1. **SSL VPN Port** – Enter the SSL VPN port number in the field. The default is **4433**.
2. **Certificate Selection** – From this drop-down menu, select the certificate that used to authenticate SSL VPN users. The default method is **Use Selfsigned Certificate**.
3. **User Domain** – Enter the user’s domain, which must match the domain field in the NetExtender client. The default is **LocalDomain**.

   > ⓘ **NOTE:** If authentication partitioning is not being used, this field has to match with the domain field in the NetExtender Client.
   >
   > If authentication partitioning is being used, then in NetExtender, the user can enter any of the domain names configured with the partitions, for this reason, selecting the partition for authenticating their name/password externally through RADIUS or LDAP. In this case, the name set here is a default for the user to enter for local authentication, or if they have no local account, for authentication in the default partition.
   >
   > Note that in either case, when used with external authentication, this user domain name is not passed to the RADIUS/LDAP server, sending just the simple user name without it.

4. **Enable Web Management over SSL VPN** – To enable web management over SSL VPN, select **Enabled** from this drop-down menu. The default is **Disabled**.

5 **Enable SSH Management over SSL VPN** – To enable SSH management over SSL VPN, select **Enabled** from this drop-down menu. The default is **Disabled**.

6 **Inactivity Timeout (minutes)** – Enter the number of minutes of inactivity before logging out the user. The default is **10** minutes.

7 Click **ACCEPT** at the bottom of the page.

RADIUS User Settings

This section is available only when either RADIUS or LDAP is configured to authenticate SSL VPN users on the **MANAGE | System Setup | Users > Settings** page. Enabling MSCHAP mode for RADIUS allows users to change expired passwords when they log in.

To configure MSCHAP or MSCHAPv2 mode:

1 Select **Use RADIUS in**.

2 Select one of these two modes:

- **MSCHAP**
- **MSCHAPV2**

> **NOTE:** In LDAP, passwords can only be changed when using either Active Directory with TLS and binding to it using an administrative account or when using Novell eDirectory.
>
> If this option is set when LDAP is selected as the authentication method of login on the **Users > Settings** page, but LDAP is not configured in a way that allows password updates, then password updates for SSL VPN users are performed using MSCHAP-mode RADIUS after using LDAP to authenticate the user.

3 Click **ACCEPT** at the bottom of the page.

SSL VPN Client Download URL

In this section of the page, you set up where the client system downloads the SSL VPN client from. You can download the files from the appliance and put them on your web server to provide your own server to host this client package. Otherwise, clients can download the SSL VPN files from the firewall.

To configure your own web server for SSL VPN client file downloads:

1 Select the link in **Click here to download the SSL VPN zip file which includes all SSL VPN client files** to download all the client SSL VPN files from the appliance. Open and unzip the file, and then put the folder on your HTTP server.

2 Select **Use customer's HTTP server as downloading URL: (http://)** to enter your SSL VPN client download URL in the supplied field.

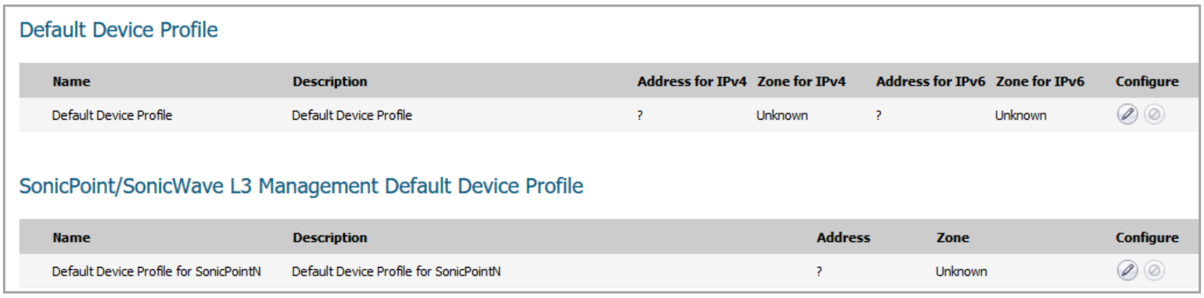
3 Click **ACCEPT**.

11

Configuring SSL VPN Client Settings

On the **SSL VPN > Client Settings** page, you can edit the Default Device Profile and the SonicPoint/SonicWave L3 Management Default Device Profile. The Default Device Profile enables SSL VPN access on zones, configures client routes, and configures the client DNS and NetExtender settings. The SonicPoint/SonicWave L3 Management Default Device Profile contains settings for configuring SSL VPN access, client routes, and the Layer 3 settings for clients connecting through SonicPoint/SonicWave wireless access points.

The **SSL VPN > Client Settings** page also displays the configured IPv4 and IPv6 network addresses and zones that have SSL VPN access enabled.



Default Device Profile

Name	Description	Address for IPv4	Zone for IPv4	Address for IPv6	Zone for IPv6	Configure
Default Device Profile	Default Device Profile	?	Unknown	?	Unknown	✎ ⊘

SonicPoint/SonicWave L3 Management Default Device Profile

Name	Description	Address	Zone	Configure
Default Device Profile for SonicPointN	Default Device Profile for SonicPointN	?	Unknown	✎ ⊘

Topics:

- Configuring the Default Device Profile
- Configuring Device Profile Settings for IPv6
- Configuring the SonicPoint/SonicWave L3 Management Default Device Profile

Configuring the Default Device Profile

Edit the Default Device Profile to select the zones and NetExtender address objects, configure client routes, and configure the client DNS and NetExtender settings.

SSL VPN access must be enabled on a zone before users can access the Virtual Office web portal. SSL VPN Access can be configured on the **MANAGE | System Setup | Network > Zones** page. Refer to the *SonicOS 6.5 System Setup* administration documentation in the Network section for more information.

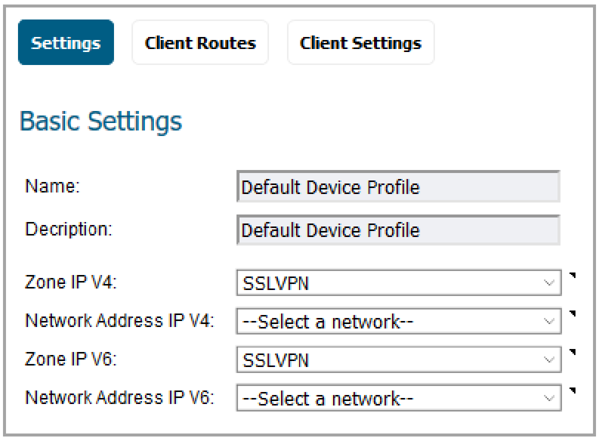
Topics:

- Configuring the Settings Options
- Configuring the Client Routes
- Configuring Client Settings

Configuring the Settings Options

To configure the Settings options for the Default Device Profile:

1. Navigate to the **MANAGE | Connectivity | SSL VPN > Client Settings** page.
2. Click the **Edit** icon for the **Default Device Profile**.



Basic Settings

Name: Default Device Profile

Decription: Default Device Profile

Zone IP V4: SSLVPN

Network Address IP V4: --Select a network--

Zone IP V6: SSLVPN

Network Address IP V6: --Select a network--

> **NOTE:** The **Name** and **Description** of the **Default Device Profile** cannot be changed.

3. In the **Zone IP V4** drop-down menu, choose **SSLVPN** or a custom zone to set the zone binding for this profile.
4. From the **Network Address IP V4** drop-down menu, select the IPv4 NetExtender address object that you created for this profile. Refer to Creating an Address Object for the NetExtender Range for instructions. This setting selects the IP Pool and zone binding for this profile. The NetExtender client gets the IP address from this address object if it matches this profile.
5. In the **Zone IP V6** drop-down menu, choose **SSLVPN** or a custom zone to set the zone binding for this profile.
6. From the **Network Address IP V6** drop-down menu, select the IPv6 NetExtender address object that you created.
7. Click **OK** to save settings and close the window or proceed to Configuring the Client Routes on page 130.

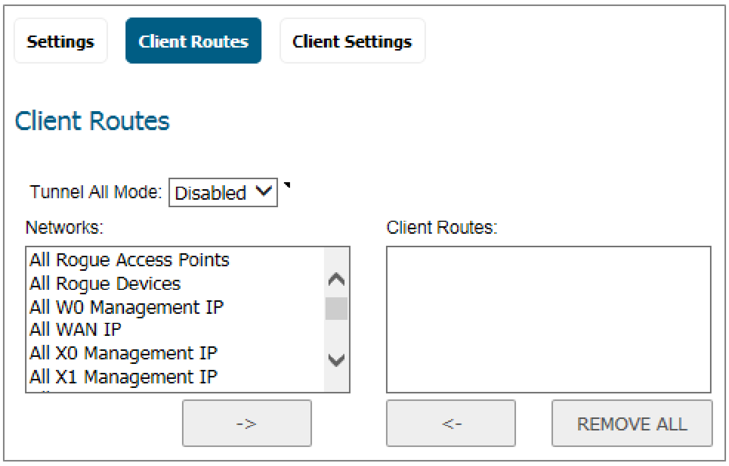
Configuring the Client Routes

On **Client Routes**, you can control the network access allowed for SSL VPN users. The NetExtender client routes are passed to all NetExtender clients and are used to govern which private networks and resources remote users can access third-party the SSL VPN connection.

To configure the client routes:

1. Navigate to the **MANAGE | Connectivity | SSL VPN > Client Settings** page.
2. Click the **Edit** icon for the **Default Device Profile**.

3 Select **Client Routes**.



4 To force all traffic for NetExtender users over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network, select **Enabled** from the **Tunnel All Mode** drop-down menu.

5 Under **Networks**, select the address object to which you want to allow SSL VPN access.

6 Click the **Right Arrow** to move the address object to the **Client Routes** list.

7 Repeat until you have moved all the address objects you want to use for Client Routes.

Creating client routes also creates access rules automatically. You can also manually configure access rules for the SSL VPN zone. Refer to *SonicOS 6.5 Policies* for details about access rules.

8 Click **OK** to save the settings and close the window or proceed to Configuring Client Settings on page 131.

Configuring Client Settings

The Client Settings screen has two sections containing options:

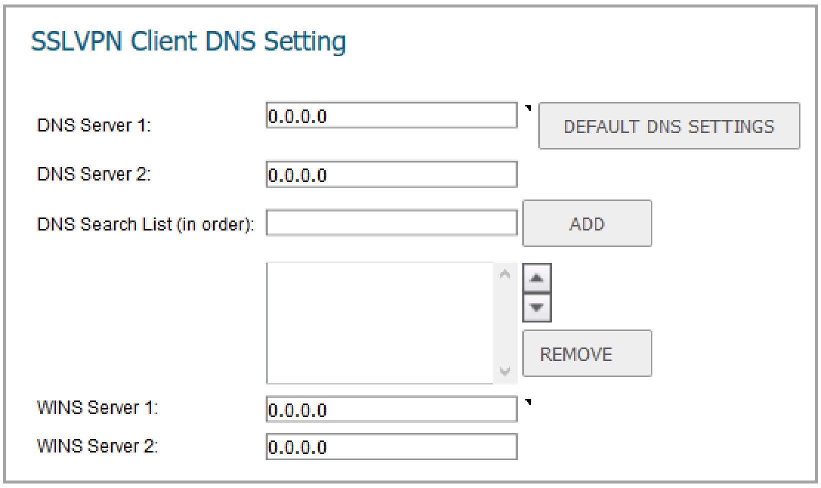
- SSLVPN Client DNS Setting
- NetExtender Client Settings

To configure SSLVPN Client DNS Settings:

1 Navigate to the **MANAGE | Connectivity | SSL VPN > Client Settings** page.

2 Click the **Edit** icon for the **Default Device Profile**.

3 Select **Client Settings**. The top of the screen displays the **SSLVPN Client DNS Setting** section.



SSLVPN Client DNS Setting

DNS Server 1: 0.0.0.0

DNS Server 2: 0.0.0.0

DNS Search List (in order):

WINS Server 1: 0.0.0.0

WINS Server 2: 0.0.0.0

4 In the **DNS Server 1** field, do one of the following:

- Enter the IP address of the primary DNS server.
- Click **DEFAULT DNS SETTINGS** to use the default settings for both the **DNS Server 1** and **DNS Server 2** fields. The fields are populated automatically.

NOTE: Both IPv4 and IPv6 are supported.

5 (Optional) In the **DNS Server 2** field, if you did not click **Default DNS Settings**, enter the IP address of the backup DNS server.

6 (Optional) To build a **DNS Search List**:

a In the **DNS Search List (in order)** field, enter the IP address for a DNS server.

b Click **ADD** to add it to the list below.

c Repeat as many times as necessary.

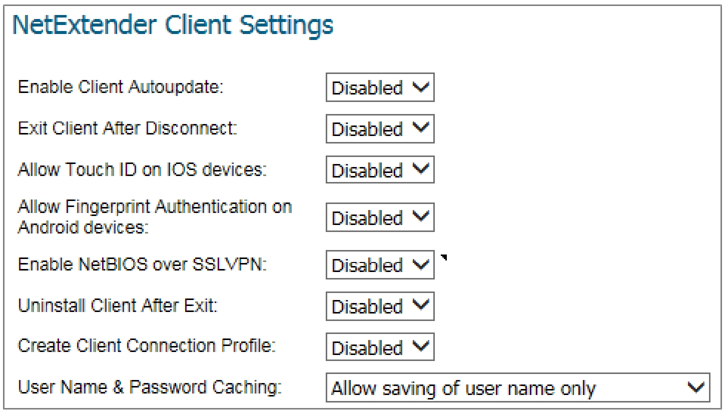
To reorder the list, select one of the addresses and then use the up and down arrow buttons to reposition it. To remove an address from the list, select it and click **REMOVE**.

7 (Optional) In the **WINS Server 1** field, enter the IP address of the primary WINS server.

NOTE: Only IPv4 is supported.

8 (Optional) In the **WINS Server 2** field, enter the IP address of the backup WINS server.

9 To customize the behavior of NetExtender when users connect and disconnect, scroll down to **NetExtender Client Settings**.



NetExtender Client Settings

Enable Client Autoupdate: Disabled

Exit Client After Disconnect: Disabled

Allow Touch ID on IOS devices: Disabled

Allow Fingerprint Authentication on Android devices: Disabled

Enable NetBIOS over SSLVPN: Disabled

Uninstall Client After Exit: Disabled

Create Client Connection Profile: Disabled

User Name & Password Caching: Allow saving of user name only

10 Select **Enabled** or **Disabled** for each of the following settings. By default, all are set to **Disabled**.

NetExtender Client Settings	Definition
Enable Client Autoupdate	The NetExtender client checks for updates every time it is launched.
Exit Client After Disconnect	The NetExtender client exits when it becomes disconnected from the SSL VPN server. To reconnect, users have to either return to the SSL VPN portal or launch the NetExtender client on their local system.
Allow Touch ID on IOS devices	The NetExtender client allows Touch ID authentication on IOS smart phones.
Allow Fingerprint Authentication on Android devices	The NetExtender client allows fingerprint authentication on Android devices.
Enable NetBIOS over SSL VPN	The NetExtender client allows NetBIOS protocol.
Uninstall Client After Exit	The NetExtender client uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users have to return to the SSL VPN portal.
Create Client Connection Profile	The NetExtender client creates a connection profile recording the SSL VPN Server name, the Domain name, and optionally the username and password.

11 To provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client, select one of these actions from the **User Name & Password Caching** field. These options enable you to balance security needs against ease of use for users.

- **Allow saving of user name only**
- **Allow saving of user name & password**
- **Prohibit saving of user name & password**

12 Click **OK**.

Configuring Device Profile Settings for IPv6

SonicOS supports NetExtender connections for users with IPv6 addresses. On the **SSL VPN > Client Settings** page, first configure the traditional IPv4 IP address pool, and then configure an IPv6 IP Pool. Clients are assigned two internal addresses: one IPv4 and one IPv6.

ⓘ | **NOTE:** IPv6 Wins Server is not supported.

On the **SSL VPN > Client Routes** page, you can select client routes from the drop-down menu of all address objects including all the predefined IPv6 address objects.

ⓘ | **NOTE:** IPv6 FQDN is supported.

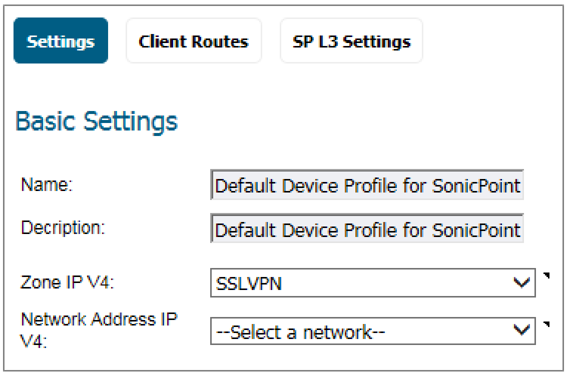
Configuring the SonicPoint/SonicWave L3 Management Default Device Profile

This section describes how to configure SSL VPN access, client routes, and the Layer 3 settings for clients connecting third-party SonicPoint/SonicWave wireless access points.

To configure the settings for the SonicPoint L3 profile:

1 Navigate to the **MANAGE | Connectivity | SSL VPN > Client Settings** page.

2 Under **SonicPoint/SonicWave L3 Management Default Device Profile**, click the **Edit** icon for **Default Device Profile for SonicPointN**.



Basic Settings

Name: Default Device Profile for SonicPoint

Decription: Default Device Profile for SonicPoint

Zone IP V4: SSLVPN

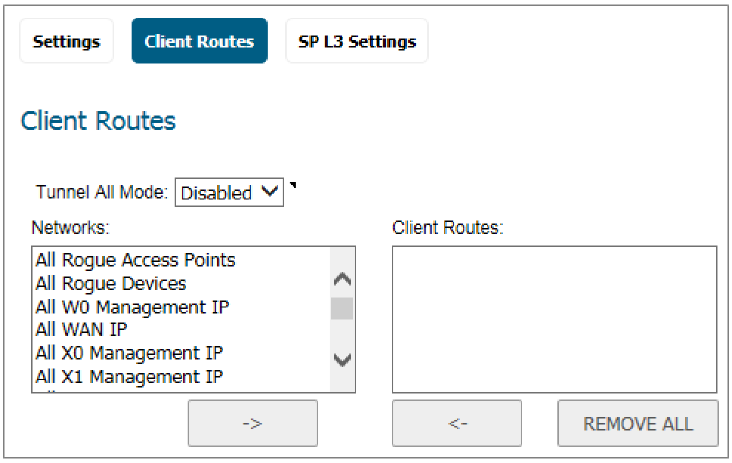
Network Address IP V4: --Select a network--

ⓘ | **NOTE:** The **Name** and **Description** cannot be changed.

3 On the **Settings** screen, select **SSLVPN** or a custom zone from the **Zone IP V4** drop-down menu to set up the zone binding for this profile.

4 For **Network Address IP V4** drop-down menu, select the IPv4 NetExtender address object that you created or select **Create new network** to create one now. Refer to Creating an Address Object for the NetExtender Range on page 121 for instructions. This setting selects the IP Pool and zone binding for this profile. The NetExtender client gets the IP address from this address object if it matches this profile.

5 Click **Client Routes**.



Client Routes

Tunnel All Mode: Disabled

Networks:
All Rogue Access Points
All Rogue Devices
All W0 Management IP
All WAN IP
All X0 Management IP
All X1 Management IP

Client Routes:

6 To force all traffic for NetExtender users over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network, select **Enabled** from the **Tunnel All Mode** drop-down menu.

7 From the **Networks** list, select the address object for which you want to allow SSL VPN access.

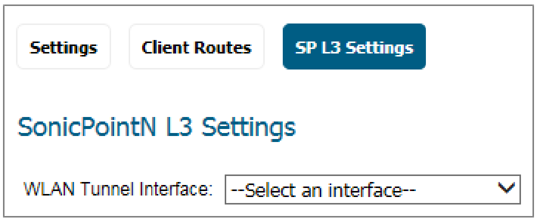
8 Click the **Right Arrow** to move the address object to the **Client Routes** list.

9 Repeat until you have moved all the address objects you want to use for Client Routes.

Creating client routes causes access rules allowing this access to be created automatically. You can also manually configure access rules for the SSL VPN zone on the **MANAGE | Policies | Rules > Access Rules** page. Refer to *SonicOS 6.5 Policies* for details about access rules.

> ⓘ **NOTE:** After configuring Client Routes for SSL VPN, you must also configure all SSL VPN NetExtender users and user groups to be able to access the Client Routes. Refer to Configuring Users for SSL VPN Access on page 123 for a quick reference list.

10 Click **SP L3 Settings**.



SonicPointN L3 Settings

WLAN Tunnel Interface: --Select an interface--

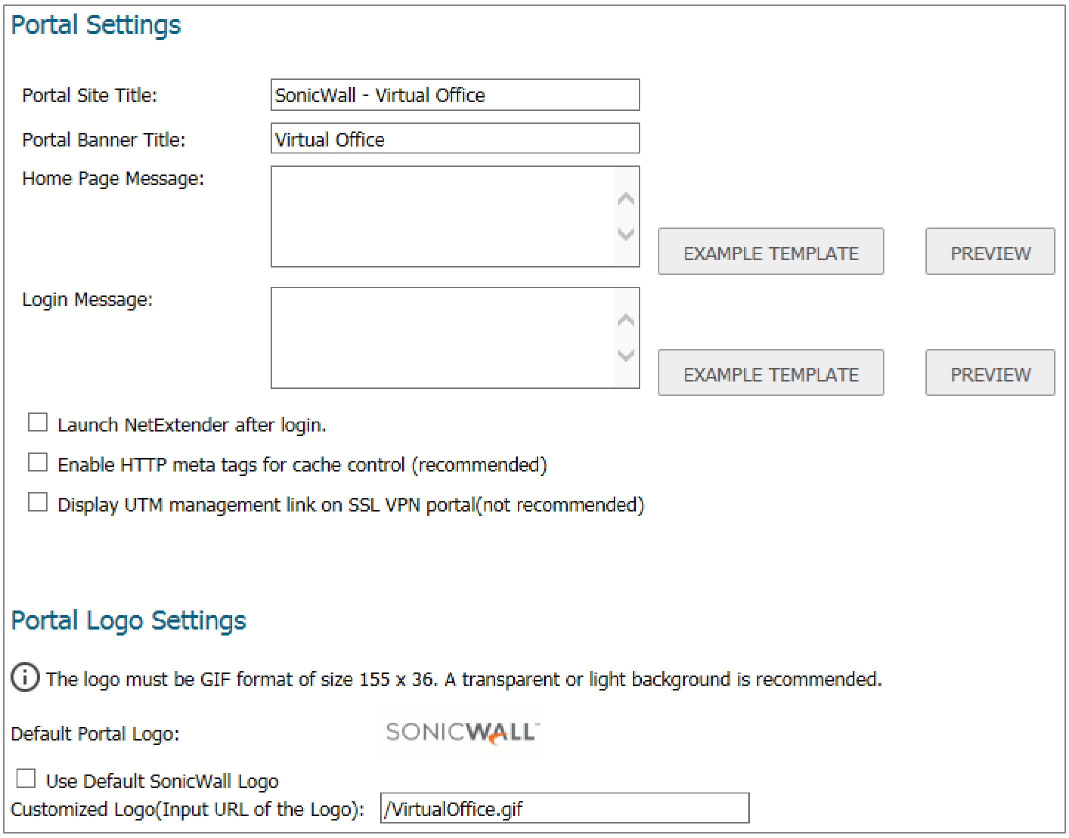
11 Select an interface from the **WLAN Tunnel Interface** drop-down menu. The WLAN Tunnel Interface must already be configured. You can configure it by selecting **WLAN Tunnel Interface** in the **Add Interface** field on the **MANAGE | System Setup | Network > Interfaces** page. See *SonicOS 6.5 System Setup* for more information.

12 Click **OK**.

12

Configuring the SSL VPN Web Portal

On the **SSL VPN > Portal Settings** page, you configure the appearance and functionality of the SSL VPN Virtual Office web portal. The Virtual Office portal is the website where users log in to launch NetExtender or access internal resources by clicking Bookmarks. It can be customized to match any existing company website or design style.



Portal Settings

Portal Site Title:	SonicWall - Virtual Office
Portal Banner Title:	Virtual Office
Home Page Message:	
Login Message:	

□ Launch NetExtender after login.

□ Enable HTTP meta tags for cache control (recommended)

□ Display UTM management link on SSL VPN portal(not recommended)

Portal Logo Settings

ⓘ The logo must be GIF format of size 155 x 36. A transparent or light background is recommended.

Default Portal Logo: SONICWALL

□ Use Default SonicWall Logo

Customized Logo(Input URL of the Logo): /VirtualOffice.gif

Topics:

- Portal Settings
- Portal Logo Settings

Portal Settings

The portal settings customize what the user sees when attempting to log in. Configure the options as needed to match your company's requirements.

Option	Definition
Portal Site Title	Enter the text to display as the top title of the portal page in this field. The default is **SonicWall - Virtual Office**.
Portal Banner Title	Enter the text to display next to the logo at the top of the page in this field. The default is **Virtual Office**.
Home Page Message	Enter the HTML code for the message to display above the NetExtender icon. Type your own text or click **EXAMPLE TEMPLATE** to populate the field with a default template that you can keep or edit. Click **PREVIEW** to see what the Home Page Message looks like.
Login Message	Enter the HTML code for the message to display when users are prompted to log into the Virtual Office. Type your own text or click **EXAMPLE TEMPLATE** to populate the field with a default template that you can keep or edit. Click **PREVIEW** to see what the Login Message looks like.

The following options customize the functionality of the Virtual Office portal:

- **Launch NetExtender after login** - Select to launch NetExtender automatically after a user logs in. This option is not selected by default.
- **Display Import Certificate Button** - Select to display an **Import Certificate** button on the Virtual Office page. This initiates the process of importing the firewall's self-signed certificate onto the web browser. This option is not selected by default.

  ⓘ **NOTE:** This option only applies to the Internet Explorer browser on PCs running Windows when **Use Selfsigned Certificate** is selected from the **Certificate Selection** drop-down menu on the **SSL VPN > Server Settings** page.

- **Enable HTTP meta tags for cache control recommended)** - Select to insert into the browser HTTP tags that instruct the web browser not to cache the Virtual Office page. This option is not selected by default.

  ⓘ **NOTE:** SonicWall recommends enabling this option.

- **Display UTM management link on SSL VPN portal (not recommended)** – Select to display the SonicWall appliance's management link on the SSL VPN portal. This option is not selected by default.

  ⓘ **IMPORTANT:** SonicWall does not recommend enabling this option.

Portal Logo Settings

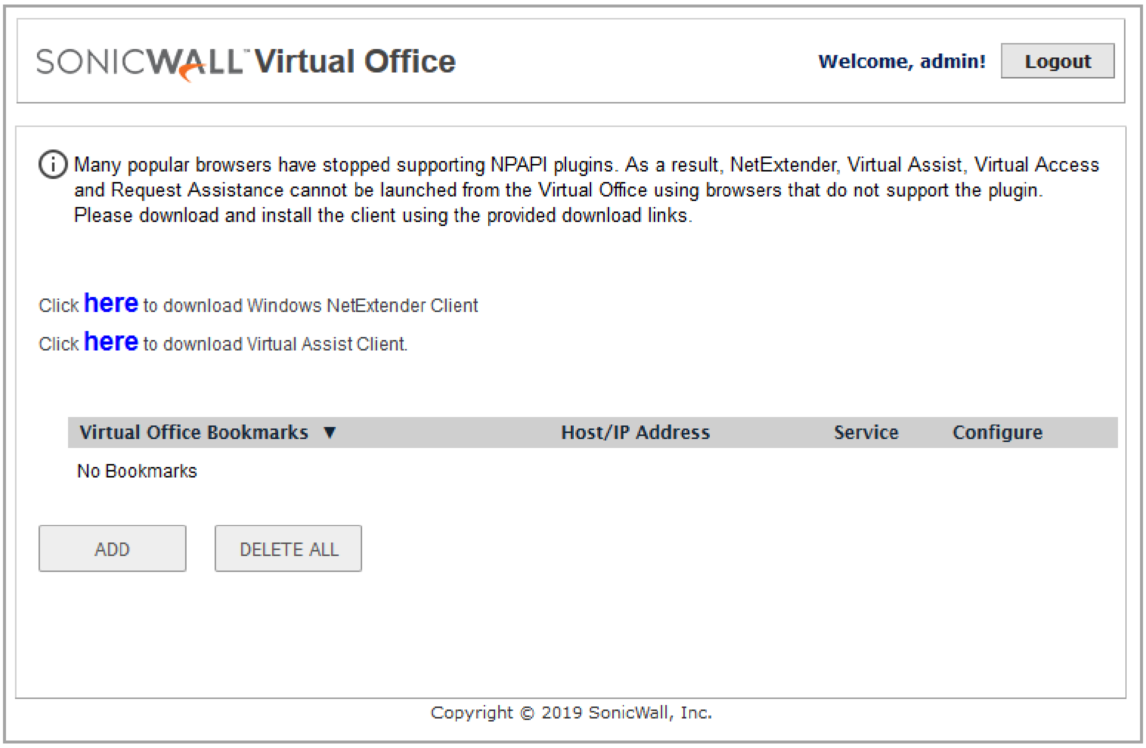
This section describes the settings for configuring the logo displayed at the top of the Virtual Office portal.

- **Default Portal Logo** – Displays the default portal logo which is the SonicWall logo.
- **Use Default SonicWall Logo** – Select this checkbox to use the SonicWall logo supplied with the appliance. This option is not selected by default.
- **Customized Logo (Input URL of the Logo)** — Enter the URL for the logo you want to display.

  ⓘ **TIP:** The logo must be in GIF format of size 155 x 36; a transparent or light background is recommended.

Configuring Virtual Office

The **SSL VPN > Virtual Office** page displays the Virtual Office web portal inside of the SonicOS management interface.



Many popular browsers have stopped supporting NPAPI plugins. As a result, NetExtender, Virtual Assist, Virtual Access and Request Assistance cannot be launched from the Virtual Office using browsers that do not support the plugin. Please download and install the client using the provided download links.

Click **here** to download Windows NetExtender Client

Click **here** to download Virtual Assist Client.

Virtual Office Bookmarks ▼	Host/IP Address	Service	Configure
No Bookmarks			

Copyright © 2019 SonicWall, Inc.

Topics:

- Accessing the Virtual Office Portal
- Using NetExtender
- Configuring SSL VPN Bookmarks

Accessing the Virtual Office Portal

You can access the Virtual Office Portal two different ways. System administrators can access it through the appliance interface and have rights to make changes applicable to the entire site. User access it differently through different process and can only make changes that affect their particular profile.

For system administrators to access the SSL VPN Virtual Office portal:

1. Select the **MANAGE** view.
2. Under **Connectivity**, select **SSL VPN > Virtual Office**.

For users to view the SSL VPN Virtual Office web portal:

1. Navigate to the IP address of the firewall.
2. Click the link at the bottom of the Login page that says **Click here for sslvpn login**.

Using NetExtender

SonicWall NetExtender is a transparent software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources as if they were on the local network. The NetExtender connection uses a Point-to-Point Protocol (PPP) connection. The Virtual Office portal displays a link to download the NetExtender client.

Users can access NetExtender two ways:

- Logging in to the Virtual Office portal provided by the SonicWall security appliance and clicking on the NetExtender download link, then installing and launching NetExtender.
- Launching the standalone NetExtender client. After downloading NetExtender from the Virtual Office portal and installing it the first time, it can thereafter be accessed directly from the user's PC as you would with any other client application.

NetExtender displays a popup window when launched. The SonicWall server is prepopulated with the server used for the initial NetExtender launch and client download. The domain is also populated with the corresponding domain. The user enters username and password and then clicks **Connect**.

After the connection is established, the NetExtender window provides three screens: **Status**, **Routes**, and **DNS**. The **Status** screen displays the server, client IP address, the number of kilobytes sent and received, and the throughput in bytes per second. The **Routes** screen displays the destination subnet IP addresses and corresponding netmasks. The **DNS** screen displays the DNS servers, DNS suffix, and WINS servers. The routes and DNS settings are controlled by the SonicOS administrator on the SonicWall appliance.

Users can close the NetExtender window after the connection is established. The connection stays open, while window is minimized and can be reopened from the system tray (on Windows).

See About NetExtender on page 121 for additional information about NetExtender.

Configuring SSL VPN Bookmarks

User bookmarks can be defined to appear on the Virtual Office home page. Individual users cannot modify or delete bookmarks created by the administrator.

When creating bookmarks, remember that some services can run on non-standard ports, and some expect a path when connecting. When you configure a portal bookmark, you need to match the **Service** type with the right format for the **Name or IP Address**. Refer to the following table when setting those options.

ⓘ **NOTE:** Service types for ActiveX and Java do not exist in SonicOS 6.5. Preferences from older versions convert to HTML5 during an upgrade.

Bookmark Name or IP Address Formats by Service Type

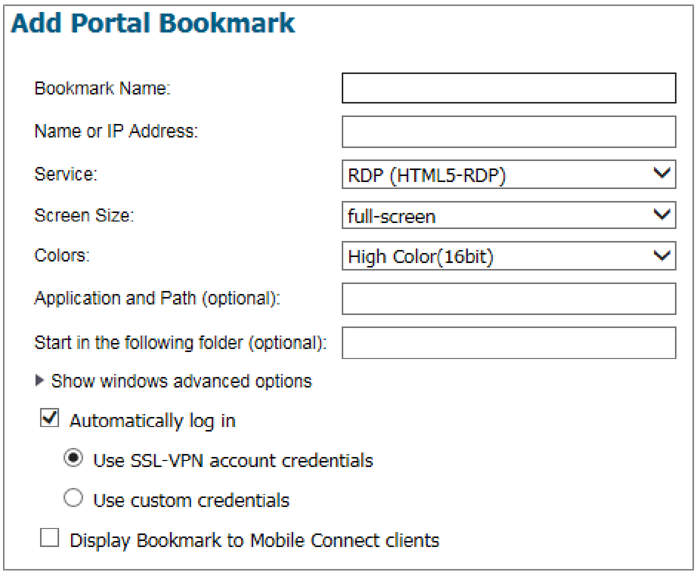
Service Type	Format	Example for Name or IP Address Field
RDP - ActiveX	IP Address	`10.20.30.4`
RDP - Java	IP:Port (non-standard)	`10.20.30.4:6818`
	FQDN	`JBJONES-PC.sv.us.sonicwall.com`
	Host name	`JBJONES-PC`
VNC	IP Address	`10.20.30.4`
	IP:Port (mapped to session)	`10.20.30.4:5901` (mapped to session 1)
	FQDN	`JBJONES-PC.sv.us.sonicwall.com`
	Host name	`JBJONES-PC`
	NOTE: Do not use session or display number instead of port.	**NOTE:** Do not use `10.20.30.4:1` **TIP:** For a bookmark to a Linux server, see the Tip below this table.
Telnet	IP Address	`10.20.30.4`
	IP:Port (non-standard)	`10.20.30.4:6818`
	FQDN	`JBJONES-PC.sv.us.sonicwall.com`
	Host name	`JBJONES-PC`
SSHv1	IP Address	`10.20.30.4`
SSHv2	IP:Port (non-standard)	`10.20.30.4:6818`
	FQDN	`JBJONES-PC.sv.us.sonicwall.com`
	Host name	`JBJONES-PC`

ⓘ **IMPORTANT:** When creating a **Virtual Network Computing (VNC)** bookmark to a Linux server, you must specify the port number and server number in addition to the Linux server IP the **Name or IP Address** field in the form of **ipaddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, the port number is 5901, and the server number is 1, the value for the **Name or IP Address** field would be **192.168.2.2:5901:1**.

To add a portal bookmark:

1 Navigate to the **MANAGE | Connectivity | SSL VPN > Portal Office** page.

2 Click **ADD**.



Add Portal Bookmark

Bookmark Name:	
Name or IP Address:	
Service:	RDP (HTML5-RDP)
Screen Size:	full-screen
Colors:	High Color(16bit)
Application and Path (optional):	
Start in the following folder (optional):	

▸ Show windows advanced options

☑ Automatically log in

● Use SSL-VPN account credentials

○ Use custom credentials

☐ Display Bookmark to Mobile Connect clients

3 Type a descriptive name for the bookmark in the **Bookmark Name** field.

4 In the **Name or IP Address** field, enter the fully qualified domain name (FQDN) or the IPv4 address of a host machine on the LAN. Refer to the Bookmark Name or IP Address Formats by Service Type table for examples of the **Name or IP Address** expected for a given **Service** type.

5 In the **Service** drop-down menu, chose the appropriate service type:

- **RDP (HTML5-RDP)**
- **SSHv2 (HTML5-SSHv2)**
- **TELNET (HTML5-TELNET)**
- **VNC (HTML5-VNC)**

Different options display, depending on what you selected.

6 Complete the remaining fields for the service you selected. For the options and definitions, refer to the following table:

If Service is set to RDP (HTML5-RDP), configure the following:

Screen Size	From the drop-down menu, choose the default terminal services screen size to be used when users execute this bookmark. Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session.
Colors	In the drop-down menu, select the default color depth for the terminal service screen when users select this bookmark.
Application and Path (optional)	If you want, enter the local path to where your application resides on your remote computer.
Start in the following folder	If you want, enter the local folder from which to execute application commands.

Show windows advanced options	Click the arrow to expand this and see all the Windows advanced options. Check the box to enable those that you want: • **Redirect clipboard** • **Auto reconnection** • **Window drag** • **Redirect audio** • **Desktop background** • **Menu/window animation**
Automatically log in	Check the box to enable automatic login. If selected, choose which credentials to use: • **Use SSL-VPN account credentials** • **Use custom credentials** If you choose custom credentials, enter the username, password and domain for the credentials. **NOTE:** You can use dynamic variables for the username and domain. Refer to the Dynamic Variables table below.
Display Bookmark to Mobile Connect clients	Check the box to display the bookmarks to Mobile Connect users.
If Service is set to SSHv2 (HTML5-SSHv2), configure the following:	
Automatically accept host key	Check the box to enable.
Display Bookmark to Mobile Connect clients	Check the box to display the bookmarks to Mobile Connect users.
If Service is set to TELNET (HTML5-TELNET), configure the following:	
Display Bookmark to Mobile Connect clients	Check the box to display the bookmarks to Mobile Connect users.
If Service is set to VNC (HTML5-VNC), configure the following:	
View Only	Check the box to set the bookmark to view only mode.
Share Desktop	Enables the shared desktop feature.
Display Bookmark to Mobile Connect clients	Check the box to display the bookmarks to Mobile Connect users.

7 Click **OK** to save the configuration.

Dynamic Variables

Text Usage	Variable	Example Usage
Login Name	%USERNAME%	US\%USERNAME%
Domain Name	%USERDOMAIN%	%USERDOMAIN\%USERNAME%

Part 3

Connectivity | Access Points

14

Understanding SonicWall Access Points

SonicWall SonicPoint and SonicWave wireless access points are specially engineered to work with SonicWall security appliances to provide wireless access throughout your enterprise. **Connectivity | Access Points** on the **MANAGE** view of the interface lets you manage the access points connected to your appliance.

> ⓘ **NOTE:** In SonicOS 6.5.3 and higher, the **Access Points** pages are displayed when **Wireless Controller Mode** on the **MANAGE | System Setup | Appliance > Base Settings** page is set to either **Full-Feature-Gateway** or **Wireless-Controller-Only**. If **Non-Wireless** is enabled for **Wireless Controller Mode**, the **Access Points** menu heading and the pages under it are ***not*** displayed. See the *SonicOS 6.5 System Setup* administration documentation for more information.

This section provides information and best practices on using SonicWall access points in your network and how you can integrate them with your SonicWall network appliance.

Topics:

SonicWall Secure Wireless Cloud Management

SonicWall Wireless Cloud Management support is available for SonicPoint and SonicWave access points. You no longer need to connect a SonicWave to your firewall to manage it. You can deploy it standalone by connecting it to your network. The appliance provides wireless services that you can manage through the cloud on our new SonicWiFi Mobile app.

The system includes the following tools to help you deploy, configure, manage, and monitor your wireless network:

- WiFi Cloud Manager — Cloud-based network management system that simplifies wireless access point deployment, configuration, management, and monitoring.

- WiFi Planner — Wireless network planning tool used to determine optimal access point placement and optimizes wireless distribution systems and mesh networks.
- SonicWiFi — Mobile application used to register access points, create mesh networks, and troubleshoot access point issues.

The wireless cloud tools are fully integrated with your Capture Security Center account. Your MySonicWall tenant information and registered devices are imported to each tool simplifying network management.

For more information, refer to the documents below found on the SonicWall Technical Documentation portal page. Select **Secure Cloud Wireless** in the **Select A Product** field.

- WiFi Cloud Manager Quick Start Guide — Manage SonicWaves
- WiFi Cloud Manager Advanced Feature Guide — Configure Capture ATP and CFS on SonicWaves
- WiFi Planner User Guide — Determine optimal placement for SonicWaves
- SonicWiFi Mobile App Quick Start Guide — Register SonicWaves

Access Point Feature Matrix

Several features are available in SonicOS, but not all features are supported on all SonicWall access points. Refer to the following table for specifics.

Wireless Feature Support by Access Point Type

Feature Name	SonicWave	SonicPoint ACe/ACi	SonicPoint N2	SonicPoint Ne/Ni/NDR/N
Band Steering	Yes	Yes	Yes	**No**
AirTime Fairness	Yes	Yes	Yes	**No**
Wireless Forensic Packet Capturing	Yes	**No**	**No**	**No**
WDS AP Support	Yes	Yes	Yes	**No**
Floor Plan View	Yes	Yes	Yes	Yes
Topology View	Yes	Yes	Yes	Yes
SSLVPN Concentrator	Yes	Yes	Yes	Yes
Real Time Monitoring Visualization	Yes	Yes	Yes	No
Dynamic VLAN	Yes	Yes	Yes	No
3G/4G/LTE Extender	Yes	Yes	Yes	No
Client Fingerprinting and Reporting	Yes	Yes	Yes	No
SNMP MIB Extension	Yes	Yes	Yes	Yes
GRE management multicore Support	Yes	Yes	Yes	Yes
Restful API Support	Yes	Yes	Yes	No
Guest Service: IP-based guest authentication bypass network	Yes	Yes	Yes	Yes
Guest Service: Cyclic quota for guest user group	Yes	Yes	Yes	Yes
Native Bridge support	Yes	Yes	Yes	Yes
Wireless Built-in Radio Repeater Mode	For TZ wireless only	For TZ wireless only	For TZ wireless only	For TZ wireless only

Wireless Feature Support by Access Point Type (Continued)

Feature Name	SonicWave	SonicPoint ACe/ACi	SonicPoint N2	SonicPoint Ne/Ni/NDR/N
Wireless Built-in Radio WDS Mode	For TZ wireless only	For TZ wireless only	For TZ wireless only	For TZ wireless only
IEEE 802.11s Mesh Network	Yes	No	No	No
Bluetooth Low Energy (BLE)	Yes	No	No	No
Capture Security Center Reporting	Yes	No	No	No
Wireless Cloud Management Support	Yes	No	No	No

Access Point Features

SonicWall access points integrate with SonicWall next-generation firewalls to create a secure wireless solution that delivers comprehensive protection for wired and wireless networks. They provide high-speed wireless access with enhanced signal quality and reliability that takes advantage of the latest capabilities to achieve gigabit wireless performance. With support for IEEE 802.11a/b/g/n/ac standards, the SonicPoint/SonicWave Series enables your organization for bandwidth-intensive mobile applications in high density environments without signal degradation.

Topics:

- SonicPoint/SonicWave Capabilities
- Certifications and Compliance
- Access Point Floor Plan View
- Access Point Topology View
- Intrusion Detection/Prevention
- Virtual Access Points
- Access Point WMM Configuration
- Japanese and International Access Point Support

SonicPoint/SonicWave Capabilities

SonicPoint/SonicWave access points provide higher throughput in the 5GHz band by providing more antennas, wider channels, more spatial streams, and other features that boost throughput and reliability. SonicPoint AC and SonicWave devices support both the 5GHz and 2.4GHz radio bands and have the following key technical components:

- **Wider Channels** — 80 MHz-wide channels for the 802.11ac radio module on SonicWave 432 series, while continuing to support 20/40 MHz channels. This allows for dynamic per packet negotiation of channel widths so that when there is interference, the SonicWave can temporarily fall back to 40 or 20MHz channels.
- **Up to 4 Spatial Streams** — Adding spatial streams increases throughput proportionally. Two streams doubles the throughput of a single stream. Four streams increases the throughput four times.
- **Multi-User MIMO** — Multiple Input Multiple Output spatial division multiplexing provides transmitting and receiving of multiple independent data streams simultaneously.

  SonicWave and SonicPoint AC provide higher throughput, better for wireless displays, HDTV, downloading large files, and campus and auditorium use.
- **Layer 3 Management Phase I** — Provides the DHCP and tunneling solution to support access point deployment in a Layer 3 network:
  - SonicWall DHCP-based Discovery Protocol (SDDP) is based on the well-known DHCP protocol and allows the SonicWall gateway and access point to discover each other automatically across Layer 3 local networks.
  - The remote network management protocol, SonicWall SSL VPN-based Management Protocol (SSMP), is based on SonicWall SSL VPN infrastructure to allow access points to be managed by a SonicWall SSL VPN enabled network security appliance over the Internet.
- **Dynamic Frequency Selection (DFS) Support** — After a DFS certificate is issued, the access points support dynamic frequency selection to allow an access point to be deployed in sensitive channels of the 5GHz frequency band.
- **Access Point Dashboard** — The **Access Point > Dashboard** page reports the statistics of each access point. The **Dashboard** summarizes bandwidth and client information in graphical form. It also provides real-time client monitoring details.
- **Band Steering** — Band Steering allows the access point to steer 5 GHz-capable clients to that band; it usually has less interference and less traffic. If, however, the signal has interference or is not as strong, the client is directed to the 2.4 GHz band. The intent is to user radio management to help improve overall capacity, throughput and user experience.
- **Open Authentication, Social Login, and LHM** — Open Authentication and Social Login for social media such as Facebook, Twitter, and Google+, and LHM (Lightweight Hotspot Message) are supported.
- **Radio Frequency Analysis** — Radio Frequency Analysis (RFA) is a feature that helps the network administrator understand how wireless channels are utilized by the access points and other neighboring wireless access points.
- **Retaining SonicWave Profile Setting** — You can configure access point profiles so the access points retain portions of their configuration even after they are deleted or resynchronized.
- **VLAN Tagging** — Prioritization is possible in VLAN over Virtual Access Point (VAP) because the SonicPoint/SonicWave allow a VAP to be configured to connect with a VLAN by using same VLAN ID. You can set priority for VLAN traffic through a firewall access rule.
- **Wireless Diagnostics** — An access point can collect critical runtime data and save it into persistent storage. If the access point fails, the SonicWall managing appliance retrieves that data when the access point reboots, and incorporates it into the Tech Support Report (TSR). A subsequent access point failure overwrites the data.

- **Access Point 3G/4G WWAN** — Users can plug a USB modem device into a SonicWall access point and the access point can perform the dial-up operation to connect to the Internet. After connecting, the access point acts as a WWAN devices for the firewall and provides WAN access.
- **Daisy Chaining** — Daisy chaining allows users with a small environment (that is, a low-density switch infrastructure) to deploy several access points while using as few switch ports as possible. For example, you can connect numerous devices scattered throughout the store into the store's switch infrastructure. This could include multiple access points to cover the entire store even though the infrastructure is small in terms of switch port density/availability. Access Points are daisy chained through the LAN2 interface.

  > **IMPORTANT:** Daisy chaining access points affects throughput; each addition lessens the throughput. If throughput is:
  >
  > - A concern, then to keep throughput at an acceptable level for the:
  >   - SonicPoint N2, daisy chain no more than three access points.
  >   - SonicPoint ACe/ACi or SonicWave, daisy chain no more than two access points.
  > - Not a concern, daisy chain no more than four access points.
  >
  > If you have a mixture of SonicWave or SonicPoint AC models with SonicPoint N or N2 models, place the SonicWave or SonicPoint AC model at the beginning of the chain.

- **Wireless Cloud Management Support** — Enables you to manage SonicWave access points from a central firewall or from the cloud using the SonicWiFi mobile app and WiFi Cloud Manager. The cloud-based infrastructure enables you to access, control, and troubleshoot WiFi issues from anywhere.
- **SonicWave Sensor Mode Enhancement** — Enables the administrator to detect rogue access points that have either been installed on a secure company network without the explicit authorization from a local network administrator or has been created to allow a cracker to conduct a man-in-the-middle attach. In sensor mode, SonicWave detects rogue access points by active probing all access points and preventing devices from connecting to such points.

Certifications and Compliance

The SonicWall access points have passed rigorous testing to earn industry certifications.

Wi-Fi Alliance Certification

> **NOTE:** SonicPoint Dual Radio (SonicWave, SonicPointNDR and SonicPoint ACe/ACi/N2) are Wi-Fi Certified by the Wi-Fi Alliance, designated by the Wi-Fi CERTIFIED logo.

The Wi-Fi CERTIFIED Logo is a certification mark of the Wi-Fi Alliance, and indicates that the product has undergone rigorous testing by the Wi-Fi Alliance and has demonstrated interoperability with other products, including those from other companies that bear the Wi-Fi CERTIFIED Logo.

FCC U-NII New Rule Compliance

FCC U-NII (Unlicensed –National Information Infrastructure) New Rule (Report and Order ET Docket No. 13-49) is supported on SonicWave and SonicPoint ACe/ACi/N2 running firmware version 9.0.1.0-2 or higher. To comply with FCC New Rules for Dynamic Frequency Selection (DFS), a SonicPoint/SonicWave access point detects and avoids interfering with radar signals in DFS bands.

ⓘ **NOTE:** SonicPoint ACe/ACi/N2 wireless access points manufactured with FCC New Rule-compliant firmware are only supported with SonicOS 6.5.2.1 and higher. Older SonicPoint ACe/ACi/N2 access points are automatically updated to the FCC New Rule-compliant firmware when connected to a firewall running SonicOS 6.5.

RED Compliance & Certification

The SonicWall TZ and SOHO Wireless appliances and SonicWall wireless access points demonstrate compliance with the European Union's Radio Equipment Directive (RED). See the *Radio Equipment Directive (RED) Addendum* on the SonicWall Support portal under Technical Documentation: https://www.sonicwall.com/Support/Technical-Documentation/Radio-Equipment-Directive-(RED)-Addendum.

Access Point Floor Plan View

SonicOS 6.5 allows for a visual approach to managing large number of SonicWall access point devices. You can also track physical location and real-time status.

Floor Plan View in SonicOS provides the real-time picture of the actual access point radio deployment environment. It increases your ability to estimate the wireless coverage of new deployment. The Floor Plan View also provides the means to monitor real-time status, configure access points, remove access points, and even show the RF coverage from the consolidated the context menu.

Access Point Topology View

Access points can be managed by topology view which can present the network topology from the SonicWall firewall to the endpoint. The access point real-time status can be monitored, and the context-menu can provide the configuration options as well.

This feature shows the logical relationship among all WLAN related devices, and enabled managing devices directly in the Topology View. When opening **Connectivity | Access Points > Topology View**, a tree-like diagram is shown by connecting devices known to the firewall and showing their relationship.

Topology View management provides a graphic presentation of the WLAN network for administrators with the most often used information and status. The devices are drawn as nodes on a tree and the tree is zoomable with the mouse and mouse wheel. Information shown in the tree includes device type, IP address, interface connected to, name, number of clients, and simulated LED light on some devices showing status. A tool tip bubble shows detailed information of a device.

Intrusion Detection/Prevention

SonicWall access points provide protection for radio frequency (RF) devices. RF technology used in wireless networking devices is a target for intruders. The access points use direct RF monitoring to detect threats without interrupting the current operation of your wireless or wired network. Such features include:

- **Intrusion Detection Services** - Intrusion Detection Services (IDS) enables the SonicWall network security appliance to recognize and take countermeasures against this common type of illicit wireless activity. IDS reports on all access points that the firewall can find by scanning the 802.11a/b/g/n/ac radio bands on the access points.
- **Advanced Intrusion Detection and Prevention** - Advanced Intrusion Detection and Prevention (IDP) monitors the radio spectrum for the presence of unauthorized access points (intrusion detection) and

automatically takes countermeasures (intrusion prevention). When Advanced IDP is enabled on an access point, its radio functions as a dedicated IDP sensor.

- **Rogue Device Detection and Prevention** – In SonicOS 6.5.3 or higher, access points with scan radios can act as sensors for rogue device detection while continuing to act as wireless access points. Prior to 6.5.3, access points can be configured in dedicated sensor mode to focus on rogue device detection and prevention, either passively or proactively on both the 2.4GHz and 5GHz bands. Both bands can be scanned even if only one is in use. The rogue device can be analyzed to report whether it is connected to the network and if it is blocked by a wired or wireless mechanism.
- **Built-in Wireless Radio Scan Schedule** – Access points can be scheduled to perform Intrusion Detection/Prevention scanning with granular scheduling options to cover up to 24 hours a day, 7 days a week. The **Schedule IDS Scan** options are available on the **Radio 0/1 Advanced** or **Advanced** screens when editing access point profiles for all access point models.

Virtual Access Points

A Virtual Access Point (VAP) is a multiplexed instantiation of a single physical access point, so that a single access point appears as multiple discrete access points or VAPs. To wireless LAN clients, each VAP appears as an independent physical access point, when only one physical access point exists.

- **Virtual Access Point Schedule Support** – Each VAP schedule can be individually enabled or disabled, for ease of use.
- **Virtual Access Point Layer 2 Bridging** – Each VAP can be bridged to a corresponding VLAN interface on the LAN zone, providing better flexibility.
- **Virtual Access Point ACL Support** – Each VAP can support an individual Access Control List (ACL) to provide more effective authentication control.
- **Virtual Access Point Group Sharing on SonicPoint N Dual Radios** – The same VAP/VLAN settings can be applied to dual radios. This allows you to use a unified policy for both radios, and to share a VLAN trunk in the network switch.

Access Point WMM Configuration

The access points support Wi-Fi Multimedia (WMM) to provide a better Quality of Service experience on miscellaneous applications, including VoIP on Wi-Fi phones and multimedia traffic on wireless networks. WMM is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard. WMM prioritizes traffic according to four access categories: voice, video, best effort, and background.

ⓘ **NOTE:** WMM does not provide guaranteed throughput.

Each Access Category has its own transmit queue. WMM requires the access point to implement multiple queues for multiple priority access categories. The access point relies on either the application or the firewall to provide type of service (TOS) information in the IP data to differentiate traffic types. One way to provide TOS is through firewall services and access rules; another way is through VLAN tagging.

The **Connectivity | Access Points > Wi-Fi Multimedia** page on the **MANAGE** view provides a way to configure WMM settings and mappings.

Japanese and International Access Point Support

SonicOS supports both Japanese and international SonicPoint ACe/ACi/N2 and SonicWave 432e/432i/432o/224w/231c/231o wireless access points. An international access point is one that is deployed and operating in a country other than the United States or Japan.

When an international access point is connected to a SonicWall network security appliance, SonicOS displays a **Register** button on the **Access Points > Base Settings** page. Clicking **Register** brings up a dialog in which you can select the appropriate **Country Code**.

ⓘ **NOTE:** Be sure to select the country code for the country in which the access point is deployed, even if you are not in that country while registering the access point.

For international access points registered with country codes other than Canada, the country code can be changed in the profile on the **Connectivity | Access Points > Base Settings** page.

ⓘ **IMPORTANT:** When the access point is registered with the country code for Canada, the country code cannot be changed except by contacting SonicWall Support.

Planning and Site Survey

Before deploying SonicWall access points in your environment, take the time to understand the requirements for the equipment. The following sections describe the prerequisites for your deployment and identify the things to check as a part of a site survey.

Topics:

- Prerequisites
- Site Survey and Planning
- PoE and PoE+

Prerequisites

The following are required for a successful access point deployment:

- SonicOS requires public Internet access for the network security appliance to download and update the firmware images for the access points. If the public Internet is not accessible, you need to obtain and download the access point firmware manually.
- One or more SonicWall wireless access points.
- If you are using a PoE/PoE+ switch to power the access point, it must be one of the following:
  - An 802.3at-compliant Ethernet switch for SonicWave 432e/432i/432o/224w/231c
  - An 802.3at-compliant Ethernet switch for SonicPointACe/ACi/N2
  - An 802.3af-compliant Ethernet switch for other access point models including 231o
- You should obtain a support contract for your SonicWall network security appliance as well as the PoE/PoE+ switch. The contract allows you to update to new versions if issues are found on the switch side, on the firewall side, or when new features are released.
- Be sure to conduct a full site survey before installation to understand what needs to be done to prepare for installation and implementation.

- Check wiring and cable infrastructure to verify that end-to-end runs between the SonicWall access points and the Ethernet switches are CAT5, CAT5e, or CAT6.
- Check building codes for installation points, and work with the building's facilities staff, as some desired install points might violate regulations.

Site Survey and Planning

Performing a site survey and planning the SonicWall access point deployment is key to a successful implementation. Include the following guidelines in your survey and planning:

- Conduct a full site walk of all areas where access points are deployed. Use a wireless spectrum scanner and note any existing access points and the channels they are broadcasting on. SonicWall currently recommends using Fluke or AirMagnet products to conduct the survey. You might also wish to try NetStumbler/MiniStumbler, a free product that does a decent job of surveying so long as it works with your wireless card.
- Get blueprints of floor plans to use during the survey. You can mark the position of access points and the range of the wireless cell. Make multiple copies of these as the site survey results might cause to start over with a new design. Also, you see where walls, halls, and elevators are located, which can influence the signal. Areas in which users are—and are not—located can be seen.

  During the site-survey, watch for electrical equipment that might cause interference (microwaves, CAT scan equipment, and so on) in areas where a lot of electrical equipment is placed, and also identify the type of cabling being used.
- Survey three dimensionally (side to side, front to back and side to side) as wireless signals cross over to different floors.
- Determine where you can locate access points based on power and cabling. Remember that you should not place access points close to metal or concrete walls, and you should put them as close to the ceiling as possible.
- Use the wireless scanning tool to check signal strengths and noise. Signal-to-noise ratio should be at least 10 dB (minimum requirements for 11 Mbps), however, 20 dB is preferred. Both factors influence the quality of the service.
- You might need to relocate some access points and re-test, depending of the results of your survey.
- Save settings, logs and note the location of the wireless access points for future reference. You might want this information to build the Floor Plan View.
- When using older SonicPoint models, you might find that certain areas, or all areas, are saturated with existing overlapping 802.11b/g channels. If that happens, you might wish to deploy the access points using the 802.11a radio. This provides a much larger array of channels to broadcast on, although the range of 802.11a is limited, and those devices do not allow additional external antennas.
- Be wary of broadcasting your wireless signal into areas that you do not control; check for areas where people might be able to leach signal and tune the access points accordingly.
- For light use, you can plan for 15-20 users for each access point. For business use, you should plan for 5-10 users for each access point.
- Plan for your roaming users—this requires tuning the power on each access point so that the signal overlap is minimal. Multiple access points broadcasting the same SSID in areas with significant overlap can cause ongoing client connectivity issues.
- Use the scheduling feature in SonicOS to shut off access points when not in use. SonicWall recommends that you do not operate your access points during non-business-hours (nights and weekends, for example).

PoE and PoE+

When planning, make sure you note the distance of cable runs from where the access point is mounted; this must be no more than 100 meters. If you are not using PoE switches or a SonicWall PoE enabled appliance, you also need to consider a power adapter or PoE injector for the access point. Make sure you are not creating an electrical fire hazard.

Long cable runs cause loss of power; 100-meter runs between the access point and PoE switch might incur up to 16 percent power/signal degradation. Because of this, the PoE switch needs to supply more power to the port to keep the access point operational.

SonicPoint ACe/ACi/N2

Full 802.3at compliance is required on any switch supplying Power over Ethernet/Power over Ethernet plus (PoE/PoE+) to SonicPoint ACe/ACi/N2. Do not operate SonicPoints on non-compliant switches as SonicWall does not support it.

ⓘ **IMPORTANT:** Turn off pre-802.3at-spec detection as it might cause connectivity issues.

SonicPoint ACs (Type 1) can be set to Class 0, 1, 2, or 3 PD. SonicPoint ACs (Type 2) are set to Class 4 PD. The minimum and maximum power output values are as follows:

- Type 1, Class 0 PD uses 0.5 W minimum to 15.4 W maximum
- Type 1, Class 1 PD uses 0.5 W minimum to 4.0 W maximum
- Type 1, Class 2 PD uses 4.0 W minimum to 7.0 W maximum
- Type 1, Class 3 PD uses 7.0 W minimum to 15.4 W maximum
- Type 2, Class 4 PD uses 15.4 W minimum to 30 W maximum

ⓘ **IMPORTANT:** A mismatch in Class causes confusion in the handshake and reboots the SonicPoint access point.

Ensure each SonicPoint ACe/ACi/N2 is guaranteed to get 25 watts.

Be particularly careful to ensure all PoE/PoE+ switches can provide a minimum of 25 watts of power to each of its PoE ports. For example, a port that supports a SonicPoint ACe/ACi/N2 needs 25 watts of power. If a switch cannot guarantee each port 25 watts to each port, an external redundant power supply must be added. You need to work closely with the manufacturer of the PoE/PoE+ switch to ensure that enough power is supplied to the switch to power all of your PoE/PoE+ devices.

Legacy and SonicPoint N/Ni/Ne/NDR

Legacy SonicPoints and SonicPoint N/Ni/Ne/NDR are set to Class 0 PD, which uses 0.44W minimum up to 12.95W maximum power.

Full 802.3af compliance is required on any switch supplying PoE to legacy SonicPoints and SonicPoint N/Ni/Ne/NDR. Do not operate SonicPoints on non-compliant switches as SonicWall does not support it.

Turn off pre-802.3af-spec detection as it might cause connectivity issues.

Ensure each port can get 10 watts guaranteed, and set the PoE priority to critical or high.

Best Practices for Access Point Deployment

This section provides SonicWall recommendations and best practices regarding the design, installation, deployment, and configuration issues for SonicWall's wireless access points. The information covered allows you to properly deploy the access points in environments of any size. This section also covers related external issues that are required for successful operation and deployment.

ⓘ **IMPORTANT:** SonicWall cannot provide any direct technical support for any of the third-party Ethernet switches referenced in this section. The material is also subject to change without SonicWall's knowledge when the switch manufacturer releases new models or firmware that might invalidate the information contained herein.

Topics:

- Switches in the Infrastructure
- Wiring Considerations
- Channels
- Spanning-Tree
- VTP and GVRP Trunking Protocols
- Port-Aggregation
- Portshielding
- Broadcast Throttling/Broadcast Storm
- Speed and Duplex
- SonicPoint Auto Provisioning

Switches in the Infrastructure

Most switches can be used in your SonicWall infrastructure. However, some customized settings or programming might be required to ensure optimum performance.

Tested Switches

The following switches have been tested with SonicWall access points. Note the guidance provided for each.

- Cisco – Most Cisco switches work well; however, certain issues were found with some models.
  - SonicWall does not recommend deploying SonicWall access points using the Cisco Express switch line of products.
  - SonicWall found SonicPointACe/ACi/N2 Ethernet has energy efficient Ethernet compatible issue with Cisco switch 2960X-PS-l. Disable EEE on the SonicPoint connected port. Refer to the following Cisco documentation for more details: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/software/15-0_2_EX1/int_hw_components/configuration_guide/b_int_152ex1_2960-xr_cg/b_int_152ex1_2960-xr_cg_chapter_01001.pdf.
- D-Link PoE switches – Shut off all their proprietary broadcast control and storm control mechanisms, as they interfere with the provisioning and acquisition mechanisms on the access point.

- Dell – Be sure to configure STP for fast start on the access point ports.
- Extreme – Be sure to configure STP for fast start on the access point ports.
- Foundry – Be sure to configure STP for fast start on the access point ports.
- HP ProCurve – Be sure to configure STP for fast start on the access point ports.
- Netgear – SonicWall does not recommend deploying SonicWall access points using Netgear PoE switches.

Switch Programming Tips

The following sections provide some sample switch commands that be used on switches in the SonicWall infrastructure. Refer to the appropriate vendor sample for details.

Sample Dell Switch Configuration (per Interface)

- spanning-tree portfast
- no back-pressure
- no channel-group
- duplex half (note: only if you are seeing FCS errors)
- speed 100
- no flowcontrol
- no gvrp enable
- no lldp enable
- mdix on
- mdix auto
- no port storm-control broadcast enable

Sample D-Link Switch Configuration

The D-Link PoE switches do not have a command line interface, so you need to use their web interface.

ⓘ **NOTE:** If you are using multicast in your environment, check with D-Link for the recommended firmware version.

Disable spanning-tree, broadcast storm control, LLDP, and the Safeguard Engine on the switch before adding SonicWall access points to the switch. Those options might impact successful provisioning, configuration, and functionality of the access points.

Sample HP ProCurve Switch Commands (per Interface)

- name ‘link to SonicPoint X’ (or SonicWave X)
- no lacp
- no cdp
- power critical
- no power-pre-std-detect (note: global command)
- speed-duplex 100-half (note: only if you are seeing FCS errors)

- spanning-tree *xx* admin-edge-port (note: replace *xx* with port number)
- mdix-mode mdix

Wiring Considerations

Work with your facilities organization to be sure these wiring guidelines are considered for your implementation.

- Make sure wiring is CAT5, CAT5e, or CAT6 end to end.
- Because of signaling limitations in 802.3af, and 802.3at for SonicPoint and SonicWave appliances, Ethernet cable runs should not extend over 100 meters between the PoE switch and the access point.
- Plan for PoE power loss as the cable run becomes longer; this can be up to 16 percent. For longer cable runs, the port requires more power to be supplied.

Channels

The default setting of SonicWall access point is **auto-channel.** When this is set, the access point does a scan at boot-up to check if other wireless devices are transmitting. Then, it looks for an unused channel to use for transmission. In larger deployments, this process might cause issues so consider assigning fixed channels to each access point.

ⓘ **TIP:** A diagram of the access points and their MAC Addresses helps to avoid overlaps. It is recommended to mark the location of the access points and MAC Addresses on a floor-plan.

In SonicOS 6.5.3 and higher, dynamic channel selection (DCS) is supported on SonicWave access points for IEEE 802.11 WLAN. With DCS, an access point can:

- Determine the optimal channel at which to operate.
- Switch all the stations (STAs) associated with its basic service set (BSS) to the newly selected channel.

With DCS, the access point monitors continuously for the best channel and, according to the RF environment, changes to it dynamically (because interfering neighbor APs and microwaves come and go). Changing the channel generates a log entry in **INVESTIGATE | Logs > Event Logs**.

Spanning-Tree

When an Ethernet port becomes electrically active, most switches, by default, activate the spanning-tree protocol on the port to determine if there are loops in the network topology. During this detection period of 50-60 seconds, the port does not pass any traffic—this feature is known to cause problems with SonicWall access points.

If you do not need the spanning-tree protocol, disable it globally on the switch or disable it on each port connected to a SonicWall access point. If this is not possible, check with the switch manufacturer to determine if they allow *fast spanning-tree detection*, which runs spanning-tree in a shortened time so as to not cause connectivity issues. Refer to Sample Dell Switch Configuration (per Interface) for programming samples on how to do this.

VTP and GVRP Trunking Protocols

Turn these trunking protocols off on ports connected directly to the access points as they have been known to cause issues with SonicPoints, especially the high-end Cisco Catalyst series switches.

Port-Aggregation

Many switches have port aggregation turned on by default, which causes a lot of issues. Port aggregation should be deactivated on ports connected directly to SonicWall access points. PAGP/Fast EtherChannel/EtherChannel and LACP should also be turned off on the ports going to SonicWall access points.

Portshielding

SonicWall access points can be port-shielded by configuring them as a member of a PortShield group. If the access points are configured to an X-Series switch, the PortShield group it is a member of must be configured as a port for a dedicated link.

Broadcast Throttling/Broadcast Storm

The Broadcast Throttling/Broadcast Storm feature is an issue on some switches, especially D-Link. Disable on a per-port basis if possible, if not, disable globally.

Speed and Duplex

Speed and duplex options might sometimes cause issues for SonicWall access points. At present, **auto-negotiation** is the only option for speed and duplex on SonicWall access points. To resolve or avoid those issues consider the following:

- Lock speed and duplex on the switch and reboot the access point to help with connectivity issues.
- Check the port for errors, as this is the best way to determine if there is a duplex issue (the port also experiences degraded throughput).

SonicPoint Auto Provisioning

Topics:

- Automatic Provisioning (SDP & SSPP)
- Enabling Auto Provisioning

Automatic Provisioning (SDP & SSPP)

The SonicWall Discovery Protocol (SDP) is a layer 2 protocol employed by SonicPoint/SonicWaves and devices running SonicOS. SDP is the foundation for the automatic provisioning of SonicPoint/SonicWave units through the following messages:

- **Advertisement** – SonicPoint/SonicWaves without a peer periodically and on startup announce or advertise themselves through a broadcast. The advertisement includes information that is used by the receiving SonicOS device to ascertain the state of the SonicPoint/SonicWave. The SonicOS device then reports the state of all peered SonicPoint/SonicWaves and takes configuration actions as needed.

- **Discovery** – SonicOS devices periodically send discovery request broadcasts to elicit responses from L2 connected SonicPoint/SonicWave units.
- **Configure Directive** – A Unicast message from a SonicOS device to a specific SonicPoint/SonicWave to establish encryption keys for provisioning and to set the parameters for and to engage configuration mode.
- **Configure Acknowledgment** – A Unicast message from a SonicPoint/SonicWave to its peered SonicOS device acknowledging a Configure Directive.
- **Keepalive** – A Unicast message from a SonicPoint/SonicWave to its peered SonicOS device used to validate the state of the SonicPoint/SonicWave.

If through the SDP exchange the SonicOS device ascertains that the SonicPoint/SonicWave requires provisioning or a configuration update (such as on calculating a checksum mismatch or when a firmware update is available), the Configure directive engages a 3DES encrypted, reliable TCP-based SonicWall Simple Provisioning Protocol (SSPP) channel. The SonicOS device then sends the update to the SonicPoint/SonicWave through this channel, and the SonicPoint/SonicWave restarts with the updated configuration. State information is provided by the SonicPoint/SonicWave and is viewable on the SonicOS device throughout the entire discovery and provisioning process.

Enabling Auto Provisioning

SonicPoint Auto Provisioning can be enabled to automatically provision the following wireless SonicPoint/SonicWave provisioning profiles:

- SonicPoint
- SonicPoint N
- SonicPointNDR
- SonicPoint AC
- SonicWave

Initial configuration of a wireless SonicPoint/SonicWave is provisioned from a SonicPoint/SonicWave profile that is attached to the wireless LAN managing zone. After a wireless SonicPoint/SonicWave is provisioned, the profile remains an off line configuration template that is not directly associated with any access point. So, modifying a profile does not automatically trigger a SonicPoint/SonicWave for reprovisioning.

Before Auto Provisioning was introduced, administrators had to manually delete all SonicPoints, and then synchronize new SonicPoints to the profile, which was time consuming. To simplify configuration and ease management overhead, SonicPoint Auto Provisioning was introduced.

Checkboxes to enable Auto Provisioning for each of the SonicPoint/SonicWave Provisioning Profiles are provided in the **Network > Zones > Configure > Wireless** configuration dialog. By default, the checkboxes for the SonicPoint/SonicWave Provisioning Profiles are not checked and Auto Provisioning is not enabled.

When the checkbox for a provisioning profile is checked and that profile is changed, all access points linked to that profile are reprovisioned and rebooted to the new operational state.

Remote MAC Access Control for SonicPoint/SonicWaves

ⓘ **IMPORTANT:** You cannot enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled. If you try to enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled, this error message displays:

```
Remote MAC address access control cannot be set
when IEEE 802.11i EAP is enabled.
```

ⓘ **NOTE:** Remote MAC Access Control is also supported for Virtual Access Points. See Remote MAC Address Access Control Settings.

You can enforce radio wireless access control based on a MAC-based authentication policy in a remote RADIUS server. For the procedure Remote MAC Address Access Control Settings.

Access Point Licensing

Licensing for SonicWave access points is different than for SonicPoint access points.

Topics:

- SonicWave Licensing
- Licensing Status
- Manual License Update
- Automatic License Update

SonicWave Licensing

SonicWall requires additional licensing for each individual SonicWave unit. The license allows you to manage SonicWave from a SonicWall firewall and from SonicWall WiFi Cloud Manager. Initially, the SonicWave unit is bundled with a 6-month management license.

The SonicWall firewall recognizes the licensing state from SonicWall License Manager (LM) and enables management capability for the underlying SonicWave access point. When the license is within 30 days of expiring, the firewall generates notices to remind the system administrator about license renewal.

If the SonicWave license expires, there is no service interruption and traffic continues to pass through the SonicWave. However, you can no longer update the configuration on the wireless network. The network operation continues to function with the last saved configuration, allowing business operations to continue. Upon renewing the SonicWave subscription license, you can again make updates to your wireless network configuration

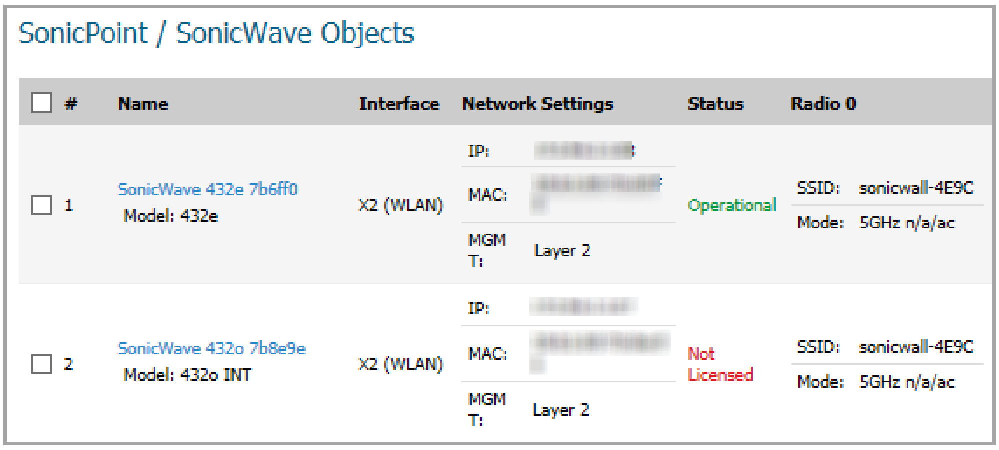
ⓘ **NOTE:** In an isolated environment, where the firewall might not be able to access License Manager, the administrator can input the SonicWave license keyset into firewall to modify the SonicWave licensing state. As long as SonicWave is holding the valid license, it can be managed by the firewall which takes the position of license proxy to synchronize the SonicWave license with License Manager.

Licensing Status

To validate status of SonicWave licensing:

1 Navigate to **Connectivity | Access Points > Base Settings**.

2 Scroll down to the SonicPoint/SonicWave Objects table and check the **Status** of the access point.



SonicPoint / SonicWave Objects

☐ #	Name	Interface	Network Settings	Status	Radio 0
☐ 1	SonicWave 432e 7b6ff0 Model: 432e	X2 (WLAN)	IP: [redacted] MAC: [redacted] MGMT: Layer 2	Operational	SSID: sonicwall-4E9C Mode: 5GHz n/a/ac
☐ 2	SonicWave 432o 7b8e9e Model: 432o INT	X2 (WLAN)	IP: [redacted] MAC: [redacted] MGMT: Layer 2	Not Licensed	SSID: sonicwall-4E9C Mode: 5GHz n/a/ac

The SonicWave access point can have one of the following statuses:

- **Operational** in green shows the access point is licensed.
- **Not Licensed** in red indicates that the access point is no longer licensed.
- **Expiring** indicates that the license is within 30 days or less of expiring.

Manual License Update

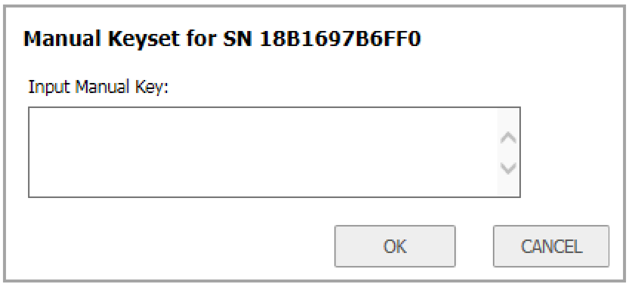
When the firewall cannot reach the License Manager to refresh the SonicWave license, you can still use GMS or SonicOS management interface to configure and update license manually.

1 Log into MySonicWall and obtain the manual keyset for the SonicWave license. Copy it to your clipboard.

2 On your firewall, navigate to **MANAGE | Connectivity | Access Points > Base Settings**.

3 Scroll down to **SonicPoint/SonicWave Objects**.

4 Click on the open lock icon in the Configure column for the SonicWave that needs to be manually renewed.



Manual Keyset for SN 18B1697B6FF0

Input Manual Key:

5 Type the license key into the key field and click **OK**.

The firewall initiates the process to update the new license key on the SonicWave access point. The SonicWave access point saves the updated license key, brings up radio interface, restores traffic bridging and opens the console access.

Automatic License Update

The firewall automatically queries the SonicWave access point periodically. If the SonicWave access point has been updated the firewall records the new license expiration time in the peer list and updates the new license keyset on the SonicWave access point and control its functionality accordingly.

Before Managing SonicPoint/SonicWaves

Before you can manage SonicPoint/SonicWaves in the SonicOS management interface, you must first:

1. Configure your access point Provisioning Profiles.
2. Configure a Wireless zone.
3. Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoint/SonicWaves in that zone uses the first profile in the list.
4. Assign an interface to the Wireless zone.
5. Attach the access points to the interfaces in the Wireless zone.
6. Test the access points.

Updating SonicPoint/SonicWave Firmware

Not all SonicOS firmware contains an image of the SonicPoint/SonicWave firmware. Check the top of the **Connectivity | Access Points > Base Settings** page and look for the **Download** link.

If your SonicWall appliance has Internet connectivity, it automatically downloads the correct version of the SonicPoint/SonicWave image from the firewall server when you connect a SonicPoint/SonicWave.

If your SonicWall appliance does *not* have Internet access, or has access only through a proxy server, you must update the SonicPoint/SonicWave image manually.

To manually update SonicPoint/SonicWave firmware:

1. Download the SonicPoint/SonicWave image from http://www.MySonicWall.com to a local system with Internet access.

   You can download the SonicPoint/SonicWave image from one of the following locations:

   - On the same page where you can download the SonicOS firmware
   - On the Download Center page, by selecting **SonicPoint/SonicWave** in the **Type** drop-down menu
2. Load the SonicPoint/SonicWave image onto a local Web server that is reachable by your SonicWall appliance.

   You can change the file name of the SonicPoint/SonicWave image, but you should keep the extension intact (for example, `.bin.sig`).
3. In the SonicOS user interface on your SonicWall appliance, to **MANAGE | System Setup | Appliance > Base Settings**.
4. In the **System Setup | Appliance > Base Settings** page, under **Download URL** section, select the appropriate checkbox for the SonicPoint/SonicWave image to download (you can download more than one image):

   - **Manually specify SonicPoint-N image URL (http://)**
   - **Manually specify SonicPoint-Ni/Ne image URL (http://)**

- **Manually specify SonicPoint-NDR image URL (http://)**
- **Manually specify SonicPoint-ACe/ACi/N2 image URL (http://)**
- **Manually specify SonicWave 432o/e/i or 224w/231c/231o image URL (http://)**

5 In the field(s), type the URL for the SonicPoint/SonicWave image file on your local Web server.

ⓘ **NOTE:** When typing the URL for the SonicPoint/SonicWave image file, do NOT include `http://` in the field.

6 Click **ACCEPT**.

Resetting the SonicPoint/SonicWave

The SonicPoints and SonicWave 432 e/i have a reset switch inside a small hole in the back of the unit, next to the console port. You can reset the access points at any time by pressing the reset switch with a straightened paper clip, a tooth pick, or other small, straight object.

ⓘ **NOTE:** The SonicWave 432o does not have a **Reset** button.

The reset button resets the configuration of the mode the access point is operating in to the factory defaults. It does not reset the configuration for the other mode. Depending on the mode the access point is operating in, and the amount of time you press the reset button, the access point behaves in one of the following ways:

- Press the reset button for **at least three seconds**, but **less than eight seconds,** with the access point operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the access point.
- Press the reset button for **more than eight seconds** with the access point operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the access point in SafeMode.
- Press the reset button for **at least three seconds**, to reset the configuration to factory defaults and reboot the access point.

Access Points and RADIUS Accounting

ⓘ **NOTE:** For using RADIUS to authenticate users, see Configuring Radius Server Settings.

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provide centralized authentication, authorization, and accounting. SonicOS uses RADIUS protocols to deliver account information from the NAS (Network Access Server), that is, the access point, to the RADIUS Accounting Server. You can take advantage of the account information to apply various billing rules on the RADIUS Accounting Server side. The accounting information can be based on session duration or traffic load being transferred for each user.

The overall authentication, authorization, and accounting process works as follows:

1 A user associates to an access point which is connected to a SonicWall firewall.

2 Authentication is performed using the method designated.

3 IP subnet/VLAN assignment is enabled.

4 The access point sends the RADIUS Account Request start message to an accounting server.

5 Re-authentication is performed as necessary.

6 Based on the results of the re-authentication, the access point sends the interim account update to the accounting server.

7 The user disconnects from the access point.

The access point sends the RADIUS Account Request stop message to the accounting server.

Setting up the Radius Accounting Server

To set up the Radius Accounting Server:

1 Add the RADIUS client entry into the file, `/etc/freeradius/clients.conf`:

```
Client <IP address> {
     Secret = “<password>”
}
```

Where *<IP address>* is the IP address of the RADIUS Server and *<password>* is the server password.

> ⓘ **NOTE:** The IP address is the WAN IP of the SonicWall GW from which the RADIUS Server is reached.

2 Add the user information into the file, `/etc/freeradius/users`:

```
user_name Cleartext-Password := “<password>”
```

Where *user_name* is the user’s ID and *<password>* should be replaced with the user’s password.

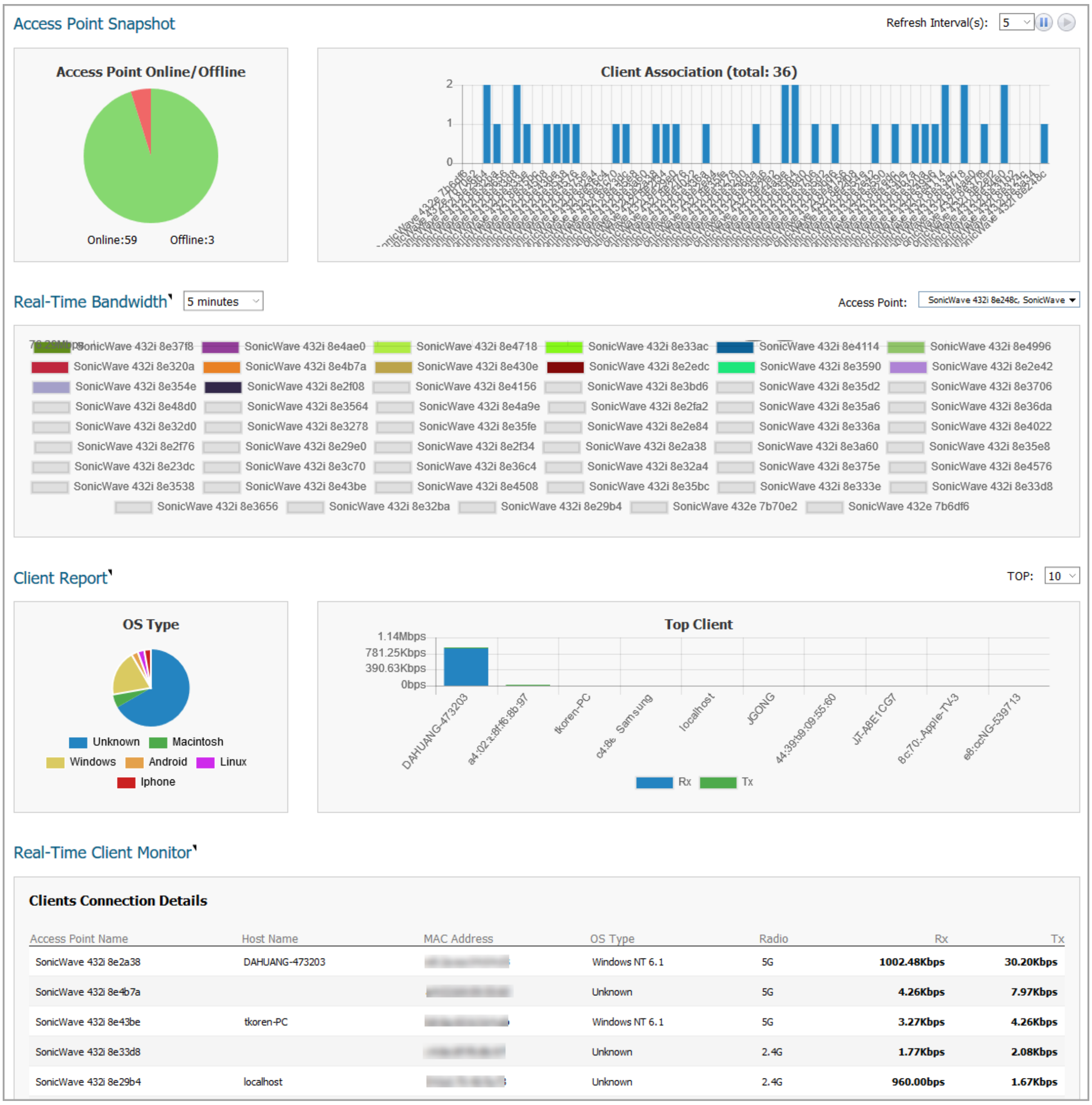
3 To start freeradius, run the command:

```
sudo feeradius -X
```

from the command line.

Access Point Dashboard

For SonicWave and SonicPoint AC devices, **Connectivity | Access Points > Dashboard** uses charts and graphs to visualize the data related to the access points that are a part of your infrastructure. You can display both real-time status and historical status, as well as each client's rate, OS type and hostname. It also displays status of the SonicWave and SonicPoint devices and provides information to help with monitoring and problem diagnosis.



Clients Connection Details

Access Point Name	Host Name	MAC Address	OS Type	Radio	Rx	Tx
SonicWave 432i 8e2a38	DAHUANG-473203	[redacted]	Windows NT 6.1	5G	**1002.48Kbps**	**30.20Kbps**
SonicWave 432i 8e4b7a		[redacted]	Unknown	5G	**4.26Kbps**	**7.97Kbps**
SonicWave 432i 8e43be	tkoren-PC	[redacted]	Windows NT 6.1	5G	**3.27Kbps**	**4.26Kbps**
SonicWave 432i 8e33d8		[redacted]	Unknown	2.4G	**1.77Kbps**	**2.08Kbps**
SonicWave 432i 8e29b4	localhost	[redacted]	Unknown	2.4G	**960.00bps**	**1.67Kbps**

ⓘ **NOTE:** The Dashboard might look different in some versions of SonicOS 6.5. Refer to the descriptions of the Dashboard page sections in the following topics for more details.

Topics:

- Feature Limitations
- Access Point Snapshot
- Real-Time Bandwidth
- Client Report
- Real-Time Client Monitor
- Client Report and Client Monitor Filtering

Feature Limitations

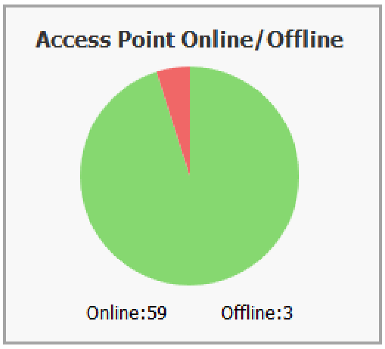
SonicWave and SonicPoint AC device status is displayed on when the device is managed by a SonicWall firewall. Both the firewall and the access point needs to be functional or no valid data can be exchanged. SonicWave access points retain a seven-day history of the dashboard data at all times. However, because of memory limitations, SonicPoint AC devices lose all history data when they are rebooted.

Access Point Snapshot

Two graphs are shown in the **Access Point Snapshot** section of the **Connectivity | Access Point > Dashboard**: **Access Point Online/Offline** and **Client Association**. In the right corner, you can specify the refresh interval for these charts. Select the number of minutes from the drop-down menu; the options range from 5 to 10 minutes.

Access Point Online/Offline

The **Access Point Online/Offline** graph shows a quick status of the access points in the infrastructure. The data is presented as a pie chart; online is green and offline is red. At the bottom of the chart, the number of access points and the status is also listed.

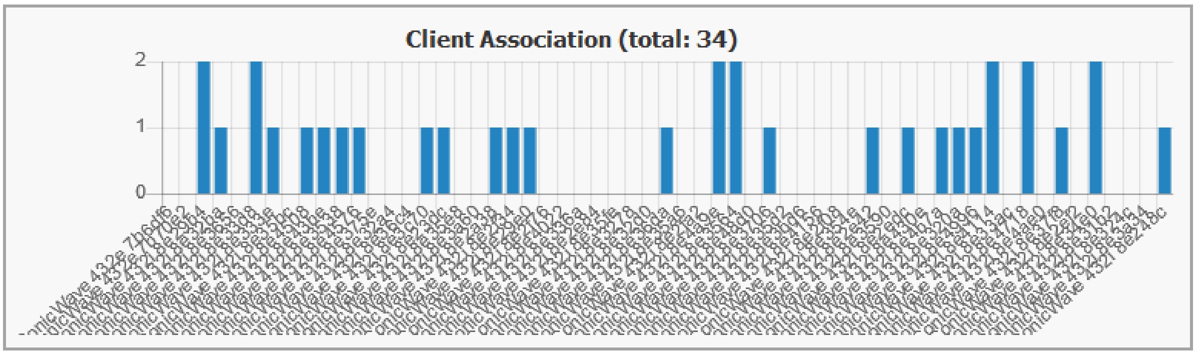


The Online status includes operational, disabled, rebooting, and in IDS scanning mode.

Offline status includes unresponsive and initializing states.

Client Association

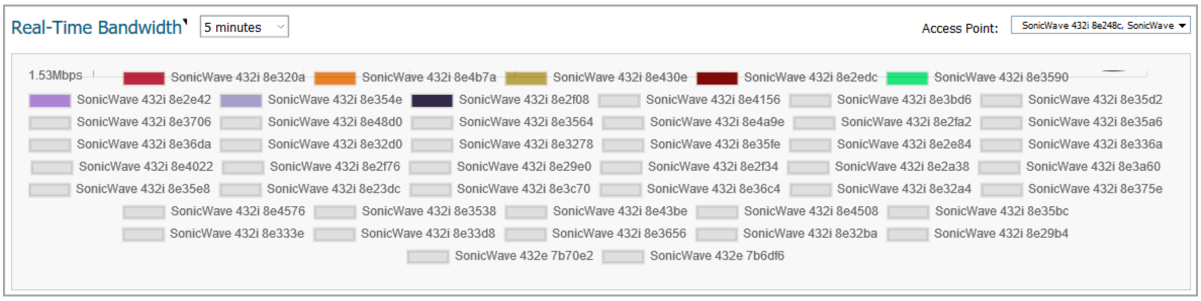
The **Client Association** chart shows the number of clients associated with each access point in the configuration. The number of users is shown in bar chart form.



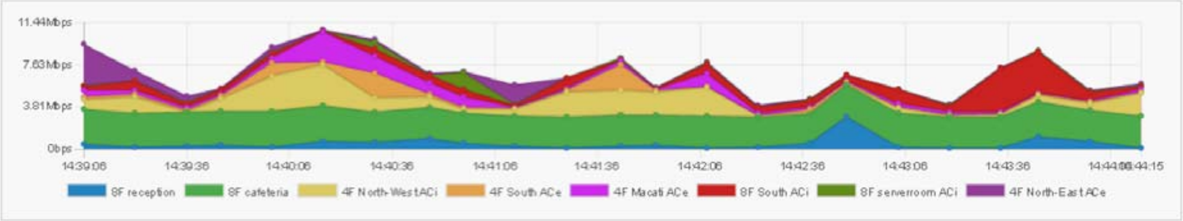
Real-Time Bandwidth

A graph showing the bandwidth being used of the selected access point is displayed in the **Real-Time Bandwidth** section of the **Connectivity | Access Point > Dashboard**.

ⓘ | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Real-Time Bandwidth** feature.



SonicOS shows a stacked chart of the real-time traffic on the selected access point(s). The Y value is the total traffic, both received and transmitted. By default, all access points are selected for the display.



To select the refresh interval, select the interval period from the drop-down menu by the chart title. Options are: **1 minute**, **2 minutes**, **5 minutes**, **10 minutes**, and **60 minutes**.

To change the access point being displayed, go to the **Access Point** drop-down menu and select a different device. The chart updates with the data for that access point.

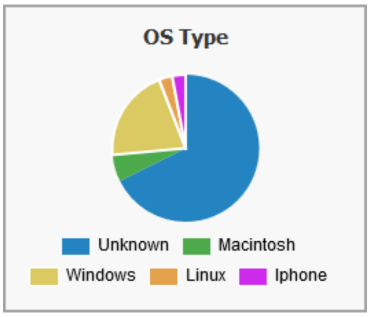
Client Report

Two graphs are shown in the **Client Report** section of the **Connectivity | Access Point > Dashboard**: **OS Type** and **Top Client**.

ⓘ | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Client Report** feature.

OS Type

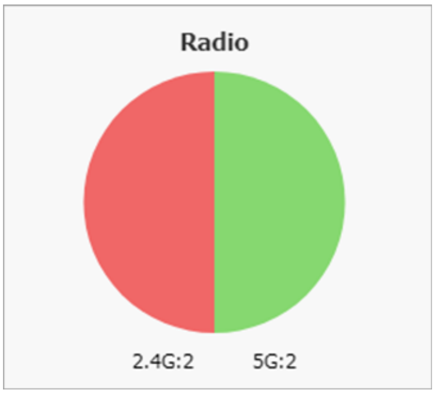
The **OS Type** pie chart displays the percentages of connected Windows clients, Macintosh clients, Linux clients, iPhones, Android, and so on. If the client has not generated any HTTP traffic, it might show as *Unknown*.



ⓘ | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **OS Type** feature.

Radio

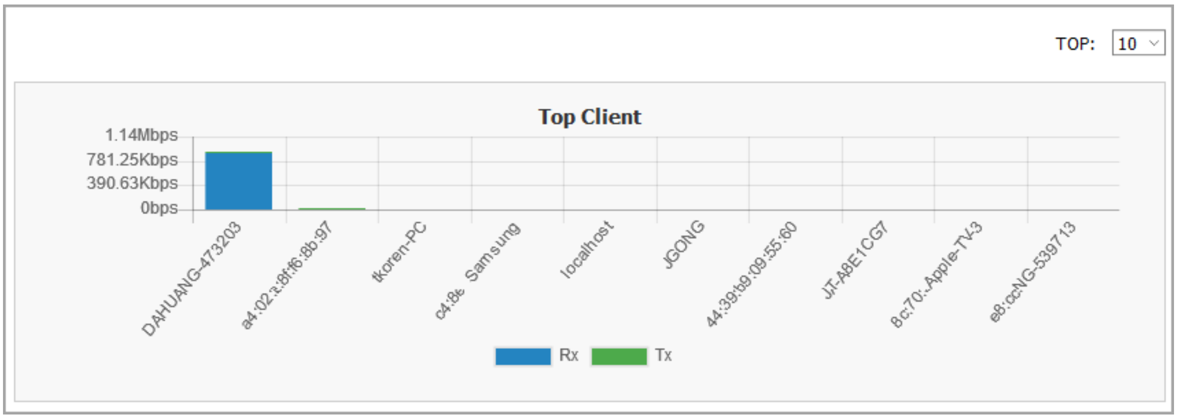
In SonicOS 6.5.2 and higher, the **Client Report** also provides a **Radio** chart. The **Radio** chart shows the percentage of clients connected to the 2.4GHz radio and the 5GHz radio.



ⓘ | **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Radio** feature.

Top Client

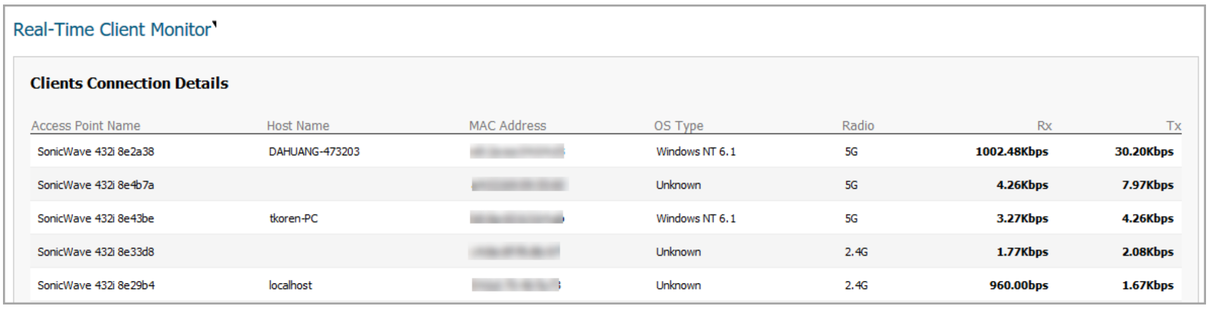
The **Top Client** chart shows the clients who are using the most bandwidth. By going to the **TOP** field and selecting a number from the drop-down menu, you can show the top 5, top 10, top 15 or top 20 consumers for bandwidth. The values for both transmitting and receiving data are shown for the top users.



NOTE: Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Top Client** feature.

Real-Time Client Monitor

A graph showing the client connection details is displayed in the **Real-Time Client Monitor** section of the **Connectivity | Access Point > Dashboard**. This provides the detail for each user connected through the access points. You can see MAC address, hostname, OS type, volume of traffic being received (Rx) and the volume of traffic being transmitted (Tx).



Real-Time Client Monitor

Clients Connection Details

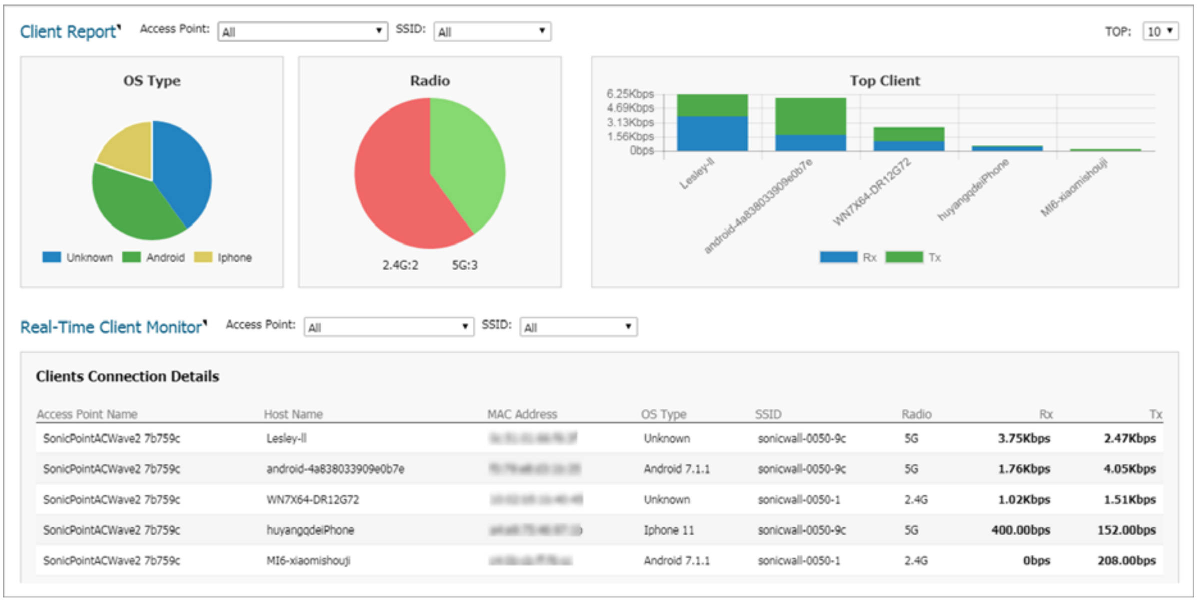
Access Point Name	Host Name	MAC Address	OS Type	Radio	Rx	Tx
SonicWave 432i 8e2a38	DAHUANG-473203	[redacted]	Windows NT 6.1	5G	**1002.48Kbps**	**30.20Kbps**
SonicWave 432i 8e4b7a		[redacted]	Unknown	5G	**4.26Kbps**	**7.97Kbps**
SonicWave 432i 8e43be	tkoren-PC	[redacted]	Windows NT 6.1	5G	**3.27Kbps**	**4.26Kbps**
SonicWave 432i 8e33d8		[redacted]	Unknown	2.4G	**1.77Kbps**	**2.08Kbps**
SonicWave 432i 8e29b4	localhost	[redacted]	Unknown	2.4G	**960.00bps**	**1.67Kbps**

NOTE: Only SonicPoint ACe/ACi/N2 and SonicWave devices support the **Real-Time Client Monitor** feature.

Client Report and Client Monitor Filtering

Beginning in SonicOS 6.5.2, you can filter the output in both the **Client Report** section and the **Real-Time Client Monitor** section by selecting *All* or a specific access point in the **Access Point** drop-down menu, and/or by selecting *All* or a specific SSID in the **SSID** drop-down menu.

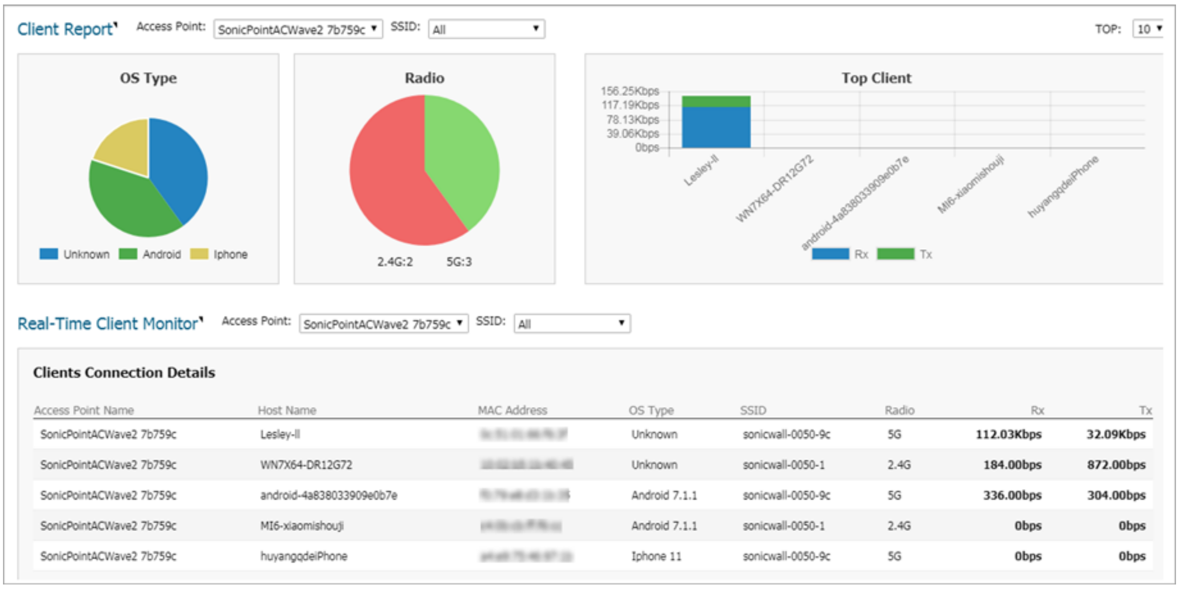
Client Detail for All



Clients Connection Details

Access Point Name	Host Name	MAC Address	OS Type	SSID	Radio	Rx	Tx
SonicPointACWave2 7b759c	Lesley-ll	[redacted]	Unknown	sonicwall-0050-9c	5G	**3.75Kbps**	**2.47Kbps**
SonicPointACWave2 7b759c	android-4a838033909e0b7e	[redacted]	Android 7.1.1	sonicwall-0050-9c	5G	**1.76Kbps**	**4.05Kbps**
SonicPointACWave2 7b759c	WN7X64-DR12G72	[redacted]	Unknown	sonicwall-0050-1	2.4G	**1.02Kbps**	**1.51Kbps**
SonicPointACWave2 7b759c	huyangqdeiPhone	[redacted]	Iphone 11	sonicwall-0050-9c	5G	**400.00bps**	**152.00bps**
SonicPointACWave2 7b759c	MI6-xiaomishouji	[redacted]	Android 7.1.1	sonicwall-0050-1	2.4G	**0bps**	**208.00bps**

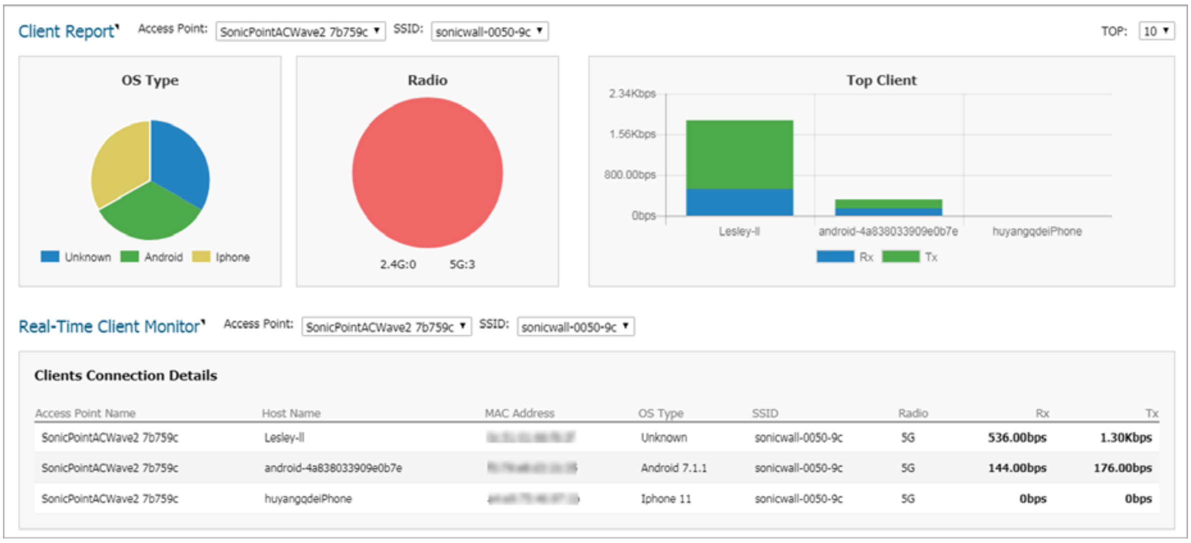
Client Detail Filtered by Access Point



Clients Connection Details

Access Point Name	Host Name	MAC Address	OS Type	SSID	Radio	Rx	Tx
SonicPointACWave2 7b759c	Lesley-ll	[redacted]	Unknown	sonicwall-0050-9c	5G	**112.03Kbps**	**32.09Kbps**
SonicPointACWave2 7b759c	WN7X64-DR12G72	[redacted]	Unknown	sonicwall-0050-1	2.4G	**184.00bps**	**872.00bps**
SonicPointACWave2 7b759c	android-4a838033909e0b7e	[redacted]	Android 7.1.1	sonicwall-0050-9c	5G	**336.00bps**	**304.00bps**
SonicPointACWave2 7b759c	MI6-xiaomishouji	[redacted]	Android 7.1.1	sonicwall-0050-1	2.4G	**0bps**	**0bps**
SonicPointACWave2 7b759c	huyangqdeiPhone	[redacted]	Iphone 11	sonicwall-0050-9c	5G	**0bps**	**0bps**

Client Detail Filtered by Access Point and SSID



Client Report Access Point: SonicPointACWave2 7b759c SSID: sonicwall-0050-9c TOP: 10

Real-Time Client Monitor Access Point: SonicPointACWave2 7b759c SSID: sonicwall-0050-9c

Clients Connection Details

Access Point Name	Host Name	MAC Address	OS Type	SSID	Radio	Rx	Tx
SonicPointACWave2 7b759c	Lesley-ll	[redacted]	Unknown	sonicwall-0050-9c	5G	**536.00bps**	**1.30Kbps**
SonicPointACWave2 7b759c	android-4a838033909e0b7e	[redacted]	Android 7.1.1	sonicwall-0050-9c	5G	**144.00bps**	**176.00bps**
SonicPointACWave2 7b759c	huyangqdeiPhone	[redacted]	Iphone 11	sonicwall-0050-9c	5G	**0bps**	**0bps**

ⓘ **NOTE:** Only SonicPoint ACe/ACi/N2 and SonicWave devices support client detail filtering.

16

Access Point Base Settings

The most effective way to provision wireless access points is let the SonicOS firewall automatically detect the access points and use one of the default profiles. SonicOS includes four default profiles, one for each generation of SonicWall access points: SonicPointN, SonicPointNDR, SonicPointACe/ACi/N2, and SonicWave. These can be used as is, or they can be customized to suit your configuration. You can also build new profiles based on the type of SonicWall access point you have.

The top of the **MANAGE | Connectivity | Access Points > Base Settings** page displays informational messages and shows the firmware version for operational access points. The **SYNCHRONIZE** button is below the messages.

The access point profiles are displayed in the **SonicPoint / SonicWave Provisioning Profiles** section. You can edit each profile or add a new profile.

The **SonicPoint / SonicWave Objects** section displays the settings for connected access points, and provides **Configure** buttons to edit them or perform other actions.

ⓘ **NOTE:** When wireless LAN is disabled, all Access Points and Wireless related pages disappear. Wireless Zone is removed from zone type. And any existing WLAN zones or objects are not editable anymore.

Topics:

- Synchronize Access Points
- Provisioning Overview
- Creating/Modifying Provisioning Profiles
- Managing Access Points

Synchronize Access Points

Click **SYNCHRONIZE ACCESS POINTS** at the top of the **Connectivity | Access Points > Base Settings** page to issue a query from the SonicWall appliance to the WLAN Zone. All connected access points report their current settings and statistics to the appliance. SonicOS also attempts to locate the presence of any newly connected access points that are not yet registered with the firewall.

ⓘ **NOTE:** The button polls the access points, but does not push configuration to them.

Provisioning Overview

SonicPoint/SonicWave Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple access points across a Distributed Wireless Architecture. SonicPoint/SonicWave Profile definitions include all of the settings that can be configured on a SonicWall access point, such as radio settings for the 2.4GHz and 5GHz radios, SSID’s, and channels of operation.

After you have defined a access point profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one access point profile. Any profile can apply to any number of zones. Then when an access point is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

When an access point is first connected and powered up, it has a factory default configuration (IP address: `192.168.1.20`, username: `admin`, password: `password`). Upon initializing, the unit attempts to find a SonicOS device with which to peer. When a SonicOS device starts up, it also searches for access points through the SonicWall Discovery Protocol. If the access point and a peer SonicOS device find each other, they communicate through an encrypted exchange where the profile assigned to the relevant Wireless zone is used to automatically provision the newly added access point unit.

As part of the provisioning process, SonicOS assigns the discovered access point a unique name and records its MAC address, the interface, and zone on which it was discovered. If part of the profile, it can also automatically assign an IP address so that the access point can communicate with an authentication server for WPA-EAP support. SonicOS then uses the profile associated with the relevant zone to configure the 2.4GHz and 5GHz radio settings.

Note that changes to profiles do not affect units that have already been provisioned and are in an operational state. Configuration changes to operational access points can occur in two ways:

- Through manual configuration changes

  This option is the best choice when a single, or a small set of changes are to be made, particularly when that individual access point requires settings that are different from the profile assigned to its zone.

- Through un-provisioning

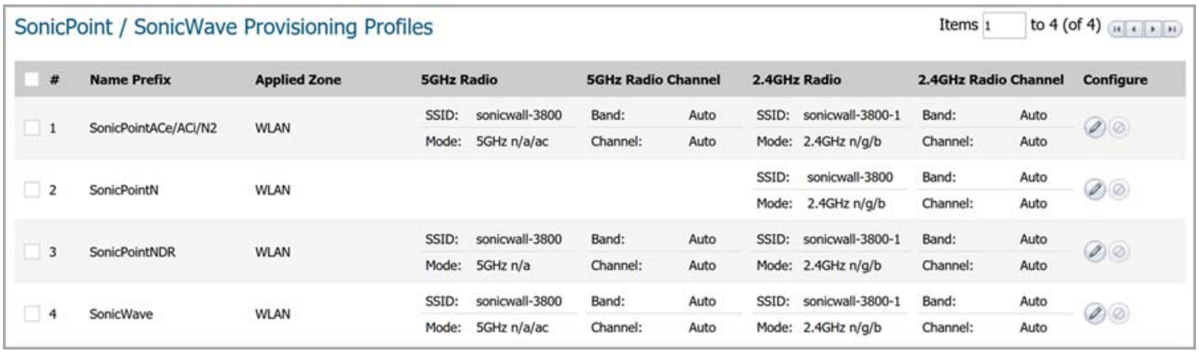
  Deleting an access point effectively un-provisions the unit. It clears its configuration and places it into a state where it automatically engages the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a zone is updated or changed, and the change is set for propagation. It can be used to update firmware on access points, or to simply and automatically update multiple access points in a *controlled* fashion, rather than changing all peered access points at the same time, causing service disruptions.

Creating/Modifying Provisioning Profiles

On the **MANAGE** view, at **Connectivity | Access Points > Base Settings**, you can configure and manage the provisioning profiles as well as the individual objects. You can add any number of profiles.

> ⓘ **NOTE:** *SonicPoint AC* refers to SonicPoint ACe/ACi/N2; *SonicPoint* refers to all SonicPoint devices. *SonicWave* refers to SonicWave 432e/432i/432o/224w/231c/231o. SonicPoint ACs are supported on appliances running SonicOS 6.2.2 and newer, while SonicWave devices are supported on SonicOS 6.5 and newer.

Navigate to the **Connectivity | Access Points > Base Settings** page. The four default SonicOS profiles are listed along with any custom profiles you've developed under the **SonicPoint/SonicWave Provisioning Profiles** section. To modify any of the default provisioning profiles, click the **Configure** icon, and make the appropriate changes.



SonicPoint / SonicWave Provisioning Profiles

Items 1 to 4 (of 4)

□	#	Name Prefix	Applied Zone	5GHz Radio	5GHz Radio Channel	2.4GHz Radio	2.4GHz Radio Channel	Configure
□	1	SonicPointACe/ACi/N2	WLAN	SSID: sonicwall-3800 Mode: 5GHz n/a/ac	Band: Auto Channel: Auto	SSID: sonicwall-3800-1 Mode: 2.4GHz n/g/b	Band: Auto Channel: Auto	
□	2	SonicPointN	WLAN			SSID: sonicwall-3800 Mode: 2.4GHz n/g/b	Band: Auto Channel: Auto	
□	3	SonicPointNDR	WLAN	SSID: sonicwall-3800 Mode: 5GHz n/a	Band: Auto Channel: Auto	SSID: sonicwall-3800-1 Mode: 2.4GHz n/g/b	Band: Auto Channel: Auto	
□	4	SonicWave	WLAN	SSID: sonicwall-3800 Mode: 5GHz n/a/ac	Band: Auto Channel: Auto	SSID: sonicwall-3800-1 Mode: 2.4GHz n/g/b	Band: Auto Channel: Auto	

IMPORTANT: Because creating or modifying the **SonicPoint/SonicWave Provisioning Profiles** are very similar across all access point types, this section reviews how to add a new profile for a SonicWave device. Significant differences in the general process are noted and described in more detail later in this section.

NOTE: The SonicWall-provided provisioning profiles cannot be deleted so the corresponding **Delete** icon is grayed out and not active.

The **Add New Profile** option has several screens where similar settings are grouped. The procedures are grouped to match those screens.

Topics:

- Adding/Editing a Provisioning Profile - Getting Started
- General Settings for Provisioning Profiles
- 5GHz/2.4GHz Radio Basic Settings for Provisioning Profiles
- 5GHz/2.4GHz Radio Advanced Settings for Provisioning Profiles
- Sensor Settings for WIDP in Provisioning Profiles
- Mesh Network Settings for Provisioning Profiles
- Bluetooth LE Settings for Provisioning Profiles
- Deleting Access Point Profiles
- Product Specific Configuration Notes

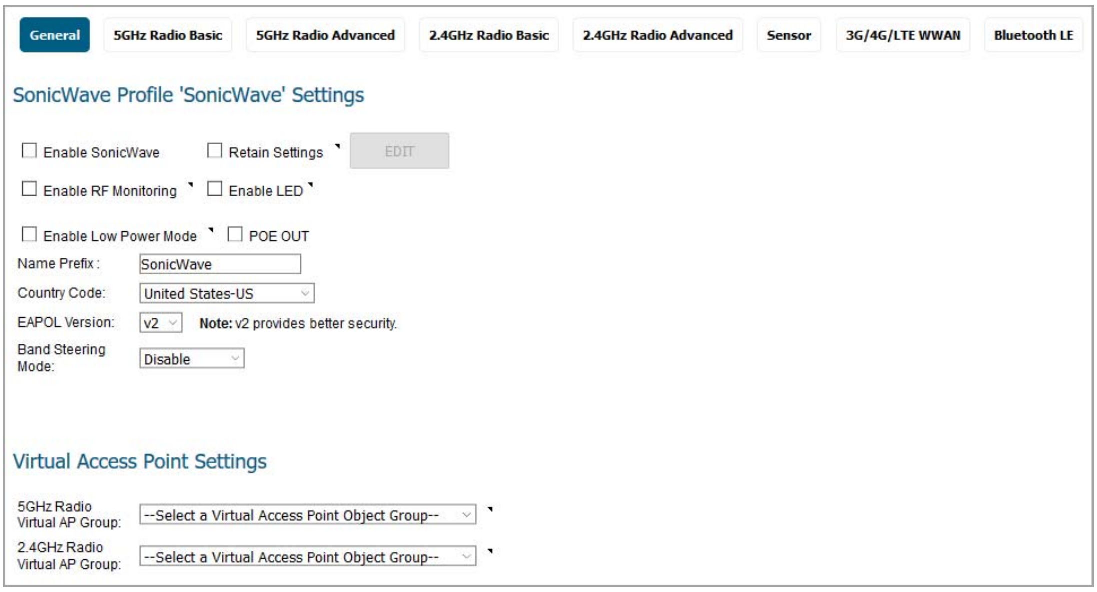
Adding/Editing a Provisioning Profile - Getting Started

To add a new provisioning profile:

1 On the **MANAGE** view, navigate to **Connectivity | Access Points > Base Settings**.

2 In the **Add New Profile** field, under the **SonicPoint/SonicWave Provisioning Profiles** section, select the type of profile you want to build. For this example **SonicWave Profile** was selected.

NOTE: To modify an existing profile, click on the **Configure** icon for profile you want to update.



SonicWave Profile 'SonicWave' Settings

□ Enable SonicWave □ Retain Settings

□ Enable RF Monitoring □ Enable LED

□ Enable Low Power Mode □ POE OUT

Name Prefix : SonicWave

Country Code: United States-US

EAPOL Version: v2 **Note:** v2 provides better security.

Band Steering Mode: Disable

Virtual Access Point Settings

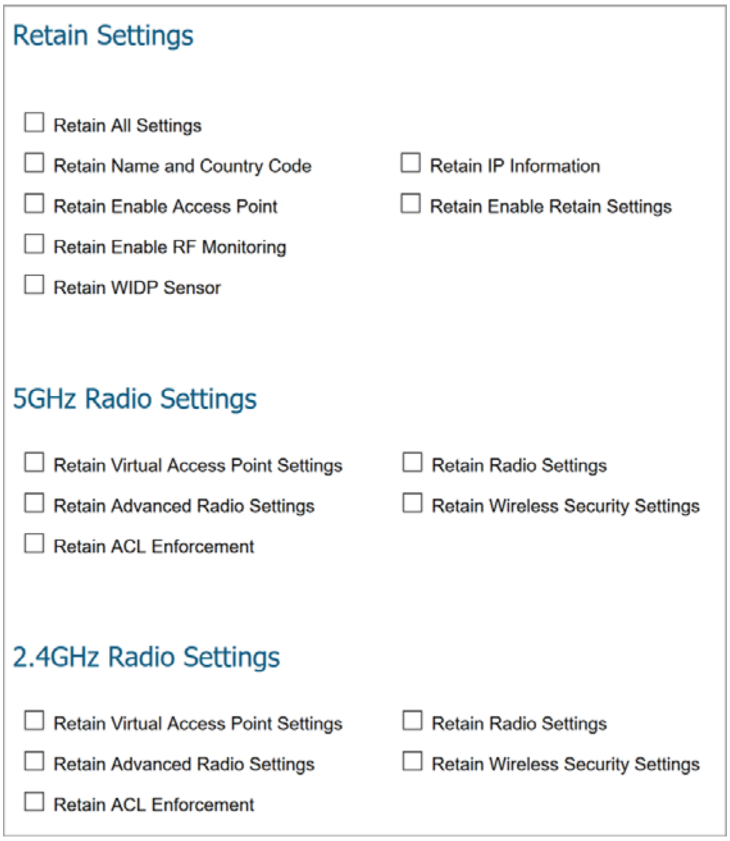
5GHz Radio Virtual AP Group: --Select a Virtual Access Point Object Group--

2.4GHz Radio Virtual AP Group: --Select a Virtual Access Point Object Group--

General Settings for Provisioning Profiles

To configure the options on the General screen:

1 Set the **SonicWave Settings**.

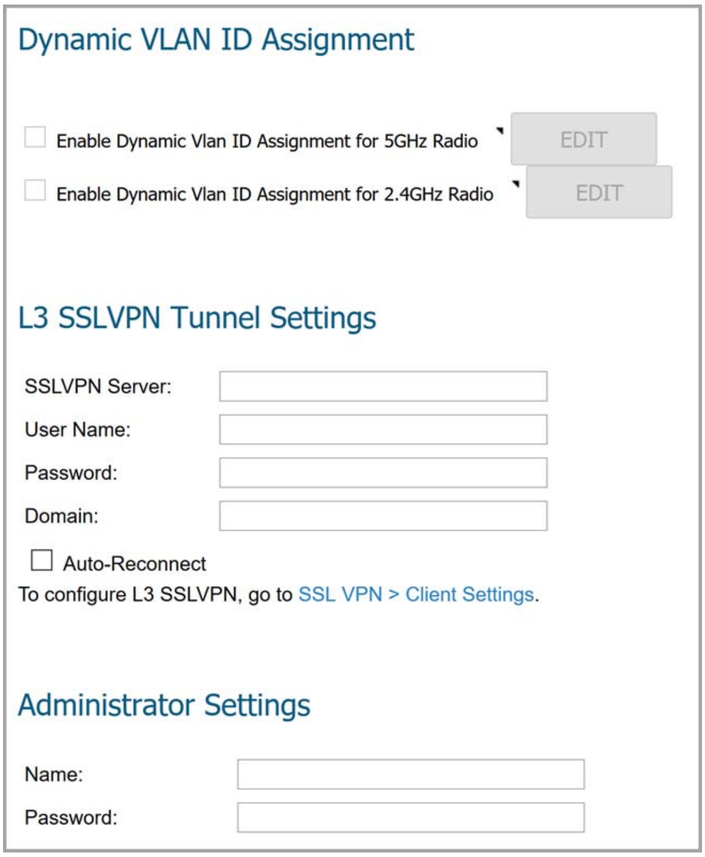
Option	Action
Enable SonicWave	When checked, enables the SonicWave access point. Default is checked.
Retain Settings	When checked, retains the customized until the next time the unit is rebooted. **EDIT** is enabled and the **Retain Settings** dialog opens so you can customize which settings should be retained.  Retain Settings □ Retain All Settings □ Retain Name and Country Code □ Retain Enable Access Point □ Retain Enable RF Monitoring □ Retain WIDP Sensor □ Retain IP Information □ Retain Enable Retain Settings 5GHz Radio Settings □ Retain Virtual Access Point Settings □ Retain Advanced Radio Settings □ Retain ACL Enforcement □ Retain Radio Settings □ Retain Wireless Security Settings 2.4GHz Radio Settings □ Retain Virtual Access Point Settings □ Retain Advanced Radio Settings □ Retain ACL Enforcement □ Retain Radio Settings □ Retain Wireless Security Settings
Enable RF Monitoring	When checked, enables wireless RF-threat, real-time monitoring and management.
Enable LED	When checked, turns on the SonicWave LEDs. If left unchecked, which is the default, the LEDs stay off.
Enable Low Power Mode	When checked, allows the SonicWave to operate in a low power mode because of the power source not being standard 802.3at PoE.
Name Prefix	Type the prefix used for the name in the field provided.
Country Code	From the drop-down menu, select the country code for the country in which the access point is deployed.
EAPOL Version	Select EAPoL version from the drop-down menu. Note that V2 provides the better security.
Band Steering Mode	Select the band steering mode from the drop-down menu. Options include: **Disable**, **Auto**, **Prefer 5GHz**, or **Force 5GHz**.

2 Set the **Virtual Access Point Settings**:

a For **5GHz Radio Virtual AP Group**, select a Virtual Access Point object group from the drop-down menu.

b For **2.4GHz Radio Virtual AP Group**, select a Virtual Access Point object group from the drop-down menu.

3 Scroll down to see the other **General** settings.



Dynamic VLAN ID Assignment

□ Enable Dynamic Vlan ID Assignment for 5GHz Radio EDIT

□ Enable Dynamic Vlan ID Assignment for 2.4GHz Radio EDIT

L3 SSLVPN Tunnel Settings

SSLVPN Server:

User Name:

Password:

Domain:

□ Auto-Reconnect

To configure L3 SSLVPN, go to SSL VPN > Client Settings.

Administrator Settings

Name:

Password:

4 Set the **Dynamic VLAN ID Assignment**.

> **NOTE:** To enable the options under **Dynamic VLAN ID Assignment**, you need create a WLAN zone and VLAN interface under **System Setup | Network**.

5 Configure the **SSLVPN Tunnel Settings**:

a Type in the **SSLVPN Server** name or IP address in the field provided.

b Type the **User Name** for the SSLVPN server in the field provided.

c Type the **Password** to authenticate on the SSLVPN server.

d Type the **Domain** name in the field provided.

e Check the box to enable **Auto-Reconnect**.

f If you want to configure Layer 3 SSLVPN, follow the link to **Connectivity | SSL VPN > Client Settings** and define the appropriate settings.

6 Set the **Administrator Settings**:

a Type in the user **Name** of the network administrator.

b Type in the **Password** for the network administrator.

5GHz/2.4GHz Radio Basic Settings for Provisioning Profiles

The basic settings for 5GHz Radio and 2.4GHz Radio across the different types of access points are similar and have only a few differences. These differences are noted in the steps.

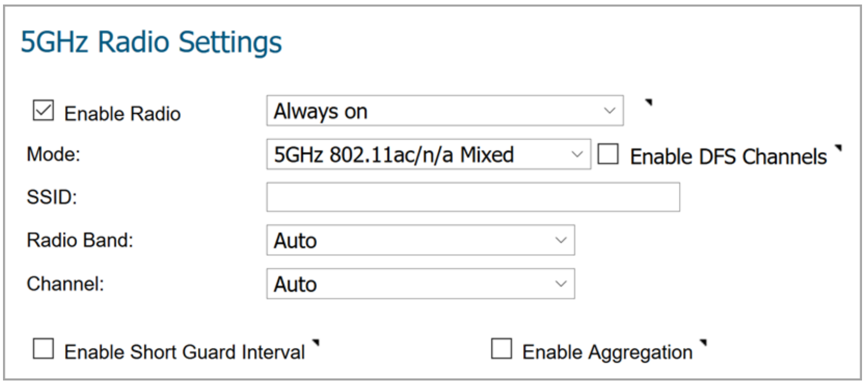
The following topics describe settings on the **5GHz/2.4GHz Radio Basic** screens:

- Radio Settings
- Wireless Security
- Protected Management Frames (PMF Option)
- About Local Radius Servers and EAP Authentication Balancing
- Configuring Radius Server Settings
- ACL Enforcement
- Remote MAC Address Access Control Settings

Radio Settings

To configure 5GHz Radio/2.4GHz Radio Basic Settings:

1 Click on **5GHz Radio Basic** or **2.4GHz Radio Basic**.



5GHz Radio Settings

☑ Enable Radio — Always on

Mode: 5GHz 802.11ac/n/a Mixed □ Enable DFS Channels

SSID:

Radio Band: Auto

Channel: Auto

□ Enable Short Guard Interval □ Enable Aggregation

2 Select **Enable Radio** to enable the radio bands automatically on all access points provisioned with this profile. This option is selected by default.

3 From the **Enable Radio** drop-down menu, select a schedule for when the radio is on or create a new schedule. The default is **Always on**.

4 Select your preferred radio mode from the **Mode** drop-down menu:

Radio Mode Choices

5GHz Radio Basic	2.4GHz Radio Basic	Definition
5GHz 802.11n Only	2.4GHz 802.11n Only	Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
5GHz 802.11n/a Mixed	2.4GHz 802.11n/g/b Mixed (SonicPoint AC/NDR default)	Supports 802.11a and 802.11n (5GHz Radio) or 802.11b, 802.11g, and 802.11n (2.4GHz Radio) clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
5GHz 802.11a Only (SonicPoint NDR default)		Select this mode if only 802.11a clients access your wireless network.
	2.4GHz 802.11g Only	If your wireless network consists only of 802.11g clients, you might select this mode for increased 802.11g performance. You might also select this mode if you wish to prevent 802.11b clients from associating.
5GHz 802.11ac/n/a Mixed (SonicWave and SonicPoint AC default)		Supports 802.11ac, 802.11a, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
5GHz 802.11ac Only		Allows only 802.11ac clients access to your wireless network. Other clients are unable to connect under this restricted radio mode.

ⓘ **TIP:** For 802.11n clients only: If you want optimal throughput, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

For optimal throughput for 802.11ac clients, SonicWall recommends the **802.11ac Only** radio mode. Use the **802.11ac/n/a Mixed** radio mode for multiple wireless client authentication compatibility.

ⓘ **NOTE:** The available **802.11n 5GHz/2.4GHz Radio Settings** options change depending on the mode selected. If the wireless radio is configured for a mode that:

- Supports 802.11n, the following options are displayed: **Radio Band**, **Primary Channel**, **Secondary Channel**, **Enable Short Guard Interval**, and **Enable Aggregation**.
- Does not support 802.11n, only the **Channel** option is displayed.

5 In the **SSID** field, enter a recognizable string for the SSID of each access point using this profile. This is the name that appears in clients' lists of available wireless connections.

ⓘ **TIP:** If all SonicPoints or SonicWaves in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one access point to another.

6 Select a radio band from the **Radio Band** drop-down menu:

ⓘ **NOTE:** When **Mode** = **5GHz 802.11a Only**, the **Radio Band** option is not available.

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. If selected for one, both the **Primary Channel** and **Secondary Channel** should set to **Auto**. This is the default setting.
- **Standard - 20MHz Channel**—Specifies that the radio uses only the standard 20MHz channel.
- **Wide - 40MHz Channel**—Available when any mode except **5GHz 802.11a Only** is selected for the **Radio Band**. It specifies that the radio uses only the wide 40MHz channel.
- **Wide - 80MHz Channel**—Available only when **5GHz 802.11ac/n/a Mixed** or **5GHz 802.11ac only** is selected for the **Radio Band**, specifies that the 5GHz Radio uses only the wide 80MHz channel. (Not available when the **Mode** is **5GHz 802.11n Only**, **5GHz 802.11n/a Mixed**, or **5GHz 802.11a Only**.)

7 Select the channel or channels based on the **Mode** and **Radio Band** options chosen:

Mode	Radio Band	Channel
5GHz 802.11n Only	Auto	The **Primary Channel** and **Secondary Channel** fields default to **Auto**.
	Standard - 20 MHz Channel	Select **Auto** or one of the radio channels specified in the **Standard Channel** drop-down menu.
	Wide - 40 MHz Channel	Select **Auto** or one of the radio channels in the **Primary Channel**. The **Secondary Channel** is automatically defined as **Auto**.
5GHz 802.11n/a Mixed	Auto	The **Primary Channel** and **Secondary Channel** fields default to **Auto**.
	Standard - 20 MHz Channel	Select **Auto** or one of the radio channels specified in the **Standard Channel** drop-down menu.
	Wide - 40 MHz Channel	Select **Auto** or one of the radio channels in the **Primary Channel**. The **Secondary Channel** is automatically defined as **Auto**.
5GHz 802.11a Only	(no option)	Select **Auto** or one of the radio channels specified in the **Channel** drop-down menu.
5GHz 802.11ac/n/a Mixed	Auto	The **Channel** field defaults to **Auto**.
	Standard - 20 MHz Channel	Select **Auto** or one of the radio channels specified in the **Channel** drop-down menu.
	Wide - 40 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** field.
	Wide - 80 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** field.

Mode	Radio Band	Channel
5GHz 802.11ac Only	Auto	The **Channel** field defaults to **Auto**.
	Standard - 20 MHz Channel	Select **Auto** or one of the radio channels specified in the **Channel** drop-down menu.
	Wide - 40 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** field.
	Wide - 80 MHz Channel	Select **Auto** or one of the radio channels in the **Channel** field.

8 Check the box to **Enable Short Guard Interval**. This allows you to increase the radio data rate by shortening the guard interval. Be sure the wireless client can support this to avoid compatibility issues.

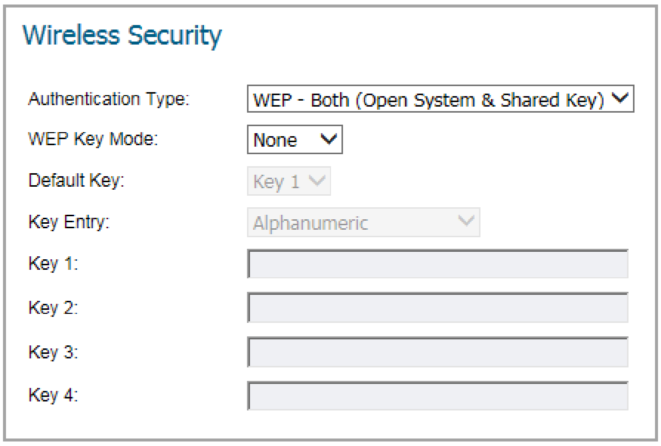
9 Check the box to **Enable Aggregation**. This allows you to increase the radio throughput by sending multiple data frames in a single transmission. Be sure the wireless client can support this to avoid compatibility issues.

Wireless Security

ⓘ **NOTE:** The SonicOS interface is context-sensitive. If a VAP Group was selected in the **General** screen, the **Wireless Security** section is hidden and you can skip this section.

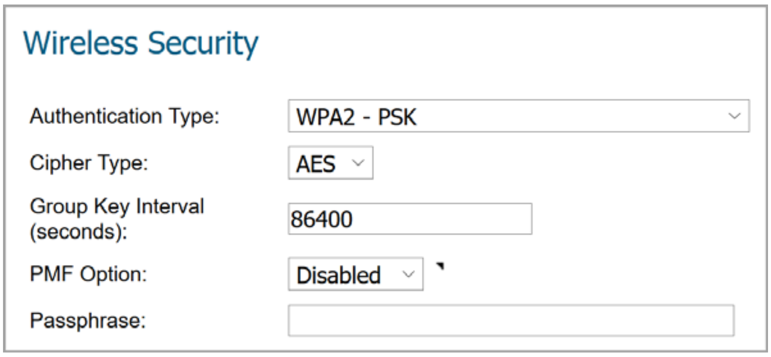
To set the Wireless Security options:

1 Scroll down to the **Wireless Security** section. The options vary depending on the selected **Authentication Type**.



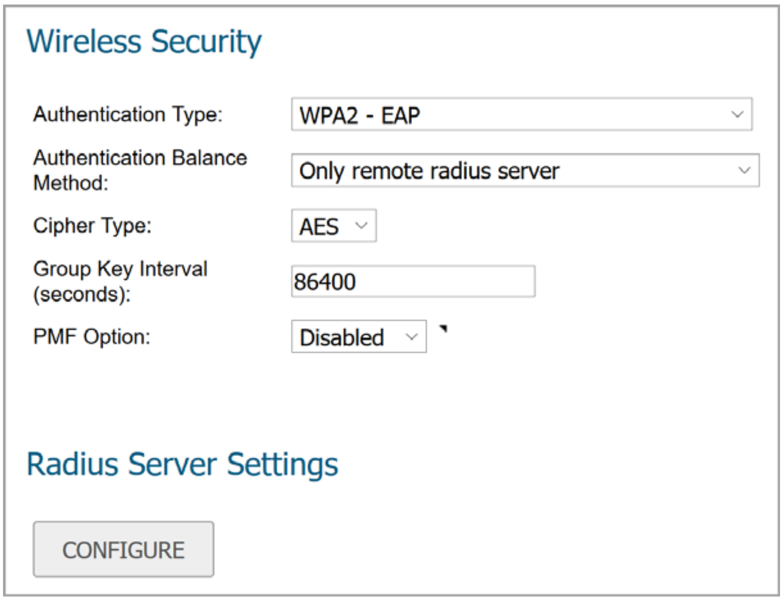
Wireless Security

Authentication Type:	WEP - Both (Open System & Shared Key)
WEP Key Mode:	None
Default Key:	Key 1
Key Entry:	Alphanumeric
Key 1:	
Key 2:	
Key 3:	
Key 4:	



Wireless Security

Authentication Type:	WPA2 - PSK
Cipher Type:	AES
Group Key Interval (seconds):	86400
PMF Option:	Disabled
Passphrase:	



Wireless Security

Authentication Type: WPA2 - EAP

Authentication Balance Method: Only remote radius server

Cipher Type: AES

Group Key Interval (seconds): 86400

PMF Option: Disabled

Radius Server Settings

To configure Wireless Security:

1. In the **Wireless Security** section, select the **Authentication Type** from the drop-down menu.

   > **NOTE:** The options available change with the type of configuration you select. If a **WPA2 - EAP** option is selected, the **Radius Server Settings** section appears with the **CONFIGURE** button.

2. Define the remaining settings, using the following tables as a reference:

WEP Settings for Wireless Security

WEP Description

Authentication Type	WEP Key Mode	Settings
WEP (Wired Equivalent Privacy) is standard for Wi-Fi wireless network security. Open system uses and exchange of information to authenticate and then encrypts the data. Shared keys uses a shared secret key to authenticate.		
WEP - Both (Open System & Shared Key)	**WEP Key Mode** = **None**	Remaining settings are grayed out and cannot be selected.
	WEP Key Mode = **64 bit**, **128 bit** or **152 bit** The number of bits indicates the key strength of the WEP key.	1 In **Default Key** field, select the default key (the key that is tried first). **Key 1** is the default. 2 In the **Key Entry** field, choose whether the key is **Alphanumeric** or **Hexadecimal (0-9, A-F)**. 3 In the fields for Key 1, Key 2, Key 3, and Key 4 enter encryption keys that are used when transferring data.

WEP Settings for Wireless Security (Continued)

	WEP Description	
Authentication Type	**WEP Key Mode**	**Settings**
WEP - Open System		Remaining settings are grayed out and cannot be selected.
WEP - Shared Key	**WEP Key Mode** = **64 bit**, **128 bit** or **152 bit** The default is **152 bit**.	1 In **Default Key** field, select the default key (the key that is tried first). **Key 1** is the default. 2 In the **Key Entry** field, choose whether the key is **Alphanumeric** or **Hexadecimal (0-9, A-F)**. The **Hexadecimal** option is the default. 3 In the fields for Key 1, Key 2, Key 3, and Key 4 enter encryption keys that are used when transferring data.

WPA2 Settings for Wireless Security

	Description
Authentication Type	**Settings**
WPA and WPA2 (Wi-Fi Protected Access) are newer protocols for protecting wireless devices. Selecting one of the **WPA2 - AUTO** options allows the WPA protocol to be used if a device is not enabled for WPA2.	
WPA2 - PSK	1 Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. 2 Set the **Group Key Interval** in seconds. The default is **86400**. 3 For SonicWave, select the **PMF Option** from the drop-down menu. See Protected Management Frames (PMF Option) on page 183 for more information. 4 Define the **Passphrase** for the public shared key.
WPA2 - EAP	1 For SonicWave, select the **Authentication Balance Method** from the drop-down menu. See About Local Radius Servers and EAP Authentication Balancing on page 184 for more information. 2 Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. 3 Set the **Group Key Interval** in seconds. The default is **86400**. 4 For SonicWave, select the **PMF Option** from the drop-down menu. See Protected Management Frames (PMF Option) on page 183 for more information.

WPA2 Settings for Wireless Security (Continued)

Authentication Type	Description Settings
WPA2 - AUTO - PSK	1 Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. 2 Set the **Group Key Interval** in seconds. The default is **86400**. 3 For SonicWave, select the **PMF Option** from the drop-down menu. See Protected Management Frames (PMF Option) on page 183 for more information. 4 Define the **Passphrase** for the public shared key.
WPA2 - AUTO - EAP	1 For SonicWave, select the **Authentication Balance Method** from the drop-down menu. See About Local Radius Servers and EAP Authentication Balancing on page 184 for more information. 2 Select **Cipher Type** from the drop-down menu. Options are **AES** (default), **TKIP**, or **Auto**. 3 Set the **Group Key Interval** in seconds. The default is **86400**. 4 For SonicWave, select the **PMF Option** from the drop-down menu. See Protected Management Frames (PMF Option) on page 183 for more information.

Protected Management Frames (PMF Option)

When **Authentication Type** is set to any **WPA2** option, the **PMF Option** setting is available. The **PMF Option** setting is supported for SonicWave profiles starting in SonicOS 6.5.2. This feature supports the IEEE 802.11w-2009 amendment to the IEEE 802.11 standard for protection of wireless management frames. It is also known as the Protected Management Frames (PMF) standard.

You can select one of the following settings from the **PMF Option** drop-down menu under **Wireless Security**:

- **Disabled** – The service is not enabled. Clients connect without PMF.
- **Enabled** – The service is optional for wireless clients. Clients can connect with or without PMF, based on client settings.
- **Required** – Clients must have PMF enabled to connect.

While the 802.11i amendment protects ***data*** frames, management frames such as authentication, de-authentication, association, dissociation, beacons, and probes are used by wireless clients to initiate and tear down sessions for network services. Unlike data traffic, which can be encrypted to provide a level of confidentiality, these frames must be heard and understood by all clients and therefore must be transmitted as open or unencrypted. While these frames cannot be encrypted, they must be protected from forgery to protect the wireless medium from attacks. For example, if an attacker obtains the MAC address of a client, it can send a disassociation request to the client in the name of an AP, or send a re-association request to an AP in the name of the client. The client is logged off in either situation.

The 802.11w amendment applies to a set of robust ***management*** frames that are protected by the Protected Management Frames (PMF) service. These include Disassociation, De-authentication, and Robust Action frames. 802.11w protects only specific management frames and does not affect the communication between access points and clients. 802.11w can only take effect when both access points and clients have 802.11w enabled.

802.11w provides the following benefits:

Confidentiality

Encrypts Unicast management frames:

- Uses same PTK as for data frames
- Protects the previously unencrypted frame header through additional authentication data (AAD)
- Extended AES-CCM to handle Unicast management frames

	• Separate Receive Sequence Counter (RSC) for replay protection
Group addressed frame protection	Broadcast/Multicast Integrity Protocol (BIP) protects the integrity of broadcasts and multi casts, prevents replay attacks, and protects clients from spoofing broadcast/multicast attacks. For Broad-/Multi casts Management Frames: • Uses new Integrity Group Temporal Key (IGTK) received during WPA key handshake • New Algorithm: Broadcast Integrity Protocol (BIP) • New Information Element: Management MIC IE with Sequence Number + Cryptographic Hash (AES128-CMAC-based)
Connection protection	Security Association (SA) Query can prevent clients from going offline caused by spoofing re-association requests.

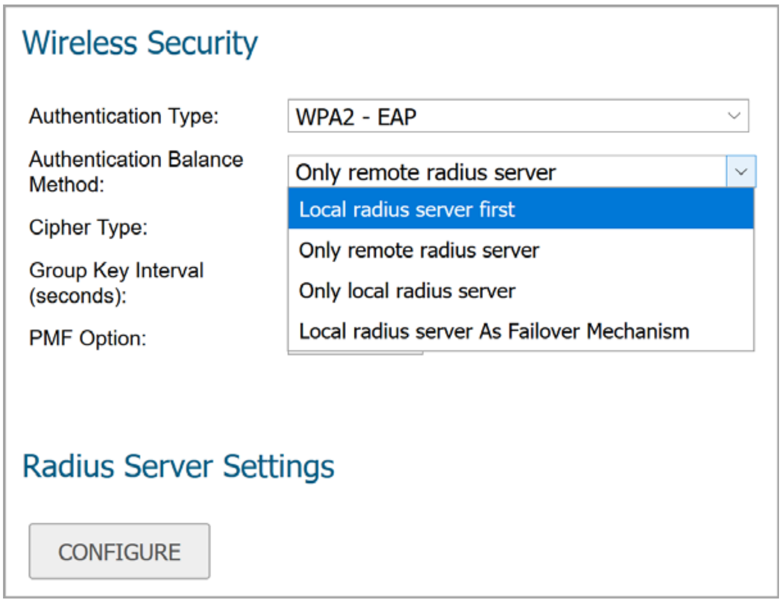
About Local Radius Servers and EAP Authentication Balancing

This feature is introduced in SonicOS 6.5.2. It allows local SonicWave access points to provide local RADIUS authentication service within selected SonicWaves and integrates with corporate directory services, including native LDAP systems and Active Directory. In this scenario, the SonicWave provides EAP authentication for clients and functions as both the authenticator and authentication server simultaneously. LDAP cache and TLS cache are supported for fast performance when reconnecting.

To configure this feature, you need:

- An interface in the WLAN zone with one or more local RADIUS servers configured in the subnet; these are the SonicWave local RADIUS servers
- WLAN zone configured with the **Enable Local Radius Server** option selected on the **Radius Server** screen; this option controls whether this feature is enabled or not.
- SonicWave profile with the following settings on the **Radio Basic** screen(s):
  - One of the **WPA2 - EAP** types selected for **Authentication Type**

    The **Radius Server Settings** section appears with the **CONFIGURE** button for configuring the local RADIUS server settings. See Configuring Radius Server Settings for details.
  - One of the **Local Radius Server** options selected for **Authentication Balance Method**



Wireless Security

Authentication Type: WPA2 - EAP

Authentication Balance Method: Only remote radius server

Cipher Type:

Group Key Interval (seconds):

PMF Option:

Local radius server first
Only remote radius server
Only local radius server
Local radius server As Failover Mechanism

Radius Server Settings

Local radius server first – With this option selected, when a client tries to authenticate, a local RADIUS server is used first. If the authentication fails, the authentication request is sent to the remote RADIUS server.

Only remote radius server – Only use the remote RADIUS server for authentication.

Only local radius server – Only use the local RADIUS server for authentication.

Local radius server As Failover Mechanism – When the remote RADIUS server is down, the local RADIUS server are used automatically.

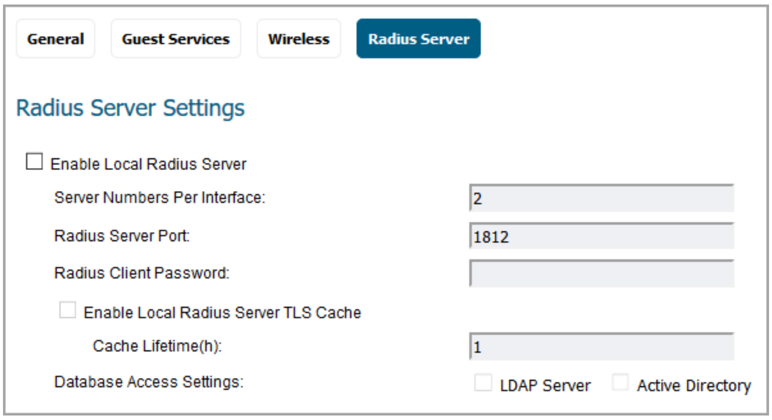
- NAT policy, Access Rule, Address Group, RADIUS pool - automatically configured

When you enable a local RADIUS server on a SonicWave, a NAT policy and access rule are automatically created. The SonicOS NAT module has failover and load balance methods, so a RADIUS server pool is supported. Additional SonicWaves with a local RADIUS server configured can be added to this pool. More than one local RADIUS server provides a failover mechanism and optimizes network performance.

The **Enable Local Radius Server** option and other settings are configured in the **Radius Server** screen available when configuring the ***WLAN zone***, configured from the **MANAGE | System Setup | Networks > Zones** page. This screen provides options for setting the number of RADIUS servers per interface, the server port, the client password, the TLS cache, and LDAP or Active Directory access settings. When you enable a local RADIUS server on a SonicWave, the configured RADIUS server port and client password are used on that SonicWave.

NOTE: The SonicWave DNS server must be able to resolve the name of the LDAP server or Active Directory server domain.

The **Server Numbers Per Interface** option controls the number of local RADIUS servers under one specific interface in this zone. Increasing this value means more SonicWaves can be add to the RADIUS pool. The minimum value is 1, and the maximum is equal to maximum number of SonicWaves per interface in a WLAN Zone. Because the number configured for the option can be smaller than the number of connected SonicWaves, the specific SonicWaves configured as local RADIUS servers is not fixed.



Radius Server Settings

☐ Enable Local Radius Server

Server Numbers Per Interface: 2

Radius Server Port: 1812

Radius Client Password:

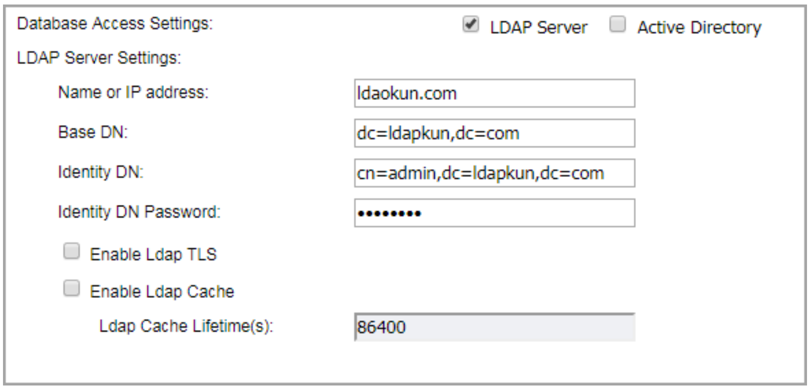
☐ Enable Local Radius Server TLS Cache

Cache Lifetime(h): 1

Database Access Settings: ☐ LDAP Server ☐ Active Directory

When the **Enable Local Radius Server TLS Cache** option is enabled, the client and the server can cache TLS session keys and use these to reduce the delay in time between an authentication request by a client and the response by the RADIUS server. Clients can also perform a fast reconnect. When enabled, you can set the **Cache Lifetime** option to the number of hours that cached entries are saved. The cache lifetime can be a number between one hour and 24 hours.

An example of LDAP **Database Access Settings** is shown below:



Database Access Settings: ☑ LDAP Server □ Active Directory

LDAP Server Settings:

Name or IP address: ldaokun.com

Base DN: dc=ldapkun,dc=com

Identity DN: cn=admin,dc=ldapkun,dc=com

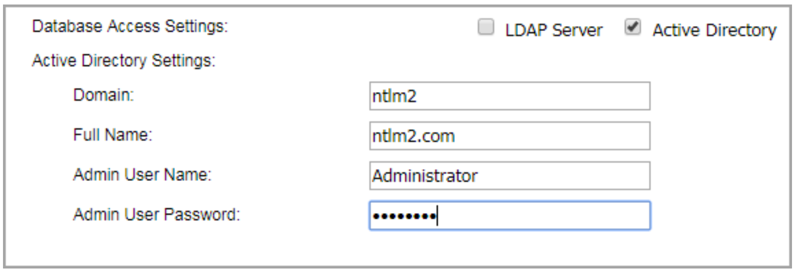
Identity DN Password: ••••••••

□ Enable Ldap TLS

□ Enable Ldap Cache

Ldap Cache Lifetime(s): 86400

An example of Active Directory **Database Access Settings** is shown below:



Database Access Settings: □ LDAP Server ☑ Active Directory

Active Directory Settings:

Domain: ntlm2

Full Name: ntlm2.com

Admin User Name: Administrator

Admin User Password: ••••••••

When the security appliance powers up, if **Enable Local Radius Server** is enabled on the WLAN zone, an address object, the RADIUS Pool, a NAT policy, and an access rule should be created. The RADIUS Pool name is a combination of the interface name plus “Radius Pool,” for example, `X2 Radius Pool`. A new address object is automatically created for the SonicWave acting as a RADIUS server, which is named with the interface name and MAC address of the SonicWave, for example, `X2 18:b1:69:7b:75:2e`. This address object is added to the RADIUS Pool if seats are available.

If **Enable Local Radius Server** is disabled, the SonicWave address object, RADIUS pool, NAT policy, and access rule are removed, and a DELETE command by restApi is sent to the SonicWaves which are in the RADIUS pool to make the local RADIUS server go down.

If the WLAN zone is edited, the NAT policy and access rule are removed and re-created. The RADIUS pool always exists unless **Enable Local Radius Server** is disabled.

If the interface changes, the NAT policy, access rule, and RADIUS pool are removed and created again if the interface is still bound to the WLAN Zone.

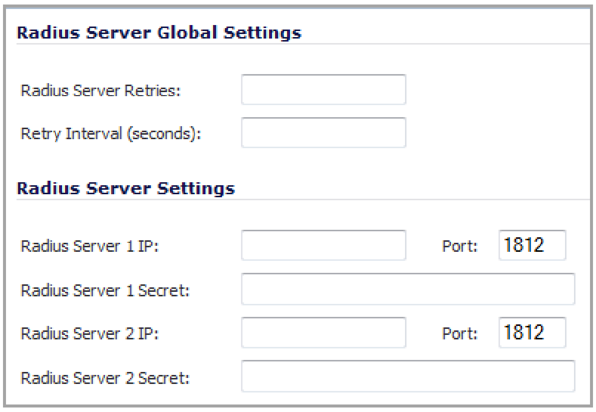
Configuring Radius Server Settings

If you selected either **WPA2 - EAP** or **WPA2 - AUTO - EAP** in the **Wireless Security** section, the **Radius Server Settings** section appears for configuration of a RADIUS server to generate authentication keys. The server has to be configured for this and for communicating with the SonicWall appliance.

To configure Radius Server Settings:

1 Click **CONFIGURE**. The **Radius Server Settings** dialog displays. The options displayed on this dialog depend on the type of SonicPoint/SonicWave.

SonicPointNDR or SonicPoint N



Radius Server Global Settings

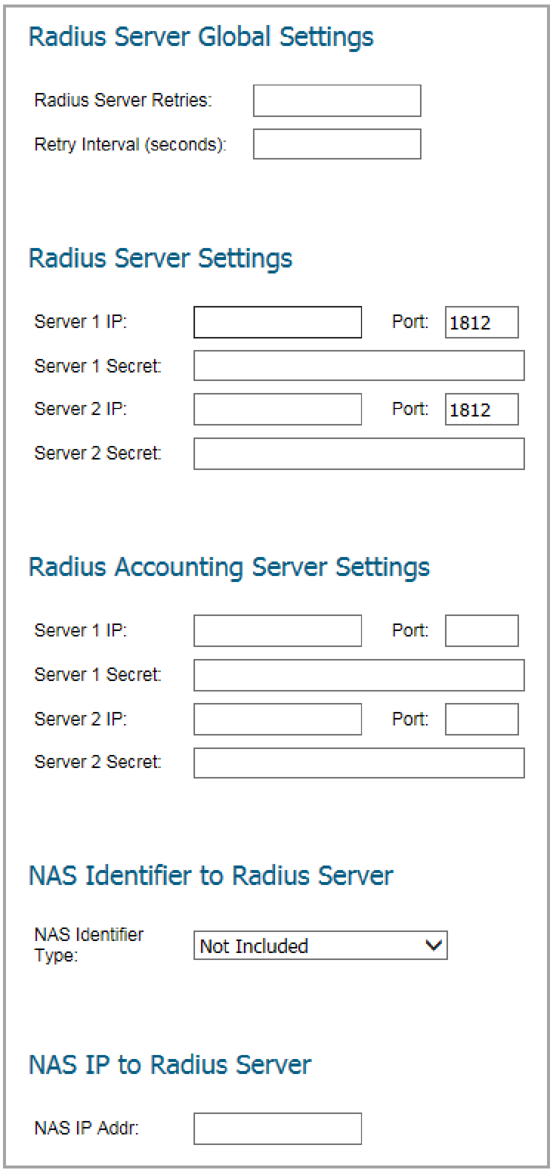
Radius Server Retries:

Retry Interval (seconds):

Radius Server Settings

Radius Server 1 IP:		Port:	1812
Radius Server 1 Secret:			
Radius Server 2 IP:		Port:	1812
Radius Server 2 Secret:			

SonicPointACe/ACi/N2 - SonicWave



Radius Server Global Settings

Radius Server Retries:

Retry Interval (seconds):

Radius Server Settings

Server 1 IP:		Port:	1812
Server 1 Secret:			
Server 2 IP:		Port:	1812
Server 2 Secret:			

Radius Accounting Server Settings

Server 1 IP:		Port:	
Server 1 Secret:			
Server 2 IP:		Port:	
Server 2 Secret:			

NAS Identifier to Radius Server

NAS Identifier Type: Not Included

NAS IP to Radius Server

NAS IP Addr:

2 In the **Radius Server Retries** field, enter the number times, from 1 to 10, the firewall attempts to connect before it fails over to the other Radius server.

3 In the **Retry Interval (seconds)** field enter the time, from 0 to 60 seconds, to wait between retries. The default number is **0** or no wait between retries.

4 Define the **Radius Server Settings** as described in the following table:

RADIUS Authentication Server Settings

Option	Description
Server 1 IP	The name/location of your RADIUS authentication server
Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices. The default port is **1812**.
Server 1 Secret	The secret passcode for your RADIUS authentication server
Server 2	The name/location of your backup RADIUS authentication server
Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices. The default port is **1812**.
Server 2 Secret	The secret passcode for your backup RADIUS authentication server

5 If you are using a Radius server to track usage for charging, set up the Radius Accounting Server:

RADIUS Accounting Server Settings

Option	Description
Server 1 IP	The name/location of your RADIUS accounting server
Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices.
Server 1 Secret	The secret passcode for your RADIUS authentication server
Server 2	The name/location of your backup RADIUS authentication server
Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices.
Server 2 Secret	The secret passcode for your backup RADIUS authentication server

6 To send the NAS identifier to the RADIUS server, select the type from the **NAS Identifier Type** drop-down menu:

- **Not Included** (default)
- **SonicPoint's Name**
- **SonicPoint's MAC Address**
- **SSID** – When the SSID option is selected, both the RADIUS authentication message and RADIUS accounting message carry the access point SSID.

7 To send the NAS IP address to the RADIUS Server, enter the address in the **NAS IP Addr** field.

8 Click **OK**.

ACL Enforcement

Each access point can support an Access Control List (ACL) to provide more effective authentication control. The ACL feature works in tandem with the wireless MAC Filter List currently available on SonicOS. Using the ACL Enforcement feature, users are able to enable or disable the MAC Filter List, set the Allow List, and set the Deny list.

To enable MAC Filter List enforcement:

1. Check the box to **Enable MAC Filter List**. When the MAC filter list is enabled, the other settings are also enabled so you can set them.
2. In the **Allow List**, select an option from the drop-down menu. This identified which MAC addresses you allow to have access.

   Choose **Create MAC Address Object Group** if you want to create a new address object group made up of those you want to have access. Refer to *SonicOS 6.5 Policies* for information on how to do that.
3. In the **Deny List**, select an option from the drop-down menu. This identified which MAC addresses that you deny access to.

   Choose **Create MAC Address Object Group** if you want to create a new address object group made up of those who should not have access. Refer to *SonicOS 6.5 Policies* for information on how to do that.
4. Check the box to **Enable MIC Failure ACL Blackist**.
5. Set a **MIC Failure Frequency Threshold** based on number of times per minute. The default is **3**.

Remote MAC Address Access Control Settings

This option allows you to enforce radio wireless access control based on the MAC-based authentication on the RADIUS Server.

To allow wireless access control:

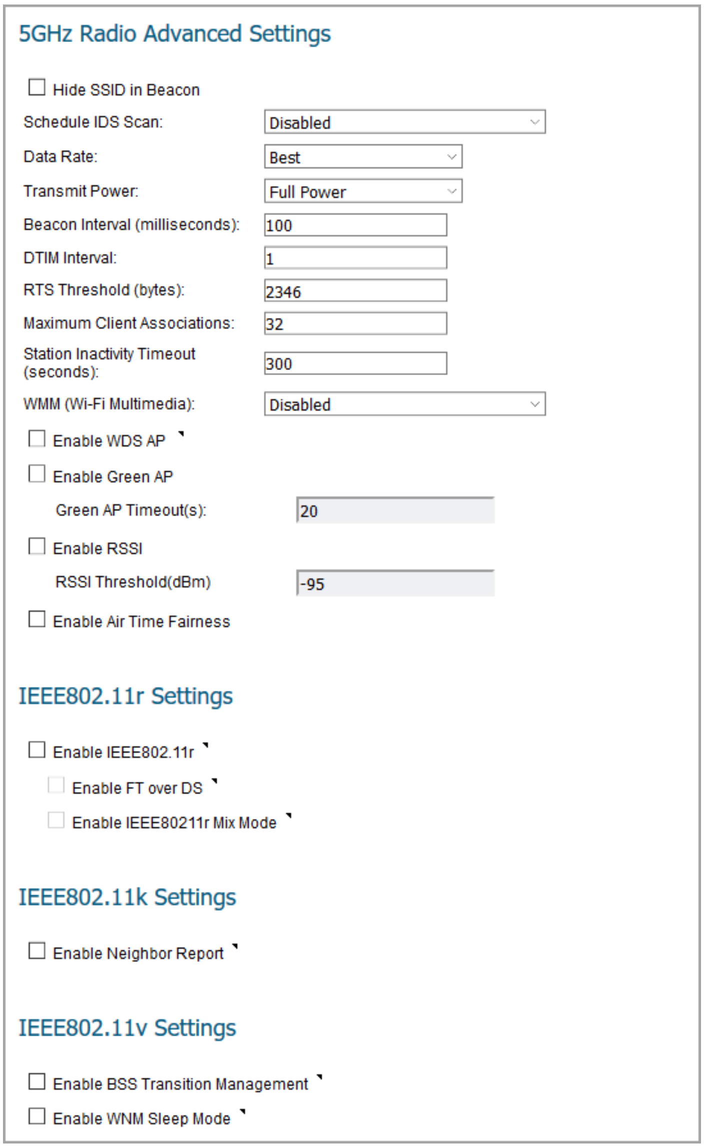
1. Check the box to **Enable Remote MAC Access Control**.
2. Click **CONFIGURE**.
3. If not already configured, set up the RADIUS Server(s) as described in Configuring Radius Server Settings.
4. Click **OK**.

5GHz/2.4GHz Radio Advanced Settings for Provisioning Profiles

These settings affect the operation of the radio bands. The SonicPoint/SonicWave has two separate radios built in. Therefore, it can send and receive on both bands at the same time.

The **5GHz Radio Advanced** screen has the same options as the **2.4GHz Radio Advanced** screen, plus other options. The screens are similar across the different access point models. Differences are noted in the procedure where needed.

Radio Advanced Settings



5GHz Radio Advanced Settings

☐ Hide SSID in Beacon

Schedule IDS Scan:	Disabled
Data Rate:	Best
Transmit Power:	Full Power
Beacon Interval (milliseconds):	100
DTIM Interval:	1
RTS Threshold (bytes):	2346
Maximum Client Associations:	32
Station Inactivity Timeout (seconds):	300
WMM (Wi-Fi Multimedia):	Disabled

☐ Enable WDS AP

☐ Enable Green AP

Green AP Timeout(s): 20

☐ Enable RSSI

RSSI Threshold(dBm) -95

☐ Enable Air Time Fairness

IEEE802.11r Settings

☐ Enable IEEE802.11r

☐ Enable FT over DS

☐ Enable IEEE80211r Mix Mode

IEEE802.11k Settings

☐ Enable Neighbor Report

IEEE802.11v Settings

☐ Enable BSS Transition Management

☐ Enable WNM Sleep Mode

To configure the 5GHz Radio /2.4GHz Radio Advanced setting:

1 Click **5GHz Radio Advanced** or **2.4GHz Radio Advanced** as needed.

2 Check the box if you want to **Hide SSID in Beacon.** This allows the SSID to send null SSID beacons in place of advertising the wireless SSID name. Sending null SSID beacons forces wireless clients to know the SSID to connect. This option is unchecked by default.

3 From the **Schedule IDS Scan** drop-down menu, select a schedule for the IDS (Intrusion Detection Service) scan.

Select a time when there are fewer demands on the wireless network to minimize the inconvenience of dropped wireless connections. You can create your own schedule by selecting **Create new schedule** or disable the feature by selecting **Disabled**, the default.

ⓘ **NOTE:** IDS offers a wide selection of intrusion detection features to protect the network against wireless threats. This feature detects attacks against the WLAN Infrastructure that consists of authorized access points, the RF medium, and the wired network. An authorized or valid-AP is defined as an access point that belongs to the WLAN infrastructure. The access point is either a SonicPoint, a SonicWave, or a third-party access point.

4 From the **Data Rate** drop-down menu, select the speed at which the data is transmitted and received. **Best** (default) automatically selects the best rate available in your area, given interference and other factors.

5 From the **Transmit Power** drop-down menu, select the transmission power. Transmission power effects the range of the SonicPoint.

- **Full Power** (default)
- **Half (-3 dB)**
- **Quarter (-6 dB)**
- **Eighth (-9 dB)**
- **Minimum**

6 If you are configuring a SonicPoint NDR: from the **Antenna Diversity** drop-down menu, select **Best** (default).

The **Antenna Diversity** setting determines which antenna the access point uses to send and receive data. When **Best** is selected, the access point automatically selects the antenna with the strongest, clearest signal.

7 In the **Beacon Interval (milliseconds)** field, enter the number of milliseconds between sending wireless SSID beacons. The minimum interval is 100 milliseconds (default); the maximum is 1000 milliseconds.

8 In the **DTIM Interval** field, enter the DTIM interval in milliseconds. The minimum number of frames is 1 (default); the maximum is 255.

For 802.11 power-save mode clients of incoming multicast packets, the **DTIM interval** specifies the number of beacon frames to wait before sending a DTIM (Delivery Traffic Indication Message).

9 If you are configuring a SonicPointNDR: in the **Fragmentation Threshold (bytes)** field, enter the number of bytes of fragmented data you want the network to allow.

The fragmentation threshold limits the maximum frame size. Limiting frame size reduces the time required to transmit the frame and, therefore, reduces the probability that the frame is corrupted (at the cost of more data overhead). Fragmented wireless frames increase reliability and throughput in areas with RF interference or poor wireless coverage. Lower threshold numbers produce more fragments. The minimum is 256 bytes, the maximum is 2346 bytes (default).

10 In the **RTS Threshold (bytes)** field, enter the threshold for a packet size, in bytes, at which a request to send (RTS) is sent before packet transmission.

Sending an RTS ensures that wireless collisions do not take place in situations where clients are in range of the same access point, but might not be in range of each other. The minimum threshold is 256 bytes, the maximum is 2346 bytes (default).

11 In the **Maximum Client Associations** field, enter the maximum number of clients you want each access point using this profile to support on this radio at one time. The minimum number of clients is 1, the maximum number is 128, and the default number is **32**.

12 In the **Station Inactivity Timeout (seconds)** field, enter the maximum length of wireless client inactivity before the access point ages out the wireless client. The minimum period is 60 seconds, the maximum is 36000 seconds, and the default is **300** seconds.

13 If you are configuring the **2.4GHz Radio Advanced** screen settings, define the following settings which are specific to that window; otherwise skip to the next step.

Options	Settings
Preamble Length	Select from the drop-down menu: • **Long** (default) • **Short**
Protection Mode	Select from the drop-down menu: • **None** • **Always** • **Auto**
Protection Rate	Select from the drop-down menu: • **1 Mbps** (default) • **2 Mbps** • **5 Mbps** • **11 Mbps**
Protection Type	Select from the drop-down menu: • **CTS Only** (default) • **RTS-CTS**
Enable Short Slot Time	Select to allow clients to disassociate and reassociate more quickly. Specifying this option increases throughput on the 802.11n/g wireless band by shortening the time an access point waits before relaying packets to the LAN.
Do not allow 802.11b Clients to Connect	Select if you are using Turbo G mode and, therefore, are not allowing 802.11b clients to connect. Specifying this option limits wireless connections to 802.11g and 802.11n clients only.

14 From the **WMM (Wi-Fi Multimedia)** drop-down menu, select whether a WMM profile is to be associated with this profile:

- **Disabled** (default)
- **Create new WMM profile**. Refer to Configuring Wi-Fi Multimedia for more details.
- A previously configured WMM profile

15 Check the box to **Enable WDS AP**. It allows a wireless network to be expanded using multiple access point without the traditional requirement for a wired backbone to link them.

16 Select **Enable Green AP** to allow the access point radio to go into sleep mode. This saves power when no clients are actively connected. The access point immediately goes into full power mode when any client attempts to connect to it. Green AP can be set on each radio independently, 5GHz Radio and 2.4GHz Radio.

17 In the **Green AP Timeout(s)** field, enter the transition time, in seconds, that the access point waits while it has no active connections before it goes into sleep mode. The transition values can range from 20 seconds to 65535 seconds with a default value of **20** seconds.

18 If configuring a SonicWave or SonicPoint ACe/ACi/N2 profile, select **Enable RSSI** to enable a RSSI threshold. Clients with signal strengths below the threshold are disassociated by the access point so that they are associated to a closer access point. This option is not selected by default.

19 If **Enable RSSI** is selected, enter the threshold value as a negative number into the **RSSI Threshold(dBm)** field. The default is -95 dBm. For more information about RSSI thresholds, see Configuring the RSSI Threshold on page 193.

20 If configuring a SonicWave device, check the box to **Enable Air Time Fairness**.

This feature is disabled by default. If enabled, it steers the traffic for devices that can use the 5GHz band to that band because it usually has less traffic and less interference. If the signal strength or signal conditions are better on the 2.4GHz band, traffic is steered to that band. The intention is to use both bands in the most effective manner.

21 Under **IEEE802.11r Settings**, select **Enable IEEE802.11r** to enable secure, fast roaming. If **Enable IEEE802.11r** is selected, you can select the other options:

- **Enable FT over DS** – enable fast transition over DS
- **Enable IEEE802.11r Mix Mode** – enable fast transition in mixed mode

For more information about these options, see Configuring IEEE802.11r Settings for Secure Fast Roaming on page 193.

22 Under **IEEE802.11k Settings**, select **Enable Neighbor Report** to enable collection of information about neighboring access points. This option is not selected by default. See Configuring IEEE802.11k Settings for Dynamic Radio Management on page 194 for more information.

23 Under **IEEE802.11v Settings**, select **Enable BSS Transition Management** to enable the access point to request a voice client to transition to a specific access point if the client sends a query to the access point. This option is not selected by default. See Configuring IEEE802.11v Settings for Dynamic Environment Management on page 195 for more information.

24 Under **IEEE802.11v Settings**, select **Enable WNM Sleep Mode** to enable a non-access point station to signal to an access point that it is sleeping for a specified time. This option is not selected by default. See Configuring IEEE802.11v Settings for Dynamic Environment Management on page 195 for more information.

Configuring the RSSI Threshold

In areas large enough to require multiple access points to provide good WiFi coverage across the whole area, one would expect a WiFi client to detect and move to the closest access point. Unfortunately, many WiFi clients tend to hang on to the original access point they associated with, rather than moving to a nearby access point that would generally be a better choice for them. This is referred to as sticky behavior and results in a low RSSI (Received Signal Strength Indicator) and a high SNR (Signal-to-Noise Ratio). The farther away from the original access point the client moves, the weaker its RSSI gets and the worse its SNR gets. Retransmissions occur, dynamic rate-shifting happens, and the client communicates at a much lower data-rate. A lower data-rate consumes more air-time to transfer the same information, resulting in higher channel utilization. Ideally, the client would roam to the closest access point, and the resulting RF space would be better for everyone.

Beginning in SonicOS 6.5.2, RSSI thresholds are supported. When the client reaches a certain RSSI level from the perspective of the access point, the access point disassociates from the client and the client then associates to a closer access point. The RSSI threshold is configurable.

RSSI measurements represent the relative quality of a received signal on a device after any possible loss at the antenna and cable level. The higher the RSSI value, the stronger the signal. When measured in negative numbers, the number that is closer to zero usually means better signal. As an example, -50 dBm is a pretty good signal, -75 dBm is fairly reasonable, and -100 dBm is no signal at all.

Configuring IEEE802.11r Settings for Secure Fast Roaming

Many deployed implementations of IEEE 802.11 WiFi have effective ranges of only a few hundred meters, so, to maintain communications, devices in motion need to hand-off from one access point to another. In an automotive environment, this could easily result in a hand-off every five to ten seconds.

Hand-offs are already supported under the existing standard. The fundamental architecture for hand-offs is identical for 802.11 with and without 802.11r: the mobile device is entirely in charge of deciding when to hand-off and to which access point it wishes to hand-off. In the early days of 802.11, hand-off was a much simpler task for the mobile device. Only four messages were required for the device to establish a connection with a new access point (five if you count the optional “I'm leaving” message [deauthentication and disassociation packet] the client could send to the old access point). However, as additional features were added to the standard, including 802.11i with 802.1X authentication and 802.11e or WMM with admission control requests, the number of messages required went up dramatically. During the time these additional messages are being exchanged, the mobile device's traffic, including that from voice calls, cannot proceed, and the loss experienced by the user could amount to several seconds. Generally, the highest amount of delay or loss that the edge network should introduce into a voice call is 50 ms.

802.11r undoes the added burden that security and quality of service added to the hand-off process and restores it to the original four-message exchange. In this way, hand-off problems are not eliminated, but at least are returned to the status quo.

The primary application currently envisioned for the 802.11r standard is voice over IP (VOIP) through mobile phones designed to work with wireless Internet networks, instead of (or in addition to) standard cellular networks.

Configuring IEEE802.11k Settings for Dynamic Radio Management

The **IEEE802.11k Settings** section of the 5GHz or 2.4GHz Radio Advanced screen provides the **Enable Neighbor Report** option. Enabling this option makes the access point collect radio measurements, as defined by the IEEE802.11k amendment to the 802.11 standard.

The Neighbor Report request is sent from a client to an access point. The access point returns a Neighbor Report report containing information about neighboring access points that are known candidates for the client to reassociate with (should the client choose to do so). Therefore, the Neighbor Report request/report pair enables the client to collect information about the neighboring access points of the access point it is currently associated to, and this information might be used as identification of potential candidates for a new point of attachment while roaming.

The benefits of the neighbor/request report are:

- **Speeds up scanning** – Instead of the client engaging in time-consuming scanning activity (either actively probing for access points or passively listening to every channel for beacons), the client can instead narrow its list to the known available neighbors. This is especially useful in high-density environments where multiple WLANs can be heard by the client
- **Reduces client power consumption** – The time taken by scanning (especially active scanning) also consumes battery power for the client. As the neighbor report provides information before roaming, less power might be consumed
- **More efficient use of WLAN air time** – Active scanning is not only time consuming from the perspective of client resources (such as CPU, memory, radio), it's also air-time consuming. For example, a client that is not neighbor-aware likely engages in so-called wildcard probe requests (some clients burst these). In this scenario, typically every access point that hears the probe request generates a probe response. In other words, for a single client, N number of access points generate N probe responses. If multiple clients engage in wildcard probing, then the RF environment can quickly become polluted with management traffic simply because the clients are not using neighbor request. This has a negative impact for the entire WLAN.

Configuring IEEE802.11v Settings for Dynamic Environment Management

802.11v refers to the IEEE802.11 Wireless Network Management (Amendment 8). This is an amendment to the IEEE 802.11 standard to allow configuration of client devices while connected to wireless networks. Stations that support WNM (Wireless Network Management) can exchange information with each other (access points and wireless clients) to improve their performance of the wireless network. 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network.

Stations use WNM protocols to exchange operational data so that each station is aware of the network conditions, allowing stations to be more cognizant of the topology and state of the network. WNM protocols provide a means for stations to be aware of the presence of collocated interference, and enable stations to manage RF parameters based on network conditions.

In addition to providing information on network conditions, WNM also provides a means to exchange location information, provide support for multiple BSSID capability on the same wireless infrastructure, support efficient delivery of group addressed frames, and enable a WNM-Sleep mode in which a STA can sleep for long periods without receiving frames from the AP.

BSS Max idle period management has been supported by SonicWall SonicPoints. SonicWave supports two more WNM services to improve the performance of wireless network:

- **Enable BSS transition management** – Enables an access point to request a voice client to transition to a specific access point, or suggest a set of preferred access points to a voice client, because of network load balancing or BSS termination. This helps the voice client identify the best access point to which that client should transition to as that client roams.

  The BSS Transition capability can improve throughput, data rates and QoS for the voice clients in a network by shifting (through transition) the individual voice traffic loads to more appropriate points of association within the ESS.

  802.11v BSS Transition Management Request is a suggestion given to the client. The client can make its own decision whether to follow the suggestion or not.

  BSS Transition Management uses these frame types:

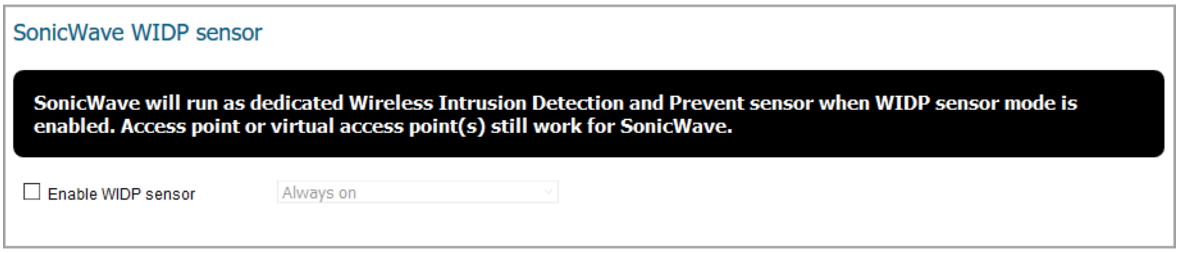
  - **Query** – A Query frame is sent by the voice client that supports BSS Transition Management requesting a BSS transition candidate list to its associated access point, if the associated access point indicates that it supports the BSS transition capability.
  - **Request** – An access point that supports BSS Transition Management responds to a BSS Transition Management Query frame with a BSS Transition Management Request frame.
  - **Response** – A Response frame is sent by the voice client back to the access point, informing whether it accepts or denies the transition.

- **WNM-Sleep mode** – An extended power-save mode for non-access point stations whereby a non-access point station need not listen for every delivery traffic indication message (DTIM) Beacon frame, and does not perform group temporal key/integrity group temporal key (GTK/IGTK) updates.

  WNM-Sleep mode enables a non-access point station to signal to an access point that it is sleeping for a specified time. This enables a non-access point station to reduce power consumption and remain associated while the station has no traffic to send to or receive from the access point.

ⓘ **IMPORTANT:** If the WNM-Sleep mode is enabled and the station supports WNM-Sleep mode, update the station to avoid Key Reinstallation Attack.

Sensor Settings for WIDP in Provisioning Profiles



SonicWave WIDP sensor

SonicWave will run as dedicated Wireless Intrusion Detection and Prevent sensor when WIDP sensor mode is enabled. Access point or virtual access point(s) still work for SonicWave.

☐ Enable WIDP sensor Always on

In the **Sensor** screen, you can enable or disable Wireless Intrusion Detection and Prevention (WIDP) mode. In SonicOS 6.5.3 and higher, SonicWave appliances can function as both an access point and as a sensor to detect any unauthorized access point connected to a SonicWall network.

In earlier releases, access point or virtual access point functionality is disabled if this option is selected.

To configure the Sensor screen options:

1. Select **Enable WIDP sensor** to have the access point operate as a WIDP sensor. This option is not selected by default.
2. From the drop-down menu, select the schedule for when the access point operates as a WIDP sensor or select **Create new schedule...** to specify a different time. The default is **Always on**.

Mesh Network Settings for Provisioning Profiles

This features provides a scalable secure wireless network infrastructure across large coverage areas. You can utilize this feature to deploy and manage SonicWave access points.

Topics:

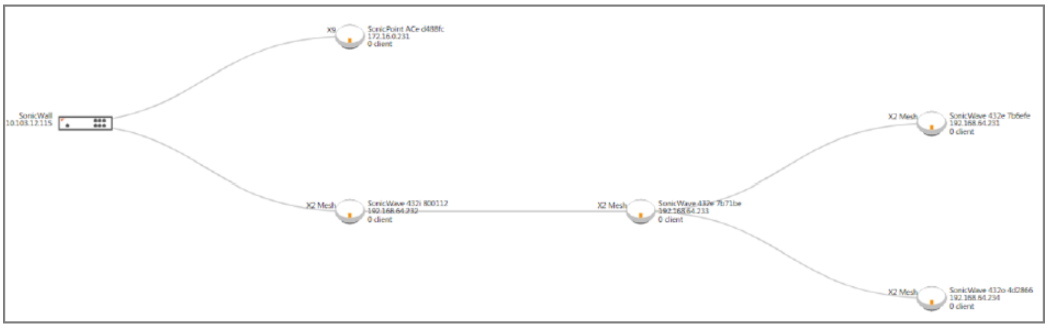
- Setting Up a Mesh Network
- Enabling a Multi-hop Mesh Network
- Active/Active Clustering Full-Mesh

Setting Up a Mesh Network

To set up a mesh network:

1. Enable mesh in the SonicWave profile for your firewall as described in Enabling a Multi-hop Mesh Network.
2. Connect each SonicWave to this firewall by an Ethernet cable.
3. When a SonicWave's state becomes operational, disconnect the cable from that appliance.
4. Keep one SonicWave connected to the firewall.
5. Move the disconnected SonicWave to its designated location.
6. Power up all the SonicWaves.

7 To view the network, navigate to **MANAGE I Connectivity > Access Points > Topology View**.



Enabling a Multi-hop Mesh Network

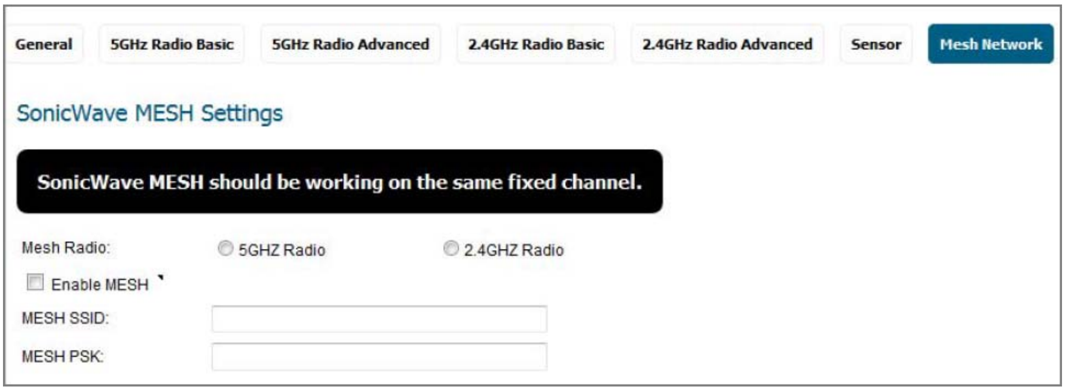
To enable multi-hop mesh networks:

1 Navigate to **MANAGE | Connectivity > Access Points > Base Settings**.

2 Click **SonicWave Provisioning Profiles**.

3 Click on the **Edit** icon for the SonicWave. The **Edit SonicWave Profile** dialog displays.

4 Click **Mesh Network**.



SonicWave MESH Settings

SonicWave MESH should be working on the same fixed channel.

Mesh Radio: ○ 5GHZ Radio ○ 2.4GHZ Radio

□ Enable MESH

MESH SSID:

MESH PSK:

5 Choose the radio to be used for the mesh network from **Mesh Radio**:

- **5GHZ Radio**
- **2.4GHZ Radio**

6 To enable the radio band Mesh on the SonicPointAC, select **Enable Mesh**.

7 Enter the SSID for the WLAN network in **Mesh SSID**.

8 Enter the preshared key in **Mesh PSK**.

9 Click **OK**.

Active/Active Clustering Full-Mesh

An Active/Active Clustering Full-Mesh configuration is an enhancement to the Active/Active Clustering configuration option and prevents any single point of failure in the network. All firewall and other network devices are partnered for complete redundancy. Full-Mesh ensures that there is no single point of failure in your deployment, whether it is a device (security appliance/switch/router) or a link. Every device is wired twice to the connected devices. Active/Active Clustering with Full-Mesh provides the highest level of availability possible with high performance; see Benefits of Active/Active Clustering Full Mesh.

ⓘ **IMPORTANT:** The routers in the security appliance's upstream network should be preconfigured for Virtual Router Redundancy Protocol (VRRP).

Full Mesh deployments require that Port Redundancy is enabled and implemented.

Benefits of Active/Active Clustering Full Mesh

No Single Point of Failure in the Core Network	In an Active/Active Clustering Full-Mesh deployment, there is no single point of failure in the entire core network, not just for the security appliances. An alternative path for a traffic flow is always available in case there are simultaneous failures of switch, router, security appliance on a path, thus providing the highest levels of availability.
Port Redundancy	Active/Active Clustering Full-Mesh utilizes port redundancy in addition to HA redundancy within each Cluster Node, and node level redundancy within the cluster. With port redundancy, a backup link takes over in a transparent manner if the primary port fails. This prevents the need for device level failover.

3G/4G/LTE WWAN Settings for Provisioning Profiles

ⓘ **NOTE:** If you are not configuring a USB modem, you can skip this section.

This features provides another wireless WAN solution for firewall appliances that use wireless access points like SonicWave devices. You can plug a USB modem device into the SonicWave and it does the dial-up operation and connects to the Internet. After connected, the SonicWave acts as a WWAN device for the firewall and provides WAN access.

When configuring the modem for the first time, you can use the wizard to take advantage of the auto-discovery features for this option.

Topics:

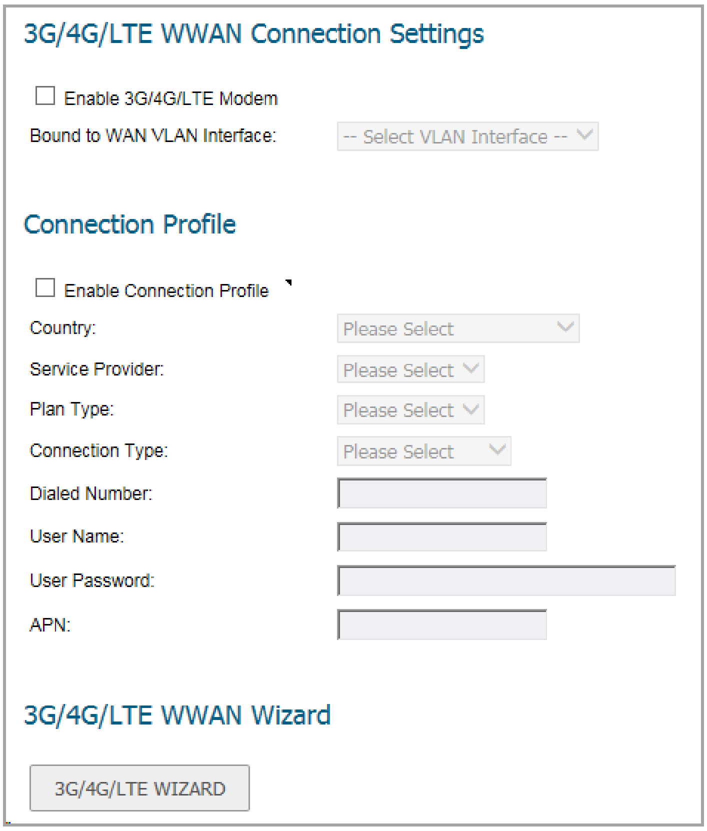
- Manually Configuring the 3G/4G/LTE WWAN Profile
- Using the 3G/4G/LTE WWAN Wizard
- Configuring Load Balancing among Multiple USB Modems

Manually Configuring the 3G/4G/LTE WWAN Profile

You can manually configure the 3G/4G/LTE WWAN profile or manually make changes by using the following procedure.

To manually configure the modem as a WWAN:

1 Click **3G/4GLTE WWAN**.



3G/4G/LTE WWAN Connection Settings

□ Enable 3G/4G/LTE Modem

Bound to WAN VLAN Interface: -- Select VLAN Interface --

Connection Profile

□ Enable Connection Profile

Country: Please Select

Service Provider: Please Select

Plan Type: Please Select

Connection Type: Please Select

Dialed Number:

User Name:

User Password:

APN:

3G/4G/LTE WWAN Wizard

2 Check the box to **Enable the 3G/4G/LTE modem**.

3 Select a VLAN interface from the **Bound to WAN VLAN Interface** drop-down menu.

If no interfaces are listed in the drop-down menu, you need to define one. Refer to the **Network > Interfaces** section in *SonicOS 6.5 System Setup*.

> **NOTE:** When building a VLAN interface, set the zone to WAN zone and the parent interface to the physical interface the access point is connected to.
>
> For 3G USB modems, set the **IP Assignment** to **Static** and assign a private IP address to it. Leave the **gateway** and **DNS server** fields blank.
>
> For 4G and QMI modems, set the **IP Assignment** to **DHCP**.

4 In the **Connection Profile** section, check the box to **Enable Connection Profile**.

> **NOTE:** Some traditional 3G/4G modems need connection profiles for dial-up.

5 In the **Country** field, select the country where the access point is deployed.

6 Select the **Service Provider** from the drop-down menu.

7 Select the **Plan Type** from the drop-down menu. Depending on the selection, other fields are auto-populated.

8 If needed, add the **User Name** and **User Password** to the appropriate fields.

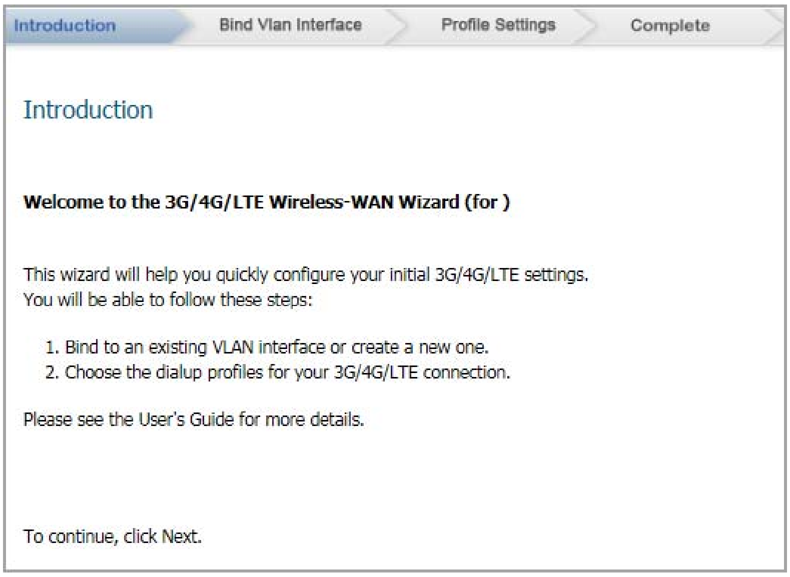
9 When all settings on the screen are done, click **OK**.

Using the 3G/4G/LTE WWAN Wizard

To configure the modem using the wizard:

1 Click **3G/4GLTE WWAN**.

2 Scroll to the bottom and click **3G/4G/LTE WIZARD**.



Introduction

Welcome to the 3G/4G/LTE Wireless-WAN Wizard (for)

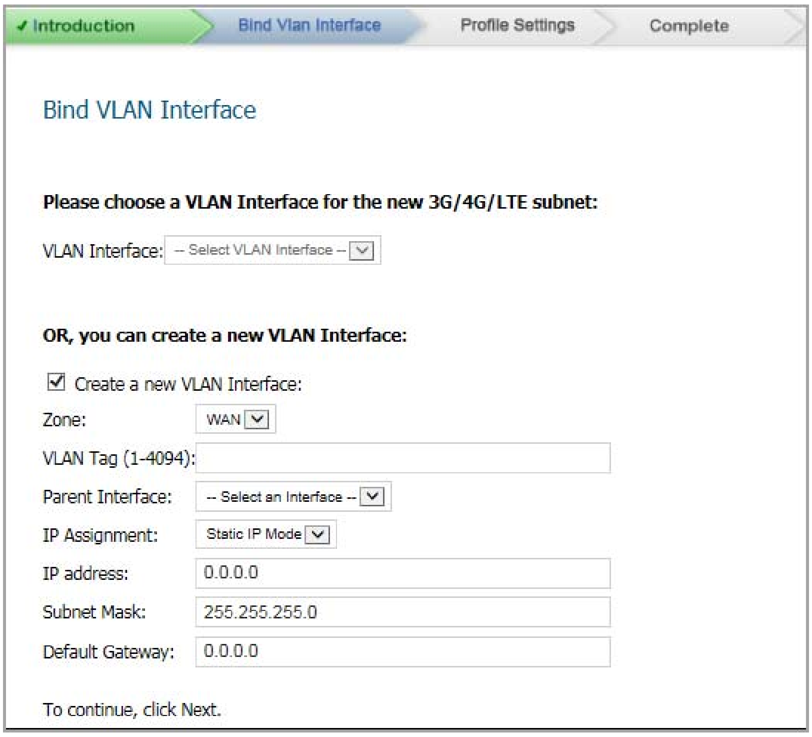
This wizard will help you quickly configure your initial 3G/4G/LTE settings.
You will be able to follow these steps:

1. Bind to an existing VLAN interface or create a new one.
2. Choose the dialup profiles for your 3G/4G/LTE connection.

Please see the User's Guide for more details.

To continue, click Next.

3 Click **Next**.



Bind VLAN Interface

Please choose a VLAN Interface for the new 3G/4G/LTE subnet:

VLAN Interface: -- Select VLAN Interface --

OR, you can create a new VLAN Interface:

☑ Create a new VLAN Interface:

Zone: WAN

VLAN Tag (1-4094):

Parent Interface: -- Select an Interface --

IP Assignment: Static IP Mode

IP address: 0.0.0.0

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

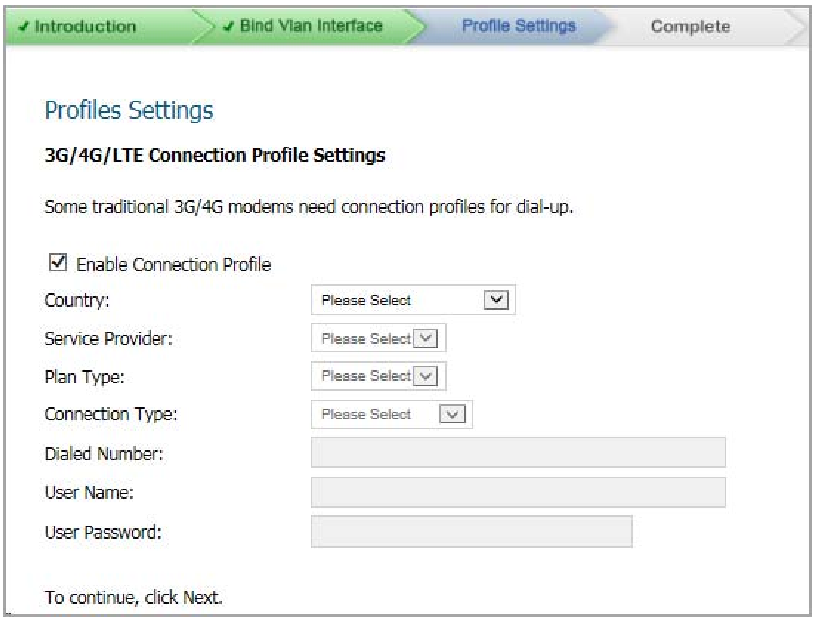
To continue, click Next.

4 Choose a **VLAN Interface** from the drop-down menu, or check the box to **Create a New VLAN Interface**.

If you opt to create a new VLAN interface, the remaining fields become active. Provide the data requested.

ⓘ **NOTE:** If you set **IP Assignment** to **DHCP**, the IP Address, Subnet Mask, and Default Gateway fields are hidden.

5 Click **Next**.



Profiles Settings

3G/4G/LTE Connection Profile Settings

Some traditional 3G/4G modems need connection profiles for dial-up.

☑ Enable Connection Profile

Country:	Please Select
Service Provider:	Please Select
Plan Type:	Please Select
Connection Type:	Please Select
Dialed Number:	
User Name:	
User Password:	

To continue, click Next.

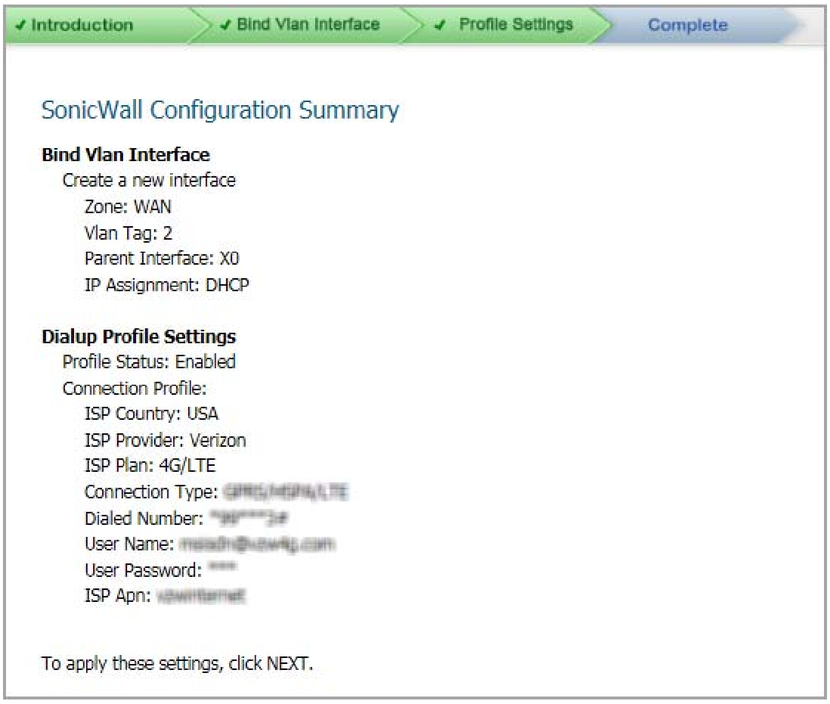
6 In the **Country** field, select the country where the access point is deployed.

7 Select the **Service Provider** for the drop-down menu.

8 Select the **Plan Type** from the drop-down menu. Depending on the selection, other fields are auto-populated.

9 If needed, add the **User Name** and **User Password** to the appropriate fields.

10 Click **Next**.



SonicWall Configuration Summary

Bind Vlan Interface

Create a new interface

Zone: WAN

Vlan Tag: 2

Parent Interface: X0

IP Assignment: DHCP

Dialup Profile Settings

Profile Status: Enabled

Connection Profile:

ISP Country: USA

ISP Provider: Verizon

ISP Plan: 4G/LTE

Connection Type: [redacted]

Dialed Number: [redacted]

User Name: [redacted]

User Password: [redacted]

ISP Apn: [redacted]

To apply these settings, click NEXT.

11 Click **Next** again to apply the settings.

Configuring Load Balancing among Multiple USB Modems

When multiple SonicPoint/SonicWaves and multiple 3G/4G modems (at least two of each) are available, load balancing can be performed among these multiple pairs of SonicPoint/SonicWaves and modems.

To configure load balancing using multiple 3G/4G modems:

1 Assign a unique VLAN to each pair of SonicPoint/SonicWaves and 3G/4G modems, manually or by using the 3G/4G/LTE Wizard.

2 Add these VLAN interfaces to a load balancing group on the **MANAGE | System Setup > Network > Failover & Load Balancing**. See the *SonicOS 6.5 System Setup* administration documentation for more information.

Bluetooth LE Settings for Provisioning Profiles

SonicWave series are equipped with Bluetooth Low Energy (BLE) functionality, which is a subset of classic Bluetooth. BLE enables smart phones, tablets, SonicWall mobile applications, and other devices, such as other SonicWaves, to easily connect to the SonicWave access point, especially when in close proximity to an appliance with iBeacon enabled. BLE also provides location estimation.

iBeacon is a protocol developed by Apple. Various vendors make iBeacon-compatible BLE devices that broadcast their identifier to nearby portable electronic devices. The technology enables smart phones, tablets, and other devices to perform actions when in close proximity to an iBeacon.

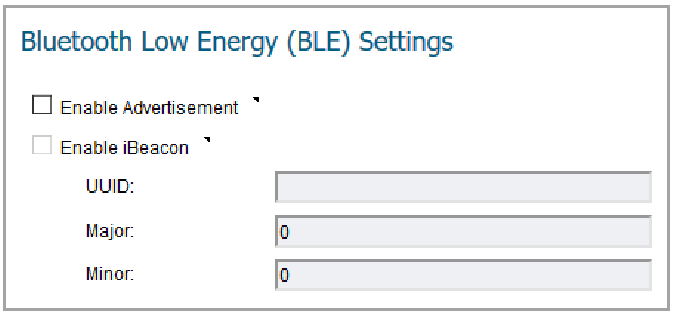
To enable and configure Bluetooth Low Energy settings:

1 Navigate to **MANAGE I Connectivity > Access Points > Base Settings**.

2 Click **SonicWave Provisioning Profiles**.

3 Click the Edit icon for **SonicWave**. The **Edit SonicWave Profile** dialog displays.

4 Click **Bluetooth LE**.



Bluetooth Low Energy (BLE) Settings

☐ Enable Advertisement

☐ Enable iBeacon

UUID:

Major: 0

Minor: 0

5 To enable BLE advertisement, select **Enable Advertisement**. This option is not selected by default. When this option is enabled, the **Enable iBeacon** option becomes available.

> **NOTE:** Enabling BLE advertisement might affect or interfere with the 2.4G radio frequencies.

6 To enable iBeacon so that BLE devices broadcast their identifiers, select **Enable iBeacon**. This option is not selected by default. The subordinate fields become available.

7 Complete the fields:

- **UUID** – Enter the 36-characters of the UUID. For example:

  `51b9d455-6a32-426c-b5cc-524181c24df3`

- **Major** – Enter the significant identity in the same geographical group. The range is 0 to 65535; the default is **0**.
- **Minor** – Enter the secondary identity in the same geographical group. The range is 0 – 65535; the default is **0**.

> **TIP:** Use different UUIDs to distinguish different geographical groups and major and minor options to distinguish areas within the geographical group. For example, you deploy several SonicWave appliances with BLE in one building, and you set the same UUID for these SonicWave appliances. The SonicWave appliances on the same floor have the same Major number, but have different Minor numbers in different places on the same floor. In this way, your mobile device is close to a SonicWave appliance and its location.

8 Click **OK**.

Deleting Access Point Profiles

> **NOTE:** You cannot delete the predefined profiles; you can only delete those you add.

You can delete individual profiles or groups of profiles from the **SonicPoint/SonicWave Provisioning Profiles** section on the **Connectivity | Access Points > Base Settings** page:

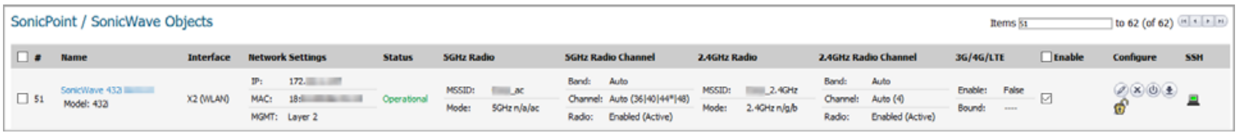
- Delete a single access point profile by:
  1) Click **Delete**. A confirmation message appears.
  2) Click **OK**.
- Delete one or more access point profiles by:
  1) Selecting the checkbox next to the name(s) of the access points to be deleted. **DELETE** becomes active.
  2) Click **DELETE**. A confirmation message appears.
  3) Click **OK**.
- Delete all profiles by:
  1) Select the checkbox next to the **#** in the column heading. **Delete All** becomes active.
  2) Click **DELETE ALL**. A confirmation message appears.
  3) Click **OK**.

Product Specific Configuration Notes

SonicPoint configuration process varies slightly depending on whether you are configuring a single-radio (SonicPointN) or a dual radio (SonicWave, SonicPoint AC and SonicPoint NDR) devices.

Managing Access Points

The **SonicPoint / SonicWave Objects** section displays the settings for connected access points, and provides buttons to edit them or perform other actions.



SonicPoint / SonicWave Objects

Items 51 to 62 (of 62)

□ #	Name	Interface	Network Settings	Status	5GHz Radio	5GHz Radio Channel	2.4GHz Radio	2.4GHz Radio Channel	3G/4G/LTE	□ Enable	Configure	SSH
□ 51	SonicWave 432i [redacted] Model: 432i	X2 (WLAN)	IP: 172.[redacted] MAC: 18:[redacted] MGMT: Layer 2	Operational	MSSID: [redacted]_ac Mode: 5GHz n/a/ac	Band: Auto Channel: Auto (36|40|44*|48) Radio: Enabled (Active)	MSSID: [redacted]_2.4GHz Mode: 2.4GHz n/g/b	Band: Auto Channel: Auto (4) Radio: Enabled (Active)	Enable: False Bound: ----	☑		

The table displays the configured values for the access points, including:

Column	Description
#	Row reference number
Name	Name of access point
Interface	Firewall interface number and zone to which the access point is connected
Network Settings	Access point IP address, MAC address, and management designation
Status	Operational, Non-responsive, or other access point states
5GHz Radio	Access point SSID (MSSID) name for this radio, frequency and 802.11 protocols
5GHz Radio Channel	Band setting, channels, and state of radio such as enabled and active
2.4GHz Radio	Access point SSID (MSSID) name for this radio, frequency and 802.11 protocols
2.4GHz Radio Channel	Band setting, channels, and state of radio such as enabled and active
3G/4G/LTE	Enabled/disabled state of 3G, 4G, or LTE and binding information
Enable	Selected if the access point is enabled
Configure	Buttons for editing, deleting, rebooting, or downloading logs from the access point. Can also show buttons for editing a manual keyset.
SSH	Button for SSH access to the access point

Topics:

- Deleting SonicPoint/SonicWave Objects
- Rebooting SonicPoint/SonicWave Objects
- Modifying SonicPoint/SonicWave Objects

Deleting SonicPoint/SonicWave Objects

You can delete individual access points or groups of access points from the **SonicPoint/SonicWave Objects** section on the **Connectivity | Access Points> Base Settings** page:

- Delete a single object by:
  - a Clicking **Delete** for that object. A confirmation message appears.
  - b Click **OK**.
- Delete one or more objects by:
  - a Selecting the checkbox next to the objects to be deleted. **DELETE** becomes active.
  - b Click **DELETE**. A confirmation message appears.
  - c Click **OK**.

- Delete all objects by:
  a Select the checkbox next to the **#** in the column heading. **DELETE ALL** becomes active.

  b Click **DELETE ALL.** A confirmation message appears.

  c Click **OK**.

Rebooting SonicPoint/SonicWave Objects

You can reboot individual access points or groups of access points from the **SonicPoint/SonicWave Objects** section on the **Connectivity | Access Points> Base Settings** page:

- Reboot a single object by:
  a Check the checkbox next to the name of the access point to be rebooted. The **REBOOT** icon becomes active.

  b Click **REBOOT.** A confirmation message displays.

  c Select the type of reboot:

    - **reboot** (default) – Reboots to the configured profile settings.
    - **reboot to factory default** – Reboots to factory default settings.

△ **CAUTION: Selecting this option overwrites the access point profiles with factory default values.**

  d Click **OK**.

- Reboot all objects by:
  a Click **REBOOT ALL**.

  b Select one of the following:

    - **reboot** (default) – Reboots to the configured profile settings.
    - **reboot to factory default**

△ **CAUTION: Selecting this option overwrites the access point profiles with factory default values.**

  c Click **OK** to apply to reboot the access points or **Cancel** to close the window without rebooting.

Modifying SonicPoint/SonicWave Objects

An access point object can be modified from the **Connectivity | Access Points> Base Settings.**

1 Click the **Edit** icon for the object you want to modify.

2 Changes the settings you want to modify.

3 Click **OK** to save the new settings.

ⓘ **NOTE:** New SonicPoint/SonicWave access points are added automatically when network appliance performs an auto-discovery process.

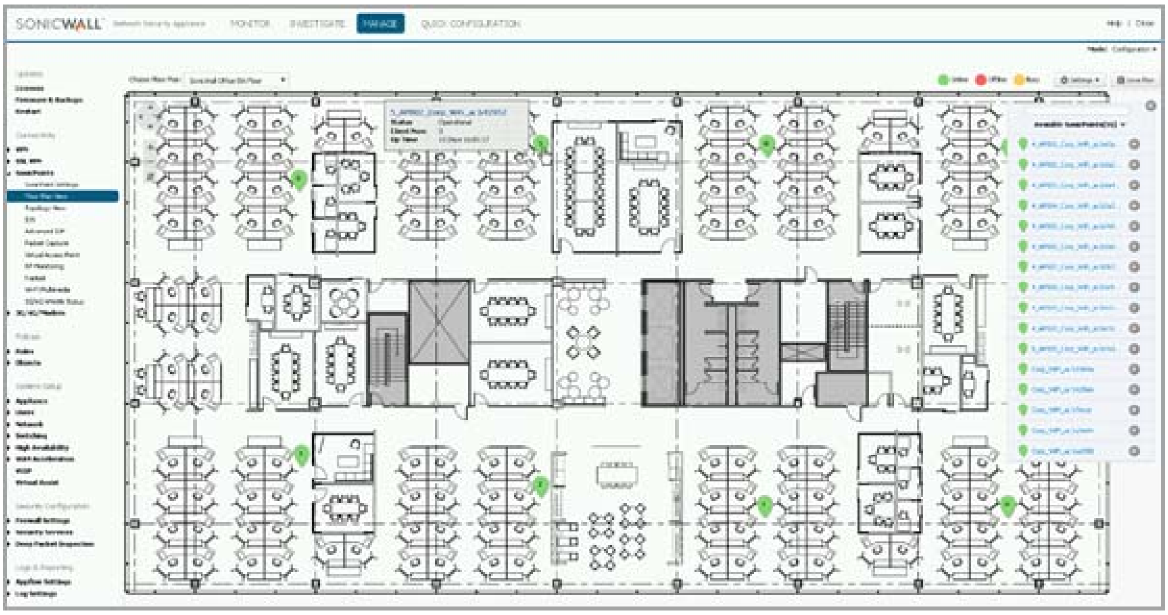
17

Access Point Floor Plan

On the **Connectivity | Access Points > Floor Plan View** page in **MANAGE** view, the in SonicOS user interface allows a more visual approach to managing large numbers of SonicWave and SonicPoint devices. You can also track physical location and real-time status.

The Floor Plan View feature is an add-on to the existing wireless access point management suite in SonicOS. It provides a real-time picture of the actual wireless radio environment and improves your ability to estimate the wireless coverage of new deployments. The FPMV also provides a single point console to check access point statistics, monitor access point real-time status, configure access points, remove access points and even show the access point RF coverage from the consolidated the context menu.

The figure below shows a sample of a typical floor plan view.



Topics:

- Managing the Floor Plans
- Managing Access Points

Managing the Floor Plans

The Floor Plan View feature has a number of ways to view, add, and edit floor plans. The most common are described in this section.

Topics:

- Selecting a Floor Plan

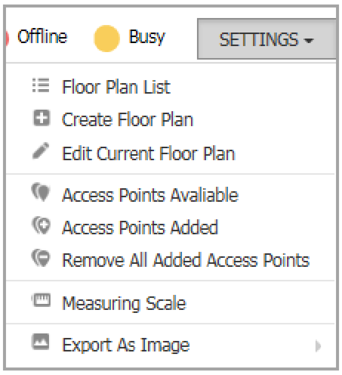
- Create a Floor Plan
- Edit a Floor Plan
- Set Measuring Scale

Selecting a Floor Plan

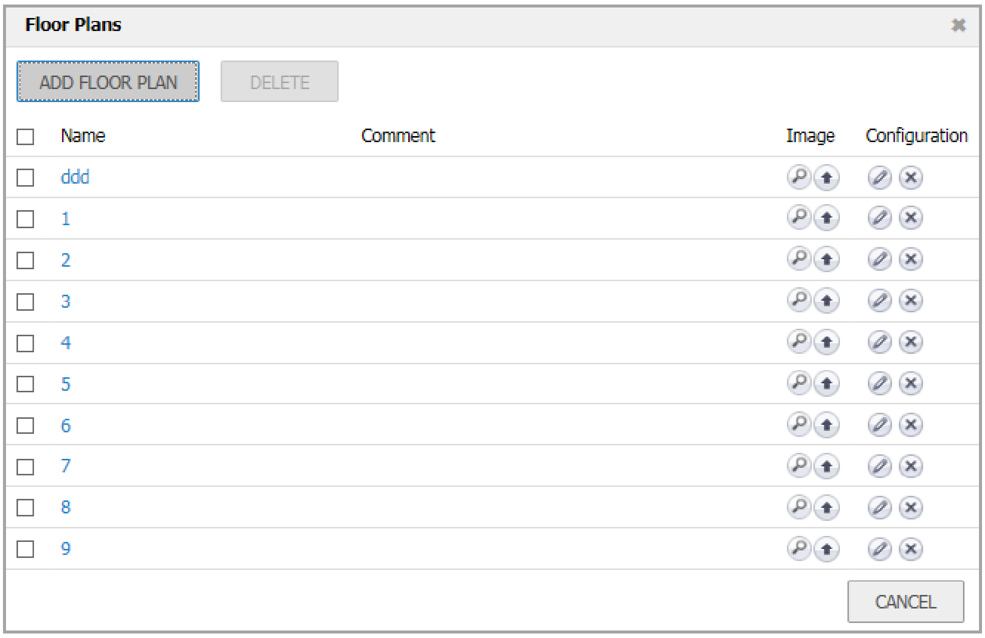
When you choose the **Connectivity | Access Points > Floor Plan View** page in the **MANAGE** view, the title of the floor plan being displayed is shown in the **Choose Floor Plan** field in the upper left corner. To see a different floor plan, select a different floor plan from the **Choose Floor Plan** drop-down menu.

Another way to choose a floor plan:

1 Click on **SETTINGS**.



2 Select Floor Plan List.



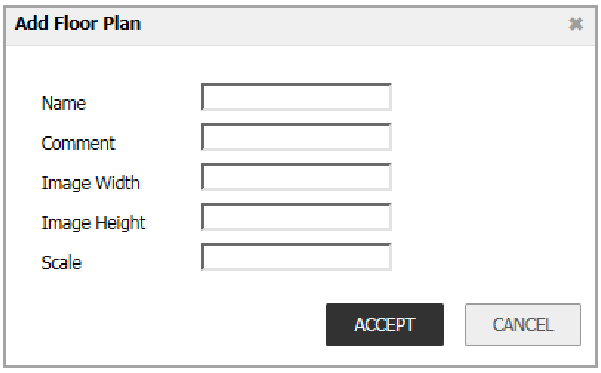
□	Name	Comment	Image	Configuration
□	ddd		🔍 ⬆	✎ ✕
□	1		🔍 ⬆	✎ ✕
□	2		🔍 ⬆	✎ ✕
□	3		🔍 ⬆	✎ ✕
□	4		🔍 ⬆	✎ ✕
□	5		🔍 ⬆	✎ ✕
□	6		🔍 ⬆	✎ ✕
□	7		🔍 ⬆	✎ ✕
□	8		🔍 ⬆	✎ ✕
□	9		🔍 ⬆	✎ ✕

3 Double-click on the name of the plan you want to display.

Create a Floor Plan

To create a floor plan:

1. Navigate to **Connectivity | Access Points > Floor Plan View**.
2. Click on **SETTINGS**.
3. Select **Create Floor Plan**.



Add Floor Plan

Name	
Comment	
Image Width	
Image Height	
Scale	

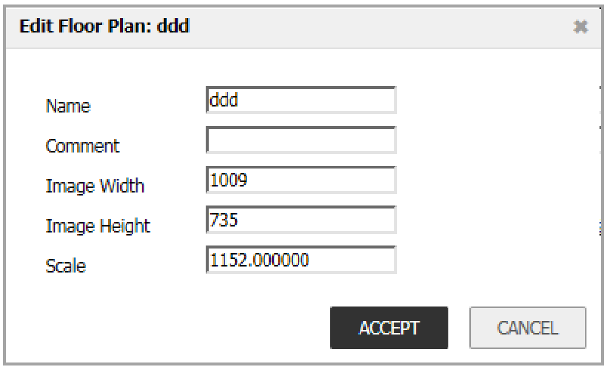
4. Fill in the fields describing the plan.
5. Click **ACCEPT**.

Edit a Floor Plan

There are different ways to edit floor plans; these are the most common.

To edit floor plan being displayed:

1. Navigate to **Connectivity | Access Points > Floor Plan View**.
2. Click on **SETTINGS**.
3. Select **Edit Current Floor Plan**.



Edit Floor Plan: ddd

Name	ddd
Comment	
Image Width	1009
Image Height	735
Scale	1152.000000

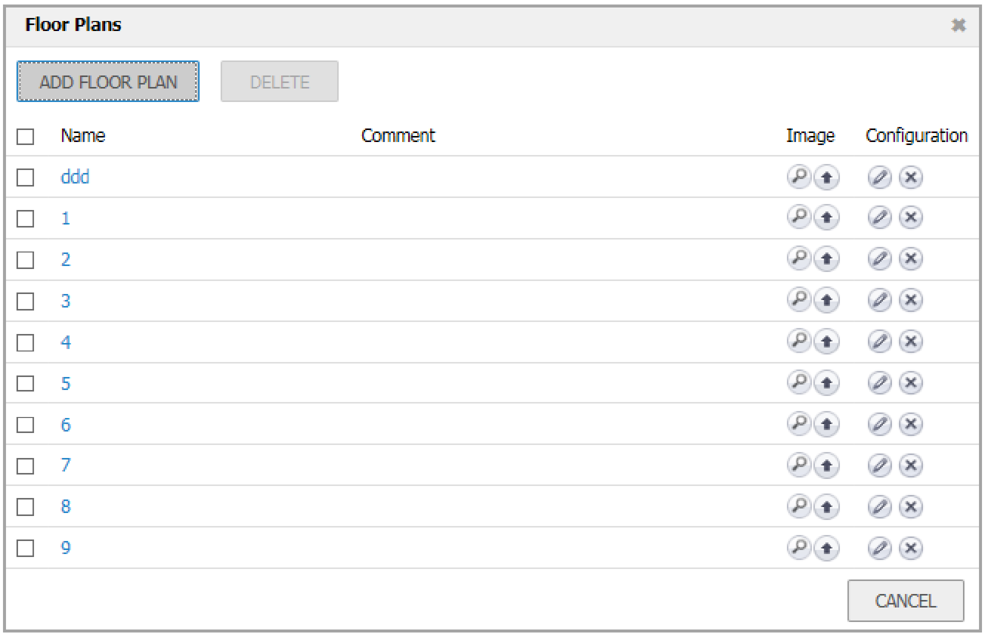
4. Change the fields as needed.
5. Click **ACCEPT**.

To edit a plan in the list:

1. Navigate to **Connectivity | Access Points > Floor Plan View**.

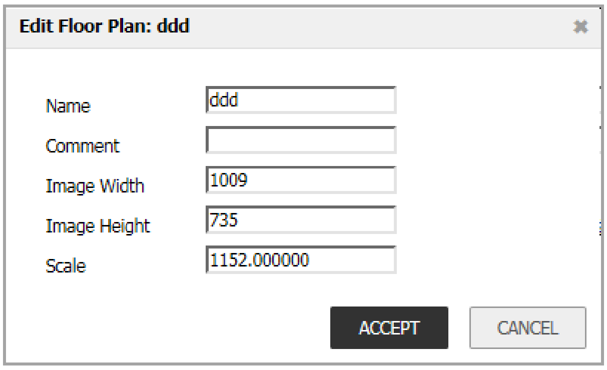
2 Click on **SETTINGS**.

3 Select **Floor Plan List**.



□	Name	Comment	Image	Configuration
□	ddd		🔍 ⬆	✎ ⊗
□	1		🔍 ⬆	✎ ⊗
□	2		🔍 ⬆	✎ ⊗
□	3		🔍 ⬆	✎ ⊗
□	4		🔍 ⬆	✎ ⊗
□	5		🔍 ⬆	✎ ⊗
□	6		🔍 ⬆	✎ ⊗
□	7		🔍 ⬆	✎ ⊗
□	8		🔍 ⬆	✎ ⊗
□	9		🔍 ⬆	✎ ⊗

4 Click the **Edit** icon.



Name	ddd
Comment	
Image Width	1009
Image Height	735
Scale	1152.000000

5 Change the fields as needed.

6 Click **ACCEPT**.

Set Measuring Scale

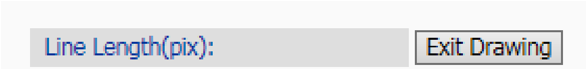
You need to set a measuring scale to show the relationship of real distance (feet) and the pixels that make up the picture of the floor plan. You can use this value to help estimate the RF coverage.

To set the measuring scale:

1 Navigate to **Connectivity | Access Points > Floor Plan View**.

2 Click on **SETTINGS**.

3 Select **Measuring Scale**. The **Line Length** field appears on the window.



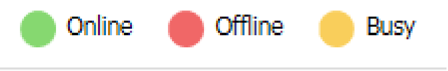
Line Length(pix):

4 Enter number of pixels per foot.

5 Click **Exit Drawing**.

Managing Access Points

Access Point status is displayed with color:



🟢 Online 🔴 Offline 🟡 Busy

The individual access points can be managed on the **Floor Plan View**.

Topics:

- Available Access Points
- Added Access Points
- Remove Access Points
- Export Image

Available Access Points

The access points that are available for deployment are shown in the **Available Access Points** list. The list typically appears in the upper right corner, but you can drag-and-drop it anywhere. You can close it by clicking on the **X** in the corner. To show the list, click **SETTINGS > Access Points Available**.

You can drag-and-drop these access points to the floor plan and place them where you want them. Be sure to **SAVE PLAN** when done.

ⓘ | **NOTE:** Access points that are already added to a floor plan do not show in this panel.

Added Access Points

The access points that have been deployed are shown in the **Added Access Points** list. The list typically appears in the upper left corner, but you can drag-and-drop it anywhere. You can close it by clicking on the **X** in the corner. To show the list, click **SETTINGS > Access Points Added**.

You can drag-and-drop these access points to different places on the floor plan, or you can delete them from the plan. Be sure to **SAVE PLAN** when done.

ⓘ | **NOTE:** Access points that are already added to a floor plan do not show in this panel.

Remove Access Points

To remove all access points:

1. Navigate to **Connectivity | Access Points > Floor Plan View**.
2. Click on **SETTINGS**.
3. Select **Remove All Added Access Points**.
4. Click **SAVE PLAN**.

Export Image

To export the floor plan images:

1. Navigate to **Connectivity | Access Points > Floor Plan View**.
2. Click on **SETTINGS**.
3. Select **Export as Image**.
4. Then choose whether you want it saved in **JPG** format for **PNG** format.
5. Save the file where you can access it later.

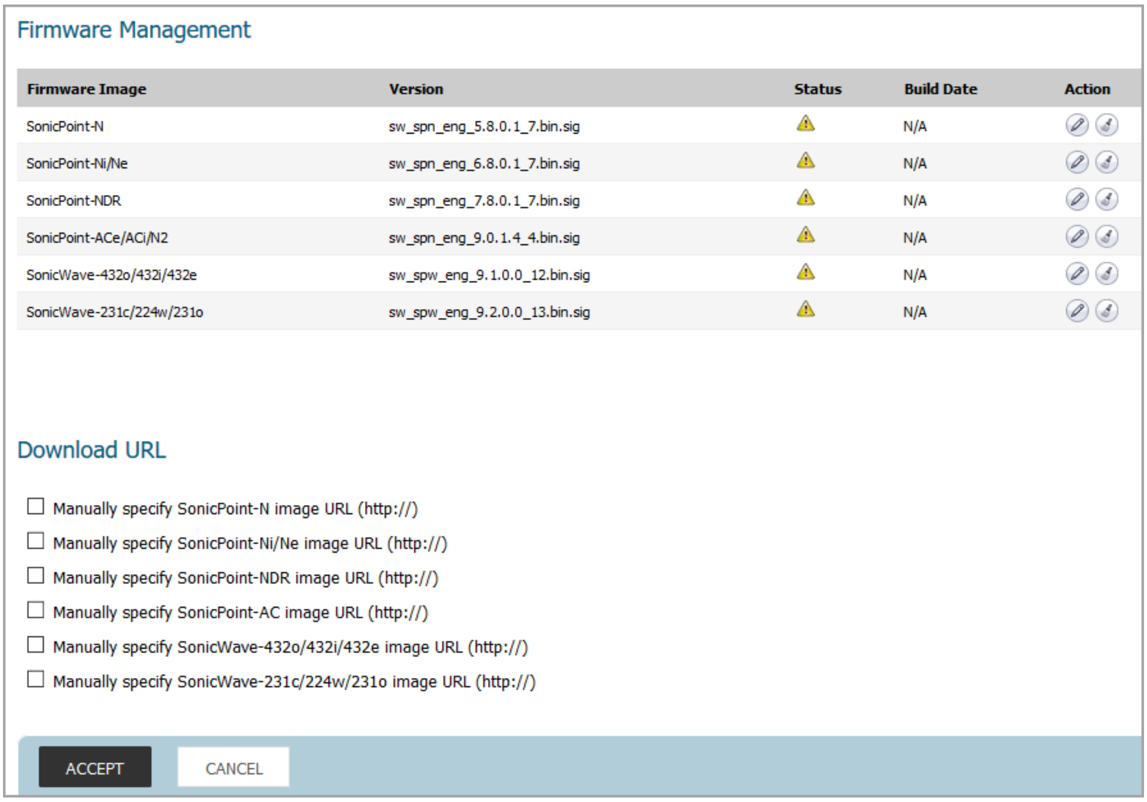
Context Menu

You can use your mouse to activate various context menus:

- When you mouse over an active access point on the floor plan, a pop-up displays access point information, including ID, status, number of clients, and up time.
- By clicking on the access point, the RF coverage is displayed.
- By double-clicking the access point, the Real-Time Monitoring window appears.
- By right-clicking the access point, a context menu appears. It has options to edit, show statistics, monitor status and so forth.

Access Point Firmware Management

The **MANAGE | Connectivity > Access Points > Firmware Management** page provides a way to obtain the latest SonicPoint/SonicWave firmware and update an access point with it.



Firmware Management

Firmware Image	Version	Status	Build Date	Action
SonicPoint-N	sw_spn_eng_5.8.0.1_7.bin.sig	⚠	N/A	✎ 🧹
SonicPoint-Ni/Ne	sw_spn_eng_6.8.0.1_7.bin.sig	⚠	N/A	✎ 🧹
SonicPoint-NDR	sw_spn_eng_7.8.0.1_7.bin.sig	⚠	N/A	✎ 🧹
SonicPoint-ACe/ACi/N2	sw_spn_eng_9.0.1.4_4.bin.sig	⚠	N/A	✎ 🧹
SonicWave-432o/432i/432e	sw_spw_eng_9.1.0.0_12.bin.sig	⚠	N/A	✎ 🧹
SonicWave-231c/224w/231o	sw_spw_eng_9.2.0.0_13.bin.sig	⚠	N/A	✎ 🧹

Download URL

☐ Manually specify SonicPoint-N image URL (http://)
☐ Manually specify SonicPoint-Ni/Ne image URL (http://)
☐ Manually specify SonicPoint-NDR image URL (http://)
☐ Manually specify SonicPoint-AC image URL (http://)
☐ Manually specify SonicWave-432o/432i/432e image URL (http://)
☐ Manually specify SonicWave-231c/224w/231o image URL (http://)

Topics:

- About Firmware Management
- Obtaining the Latest SonicWall Firmware
- Downloading Firmware from a Specific URL
- Uploading Firmware to an Access Point

About Firmware Management

The **Firmware Management** table displays the status of the current access point firmware images, and provides buttons to obtain new firmware and upload it to the access points.

Column	Description
Firmware Image	Displays the type of access point for the firmware image.
Version	Displays the firmware version supported by the firewall that the access point needs to match. When a new version of AP firmware is available and supported by the firewall, then the **Version** entry displays it and the access point is automatically updated to it after connecting.
Status	Initially, all firmware status is *Need Download*. If a different firmware image is uploaded to the firewall buffer, it changes to a check mark indicating *Ready*.
Build Date	Displays the date that the uploaded firmware was created.
Action	Provides two buttons: • **Upload Firmware** button – Click to upload the downloaded firmware to the firewall buffer. As previously described for **Version**, a new, supported AP firmware is automatically pushed to the access point. To push the firmware to an access point that is already in operational status, you must use an internal setting. Contact SonicWall Support for information about using internal settings. • **Reset Firmware** button – Click to remove the downloaded firmware image from the buffer.

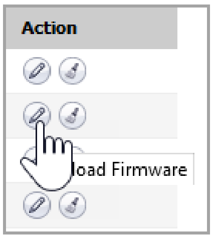
The **Download URL** section of the page provides a way to download access point firmware images from a specific location over HTTP. This allows you to load alternate firmware, such as a version provided by SonicWall Support which is not yet officially released.

Obtaining the Latest SonicWall Firmware

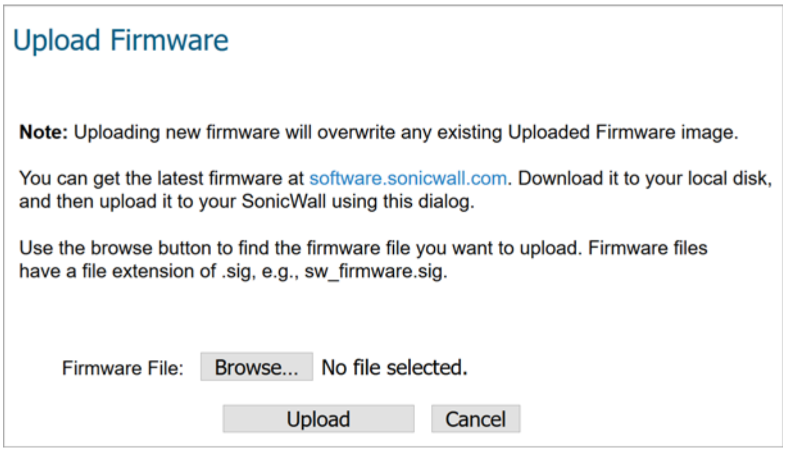
To obtain the latest firmware version from SonicWall:

1 Navigate to the **MANAGE | Connectivity | Access Points > Firmware Management** page.

2 In the **Firmware Management** table, click **Upload Firmware** under **Action** in the row for the desired access point type.



3 In the **Upload Firmware** dialog box, click the **software.sonicwall.com** link.



Upload Firmware

Note: Uploading new firmware will overwrite any existing Uploaded Firmware image.

You can get the latest firmware at software.sonicwall.com. Download it to your local disk, and then upload it to your SonicWall using this dialog.

Use the browse button to find the firmware file you want to upload. Firmware files have a file extension of .sig, e.g., sw_firmware.sig.

Firmware File: Browse... No file selected.

4 The file, for example **sw_spn_eng_9.0.1.5_7.bin.sig**, is saved to your default location, such as your *Downloads* folder.

Downloading Firmware from a Specific URL

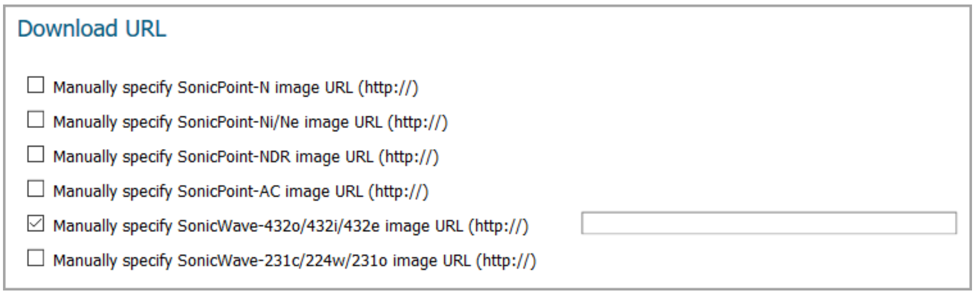
You can manually specify a URL location and download a firmware image from it for use on your access point.

To specify a URL for the image:

1 Navigate to **MANAGE | Connectivity | Access Points > Firmware Management**.

2 Scroll to **Download URL**.

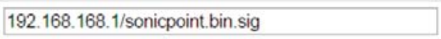
3 Select the checkbox for the type of image to be downloaded. A field becomes available.



Download URL

□ Manually specify SonicPoint-N image URL (http://)
□ Manually specify SonicPoint-Ni/Ne image URL (http://)
□ Manually specify SonicPoint-NDR image URL (http://)
□ Manually specify SonicPoint-AC image URL (http://)
☑ Manually specify SonicWave-432o/432i/432e image URL (http://)
□ Manually specify SonicWave-231c/224w/231o image URL (http://)

4 Enter the URL of the image’s location in the field. You do not need to enter “*http://*” in the field.



192.168.168.1/sonicpoint.bin.sig

5 Click **ACCEPT**. The file is saved to the firewall buffer.

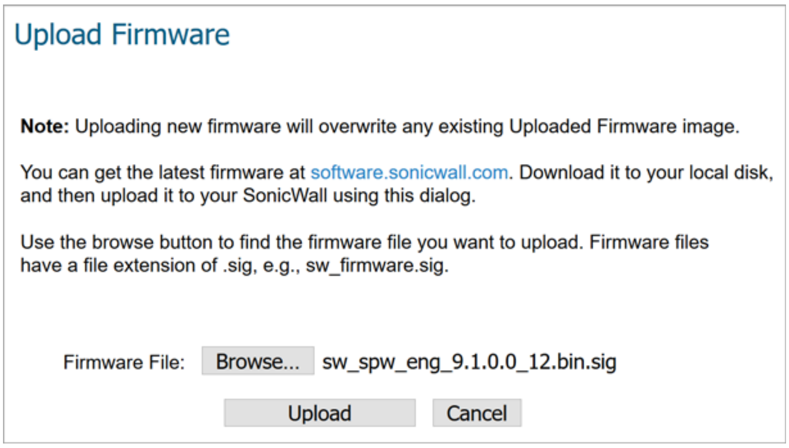
Uploading Firmware to an Access Point

You can upload any locally saved firmware image file to an access point. The saved file can be an official SonicWall firmware version, or a firmware image downloaded from a manually specified URL.

To upload a firmware image to an access point:

1. Do one of the following to obtain the firmware image and save it on your local workstation:
    - Download an official SonicWall version as described in Obtaining the Latest SonicWall Firmware.

      This procedure leaves you in the **Upload Firmware** dialog after saving the image file to your local computer.
    - Download a firmware image from a manually specified URL as described in Downloading Firmware from a Specific URL.
2. If you want to upload a firmware image, click Upload Firmware under Action in the row for the desired access point type to open the Upload Firmware dialog box. If you downloaded the image file using the link to software.sonicwall.com, the dialog is already open.
3. In the **Upload Firmware** dialog, click **Browse**, navigate to the saved image and select it. The **Upload Firmware** dialog now displays the firmware image name.
4. In the **Upload Firmware** dialog, click **Upload**.



Upload Firmware

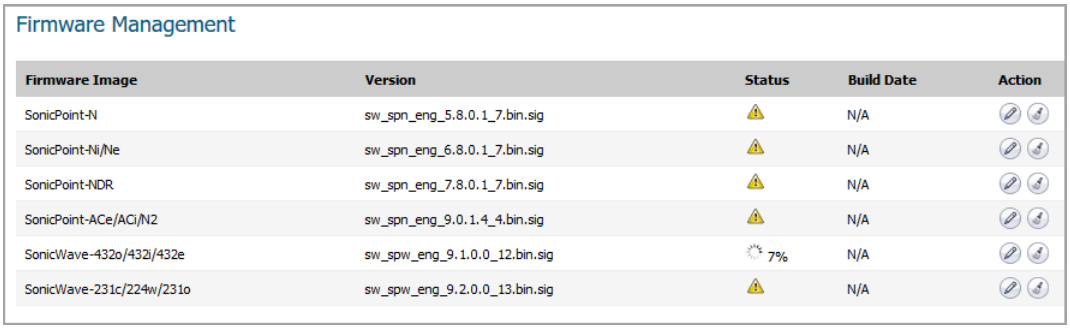
Note: Uploading new firmware will overwrite any existing Uploaded Firmware image.

You can get the latest firmware at software.sonicwall.com. Download it to your local disk, and then upload it to your SonicWall using this dialog.

Use the browse button to find the firmware file you want to upload. Firmware files have a file extension of .sig, e.g., sw_firmware.sig.

Firmware File: Browse... sw_spw_eng_9.1.0.0_12.bin.sig

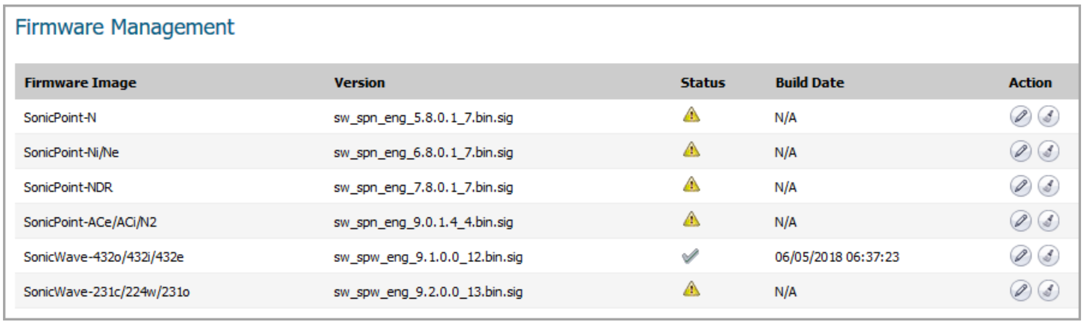
The firmware image is uploaded to the buffer on your security appliance. While uploading, the **Status** indicates the percentage of the upload.



Firmware Management

Firmware Image	Version	Status	Build Date	Action
SonicPoint-N	sw_spn_eng_5.8.0.1_7.bin.sig	⚠	N/A	✎ ⇪
SonicPoint-Ni/Ne	sw_spn_eng_6.8.0.1_7.bin.sig	⚠	N/A	✎ ⇪
SonicPoint-NDR	sw_spn_eng_7.8.0.1_7.bin.sig	⚠	N/A	✎ ⇪
SonicPoint-ACe/ACi/N2	sw_spn_eng_9.0.1.4_4.bin.sig	⚠	N/A	✎ ⇪
SonicWave-432o/432i/432e	sw_spw_eng_9.1.0.0_12.bin.sig	7%	N/A	✎ ⇪
SonicWave-231c/224w/231o	sw_spw_eng_9.2.0.0_13.bin.sig	⚠	N/A	✎ ⇪

When the upload completes, the **Version** column displays the new firmware version. If the access point is connected, the firmware version is automatically pushed to it and the **Status** changes to a check mark, indicating that the firmware image is *Ready*, and the **Build Date** shows the date that the image was created. The access point is now running the new firmware.



Firmware Management

Firmware Image	Version	Status	Build Date	Action
SonicPoint-N	sw_spn_eng_5.8.0.1_7.bin.sig	⚠	N/A	✎ ⟲
SonicPoint-Ni/Ne	sw_spn_eng_6.8.0.1_7.bin.sig	⚠	N/A	✎ ⟲
SonicPoint-NDR	sw_spn_eng_7.8.0.1_7.bin.sig	⚠	N/A	✎ ⟲
SonicPoint-ACe/ACi/N2	sw_spn_eng_9.0.1.4_4.bin.sig	⚠	N/A	✎ ⟲
SonicWave-432o/432i/432e	sw_spw_eng_9.1.0.0_12.bin.sig	✓	06/05/2018 06:37:23	✎ ⟲
SonicWave-231c/224w/231o	sw_spw_eng_9.2.0.0_13.bin.sig	⚠	N/A	✎ ⟲

5 To clear the downloaded firmware from the buffer, click **Reset Firmware** under **Action**. The **Status** indicator and **Build Date** return to the default display.

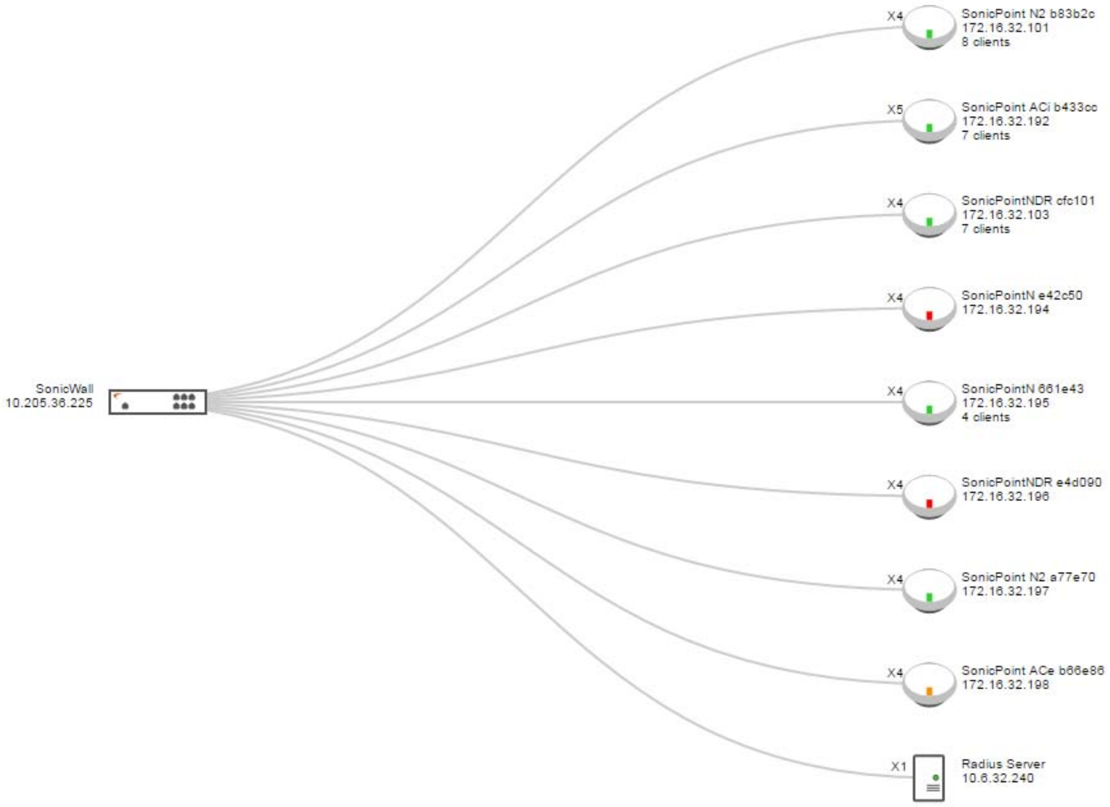
19

Access Point Topology View

On the **Connectivity | Access Points > Topology View** page in **MANAGE** view, access points can be managed by the new Topology View feature. The Topology View shows the network topology from the SonicWall firewall to the wireless access point. The access point real-time status can be monitored, and the context menu also provides configuration options.

This feature shows the logical relationship among all WLAN zone devices, and provides a way to manage devices directly in the Topology View.

The **Connectivity | Access Points > Topology View** page displays a tree-like or mesh diagram showing connected devices known to the firewall and their relationships, similar to the figure below:



Topics:

- Managing the Topology View
- Managing Access Points in the Topology View

Managing the Topology View

The Topology View is a simple interface. It provides the means to keep the view current and to modify the access points in the infrastructure.

Whenever you want to validate that the topology is current, click **REDISCOVER** on the bottom right corner. This forces the appliance to check if any changes have been made to the wireless infrastructure.

You can also get detailed information on each of the devices in the Topology View. Just run your cursor over the device and a tooltip bubble pops up. Depending on the type of device, it shows information like Name, IP address, Interface, and Model. For the access points, you can also see additional information like status and number of clients.

Each access point also uses color to indicate status:

- Green = online
- Red = offline
- Yellow = busy

Managing Access Points in the Topology View

The Topology View has a context menu with commands that can be used to manage the access points.

ⓘ **NOTE:** Only access points have context menus. None of the other devices in the topology map do.

Topics:

- Editing an Access Point
- Showing Statistics
- Monitor Status on an Access Point
- Delete an Access Point

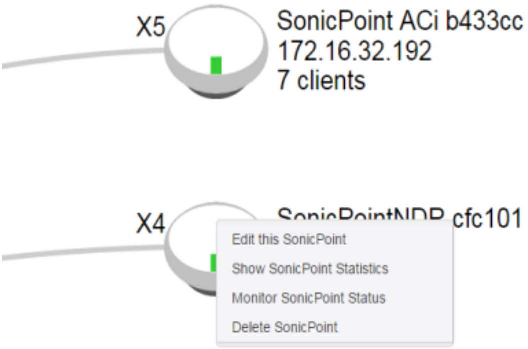
Editing an Access Point

To edit an access point in the Topology View:

1 Navigate to **Connectivity | Access Points > Topology View**.

2 Roll mouse over the access point you want to edit.

3 Right-click on the access point.



4 Select **Edit this Access Point**.

5 Make changes to the object configuration as needed.

6 Click **OK** to save new settings.

Showing Statistics

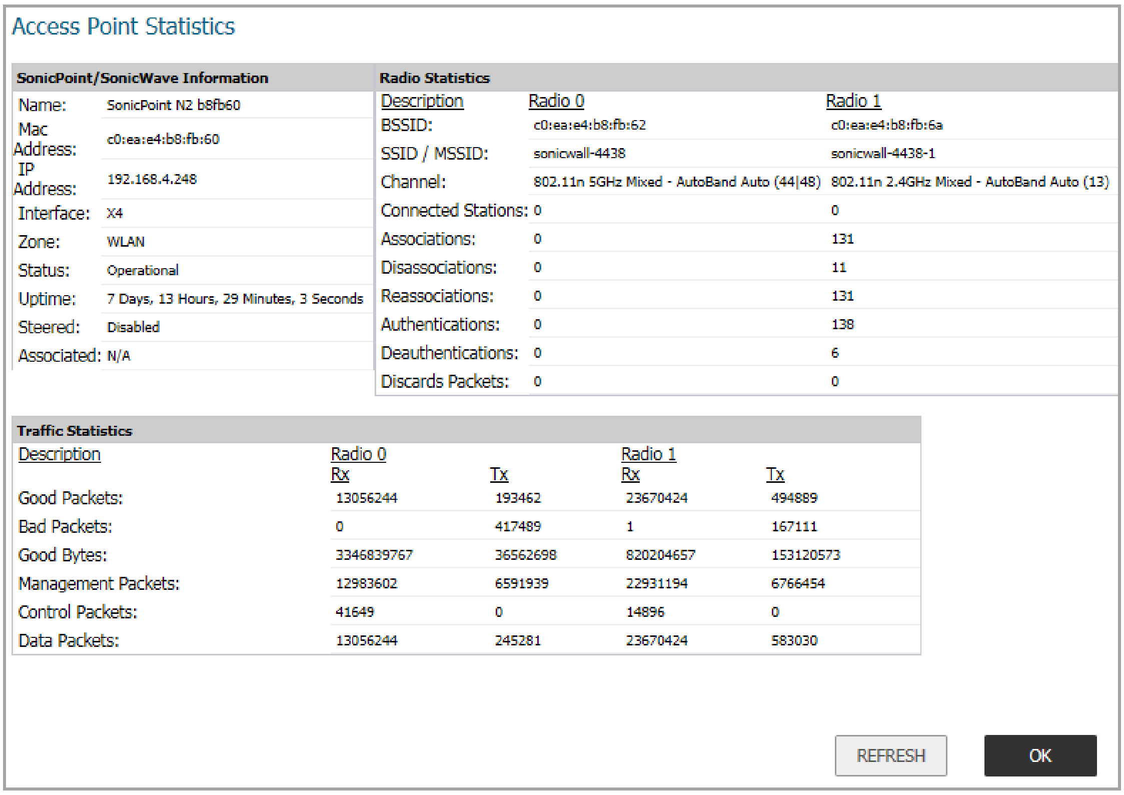
To show statistics for an access point:

1 Navigate to **Connectivity | Access Points > Topology View**.

2 Roll mouse over the access point you want to show.

3 Right-click on the access point.

4 Select Show **Access Point Statistics**.



Access Point Statistics

SonicPoint/SonicWave Information	
Name:	SonicPoint N2 b8fb60
Mac Address:	c0:ea:e4:b8:fb:60
IP Address:	192.168.4.248
Interface:	X4
Zone:	WLAN
Status:	Operational
Uptime:	7 Days, 13 Hours, 29 Minutes, 3 Seconds
Steered:	Disabled
Associated:	N/A

Radio Statistics

Description	Radio 0	Radio 1
BSSID:	c0:ea:e4:b8:fb:62	c0:ea:e4:b8:fb:6a
SSID / MSSID:	sonicwall-4438	sonicwall-4438-1
Channel:	802.11n 5GHz Mixed - AutoBand Auto (44|48)	802.11n 2.4GHz Mixed - AutoBand Auto (13)
Connected Stations:	0	0
Associations:	0	131
Disassociations:	0	11
Reassociations:	0	131
Authentications:	0	138
Deauthentications:	0	6
Discards Packets:	0	0

Traffic Statistics

Description	Radio 0		Radio 1	
	Rx	Tx	Rx	Tx
Good Packets:	13056244	193462	23670424	494889
Bad Packets:	0	417489	1	167111
Good Bytes:	3346839767	36562698	820204657	153120573
Management Packets:	12983602	6591939	22931194	6766454
Control Packets:	41649	0	14896	0
Data Packets:	13056244	245281	23670424	583030

5 Click **REFRESH** if you want to refresh the statistics.

6 Click **OK** when done.

Monitor Status on an Access Point

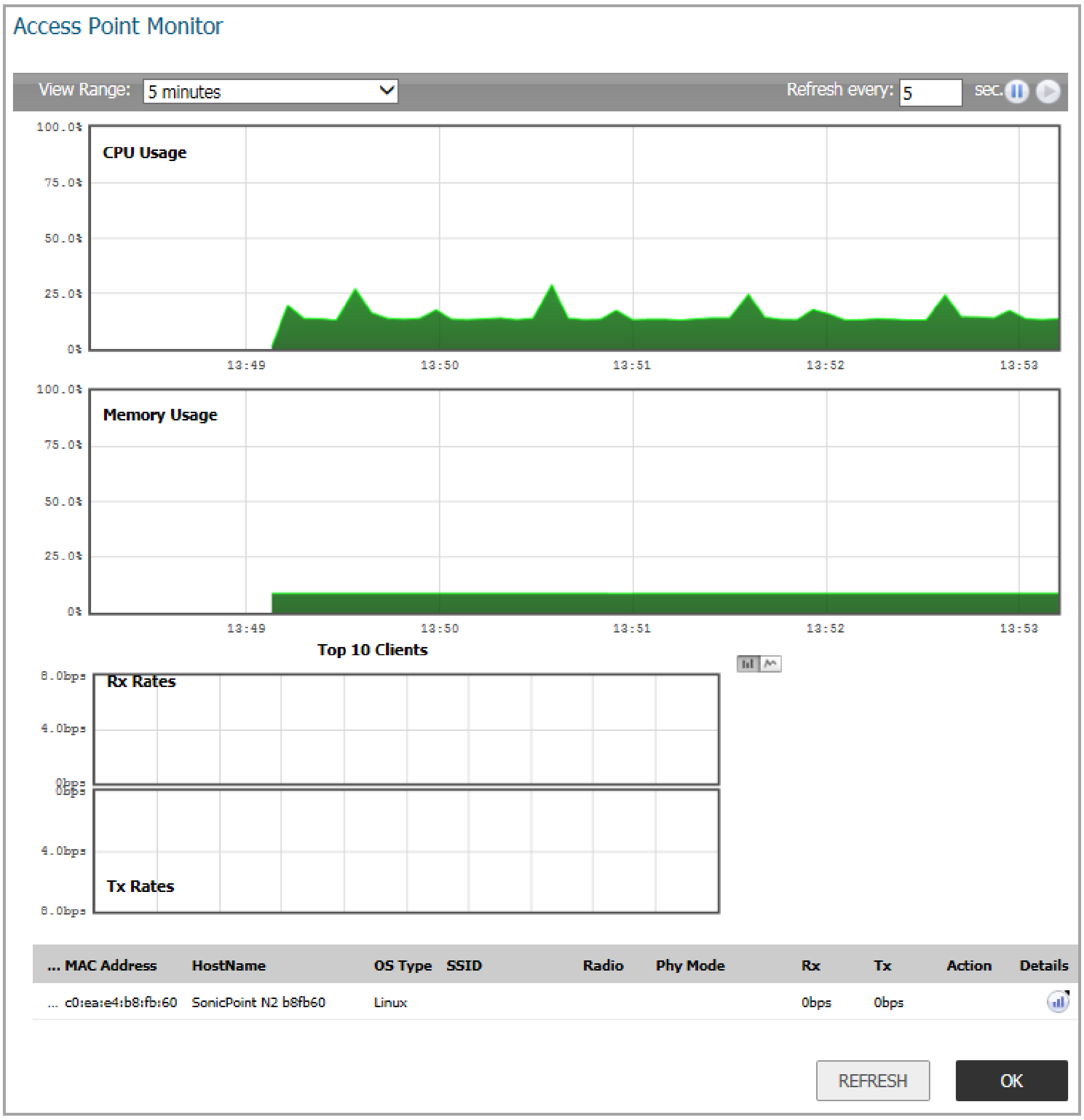
To edit an access point in the Topology View:

1 Navigate to **Connectivity | Access Points > Topology View**.

2 Roll mouse over the access point you want to monitor.

3 Right-click on the access point.

4 Select **Monitor Access Point Status**.



Access Point Monitor

View Range: 5 minutes

Refresh every: 5 sec.

... MAC Address	HostName	OS Type	SSID	Radio	Phy Mode	Rx	Tx	Action	Details
... c0:ea:e4:b8:fb:60	SonicPoint N2 b8fb60	Linux				0bps	0bps		

The Access Point Monitor shows system status for the access point. It includes CPU usage, Memory Usage, Rx Rates and Tx Rates.

5 Click **REFRESH** if you want to refresh the data.

6 Click the **Details** icon if you want to see the details on the access point.

7 Click **OK** when done.

Delete an Access Point

To edit an access point in the Topology View:

1. Navigate to **Connectivity | Access Points > Topology View**.
2. Roll mouse over the access point you want to delete.
3. Right-click on the access point.
4. Select **Delete Access Point**.
5. Confirm that you want to delete the access point; cancel if you do not.

20

Configuring Access Point Intrusion Detection Services

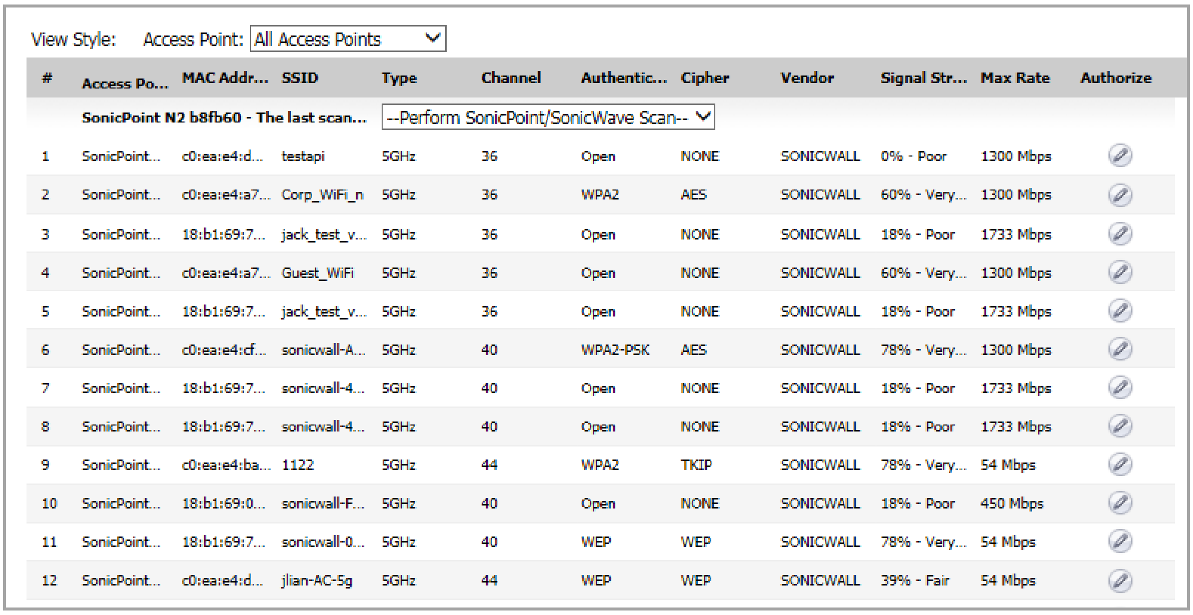
Rogue devices have emerged as one of the most serious and insidious threats to wireless security. In general terms, a device is considered rogue when it has not been authorized for use on the network. The convenience, afford-ability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue devices. The real threat emerges in a number of different ways:

- Unintentional and unwitting connections to the rogue device
- Transmission of sensitive data over non-secure channels
- Unwanted access to LAN resources

While this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

Intrusion Detection Services (IDS) greatly increase the security capabilities of the firewall because it helps the appliance recognize and take countermeasures against the most common types of illicit wireless activity. IDS reports on all access points the firewall can find by scanning the 802.11a, 802.11g, and 802.11n radio bands on the access points.

The **Connectivity | Access Points > IDS** page on the **MANAGE** view reports on all devices detected by the firewall and its associated access points, and provides the ability to authorize legitimate devices.



View Style: Access Point: All Access Points

#	Access Po...	MAC Addr...	SSID	Type	Channel	Authentic...	Cipher	Vendor	Signal Str...	Max Rate	Authorize
	SonicPoint N2 b8fb60 - The last scan...		--Perform SonicPoint/SonicWave Scan--								
1	SonicPoint...	c0:ea:e4:d...	testapi	5GHz	36	Open	NONE	SONICWALL	0% - Poor	1300 Mbps	✎
2	SonicPoint...	c0:ea:e4:a7...	Corp_WiFi_n	5GHz	36	WPA2	AES	SONICWALL	60% - Very...	1300 Mbps	✎
3	SonicPoint...	18:b1:69:7...	jack_test_v...	5GHz	36	Open	NONE	SONICWALL	18% - Poor	1733 Mbps	✎
4	SonicPoint...	c0:ea:e4:a7...	Guest_WiFi	5GHz	36	Open	NONE	SONICWALL	60% - Very...	1300 Mbps	✎
5	SonicPoint...	18:b1:69:7...	jack_test_v...	5GHz	36	Open	NONE	SONICWALL	18% - Poor	1733 Mbps	✎
6	SonicPoint...	c0:ea:e4:cf...	sonicwall-A...	5GHz	40	WPA2-PSK	AES	SONICWALL	78% - Very...	1300 Mbps	✎
7	SonicPoint...	18:b1:69:7...	sonicwall-4...	5GHz	40	Open	NONE	SONICWALL	18% - Poor	1733 Mbps	✎
8	SonicPoint...	18:b1:69:7...	sonicwall-4...	5GHz	40	Open	NONE	SONICWALL	18% - Poor	1733 Mbps	✎
9	SonicPoint...	c0:ea:e4:ba...	1122	5GHz	44	WPA2	TKIP	SONICWALL	78% - Very...	54 Mbps	✎
10	SonicPoint...	18:b1:69:0...	sonicwall-F...	5GHz	40	Open	NONE	SONICWALL	18% - Poor	450 Mbps	✎
11	SonicPoint...	18:b1:69:7...	sonicwall-0...	5GHz	40	WEP	WEP	SONICWALL	78% - Very...	54 Mbps	✎
12	SonicPoint...	c0:ea:e4:d...	jlian-AC-5g	5GHz	44	WEP	WEP	SONICWALL	39% - Fair	54 Mbps	✎

The following table describes the **Discovered Access Points** Table and entities that are displayed on the **Connectivity | Access Points > IDS** page.

Discovered Access Points Table Components

Table Column or Entity	Description
Entity	
REFRESH button	Refreshes the screen to display the most current list of access points in your network.
SCAN ALL button	Initiates an operation to call all access points and identify connected devices.
View Style: Access Point	If you have more than one access point, you can select an individual access point from the **Access Point** drop-down menu or **All Access Points** if you want to see all of them.
Discovered Access Points Table	
Access Point	The access point name: shows only when **All SonicPoints** is selected in the **View Style: Access Point** drop-down menu
MAC Address (BSSID)	The MAC address of the radio interface of the detected access point
SSID	The radio SSID of the device
Type	The radio band being used by the device: 2.4 GHz or 5 GHz
Channel	The radio channel used by the device
Authentication	The authentication type
Cipher	The cipher mode
Manufacturer	The manufacturer of the access point
Signal Strength	The strength of the detected radio signal
Max Rate	The fastest allowable data rate for the access point radio
Authorize	When the Edit icon is clicked, the device is added to the address object group of authorized devices.

Topics:

- Scanning Access Points
- Authorizing Access Points

Scanning Access Points

Active scanning occurs when the security appliance starts up. When you request a scan after start-up, the wireless clients are interrupted for a few seconds. The scan can effect traffic in the following ways:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.
- WiFiSec connections should automatically re-establish and resume with no noticeable interruption to the client.

△ CAUTION: **Clicking SCAN ALL causes all active wireless clients to be disconnected while the scan is performed. If service interruption is a concern, you should not request a scan while the SonicWall security appliance is in Access Point mode. Wait until no clients are active or a short interruption in service is acceptable.**

To perform a scan:

1 Navigate to **Connectivity | Access Points > IDS**.

2 In the **View Style: Access Point** drop-down menu (at the top of the table), select **All Access Points** to scan all devices or choose a specific access point to scan only one device.

3 At the bottom of the table:

- If you are scanning all access points, click SCAN ALL.

  You can optionally choose one of the options in the drop-down menu for **--Perform Access Point Scan--**: Scan Both Radios, **Scan Radio 0 (5GHz)** or **Scan Radio 1 (2.4GHz)**.

- If you are scanning only access point, choose one of the options in the drop-down menu for **--Perform Access Point Scan--**: Scan Both Radios, **Scan Radio 0 (5GHz)** or **Scan Radio 1 (2.4GHz)**.

> **NOTE:** If viewing only one access point the **--Perform Access Point Scan--** moves from the top center of the table to the bottom right.

4 Confirm that you want to perform the scan.

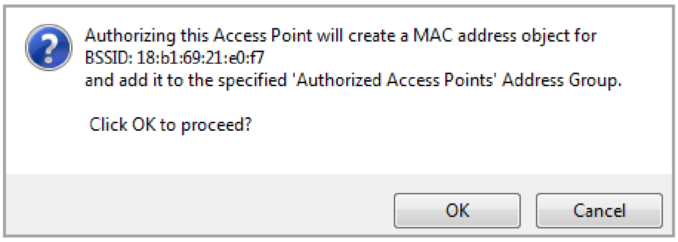
Authorizing Access Points

Access Points that the security appliance detects are regarded as rogue access points until the security appliance is configured to authorize them for operation.

To authorize an access point:

1 Navigate to **Connectivity | Access Points > IDS**.

2 Click the **Edit** icon in the **Authorize** column for the access point you want to authorize. A pop-up displays.



Authorizing this Access Point will create a MAC address object for
BSSID: 18:b1:69:21:e0:f7
and add it to the specified 'Authorized Access Points' Address Group.

Click OK to proceed?

3 Click **OK**.

4 Verify that authorization was successful by checking that the access point's MAC address was added. (Refer to the *SonicOS 6.5 System Setup* for more information.)

21

Configuring Advanced IDP

Advanced Intrusion Detection and Prevention (IDP), or Wireless Intrusion Detection and Prevention (WIDP), monitors the radio spectrum for presence of unauthorized devices (intrusion detection) and to take countermeasures automatically (intrusion prevention) according to administrator settings. When Advanced IDP is enabled on an access point, the radio functions as a dedicated IDP sensor.

△ **CAUTION: When Advanced IDP is enabled on a SonicWall access point radio, its access point functions are disabled and any wireless clients are disconnected.**

SonicOS Wireless Intrusion Detection and Prevention is based on SonicPoint and SonicWave access points cooperating with a SonicWall gateways. This feature turns your access points into dedicated WIDP sensors that detect unauthorized access points connected to a SonicWall network. This includes detection of KRACK Man-in-the-Middle access points.

△ **CAUTION: A SonicPoint N configured as a WIDP sensor cannot function as an access point.**

When an access point is identified as a rogue access point, its MAC address is added to the All Rogue Access Points address object group.

Topics:

- Enabling Wireless IDP on a Profile
- Configuring Wireless IDP Settings
- Viewing KRACK Sniffer Packets

Enabling Wireless IDP on a Profile

You can enable wireless intrusion detection and prevention on an access point profile, including setting a schedule for scanning. For more information about access point profiles, refer to Creating/Modifying Provisioning Profiles.

To enable Wireless IDP scanning on an access point profile:

1. Navigate to **SonicPoint/SonicWave Provisioning Profiles** section of the **Connectivity | Access Points > Base Settings** page.
2. Click the **Edit** icon for the appropriate profile.
3. Click **Sensor**.

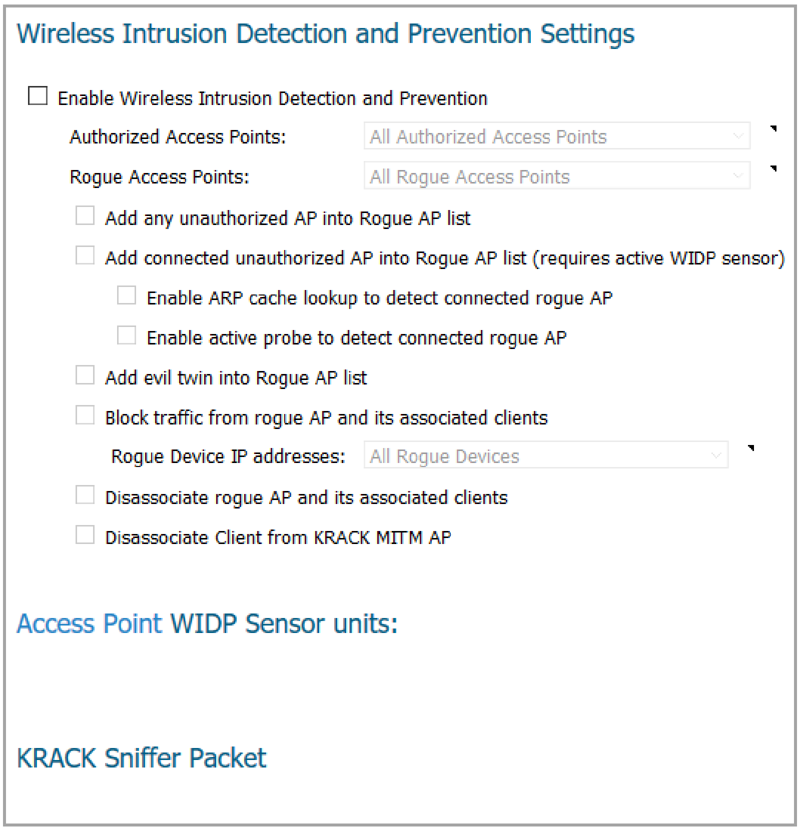
   ⓘ **TIP:** The **Sensor** screen is the same for all SonicPoint or SonicWave profiles.

4. Select **Enable WIDP Sensor**. The drop-down menu becomes active.
5. In the drop-down menu, select the appropriate schedule for IDP scanning, or select **Create new schedule** to create a custom schedule.

CAUTION: When Advanced IDP scanning is enabled on a SonicPoint/SonicWave radio, its access point functions are disabled and any wireless clients are disconnected.

6 Click **OK**.

Configuring Wireless IDP Settings



Wireless Intrusion Detection and Prevention Settings

☐ Enable Wireless Intrusion Detection and Prevention

Authorized Access Points: All Authorized Access Points

Rogue Access Points: All Rogue Access Points

☐ Add any unauthorized AP into Rogue AP list

☐ Add connected unauthorized AP into Rogue AP list (requires active WIDP sensor)

☐ Enable ARP cache lookup to detect connected rogue AP

☐ Enable active probe to detect connected rogue AP

☐ Add evil twin into Rogue AP list

☐ Block traffic from rogue AP and its associated clients

Rogue Device IP addresses: All Rogue Devices

☐ Disassociate rogue AP and its associated clients

☐ Disassociate Client from KRACK MITM AP

Access Point WIDP Sensor units:

KRACK Sniffer Packet

To configure Wireless IDP settings:

1 Navigate to **Connectivity | Access Points > Advanced IDP**.

2 Select **Enable Wireless Intrusion Detection and Prevention** to enable the appliance to search for rogue access points, including KRACK Man-in-the-Middle access points. This option is not selected by default, so when selected, the other options become active.

> **NOTE:** All detected access points are displayed in the **Discovered Access Points** table on the **Connectivity | Access Points > IDS** page, and you can authorize any allowed access points.

3 For **Authorized Access Points**, select the Address Object Group to which authorized Access Points are assigned. By default, this is set to **All Authorized Access Points**.

> **NOTE:** For SonicPoint Ns, no access point mode Virtual Access Point (VAP) is created. One station mode VAP is created, which is used to do IDS scans, and to connect to and send probes to unsecured access points.

4 For **Rogue Access Points**, select the Address Object Group to which unauthorized Access Points are assigned. By default, this is set to **All Rogue Access Points**.

5 Select one of the following two options to determine which access points are considered rogue (only one can be enabled at a time):

- **Add any unauthorized AP into Rogue AP list** automatically assigns all detected unauthorized access points—regardless if they are connected to your network—to the Rogue list.
- **Add connected unauthorized AP into Rogue AP list** assigns unauthorized devices to the Rogue list only if they are connected to your network. The following options determine how IDP detects connected rogue devices; both can be selected:
  - **Enable ARP cache search to detect connected rogue AP** – Advanced IDP searches the ARP cache for clients' MAC addresses. When one is found and the AP it is connected to is not authorized, the AP is classified as rogue.
  - **Enable active probe to detect connected rogue AP** – The SonicPoint/SonicWave connects to the suspect device and sends probes to all LAN, DMZ and WLAN interfaces of the firewall. If the firewall receives any of these probes, the AP is classified as rogue.

6 Select **Add evil twin into Rogue AP list** to add devices to the rogue list when they are not in the authorized list, but have the same SSID as a managed access point.

7 Select **Block traffic from rogue AP and its associated clients** to drop all incoming traffic that has a source IP address that matches the rogue list. From the **Rogue Device IP addresses** drop-down menu, either:

- Select **All Rogue Devices** (default) or an address object group you've created.
- Create a new address object group by selecting **Create New IP Address Object Group**. The **Add Address Object Group** window displays.

8 Select **Disassociate rogue AP and its clients** to send de-authentication messages to clients of a rogue device to stop communication between them.

9 Select **Disassociate Client from KRACK MITM AP** to enable the KRACK prevention function. When enabled, the SonicWave periodically checks for KRACK Man-in-the-Middle access points and actively disassociates the client from the KRACK MITM access point when it detects a client associated to it.

10 Click **ACCEPT** to save your changes.

Viewing KRACK Sniffer Packets

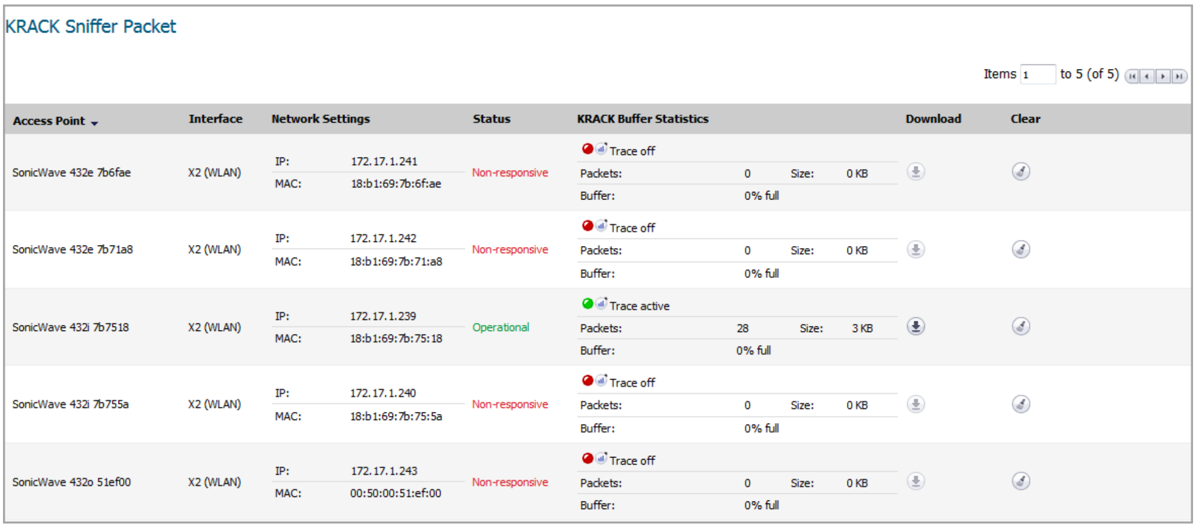
When the **Enable Wireless Intrusion Detection and Prevention** option is enabled, the SonicWave periodically scans the wireless environment looking for a KRACK Man-in-the-Middle access point and any clients interacting with it. ***KRACK*** is the acronym for ***Key Reinstallation Attack***.

The KRACK MITM attack clones the real access point on a different channel with the same MAC address as the real access point. When a KRACK MITM access point is detected, the SonicWave opens a monitoring interface on the same channel as the KRACK MITM, and sniffs the packets on the channel for a period of time. If a wireless client is associated with the MITM access point and the **Disassociate Client from KRACK MITM AP** option is enabled, the client is disassociated from the MITM access point. Log messages are reported in the **INVESTIGATE | Logs > Event Logs** page when any of the following events occur:

- KRACK MITM access point is detected
- Client is detected communicating with the MITM access point
- Client is disassociated from the MITM access point

Because the sniffing is done during the KRACK detection process, the captured packets are saved in the buffer of the SonicWave. The KRACK Sniffer Statistics image shows the KRACK sniffer results from multiple SonicWaves.

KRACK Sniffer Statistics

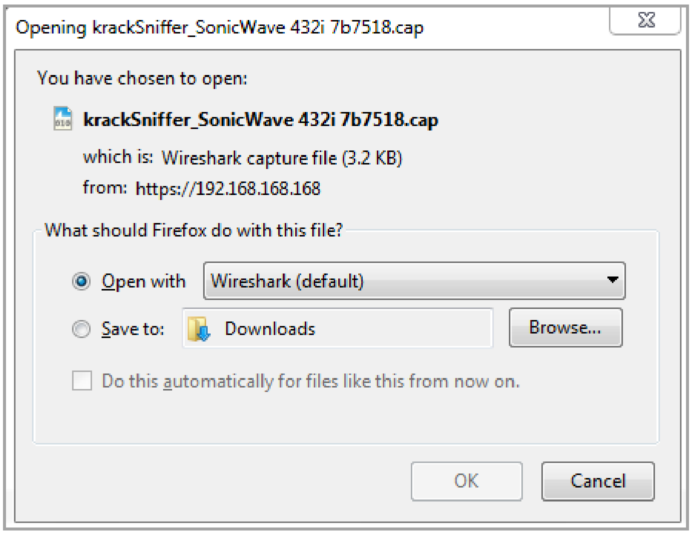


KRACK Sniffer Packet

Items 1 to 5 (of 5)

Access Point	Interface	Network Settings	Status	KRACK Buffer Statistics	Download	Clear
SonicWave 432e 7b6fae	X2 (WLAN)	IP: 172.17.1.241 MAC: 18:b1:69:7b:6f:ae	Non-responsive	● Trace off Packets: 0 Size: 0 KB Buffer: 0% full		
SonicWave 432e 7b71a8	X2 (WLAN)	IP: 172.17.1.242 MAC: 18:b1:69:7b:71:a8	Non-responsive	● Trace off Packets: 0 Size: 0 KB Buffer: 0% full		
SonicWave 432i 7b7518	X2 (WLAN)	IP: 172.17.1.239 MAC: 18:b1:69:7b:75:18	Operational	● Trace active Packets: 28 Size: 3 KB Buffer: 0% full		
SonicWave 432i 7b755a	X2 (WLAN)	IP: 172.17.1.240 MAC: 18:b1:69:7b:75:5a	Non-responsive	● Trace off Packets: 0 Size: 0 KB Buffer: 0% full		
SonicWave 432o 51ef00	X2 (WLAN)	IP: 172.17.1.243 MAC: 00:50:00:51:ef:00	Non-responsive	● Trace off Packets: 0 Size: 0 KB Buffer: 0% full		

To analyze the KRACK process, click **Download** for a SonicWave to export the packet data to the file *krackSniffer_[SonicWave name].cap*, where *[SonicWave name]* is the name of the SonicWave. Then open the file and view it using Wireshark or another PCAP analyzer tool.



Opening krackSniffer_SonicWave 432i 7b7518.cap

You have chosen to open:

krackSniffer_SonicWave 432i 7b7518.cap

which is: Wireshark capture file (3.2 KB)

from: https://192.168.168.168

What should Firefox do with this file?

● Open with Wireshark (default)

○ Save to: Downloads

□ Do this automatically for files like this from now on.

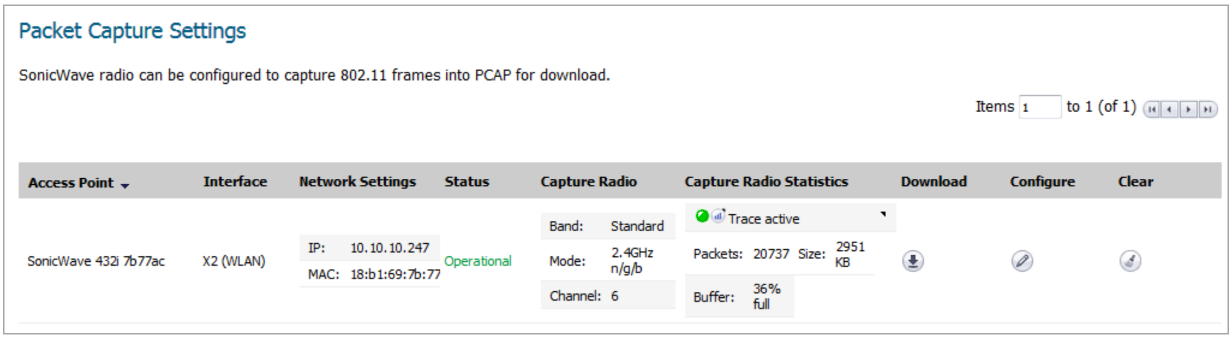
22

Access Point Packet Capture

The **Connectivity | Access Points > Packet Capture** feature on the **MANAGE** view provides an in-depth type of wireless troubleshooting that you can use to gather wireless data from a client site and output into a readable file. This feature is supported for SonicWave access points.

ⓘ **NOTE:** Because the antenna of the scan radio is 1x1, some data frames cannot be captured by the scan radio because of hardware restrictions.

The capture view on the **Access Points > Packet Capture** page shows the status of the SonicWave, the number of packets captured, and the size of the packet buffer. At the right, the **Configure** column provides buttons you can click to configure the capture settings for each SonicWave.



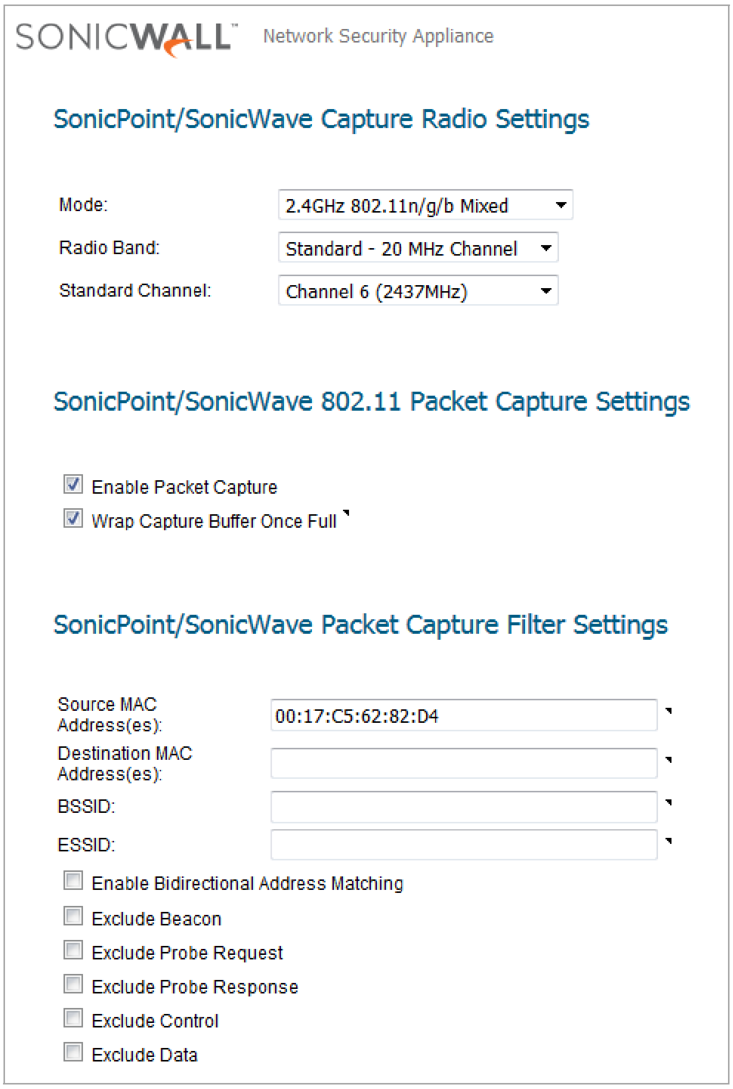
Packet Capture Settings

SonicWave radio can be configured to capture 802.11 frames into PCAP for download.

Items 1 to 1 (of 1)

Access Point	Interface	Network Settings	Status	Capture Radio	Capture Radio Statistics	Download	Configure	Clear
SonicWave 432i 7b77ac	X2 (WLAN)	IP: 10.10.10.247 MAC: 18:b1:69:7b:77	Operational	Band: Standard Mode: 2.4GHz n/g/b Channel: 6	● Trace active Packets: 20737 Size: 2951 KB Buffer: 36% full			

You can configure the mode, band and channel settings in the configuration dialog, allowing you to capture wireless packets in a specific channel. You can configure up to five source and destination MAC addresses. Click **Edit** for the SonicWave you want to configure.



SONICWALL Network Security Appliance

SonicPoint/SonicWave Capture Radio Settings

Mode: 2.4GHz 802.11n/g/b Mixed

Radio Band: Standard - 20 MHz Channel

Standard Channel: Channel 6 (2437MHz)

SonicPoint/SonicWave 802.11 Packet Capture Settings

☑ Enable Packet Capture

☑ Wrap Capture Buffer Once Full

SonicPoint/SonicWave Packet Capture Filter Settings

Source MAC Address(es): 00:17:C5:62:82:D4

Destination MAC Address(es):

BSSID:

ESSID:

☐ Enable Bidirectional Address Matching

☐ Exclude Beacon

☐ Exclude Probe Request

☐ Exclude Probe Response

☐ Exclude Control

☐ Exclude Data

To capture the data for one of configured SonicWave radios, click **Download** for that row on the **Connectivity | Access Points > Packet Capture** page. The capture file is named with the format, “`wirelessCapture_[SW name].cap`,” where *SW name* is the SonicWave name. Wireshark™ can be used to read the file.

23

Configuring Virtual Access Points

ⓘ **NOTE:** Virtual access points are supported when using wireless access points along with SonicWall NSA appliances.

A Virtual Access Point (VAP) is a multiplexed representation of a single physical access point—it presents itself as multiple discrete access points. To wireless LAN clients, each virtual access point appears to be an independent physical access point, when actually only one physical access point exists. VAPs allow you to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point and can be grouped and enforced on a single internal wireless radio.

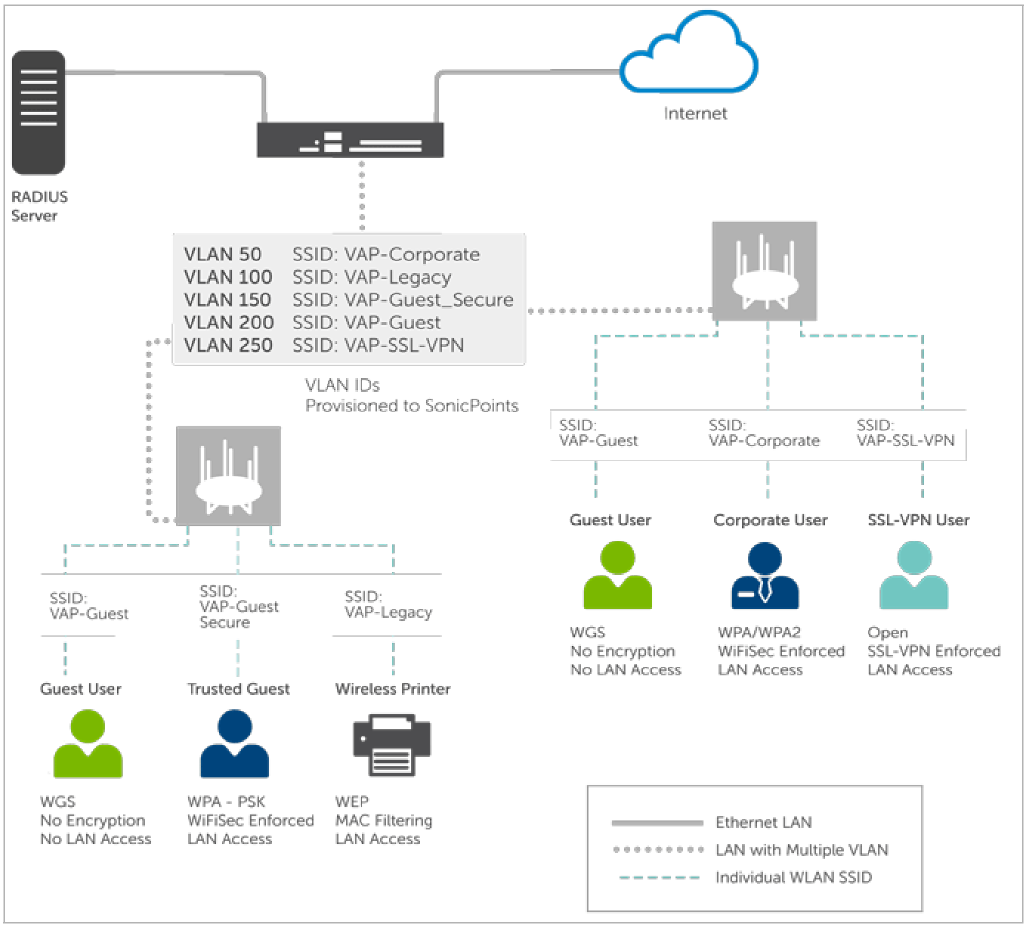
The SonicWall VAP feature is in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This segments the wireless network services within a single radio frequency footprint on a single physical access point.

VAPs allow you to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on single or multiple physical access points simultaneously.

Topics:

- Before Configuring VAPs
- Access Point VAP Configuration Task List
- Virtual Access Points Profiles
- Virtual Access Points
- Virtual Access Point Groups

Virtual Access Point Configuration


Internet
RADIUS Server
VLAN 50 SSID: VAP-Corporate
VLAN 100 SSID: VAP-Legacy
VLAN 150 SSID: VAP-Guest_Secure
VLAN 200 SSID: VAP-Guest
VLAN 250 SSID: VAP-SSL-VPN
VLAN IDs Provisioned to SonicPoints
SSID: VAP-Guest
SSID: VAP-Corporate
SSID: VAP-SSL-VPN
Guest User
Corporate User
SSL-VPN User
WGS No Encryption No LAN Access
WPA/WPA2 WiFiSec Enforced LAN Access
Open SSL-VPN Enforced LAN Access
SSID: VAP-Guest
SSID: VAP-Guest Secure
SSID: VAP-Legacy
Guest User
Trusted Guest
Wireless Printer
WGS No Encryption No LAN Access
WPA - PSK WiFiSec Enforced LAN Access
WEP MAC Filtering LAN Access
Ethernet LAN
LAN with Multiple VLAN
Individual WLAN SSID

VAPs afford the following benefits:

- Each VAP can have its own security services settings (for example, GAV, IPS, CFS, and so on).
- Traffic from each VAP can be easily controlled using access rules configured from the zone level.
- Separate Guest Services or Lightweight Hotspot Messaging (LHM) configurations can be applied to each, facilitating the presentation of multiple guest service providers with a common set of access points.
- Bandwidth management and other access rule-based controls can easily be applied.

Before Configuring VAPs

Before configuring your virtual access points, you need to have in understanding of what your options are and what you can do.

Topics:

- Determining Your VAP Needs
- Determining Security Configurations
- Sample Network Definitions
- Determining Security Configurations
- VAP Configuration Worksheet

Determining Your VAP Needs

When deciding how to configure your VAPs, begin by considering your communication needs, particularly:

- How many different classes of wireless users do I need to support?
- How do I want to secure these different classes of wireless users?
- Do my wireless client have the required hardware and drivers to support the chosen security settings?
- What network resources do my wireless users need to communicate with?
- Do any of these wireless users need to communicate with other wireless users?
- What security services do I wish to apply to each of these classes or wireless users?

Determining Security Configurations

After understanding your security requirements, you can then define the zones (and interfaces) and VAPs that provide the most effective wireless services to these users. The following are examples of ways you can define certain types of users.

- **Corp Wireless** – Highly trusted wireless zone. Employs WPA2-AUTO-EAP security. WiFiSec (WPA) Enforced.
- **WEP & PSK** – Moderate trust wireless zone. Comprises two virtual APs and subinterfaces, one for legacy WEP devices (for example, wireless printers, older hand-held devices) and one for visiting clients who use WPA-PSK security.
- **Guest Services** – Using the internal Guest Services user database.
- **LHM** – Lightweight Hotspot Messaging enabled zone, configured to use external LHM authentication-back-end server.

Sample Network Definitions

The following list shows one possible way you and configure your virtual access points to ensure proper access:

- **VAP #1, Corporate Wireless Users** – A set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services.
- **VAP#2, Legacy Wireless Devices** – A collection of older wireless devices, such as printers, PDAs and hand-held devices, that are only capable of WEP encryption.
- **VAP#3, Visiting Partners** – Business partners, clients, and affiliated who frequently visit the office, and who need access to a limited set of trusted network resources, as well as the Internet. These users are not located in the company's Directory Services.
- **VAP# 4, Guest Users** – Visiting clients to whom you wish to provide access only to untrusted (for example, Internet) network resources. Some guest users are provided a simple, temporary username and password for access.
- **VAP#5, Frequent Guest Users** – Same as Guest Users, however, these users have more permanent guest accounts through a back-end database.

Prerequisites

Before configuring your virtual access points, be aware of the following:

- Each SonicWall access point must be explicitly enabled for virtual access point support. To verify, navigate to **Connectivity | Access Points > Base Settings.** Then click the **Edit** icon for the **SonicPoint/SonicWave Provisioning Profiles > General Settings**: **Enable SonicPoint/SonicWave** checkbox and enabling either Radio A or G.
- Access points must be linked to a WLAN zone on your SonicWall network security appliance to provision the access points.
- When using VAPs with VLANs, you must ensure that the physical access point discovery and provisioning packets remain untagged (unless being terminated natively into a VLAN subinterface on the firewall).
- You must also ensure that VAP packets that are VLAN tagged by the access point are delivered unaltered (neither un-encapsulated nor double-encapsulated) by any intermediate equipment, such as a VLAN capable switch, on the network.
- Be aware that maximum access point restrictions apply and differ based on your SonicWall security appliance.

VAP Configuration Worksheet

The the VAP Configuration Worksheet table provides some common VAP setup questions and solutions along with a space for you to record your own configurations.

VAP Configuration Worksheet

Questions	Examples	Solutions
How many different types of users do I need to support?	Corporate wireless, guest access, visiting partners, wireless devices are all common user types, each requiring their own VAP	Plan out the number of different VAPs needed. Configure a zone and VLAN for each VAP needed
	Your Configurations:	
How many users does each VAP need to support?	A corporate campus has 100 employees, all of whom have wireless capabilities	The DHCP scope for the visitor zone is set to provide at least 100 addresses
	A corporate campus often has a few dozen wireless capable visitors	The DHCP scope for the visitor zone is set to provide at least 25 addresses
	Your Configurations:	

VAP Configuration Worksheet (Continued)

Questions	Examples	Solutions
How do I want to secure different wireless users?	A corporate user who has access to corporate LAN resources.	Configure WPA2-EAP
	A guest user who is restricted to only Internet access	Enable Guest Services but configure no security settings
	A legacy wireless printer on the corporate LAN	Configure WEP and enable MAC address filtering
	Your Configurations:	
What network resources do my users need to communicate with?	A corporate user who needs access to the corporate LAN and all internal LAN resources, including other WLAN users.	Enable Interface Trust on your corporate zone.
	A wireless guest who needs to access InternetInternet and should not be allowed to communicate with other WLAN users.	Disable Interface Trust on your guest zone.
	Your Configurations:	
What security services to I wish to apply to my users?	Corporate users who you want protected by the full SonicWall security suite.	Enable all SonicWall security services.
	Guest users who you do not care about because they are not even on your LAN.	Disable all SonicWall security services.
	Your Configurations:	

Access Point VAP Configuration Task List

An access point VAP deployment requires several steps to configure. The following section provides a brief overview of the steps involved.

1. **Network Zone** - The zone is the backbone of your VAP configuration. Each zone you create has its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of VLAN subinterfaces. For more information on network zones, refer to the section on **Manage | Network > Zones** in *SonicOS 6.5 System Setup*.
2. **Interface (or VLAN Subinterface)** - The Interface (X2, X3, and so on) represents the physical connection between your SonicWall network security appliance and your physical access points. Your individual zone settings are applied to these interfaces and then forwarded to your access points. For more information

on wireless interfaces, refer to the section on **Manage | Network > Interfaces** in *SonicOS 6.5 System Setup*.

3 **DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as *Scopes*. The default ranges for DHCP scopes are often excessive for the needs of most access points, for instance, a scope of 200 addresses for an interface that only uses 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted. For more information on setting up the DHCP server, refer to the section on **Manage | Network > DHCP Server** in *SonicOS 6.5 System Setup*.

4 **Virtual Access Point Profiles** - The **Virtual Access Point Profile** feature allows for creation of access point configuration profiles which can be easily applied to new virtual access points as needed. Refer to **Virtual Access Points Profiles** for more information.

5 **Virtual Access Point Objects** - The **Virtual Access Point Objects** feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings. Refer to **Virtual Access Points** for more information.

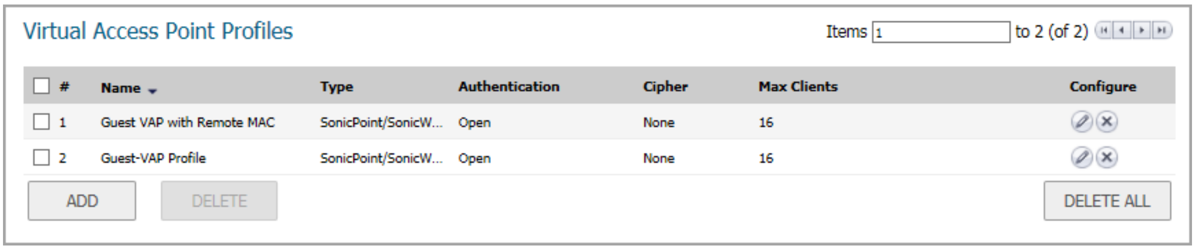
6 **Virtual Access Point Groups** - The **Virtual Access Point Groups** feature allows grouping of multiple virtual access point objects to be simultaneously applied to your access points.

7 **Assign Virtual Access Group to Access Point Provisioning Profile Radio**- The Provisioning Profile allows a VAP Group to be applied to new access points as they are provisioned.

8 **Assign WEP Key (for WEP encryption only)** - The Assign WEP Key allows for a WEP Encryption Key to be applied to new access points as they are provisioned. WEP keys are configured per-access point, meaning that any WEP-enabled virtual access points assigned to a physical access point must use the same set of WEP keys. Up to 4 keys can be defined, and WEP-enabled VAPs can use these 4 keys independently. WEP keys are configured on individual physical access points or on Access Point Profiles from the **Configuration | Access Points > Base Settings** page.

Virtual Access Points Profiles

A Virtual Access Point Profile allows you to pre-configure and save access point settings in a profile. Virtual Access Point Profiles allows settings to be easily applied to new virtual access points. Virtual Access Point Profiles are configured from the **Virtual Access Point Profiles** section of the **Connectivity | Access Points > Virtual Access Point** page.



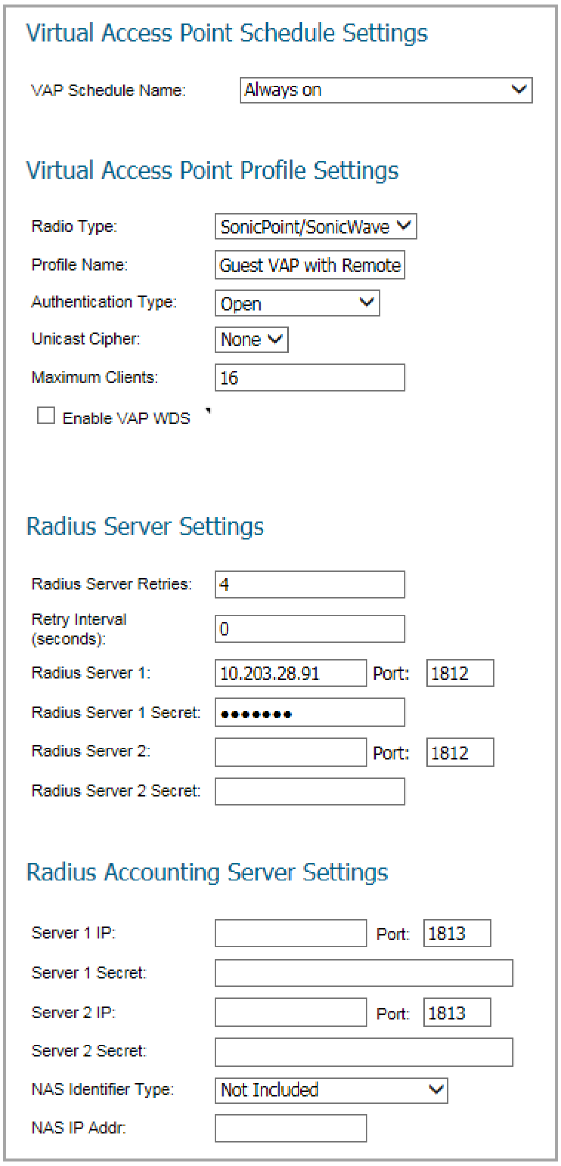
Virtual Access Point Profiles

Items 1 to 2 (of 2)

☐	#	Name	Type	Authentication	Cipher	Max Clients	Configure
☐	1	Guest VAP with Remote MAC	SonicPoint/SonicW...	Open	None	16	
☐	2	Guest-VAP Profile	SonicPoint/SonicW...	Open	None	16	

To configure an existing VAP profile, click the **Edit** icon for that profile. To add a new VAP profile, click **ADD**.

NOTE: Options displayed change depending on your selection of other options.



Virtual Access Point Schedule Settings

VAP Schedule Name: Always on

Virtual Access Point Profile Settings

Radio Type: SonicPoint/SonicWave

Profile Name: Guest VAP with Remote

Authentication Type: Open

Unicast Cipher: None

Maximum Clients: 16

□ Enable VAP WDS

Radius Server Settings

Radius Server Retries: 4

Retry Interval (seconds): 0

Radius Server 1: 10.203.28.91 Port: 1812

Radius Server 1 Secret: •••••••

Radius Server 2: Port: 1812

Radius Server 2 Secret:

Radius Accounting Server Settings

Server 1 IP: Port: 1813

Server 1 Secret:

Server 2 IP: Port: 1813

Server 2 Secret:

NAS Identifier Type: Not Included

NAS IP Addr:

Topics:

- Virtual Access Point Schedule Settings
- Virtual Access Point Profile Settings
- ACL Enforcement
- Remote MAC Address Access Control Settings

Virtual Access Point Schedule Settings

Each Virtual Access Point can have its own schedule associated with it and by extension each profile can have a set schedule defined for it as well.

To associate a schedule with a Virtual Access Point Profile:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Access Points > Virtual Access Point**.

3 Select **ADD** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.

4 In the **VAP Schedule Name** field, select the schedule you want from the options in the drop-down menu.

Virtual Access Point Profile Settings

To set the Virtual Access Point Profile settings:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Virtual Access Point**.

3 Select **ADD** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.

4 Set the **Radio Type**. It is set to **SonicPoint/SonicWave** by default if using the access points as virtual access points (currently the only supported radio type).

5 In the **Profile Name** field, type a friendly name for this Virtual Access Point Profile. Choose something descriptive and easy to remember as you apply this profile to new VAPs.

6 Select the **Authentication Type** from the drop-down menu. Choose from these options:

Authentication Type	Definition
Open	No authentication is specified; unsecured access.
Shared	A shared key is used to authenticate and ensure basis security.
Both	Unsecured, shared access.
WPA2-PSK	Best security used with trusted corporate wireless clients. Transparent authentication with Windows login. Supports fast-roaming feature. Uses preshared key for authentication.
WPA2-EAP	Best security used with trusted corporate wireless clients. Transparent authentication with Windows login. Supports fast-roaming feature. Uses extensible authentication protocol.
WPA2-AUTO-PSK	Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection defaults to WPA.Uses preshared key for authentication.
WPA2-AUTO-EAP	Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection defaults to WPA. Uses extensible authentication protocol.

The **Unicast Cipher** field is auto-populated based on what authentication type you selected.

ⓘ **NOTE:** Different setting appear on the page depending upon which option you select.

Depending on the **Authentication Type** selected, an additional section with options is added to the Add/Edit Virtual Access Point Profile page.

- If you selected Open, refer to Radius Server and Radius Accounting on RADIUS settings.
- If you selected **Both** or **Shared**, refer to WEP Encryption Settings for information on the settings.

- If you selected an option requiring a preshared key (PSK), refer to WPA-PSK > WPA2-PSK Encryption Settings for information on the settings.
- If you selected an option using the extensible authentication protocol (EAP), refer to Radius Server and Radius Accountingfor information on the settings.

WEP Encryption Settings

If you selected **Both** or **Shared** in Step 6 of the prior procedure, the section called **WEP Encryption Settings** appears. WEP settings are commonly shared by virtual access points within a common physical access point.

To set the encryptions settings:

1. In the **Encryption Key** field, select **Key 1**, **Key 2**, **Key 3** or **Key 4** from the drop-down menu.
2. Go to Radius Server and Radius Accounting to set up the RADIUS settings, if you kept Remote MAC Access Control enabled.

WPA-PSK > WPA2-PSK Encryption Settings

If you selected an option in Step 6 that requires a preshared key—**WPA2-PSK** or **WPA2-AUTO-PSK**—the section called **WPA/WPA2-PSK Encryption Settings** appears. When these settings are defined, a preshared key is used for authentication.

To set the encryptions settings:

1. Input a password in the **Pass Phrase** field.
2. Go to Radius Server and Radius Accounting to set up the RADIUS settings, if you kept Remote MAC Access Control enabled.

Radius Server and Radius Accounting

You can set up a RADIUS server for any of the options selected in Step 6. When these settings are defined, an external 802.1x/EAP capable RADIUS server is used for key generation and authentication. Input values in the following fields:

To set the Radius Server Settings:

Field Name	Description
Radius Server Retries	Enter the number times a user can try to authenticate before access is denied. The default is 4.
Retry Interval (seconds)	Enter the time period during which retries are valid. The default is 0.
RADIUS Server 1	Input the name/location of the RADIUS authentication server.
Port	Input the port on which your primary RADIUS authentication server communicates with clients and network devices.
RADIUS Server 1 Secret	Enter the secret passcode for your primary RADIUS authentication server.
RADIUS Server 2	Input the name/location of your backup RADIUS authentication server.
Port	Input the port on which your backup RADIUS authentication server communicates with clients and network devices.
RADIUS Server 2 Secret	Enter the secret passcode for your backup RADIUS authentication server.

To set the Radius Accounting Server Settings:

No

Field Name	Description
Server 1 IP	Enter the IP address for the first RADIUS server.
Port	Input the port on which your primary RADIUS accounting server communicates with clients and network devices.
Server 1 Secret	Enter the secret passcode for your primary RADIUS accounting server.
Server 2 IP	Enter the IP address for the backup RADIUS server.
Port	Input the port on which your backup RADIUS accounting server communicates with clients and network devices.
Server 2 Secret	Enter the secret passcode for your backup RADIUS accounting server.
NAS Identifier Type	Select the NAS Identifier Type from the drop-down menu. Options include: Not Included (default), Access Point Name, Access Point MAC Address, and SSID. When the SSID option is selected, both the RADIUS authentication message and RADIUS accounting message carry the VAP SSID.
NAS IP Addr	Input the NAS system IP address.
Group Key Interval	The time period, in seconds, for which a group key is valid and after which the group key is forced to be updated. The default is **86400** seconds (24 hours).

ACL Enforcement

Each virtual access point can support an individual Access Control List (ACL) to provide more effective authentication control. The wireless ACL feature works in tandem with the wireless MAC Filter List currently available on SonicOS. Using the ACL Enforcement feature, users are able to enable or disable the MAC Filter List, set the Allow List, and set the Deny list.

Each VAP can have its own MAC Filter List settings or use the global settings. When the global settings are enabled, the SonicWave, SonicPoint-N/ SonicPointNDR/ SonicPoint Ni/Ne, the SonicPoint, or SonicPoint-N appliance uses these settings by default. In Virtual Access Point (VAP) mode, each VAP of this group shares the same MAC Filter List settings.

ACL Enforcement Settings

Option	Description
Enable MAC Filter List	Enforces Access Control by allowing or denying traffic from specific devices. By default, this option is not selected and all options in this section are dimmed and unavailable.
Use Global ACL Settings	Uses global ACL settings. **NOTE:** ACL support per virtual access point is only supported by SonicPointN. If one virtual access point is used by SonicPoint/SonicWave, global ACL configuration is applied by default.

ACL Enforcement Settings (Continued)

Option	Description
Allow List	Select a MAC address group to automatically allow traffic from all devices with the MAC addresses listed in a particular group: • **Create new Mac Address Object Group...** • **All MAC Addresses** **NOTE:** It is recommended that the **Allow List** be set to **All MAC Addresses**. • **Default SonicPoint/SonicWave ACL Allow Group** • Custom MAC Address Object Groups that you developed
Deny List	Select a MAC address group from the drop-down menu to automatically deny traffic from all devices with MAC address in the group. **NOTE:** The **Deny List** is enforced before the **Allow List**. • **Create new Mac Address Object Group...** • **No MAC Addresses** • **Default SonicPoint/SonicWave ACL Deny Group** **NOTE:** It is recommended that the **Deny List** be set to **Default SonicPoint/SonicWave ACL Deny Group**. • Custom MAC Address Object Groups that you developed

Remote MAC Address Access Control Settings

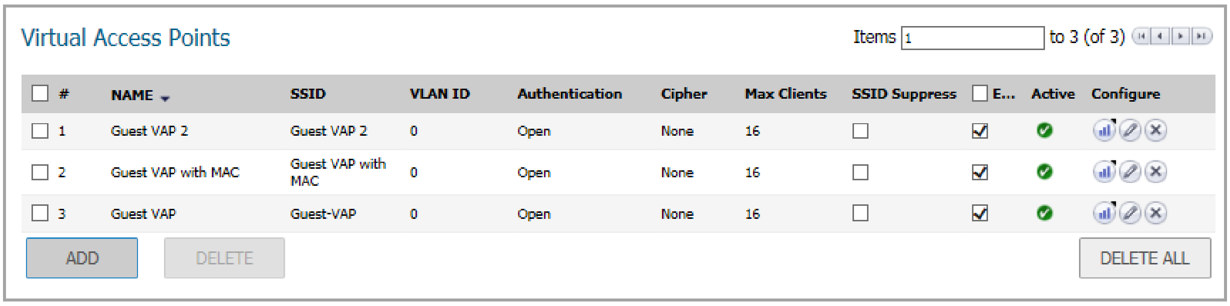
NOTE: This section is not displayed if **WPA2-EAP/WPA2-AUTO-EAP** is selected for **Authentication Type**.

Remote MAC Address Access Control Settings

Option	Description
Enable Remote MAC Access Control	Check the box to enforce radio wireless access control based on MAC-based authentication policy in a remote Radius server. By default, this option is not selected. **NOTE:** If you selected other than **WPA2-EAP/WPA2-AUTO-EAP** for **Authentication Type**, selecting **Enable Remote MAC Access Control** displays the **Radius Server Settings** section.

Virtual Access Points

The VAP Settings feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings. virtual access points are configured from the **Access Point > Virtual Access Point** page.



Virtual Access Points

Items 1 to 3 (of 3)

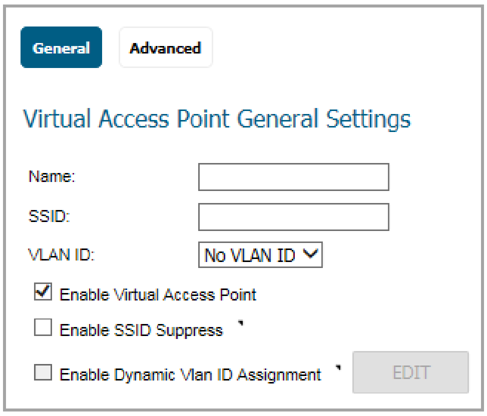
☐	#	NAME	SSID	VLAN ID	Authentication	Cipher	Max Clients	SSID Suppress	☐ E...	Active	Configure
☐	1	Guest VAP 2	Guest VAP 2	0	Open	None	16	☐	☑	✓	
☐	2	Guest VAP with MAC	Guest VAP with MAC	0	Open	None	16	☐	☑	✓	
☐	3	Guest VAP	Guest-VAP	0	Open	None	16	☐	☑	✓	

To configure an existing VAP, click the **Edit** icon for that virtual access point. To add a new VAP, click **ADD**.

Topics:

- General Panel on page 243
- Advanced Tab on page 244

General Panel



Virtual Access Point General Settings

Name:

SSID:

VLAN ID: No VLAN ID

☑ Enable Virtual Access Point

□ Enable SSID Suppress

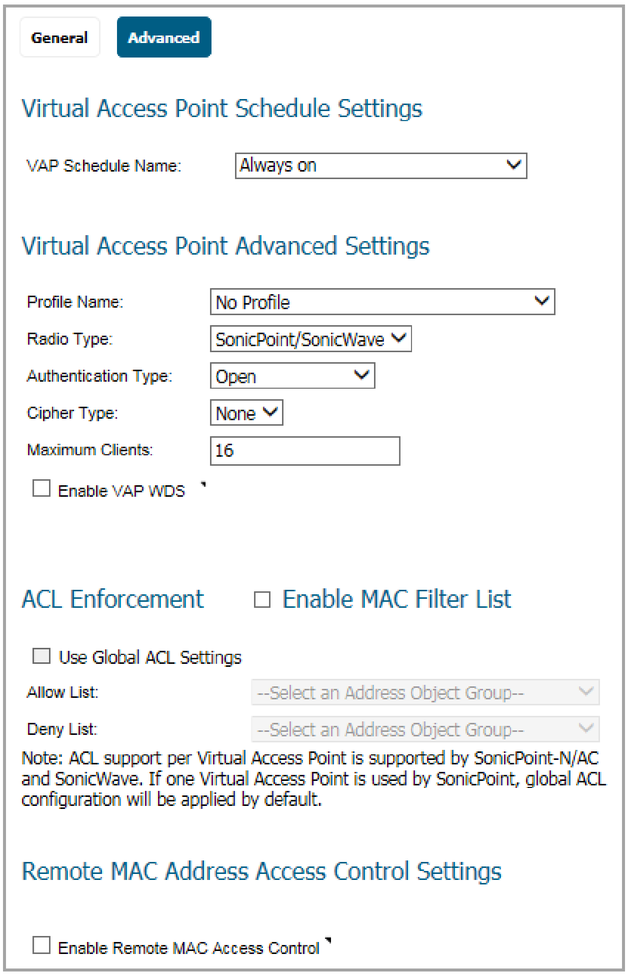
□ Enable Dynamic Vlan ID Assignment

Set the following features on the **General** panel.

Virtual Access Point General Settings

Feature	Description
Name	Create a friendly name for your VAP.
SSID	Enter an SSID name for the access points using this VAP. This name appears in wireless client lists when searching for available access points.
VLAN ID	When using platforms that support VLAN, you can optionally select a VLAN ID to associate this VAP with. Settings for this VAP are inherited from the VLAN you select.
Enable Virtual Access Point	Enables this VAP. This option is selected by default.
Enable SSID Suppress	Suppresses broadcasting of the SSID name and disables responses to probe requests. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients. This option is not selected by default.
Enable Dynamic VLAN ID Assignment	Check to enable. Dynamic VLAN can only be enabled when the authentication type is set to EAP.

Advanced Tab



Virtual Access Point Schedule Settings

VAP Schedule Name: Always on

Virtual Access Point Advanced Settings

Profile Name: No Profile

Radio Type: SonicPoint/SonicWave

Authentication Type: Open

Cipher Type: None

Maximum Clients: 16

□ Enable VAP WDS

ACL Enforcement □ Enable MAC Filter List

□ Use Global ACL Settings

Allow List: --Select an Address Object Group--

Deny List: --Select an Address Object Group--

Note: ACL support per Virtual Access Point is supported by SonicPoint-N/AC and SonicWave. If one Virtual Access Point is used by SonicPoint, global ACL configuration will be applied by default.

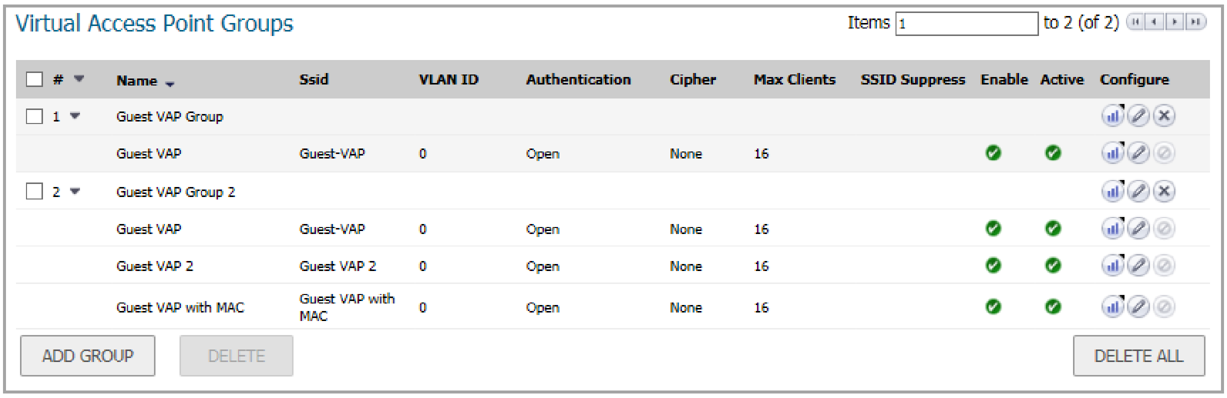
Remote MAC Address Access Control Settings

□ Enable Remote MAC Access Control

Advanced settings allows you to configure authentication and encryption settings for a specific virtual access point. Choose a **Profile Name** to inherit these settings from a user-created profile. As the **Advanced** tab of the **Add/Edit Virtual Access Point** window is the same as **Add/Edit Virtual Access Point Profile** window, see Virtual Access Points Profiles for complete authentication and encryption configuration information.

Virtual Access Point Groups

The Virtual Access Point Groups feature is available on SonicWall NSA appliances. It allows for grouping of multiple VAP objects to be simultaneously applied to your access points. Virtual Access Point Groups are configured from the **Connectivity | Access Points > Virtual Access Point** page.



Virtual Access Point Groups

Items 1 to 2 (of 2)

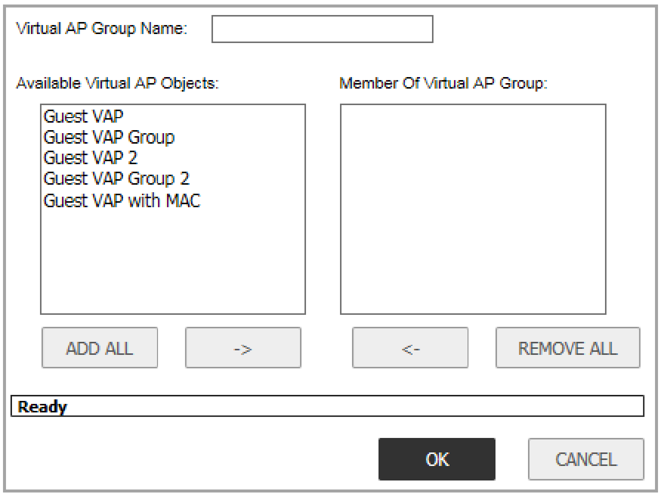
□	#	Name	Ssid	VLAN ID	Authentication	Cipher	Max Clients	SSID Suppress	Enable	Active	Configure
□	1	Guest VAP Group									
		Guest VAP	Guest-VAP	0	Open	None	16		✓	✓	
□	2	Guest VAP Group 2									
		Guest VAP	Guest-VAP	0	Open	None	16		✓	✓	
		Guest VAP 2	Guest VAP 2	0	Open	None	16		✓	✓	
		Guest VAP with MAC	Guest VAP with MAC	0	Open	None	16		✓	✓	

Add a virtual access point group:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Virtual Access Point**.

3 Select **ADD** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.



Virtual AP Group Name:

Available Virtual AP Objects:

Guest VAP
Guest VAP Group
Guest VAP 2
Guest VAP Group 2
Guest VAP with MAC

Member Of Virtual AP Group:

Ready

4 Enter the **Virtual AP Group Name** in the field provided.

5 Select the objects you want to add from the **Available Virtual AP Objects** list and click the **Left Arrow** to move it to the **Member of Virtual AP Group** list.

Or, click **ADD ALL** to add all the objects to the group.

6 Select an object and use the **Right Arrow** or **REMOVE ALL** to remove objects from the group.

7 Click **OK** to save your settings.

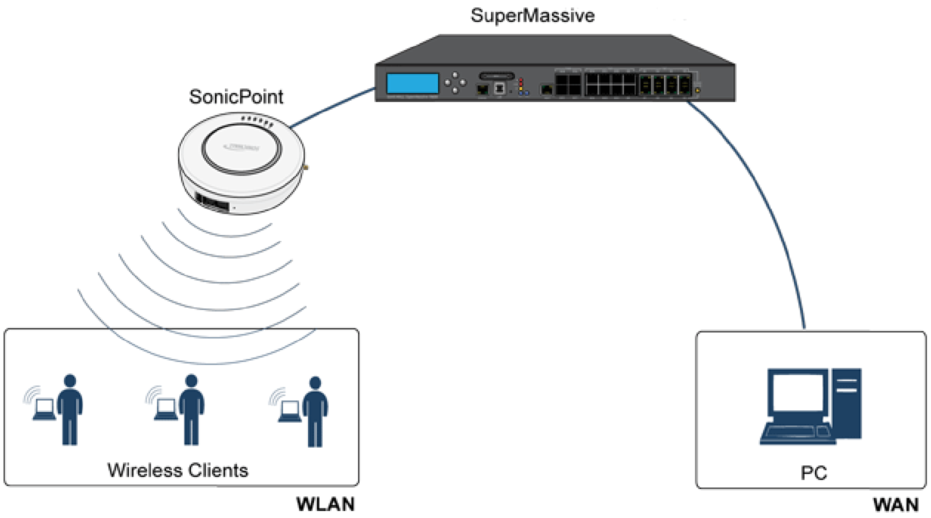
24

Configuring FairNet

The FairNet feature provides an easy-to-use method for network administrators to control the bandwidth of associated wireless clients and make sure it is distributed fairly between them. Administrators can configure the FairNet bandwidth limits for all wireless clients, specific IP address ranges, or individual clients to provide fairness and network efficiency.

This is an example of typical FairNet topology:

Typical FairNet Topology



To deploy the FairNet feature, you must have a laptop or PC with a IEEE802.11b/g/n wireless network interface controller.

Topics:

- Supported Platforms
- FairNet Features
- Management Interface Overview
- Configuring FairNet

Supported Platforms

The FairNet feature is currently supported on the following appliance models:

- SonicWall TZ Series
- SonicWall NSA Series

- SonicWall E-Class NSA Series
- SonicWall SuperMassive Series

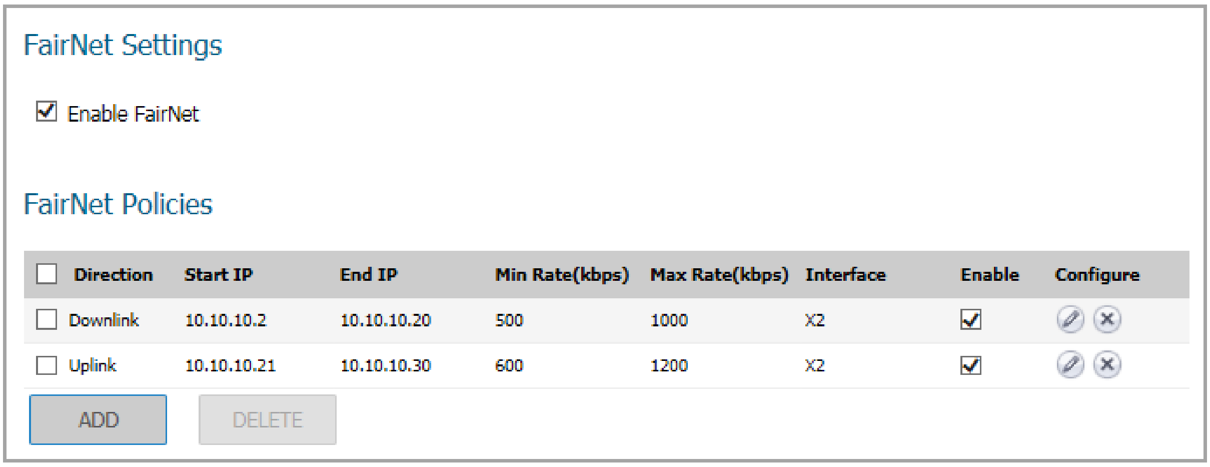
FairNet Features

The Distributed Coordination Function (DCF) provides timing fairness for each client to access a medium with equal opportunity. However, it cannot guarantee the per-station data traffic fairness among all wireless clients. The FairNet feature is implemented on top of the existing 802.11 DCF to guarantee fair bandwidth among wireless clients regardless of the number and direction of flows.

The traffic control feature decides if packets are queued or dropped (for example, if the queue has reached some length limit, or if the traffic exceeds some rate limit). It can also decide in which order packets are sent (for example, to give priority to certain ones), and it can delay the sending of packets (for example, to limit the rate of outbound traffic). After traffic control has released a packet for sending, the device driver picks it up and emits it on the network.

Management Interface Overview

The components of the FairNet display are described in the following table.



FairNet Settings

☑ Enable FairNet

FairNet Policies

□ Direction	Start IP	End IP	Min Rate(kbps)	Max Rate(kbps)	Interface	Enable	Configure
□ Downlink	10.10.10.2	10.10.10.20	500	1000	X2	☑	
□ Uplink	10.10.10.21	10.10.10.30	600	1200	X2	☑	

FairNet Interface Components

Name	Description
Buttons and Checkboxes	
ADD	Adds a FairNet policy for an IP address or range of addresses. Displays the **Add Fairnet Policy** dialog.
DELETE	Deletes the selected FairNet policies.
Accept	Applies the latest configuration settings.
Cancel	Cancels any changed configuration settings.
Checkboxes	
Enable FairNet	Enables the FairNet feature.
FairNet Policies	In the **FairNet Policies** table header: Selects or deselects all the policies in the **FairNet Polices** table. Individual policies can also be selected from the policies list.

FairNet Interface Components (Continued)

Name	Description
Fairnet Policies Table Columns	
Direction	Displays the direction for each policy. The directions include: • Uplink • Downlink • Both
Start IP	Displays the start point for the IP address range.
End IP	Displays the end point for the IP address range.
Min Rate (kbps)	The minimum bandwidth that clients are guaranteed. Minimum rate is 1 Kbps.
Max Rate (kbps)	The maximum bandwidth that clients are guaranteed. Maximum rate is 54000 Kbps.
Interface	Displays the interface to which the FairNet policy applies. This is the interface on the managing firewall that the access point is connected to.
Enable	Enables the selected FairNet policy when the box is checked.
Configure	Edits existing FairNet policies when the **Edit** icon is clicked. Deletes the specific FairNet policy when the **Delete** icon is clicked.

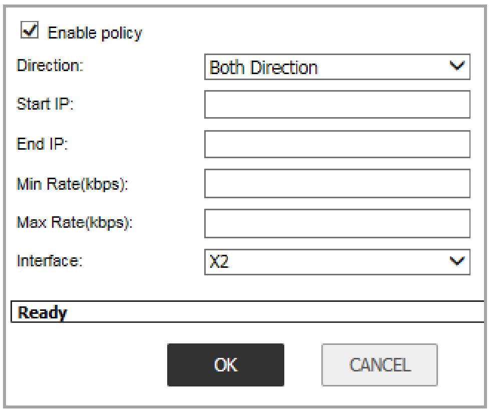
Configuring FairNet

This section contains an example FairNet configuration.

To configure FairNet to provide more bandwidth in both directions:

1 Navigate to the **Connectivity | Access Points > FairNet** page.

2 Click **ADD**.



☑ Enable policy

Direction: Both Direction

Start IP:

End IP:

Min Rate(kbps):

Max Rate(kbps):

Interface: X2

Ready

3 Check **Enable Policy**. This is checked by default.

4 From the **Direction** drop-down menu, select **Both Directions**. This applies the policy to clients uploading content and downloading content. This is the default.

5 In the **Start IP** field, enter the starting IP address (for example, `172.16.29.100`) for the FairNet policy.

6 In the **End IP** field, enter the ending IP address (for example, `172.16.29.110`) for the FairNet policy.

> **TIP:** The IP address range must be on a subnet that is configured for a WLAN interface.

7 In the **Min Rate (kbps)** field, enter the minimum bandwidth for the FairNet policy. The minimum and default is 100Kbps, and the maximum is 300Mbps (300,000Kbps).

8 In the **Max Rate (kbps)** field, enter the maximum bandwidth for the FairNet policy. The minimum and default is 100Kbps, and the maximum is 300Mbps (300,000Kbps), although a typical setting is 20Mbps.

9 From the **Interface** drop-down menu, select the interface (for example, X2) that the access point is connected to.

10 Click **OK** and the FairNet Policy is added to the **FairNet Policies** table.

11 Click **Enable**.

12 Click **Accept**.

Your SonicWall FairNet policy is now configured.

25

Configuring Wi-Fi Multimedia

SonicOS access points support Wi-Fi Multimedia (WMM) to provide a better Quality of Service (QoS) experience on bandwidth-intensive applications such as VoIP, VoIP on Wi-Fi phones, and multimedia traffic on wireless IEEE 802.11 networks.

WMM is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard that prioritizes traffic according to four Access Categories:

- **Voice**—highest priority
- **Video**—second priority
- **Best effort**—third priority (intended for applications like email and Internet surfing)
- **Background**—fourth priority (intended for applications that are not latency sensitive, such as printing)

> ⓘ **NOTE:** WMM does not provide guaranteed throughput.

SonicWall Wireless Cloud Management Support is also available for SonicWave access points. You no longer need to connect a SonicWave to your central firewall to manage it. You can deploy it standalone by connecting it to your network. The appliance provides wireless services that you can manage through the cloud on our new mobile application.

Topics:

WMM Access Categories

Each Access Category has its own transmit queue. Traffic is assigned to the appropriate Access Category based on type of service (ToS) information that is provided by either the application or the firewall. SonicWall security appliances assign ToS either through access rules or VLAN tagging.

The following table shows how the WMM Access Categories map to 802.1D user priorities.

Wi-Fi Multimedia Access Categories

Priority	User Priority (Same as 802.1D user priority)	802.1D designation	WMM Access Category (AC)	WMM AC Designation (informative)
Lowest	1	BK	AC_BK	Background
	2	—	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
Highest	7	NC	AC_VO	Voice

WMM prioritizes traffic through a process known as Enhanced distributed channel access (EDCA). It prioritizes traffic by defining a different range of “backoff” periods for each Access Category. The WMM backoff periods are defined by two parameters:

- **Arbitration Inter-Frame Space (AIFS)** – The time interval between the wireless channel becomes idle and when the AC can begin negotiating access to the channel.
- **Contention Window (CW)** – The range of possible values for the random backoff periods. A range of time that specifies the random backoff period. The CW is defined by a minimum and maximum value:
  - **Minimum contention window size (CWMin)** – The initial upper limit of the length of the CW. The AC waits for a random time between 0 and CWMin before attempting to transmit. Higher priority AC with higher priority is assigned a shorter CWMin.
  - **Maximum contention window size (CWMax)** – The upper limit of the CW. If a collision occurs, the AC doubles the size of the CW, up to the CWMax, and attempts to transmit again. The CWMax must be larger than the CWMin.

Higher priority ACs are generally given lower values for AIFS, CWMin, CWMax.

NOTE: The unit of measure for AIFS, CWMin, and CWMax is multiples of the slot time for the 802.11 standard that is being used. For 802.11b, one slot is 20 microseconds. For 802.11a and 802.11g, one slot is 9 microseconds.

Separate WMM parameters are configured for the access points and for the station (the SonicWall security appliance). The following tables show the default WMM parameters for the access points and SonicWall security appliances.

Default WMM Parameters for Access Points

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
AC_BE(0)	Best Effort	4	6	3
AC_BK(1)	Background	4	10	7
AC_VI(2)	Video	3	4	1
AC_VO(3)	Voice	2	3	1

Default WMM Parameters for SonicWall Security Appliances

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
AC_BE(0)	Best Effort	4	10	3
AC_BK(1)	Background	4	10	7
AC_VI(2)	Video	3	4	2
AC_VO(3)	Voice	2	3	2

Assigning Traffic to Access Categories

WMM requires the access points to implement multiple queues for multiple priority access categories. To differentiate traffic types, the access point relies on either the application or the firewall to provide type of service (TOS) information in the IP data. SonicWall security appliances assign traffic to WMM Access Categories through two methods:

- Specifying Firewall Services and Access Rules
- VLAN Tagging

Specifying Firewall Services and Access Rules

Services using a certain port can be prioritized and put into a proper transmit queue. For example, UDP traffic sending to port 2427 can be regarded as a video stream. Add a custom service on the **Policies | Objects > Service Objects** page. Refer to *SonicOS 6.5 Policies* for more information.

At least one access rule should be added on the **Policies | Rules > Access Rules** page for the new service. For example, when such a service happens from a station on the LAN zone to a wireless client on the LAN zone to a wireless client on the WLAN zone, an access rule can be configured in the **General** tab of the **Add Rule** window. In the **QoS** tab of the **Add Rule** window, an explicit DSCP value is defined.

Later, when packets are sent to the access point through the firewall using UDP protocol with destination port 2427, their TOS fields are set according to the QoS setting in the access rule.

VLAN Tagging

Prioritization is possible in VLAN over virtual access point because the SonicWave, SonicPoint N and ACs allow a virtual access point to be configured to connect with a VLAN by using same VLAN ID. You can set priority for VLAN traffic through a firewall access rule.

The firewall access rule is similar to setting priority for a UDP service destined to a port such as 2427, but is configured with a VLAN (VLAN over VAP) interface, such as WLAN Subnets, as the **Source** and **Destination** is a WLAN-to-WLAN rule. Refer to Policies | Rules > Access Rules in *SonicOS 6.5 Policies* for more information.

Configuring Wi-Fi Multimedia Parameters

By default, a single WMM profile is configured on the SonicWall security appliance with the parameters set to the values on the 802.11e standard.

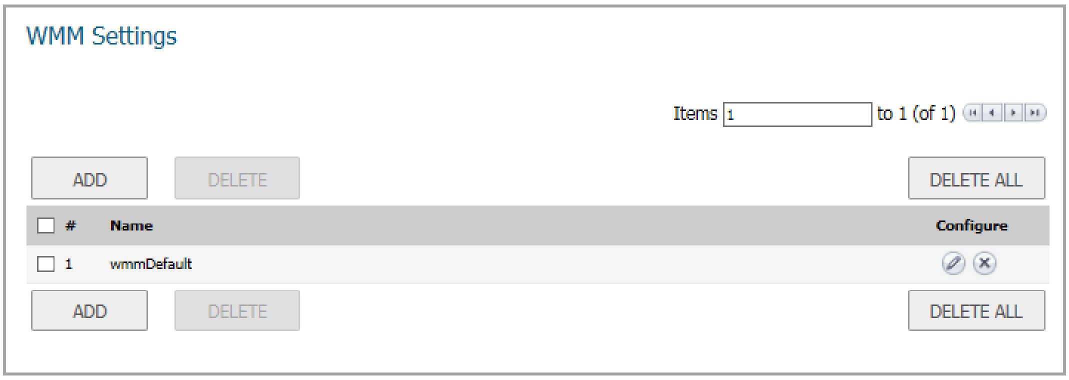
Topics:

- Configuring WMM
- Creating a WMM Profile for an Access Point
- Deleting WMM Profiles

Configuring WMM

To customize the WMM configuration:

1 Navigate to the **Connectivity | Access Points > Wi-Fi Multimedia** page.

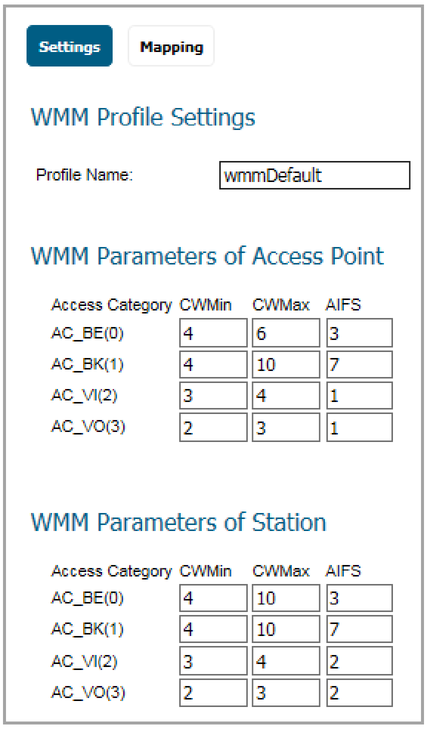


WMM Settings

Items 1 to 1 (of 1)

□	#	Name	Configure
□	1	wmmDefault	

2 To modify the a WMM profile, click the **Edit** icon for that profile. Or, to create a new WMM profile, click **ADD**.



WMM Profile Settings

Profile Name: wmmDefault

WMM Parameters of Access Point

Access Category	CWMin	CWMax	AIFS
AC_BE(0)	4	6	3
AC_BK(1)	4	10	7
AC_VI(2)	3	4	1
AC_VO(3)	2	3	1

WMM Parameters of Station

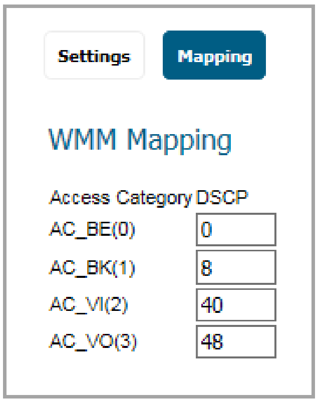
Access Category	CWMin	CWMax	AIFS
AC_BE(0)	4	10	3
AC_BK(1)	4	10	7
AC_VI(2)	3	4	2
AC_VO(3)	2	3	2

3 For a new WMM profile, enter a **Profile Name**. The default name is **wmmDefault**.

4 Modify the parameters to customize the WMM profile; the default WMM parameter values are auto-populated in the window. For information about these categories, see the Wi-Fi Multimedia Access Categories table.

> **NOTE:** When configuring the WMM profile, you can configure the size of the contention window (CWMin/CWMax) and the arbitration interframe space (AIFS) number when creating a WMM profile. These values can be configured individually for each priority, AC_BK, AC_BE, AC_VI, and AC_VO on the access point (SonicPointN) and for the station (firewall).

5 Click the **Mapping** tab to customize how the Access Categories are mapped to DSCP values.



WMM Mapping

Access Category	DSCP
AC_BE(0)	0
AC_BK(1)	8
AC_VI(2)	40
AC_VO(3)	48

6 Map priority levels to DSCP values. The default DSCP values are as same as the ones in **Policies | Rules > Access Rules, QoS** mapping.

7 Click **OK**.

Creating a WMM Profile for an Access Point

The **Connectivity | Access Points > Wi-Fi Multimedia** page on the **MANAGE** view provides a way to configure WMM profiles, including parameters and priority mappings.

You can also create a WMM profile or select an existing WMM profile when configuring a SonicWave, SonicPoint N or a SonicPoint AC Profile from the **Access Points > Base Settings** page. The **Configuration** window provides a **WMM (Wi-Fi Multimedia)** drop-down menu on the **Advanced/Radio 0/1 Advanced** tabs.

Selecting **Create New WMM Profile…** from the **WMM (Wi-Fi Multimedia)** drop-down menu displays the **Add Wlan WMM Profile** Window.

Deleting WMM Profiles

To delete a single WMM Profile, click the **Delete** icon in the profile's **Configure** column.

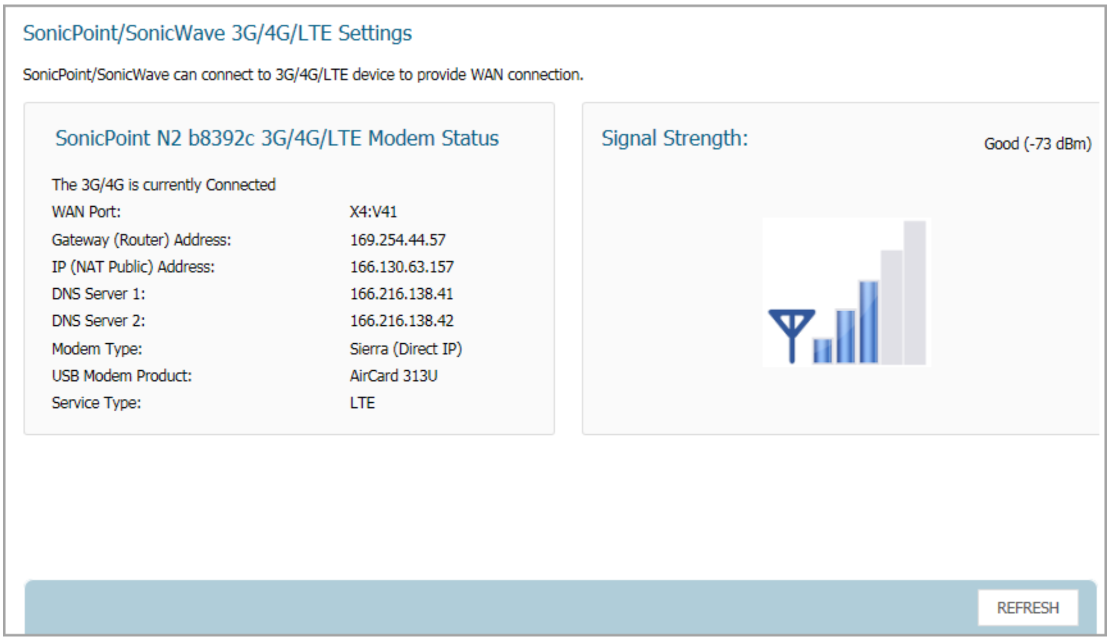
To delete multiple WMM Profiles, check the boxes next to the profiles to delete, and then click **DELETE**.

To delete all WMM Profiles, click **DELETE ALL**. A pop-up message appears to confirm that all profiles are to be deleted.

26

Access Point 3G/4G/LTE WWAN

If you have a 3G/4G/LTE device connected to one of your access points, the **Connectivity | Access Points > 3G/4G/LTE WWAN** page offers monitoring information on that device.



SonicPoint/SonicWave 3G/4G/LTE Settings

SonicPoint/SonicWave can connect to 3G/4G/LTE device to provide WAN connection.

SonicPoint N2 b8392c 3G/4G/LTE Modem Status

The 3G/4G is currently Connected

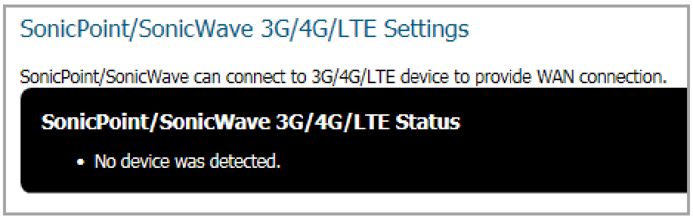
WAN Port:	X4:V41
Gateway (Router) Address:	169.254.44.57
IP (NAT Public) Address:	166.130.63.157
DNS Server 1:	166.216.138.41
DNS Server 2:	166.216.138.42
Modem Type:	Sierra (Direct IP)
USB Modem Product:	AirCard 313U
Service Type:	LTE

Signal Strength: Good (-73 dBm)

The first panel provides connectivity data and modem status, and the second panel shows a graphical representation of the device's signal strength.

Click **REFRESH** to refresh the data in panels.

If no 3G/4G/LTE device is detected on one of your access points, you get the following message on the **Connectivity | Access Points > 3G/4G/LTE WWAN** page:



SonicPoint/SonicWave 3G/4G/LTE Settings

SonicPoint/SonicWave can connect to 3G/4G/LTE device to provide WAN connection.

SonicPoint/SonicWave 3G/4G/LTE Status

- No device was detected.

27

Viewing Bluetooth LE Devices

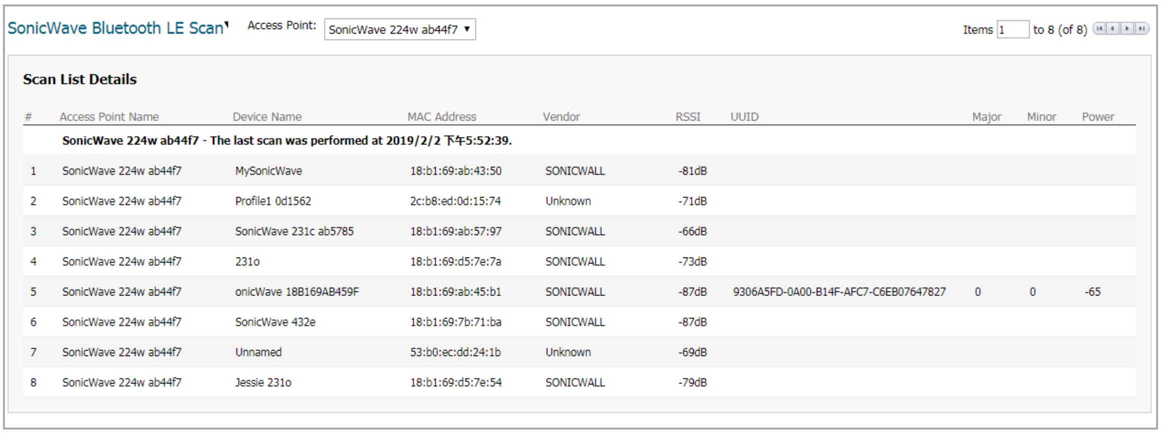
SonicWave 432 and 200 series appliances now support Bluetooth Low Energy (BLE), a wireless personal area network technology that provides considerably reduced power consumption and cost while maintaining a similar communication range to standard Bluetooth appliances. Bluetooth Low Energy (BLE) is a subset of classic Bluetooth that enables smart phones, tablets, SonicWall mobile applications, and other devices, such as other SonicWaves, to easily connect to the SonicWave access point, especially when in close proximity to an iBeacon appliance. BLE also provides location estimation and an easier SonicWave configuration.

> **NOTE:** IBeacon is a protocol developed by Apple. Various vendors make iBeacon-compatible BLE devices that broadcast their identifier to nearby portable electronic devices. The technology enables smart phones, tablets, and other devices to perform actions when in close proximity to an iBeacon.

Viewing BLE Scanned Data

The **MANAGE | Connectivity > Access Points > Bluetooth LE** page displays information about nearby Bluetooth Low Energy (BLE) devices. You can control the display by selecting a single SonicWave or **All Access Points** from the **Access Point** drop-down menu at the top of the page.

See Bluetooth LE Settings for Provisioning Profiles on page 202 for information about enabling iBeacon on your SonicWave.


SonicWave Bluetooth LE Scan
Access Point: SonicWave 224w ab44f7
Items 1 to 8 (of 8)

Scan List Details

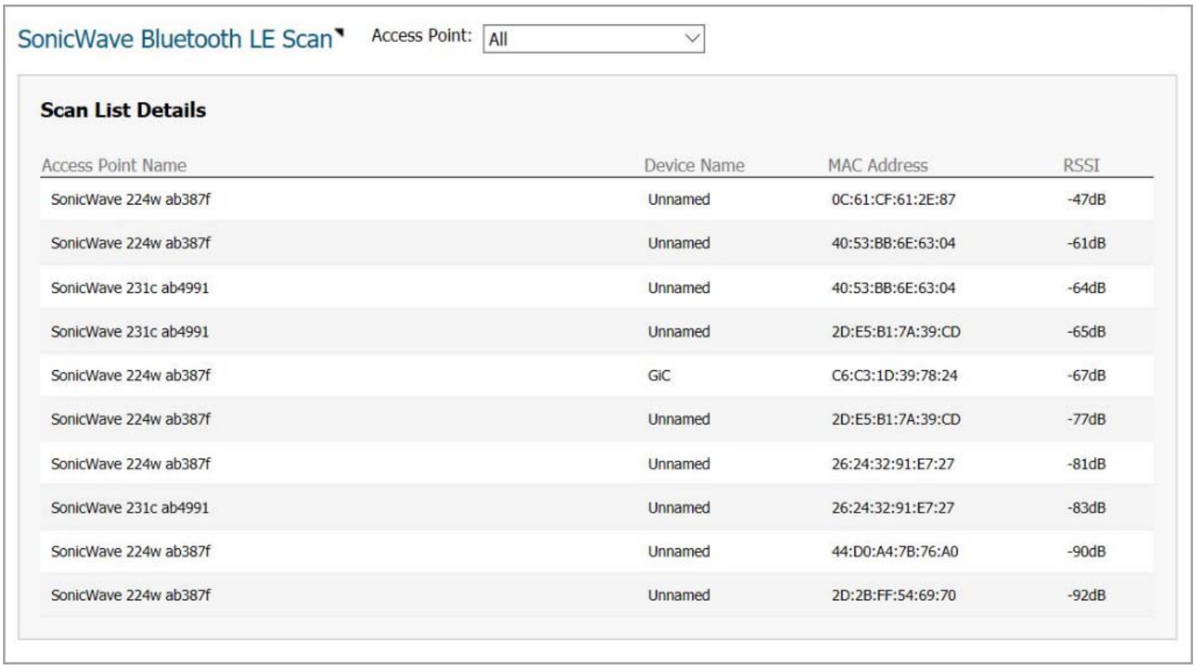
#	Access Point Name	Device Name	MAC Address	Vendor	RSSI	UUID	Major	Minor	Power
	SonicWave 224w ab44f7 - The last scan was performed at 2019/2/2 下午5:52:39.								
1	SonicWave 224w ab44f7	MySonicWave	18:b1:69:ab:43:50	SONICWALL	-81dB				
2	SonicWave 224w ab44f7	Profile1 0d1562	2c:b8:ed:0d:15:74	Unknown	-71dB				
3	SonicWave 224w ab44f7	SonicWave 231c ab5785	18:b1:69:ab:57:97	SONICWALL	-66dB				
4	SonicWave 224w ab44f7	231o	18:b1:69:d5:7e:7a	SONICWALL	-73dB				
5	SonicWave 224w ab44f7	onicWave 18B169AB459F	18:b1:69:ab:45:b1	SONICWALL	-87dB	9306A5FD-0A00-B14F-AFC7-C6EB07647827	0	0	-65
6	SonicWave 224w ab44f7	SonicWave 432e	18:b1:69:7b:71:ba	SONICWALL	-87dB				
7	SonicWave 224w ab44f7	Unnamed	53:b0:ec:dd:24:1b	Unknown	-69dB				
8	SonicWave 224w ab44f7	Jessie 231o	18:b1:69:d5:7e:54	SONICWALL	-79dB				

The **Scan List Details** table displays information scanned from nearby BLE devices. The columns provide the following information, if available:

Column	Description
#	Reference number for the table row.
Access Point Name	Name of the access point (the SonicWave) scanning the BLE device.
Device Name	Name of the BLE device.
MAC Address	Unique hardware address of the device.
Vendor	Device manufacturer.

Column	Description
RSSI	Received signal strength indicator for the BLE device, expressed as a negative number (dB). Higher numbers (closer to zero) indicate stronger signals.
UUID	Proximity UUID, unique identifier of the BLE device. Exactly 36 hex characters and hyphens. Must not be set to all zeros.
Major	The significant identity within the group of BLE devices. Valid values are 0 - 65535. 0x0000 = unset.
Minor	The secondary identity within the group of BLE devices. Valid values are 0 - 65535. 0x0000 = unset.
Power	Power level of the BLE device in dBm. This is the ***measured power*** of the scanned devices, which is calculated by averaging multiple RSSI samples in a process corresponding to that defined by Apple.

The following image displays some of this data:



Scan List Details

Access Point Name	Device Name	MAC Address	RSSI
SonicWave 224w ab387f	Unnamed	0C:61:CF:61:2E:87	-47dB
SonicWave 224w ab387f	Unnamed	40:53:BB:6E:63:04	-61dB
SonicWave 231c ab4991	Unnamed	40:53:BB:6E:63:04	-64dB
SonicWave 231c ab4991	Unnamed	2D:E5:B1:7A:39:CD	-65dB
SonicWave 224w ab387f	GiC	C6:C3:1D:39:78:24	-67dB
SonicWave 224w ab387f	Unnamed	2D:E5:B1:7A:39:CD	-77dB
SonicWave 224w ab387f	Unnamed	26:24:32:91:E7:27	-81dB
SonicWave 231c ab4991	Unnamed	26:24:32:91:E7:27	-83dB
SonicWave 224w ab387f	Unnamed	44:D0:A4:7B:76:A0	-90dB
SonicWave 224w ab387f	Unnamed	2D:2B:FF:54:69:70	-92dB

28

Radio Resource Management

This section describes the settings available for Radio Resource Management and Dynamic Channel Selection in SonicOS.

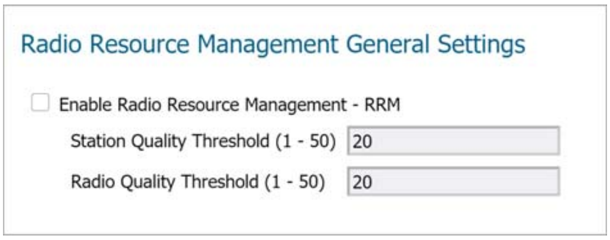
> **NOTE:** Radio Resource Management is supported on SonicWall access points that have a dedicated scan radio, including SonicWave 231c, 231o, 432e, 432i, and 432o. The RRM feature is not supported on SonicWave 224w or on SonicPoints.

Topics:

- Configuring Radio Resource Management
- Configuring Dynamic Channel Selection

Configuring Radio Resource Management

Radio Resource Management settings are available on the **MANAGE | Connectivity > Access Points > Radio Resource Management** page.



Radio Resource Management General Settings

□ Enable Radio Resource Management - RRM

Station Quality Threshold (1 - 50) 20

Radio Quality Threshold (1 - 50) 20

Radio Resource Management General Settings

Option Name	Description
Enable Radio Resource Management - RRM	Enable this option to activate the settings for **Station Quality Threshold** and **Radio Quality Threshold**. This option is disabled by default.

Radio Resource Management General Settings

Option Name	Description
Station Quality Threshold (1-50)	Health index to track and assess the status of wireless client connections, from 1 to 50. A higher index value means the wireless station is connected with higher data rate and less packet drop. Wireless clients will be disconnected if station quality drops below the configured threshold. • Minimum value = 1 • Maximum value = 50 • Default value = 20
Radio Quality Threshold (1-50)	Health index to track and assess the status of radio band utilization, which varies between 1 and 50. A higher index value means radio band utilization is lower with less packet drop. The radio transmit power will be lowered if the radio quality drops below the configured threshold. • Minimum value = 1 • Maximum value = 50 • Default value = 20

To configure Radio Resource Management settings:

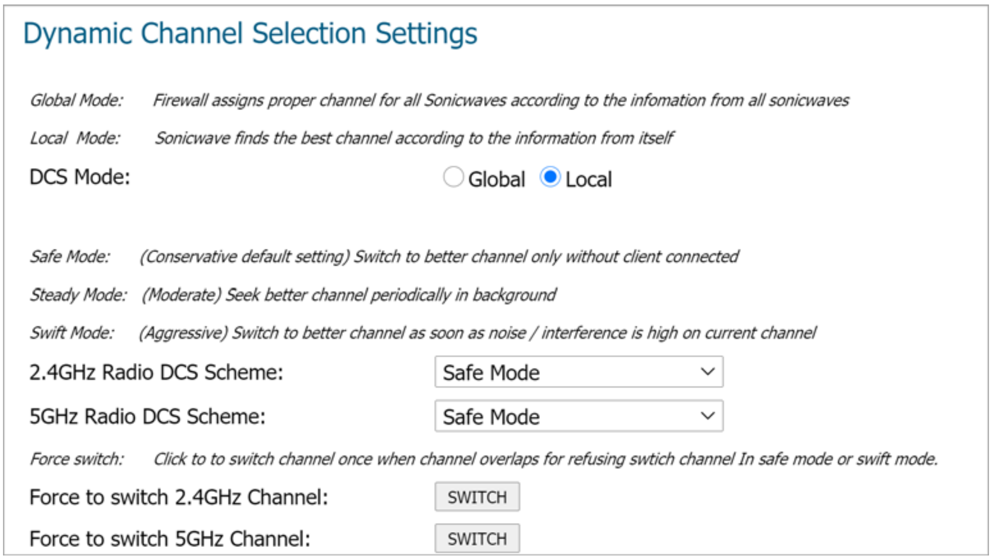
1. Navigate to the **MANAGE | Connectivity > Access Points > Radio Resource Management** page.
2. Select the **Enable Radio Resource Management - RRM** checkbox to enable this feature.
3. For **Station Quality Threshold (1-50)**, enter a value between 1 and 50 or accept the default setting of 20.

   A higher index value means the wireless station is connected with higher data rate and less packet drop. Wireless clients will be disconnected if station quality drops below the configured threshold.
4. For **Radio Quality Threshold (1-50)**, enter a value between 1 and 50 or accept the default setting of 20.

   A higher index value means radio band utilization is lower with less packet drop. The radio transmit power will be lowered if the radio quality drops below the configured threshold.
5. Click **Accept**.

Configuring Dynamic Channel Selection

Dynamic Channel Selection settings are available on the **MANAGE | Connectivity > Access Points > Radio Resource Management** page.



Dynamic Channel Selection Settings

Global Mode: *Firewall assigns proper channel for all Sonicwaves according to the infomation from all sonicwaves*

Local Mode: *Sonicwave finds the best channel according to the information from itself*

DCS Mode: ○ Global ● Local

Safe Mode: *(Conservative default setting) Switch to better channel only without client connected*

Steady Mode: *(Moderate) Seek better channel periodically in background*

Swift Mode: *(Aggressive) Switch to better channel as soon as noise / interference is high on current channel*

2.4GHz Radio DCS Scheme: Safe Mode

5GHz Radio DCS Scheme: Safe Mode

Force switch: *Click to to switch channel once when channel overlaps for refusing swtich channel In safe mode or swift mode.*

Force to switch 2.4GHz Channel: SWITCH

Force to switch 5GHz Channel: SWITCH

Dynamic Channel Selection Settings

Option Name	Description
Dynamic Channel Selection Mode **DCS Mode**: **Global / Local**	**DCS Mode** supports two settings for automatic channel selection: • **Global Mode** – Firewall assigns proper channel for all SonicWaves according to information received from all SonicWaves. • **Local Mode** – SonicWave finds the best channel according to the information from itself.
Auto Channel Enable: **2.4GHz Radio DCS Scheme** **5GHz Radio DCS Scheme**	**2.4GHz** or **5GHz Radio DCS Scheme** options are: • **Safe Mode** SonicWaves switch to a better channel only without clients connected. This is conservative mode. • **Steady Mode** SonicWaves seek a better channel periodically in the background. This is moderate mode. • **Swift Mode** SonicWaves switch to a better channel as soon as noise/interference becomes high on the current channel. This is aggressive mode. **Safe Mode** is the default.

To configure Dynamic Channel Selection settings:

1. Navigate to the **MANAGE | Connectivity > Access Points > Radio Resource Management** page.
2. For **DCS Mode**, select either **Global** or **Local**.

   If **Global** is selected, the firewall assigns the proper channel for all SonicWaves according to information received from all SonicWaves. If **Local** is selected, each SonicWave finds the best channel according to the information from itself.
3. For **2.4GHz Radio DCS Scheme**, select one of the following:
   - **Safe Mode**

     SonicWaves switch to a better channel only without clients connected. This is conservative mode.

- **Steady Mode**

  SonicWaves seek a better channel periodically in the background. This is moderate mode.
- **Swift Mode**

  SonicWaves switch to a better channel as soon as noise/interference becomes high on the current channel. This is aggressive mode.

4 For **5GHz Radio DCS Scheme**, select one of the following:

- **Safe Mode**

  SonicWaves switch to a better channel only without clients connected. This is conservative mode.
- **Steady Mode**

  SonicWaves seek a better channel periodically in the background. This is moderate mode.
- **Swift Mode**

  SonicWaves switch to a better channel as soon as noise/interference becomes high on the current channel. This is aggressive mode.

5 Click **ACCEPT**.

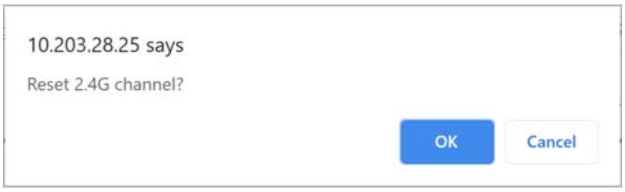
Forcing SonicWaves to Switch Channels

If the SonicWave does not switch to a better channel when needed and according to the configured DCS Scheme, you can force it to seek a better channel and switch to it.

To force the SonicWave to switch to a new channel

1 To force the SonicWave to switch to a new 2.4GHz channel, click the **SWITCH** button for **Force to switch 2.4GHz Channel**.

2 Click **OK** in the confirmation dialog box.



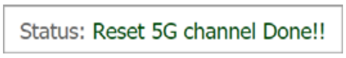
10.203.28.25 says

Reset 2.4G channel?

3 To force the SonicWave to switch to a new 5GHz channel, click the **SWITCH** button for **Force to switch 5GHz Channel**.

4 Click **OK** in the confirmation dialog box.

The status bar at the bottom of the window displays a success message when the 2.4GHz or 5GHz channel is switched.



Status: Reset 5G channel Done!!

Part 4

Connectivity | Wireless

29

Wireless Overview

Only SonicWall Wireless security appliances provide the pages under **MANAGE | Connectivity | Wireless** for configuring wireless settings on the appliance.

ⓘ **NOTE:** In SonicOS 6.5.3 and higher, the **Wireless** pages are displayed when **Wireless Controller Mode** on the **MANAGE | System Setup | Appliance > Base Settings** page is set to either **Full-Feature-Gateway** or **Wireless-Controller-Only**. If **Non-Wireless** is enabled for **Wireless Controller Mode**, the **Wireless** menu heading and the pages under it are ***not*** displayed. See the *SonicOS 6.5 System Setup* administration documentation for more information.

The SonicWall Wireless security appliances support wireless protocols IEEE 802.11a, 802.11ac, 802.11b, 802.11g, and 802.11n and send data through radio transmissions. These transmissions are commonly known as Wi-Fi or wireless. The SonicWall wireless security appliance combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination as well as initiation capabilities. With this combination, the wireless security appliance offers the flexibility of wireless without compromising network security.

Typically, the wireless security appliance is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Because the wireless security appliance also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a DSL or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks which means you should establish a wireless security policy for your wireless LAN. On the wireless security appliance, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated through User Level Authentication. Wireless access to Guest Services and MAC Filter Lists are managed by the wireless security appliance. If all of the security criteria are met, then wireless network traffic can then pass through one of the following distribution systems:

- LAN
- WAN
- Wireless Client on the WLAN
- DMZ or other zone on Opt port
- VPN tunnel

Topics:

Device Support

The wireless devices supported by SonicOS include:

- TZ500W
- TZ400W
- TZ350/350W
- TZ300W
- SOHO W
- SOHO 250/250W
- SonicWave 231c
- SonicWave 231o
- SonicWave2 AC 2x2c

Compliance

The wireless devices are required to comply with various requirements for sale and use of these devices in specific areas. For the latest information about regulatory approvals and restrictions for SonicWall wireless devices, see the Product Documentation pages for your product at https://www.sonicwall.com/support. Each device has a unique regulatory document or *Getting Started Guide* that provides the relevant information.

FCC U-NII New Rule Compliance

Beginning in SonicOS 6.2.5.1, FCC U-NII (Unlicensed –National Information Infrastructure) New Rule (Report and Order ET Docket No. 13-49) is supported on TZ series and SOHO wireless appliances. To comply with FCC New Rules for Dynamic Frequency Selection (DFS), a TZ series or SOHO wireless appliance detects and avoids interfering with radar signals in DFS bands.

ⓘ **NOTE:** TZ series and SOHO wireless appliances manufactured with FCC New Rule-compliant firmware are only supported with SonicOS 6.2.5.1 and higher.

RED Compliance

Beginning with SonicOS 6.5, the Radio Compliance Directive (RED) is supported on the TZ series and SOHO wireless appliances. RED (2014/53/EU) sets essential requirements for safety and health, electromagnetic compatibility and the efficient use of the radio spectrum.

Considerations for Using Wireless Connections

When evaluating wireless versus wired connections, consider the advantages and disadvantages give your infrastructure and environment:

Mobility	Are the majority of your network is laptop computers? Wireless is more portable than wired connections.
Convenience	Wireless networks do not require cabling to individual computers or opening computer cases to install network cards.
Speed	If network speed is important to you, you might want to consider using Ethernet connections rather than wireless connections.
Range and Coverage	If your network environment contains numerous physical barriers or interference factors, wireless networking might not be suitable for your network.
Security	Wireless networks have inherent security issues because of the unrestricted nature of the wireless transmissions. However, the wireless security appliance is a firewall and has NAT capabilities which provides security, and you can use WPA or WPA2 to secure data transmissions.

Recommendations for Optimal Wireless Performance

SonicWall recommends the following for optimal wireless performance:

- Place the wireless security appliance near the center of your intended network. This reduces the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the wireless security appliance and the receiving points such as PCs or laptops.
- Try to place the wireless security appliance in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.
- Building construction can affect wireless performance.
  - Avoid placing the wireless security appliance near walls, fireplaces, or other large solid objects.
  - Placing the wireless security appliance near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
  - Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the wireless security appliance is installed near these types of materials.
- Installing the wireless security appliance in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the wireless security appliance.
- Devices such as cordless phones, radios, microwave ovens, and televisions might cause interference on the wireless security appliance.

Adjusting the Antennas

The antennas on the wireless security appliance can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the wireless security appliance, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

Wireless Node Count Enforcement

Users connecting to the WLAN or connecting through the SonicWall GroupVPN are not counted toward the node enforcement on the SonicWall wireless network appliance. Only users on the LAN and non-Wireless zones on the Opt port are counted toward the node limit.

The Station Status table lists all the wireless nodes connected.

MAC Filter List

The SonicWall wireless security appliance networking protocol provides native MAC address filtering capabilities. When MAC address filtering is enabled, filtering occurs at the 802.11 layer, wireless clients are prevented from authenticating and associating with the wireless access point. Because data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

30

Configuring Wireless Settings

You can set up your wireless appliance as an access point, a wireless client bridge, or as an access point and a station.

To configure settings for the 802.11 wireless antenna:

1. Navigate to the **MANAGE** view and select **Connectivity | Wireless > Base Settings**.
2. Choose the **Radio Role** you want your wireless appliance to perform.

   ⓘ | **IMPORTANT:** Changing from one mode to the other drops clients and requires a reboot.

   ⓘ | **NOTE:** The options on the page change depending on which **Radio Role** you chose.

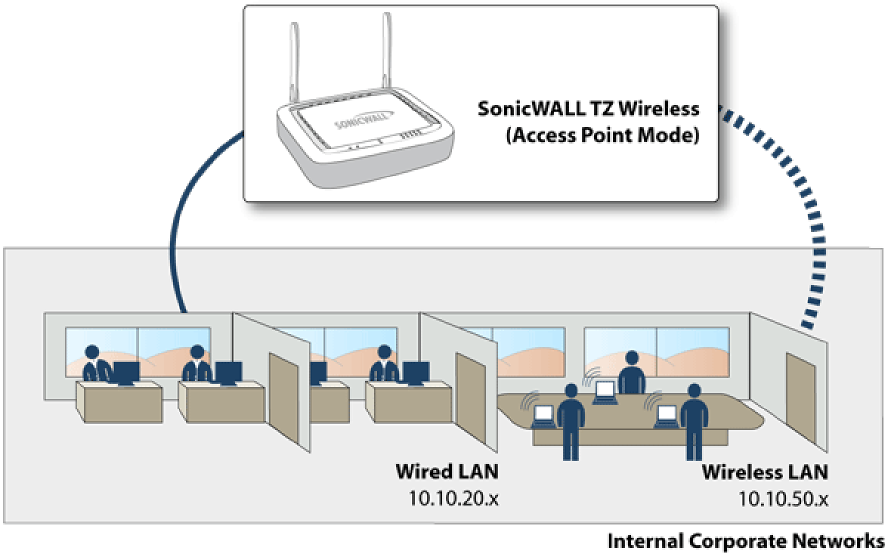
The following sections describe how to configure your device for each **Radio Role** option:

- Access Point
- Wireless Client Bridge
- Access Point and Station

Access Point

Selecting **Access Point** for the **Radio Role** configures the SonicWall as an Internet/network gateway for wireless clients as shown in the following figure:

Wireless Radio Mode: Access Point



Topics:

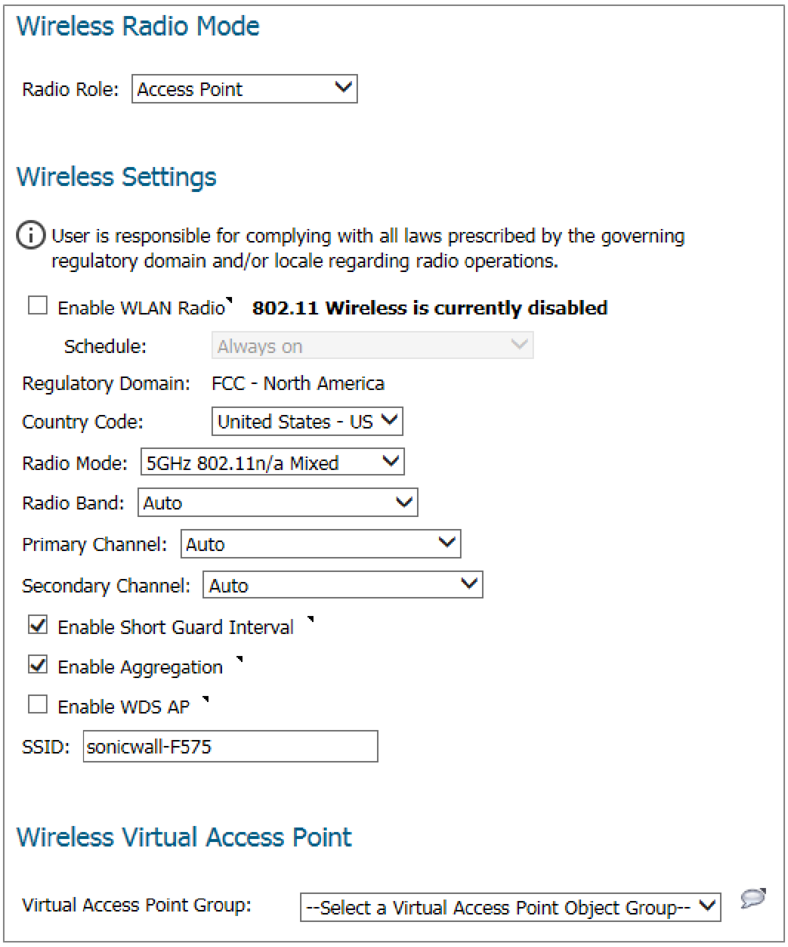
- Access Point Wireless Settings
- Access Point Wireless Virtual Access Point

Access Point Wireless Settings

IMPORTANT: When setting up the wireless appliance as an access point, you are responsible for complying with all laws prescribed by he governing regulatory domain and/or locale regarding radio operations.

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Base Settings**.



Wireless Radio Mode

Radio Role: Access Point

Wireless Settings

User is responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

□ Enable WLAN Radio **802.11 Wireless is currently disabled**

Schedule: Always on

Regulatory Domain: FCC - North America

Country Code: United States - US

Radio Mode: 5GHz 802.11n/a Mixed

Radio Band: Auto

Primary Channel: Auto

Secondary Channel: Auto

☑ Enable Short Guard Interval

☑ Enable Aggregation

□ Enable WDS AP

SSID: sonicwall-F575

Wireless Virtual Access Point

Virtual Access Point Group: --Select a Virtual Access Point Object Group--

3 In the **Radio Role** field, chose **Access Point** from the drop-down menu.

4 Check the box to **Enable WLAN Radio**. This provides clean wireless access to your mobile users. Click **Apply** to have this setting take effect. The WLAN radio is disabled by default.

5 In the **Schedule** field, select the time that WLAN radio is active from the drop-down menu. The Schedule list displays the schedule objects you create and manage in the **System Setup | Appliance > System Schedules** page. The default value is **Always on**.

6 In the **Country Code** field, select the country in which the appliance is being used. The country code determines which regulatory domain the radio operation falls under.

7 In the **Radio Mode** field, select your preferred radio mode from the drop-down menu. The wireless security appliance supports the following modes:

> **TIP:** For optimal throughput speed solely for 802.11n clients, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

- **802.11n/a/ac Mixed** - Select this mode if 802.11a, 802.11ac, and 802.11n clients access your wireless network.
- **802.11ac Only** - Select this mode if only 802.11ac clients access your wireless network.

Radio Mode	Definition
2.4GHz 802.11n/g/b Mixed	Supports 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.
2.4GHz 802.11n Only	Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
2.4GHz 802.11g/b Mixed	Supports 802.11g and 802.11b clients simultaneously. If your wireless network comprises both types of clients, select this mode.
2.4GHz 802.11g Only	If your wireless network consists only of 802.11g clients, select this mode for increased 802.11g performance. You might also select this mode if you wish to prevent 802.11b clients from associating.
5GHz 802.11n/a Mixed	Select this mode if 802.11a and 802.11n clients access your wireless network.
5GHz 802.11n Only	Select this mode if only 802.11n clients access your wireless network.
5GHz 802.11a Only	Select this mode if only 802.11a clients access your wireless network.
5GHz 802.11n/a/ac Mixed	Select this mode if 802.11a, 802.11n, and 802.11ac clients access your wireless network.
5GHz 802.11ac Only	Select this mode if you want to provide improved throughput.

The remaining options in the Wireless Settings section might change, depending on which Radio Mode you selected.

Topics:

- 802.11n Wireless Settings
- 802.11a/b/g Wireless Settings
- 802.11ac Wireless Settings

802.11n Wireless Settings

When the **Radio Mode** field is configured for a mode that supports 802.11n only or a mixed mode that includes 802.11n, set following options:

> **NOTE:** The option you see could vary slightly, depending on the on the type of appliance being configured.

Radio Band	Sets the band for the 802.11n radio.
Auto	Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting.

Standard - 20 MHz Channel	Specifies that the 802.11n radio uses only the standard 20 MHz channel. When this option is selected, the **Standard Channel** drop-down menu is displayed.
Standard Channel	Is set to **Auto**, by default, which allows the appliance to set the optimal channel based on signal strength and integrity. You can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help the appliance avoid interference with other wireless networks in the area.
Wide - 40 MHz Channel	Specifies that the 802.11n radio uses only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are displayed.
Primary Channel	Set to **Auto** by default, or you can specify a specific primary channel.
Secondary Channel	The configuration of this drop-down menu is controlled by your selection for the primary channel: • If the primary channel is set to Auto, the secondary channel is also set to Auto. • If the primary channel is set to a specific channel, the secondary channel is set to the optimum channel to avoid interference with the primary channel.
Enable Short Guard Interval	Enable this to have a higher Tx/Rx rate if supported. It applies only to 802.11ac/n mode.
Enable Aggregation	Enables 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput. It applies only to 802.11ac/n mode.
Enable WDS AP	Allows the WDS client to connect to this access point.
SSID	Is filled with a default value of **sonicwall-** plus the last four characters of BSSID; for example, `sonicwall-C587`. The SSID can be changed to any alphanumeric value with a maximum of 32 characters.

TIP: The **Enable Short Guard Interval** and **Enable aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, and so on), these options could introduce transmission errors that eliminate any efficiency gains in throughput.

802.11a/b/g Wireless Settings

When the **Radio Mode** field is configured for a mode that supports 802.11a only, 802.11g/b mixed, or 802.11b only, set the following option displays:

Channel	Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting. You can select a single channel within the range of your regulatory domain.
Enable WDS AP	Allows the WDS client to connect to this access point.
SSID	Is filled with a default value of **sonicwall-** plus the last four characters of BSSID; for example, `sonicwall-C587`. The SSID can be changed to any alphanumeric value with a maximum of 32 characters.

802.11ac Wireless Settings

When the wireless radio is configured for 802.11ac only, these options display:

- Radio Band drop-down menu – Sets the band for the 802.11ac radio which also allows support Band Wide-80 MHz Channel.
- **Channel** drop-down menu – Select a channel:
    - **Auto** – Allows the wireless security appliance to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. **Auto** is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.
    - Specific channel – For the available channels, see 5GHz/2.4GHz Radio Basic Settings for Provisioning Profiles.

Access Point Wireless Virtual Access Point

If using wireless virtual access points, select a **Virtual Access Point Group** from the drop-down menu in the **Wireless Virtual Access Point** section. Or you can select a VAP group previously defined.

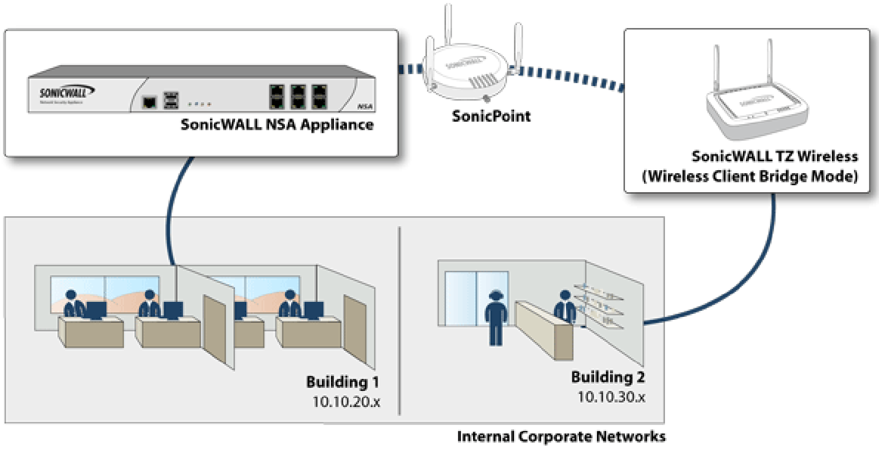
When done with all Access Point settings, click **Accept** to save the settings.

Wireless Client Bridge

The wireless appliance provides Internet/network access by bridging wirelessly to another SonicWall wireless device or SonicPoint access point as shown in Wireless Radio Mode: Wireless Client Bridge. Selecting **Wireless Client Bridge** as the **Radio Role** allows secure network communications between physically separate locations, without the need for long and costly Ethernet cabling runs.

NOTE: The appliance cannot be used as a Wireless Client Bridge if a wireless virtual access point is in use.

Wireless Radio Mode: Wireless Client Bridge



NOTE: For more information on Wireless Client Bridging, refer to the *SonicWall Secure Wireless Network Integrated Solutions Guide*, or the *SonicWall Wireless Bridging Technote*, available at http://www.SonicWall.com/us/support.html.

Topics:

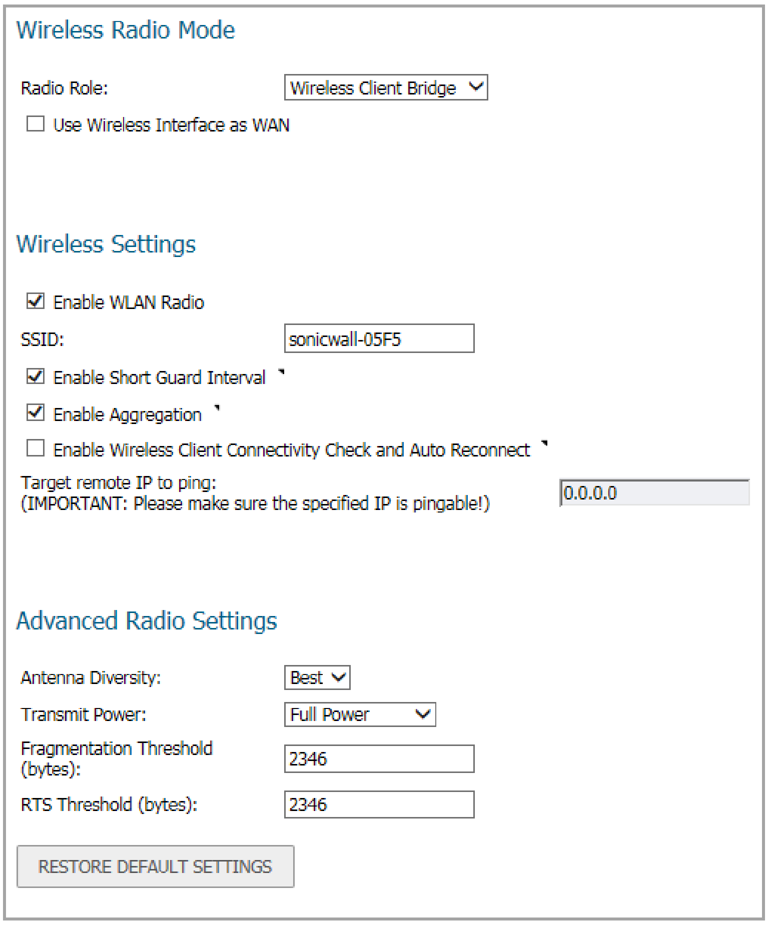
- Client Bridge Wireless Settings
- Client Bridge Advanced Radio Settings

Client Bridge Wireless Settings

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Base Settings**.

3 In the **Radio Role** field, chose **Wireless Client Bridge** from the drop-down menu.



Wireless Radio Mode

Radio Role: Wireless Client Bridge

□ Use Wireless Interface as WAN

Wireless Settings

☑ Enable WLAN Radio

SSID: sonicwall-05F5

☑ Enable Short Guard Interval

☑ Enable Aggregation

□ Enable Wireless Client Connectivity Check and Auto Reconnect

Target remote IP to ping:
(IMPORTANT: Please make sure the specified IP is pingable!) 0.0.0.0

Advanced Radio Settings

Antenna Diversity: Best

Transmit Power: Full Power

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2346

4 Check the box if you want to **Use Wireless Interface as WAN**. The default value is not checked.

5 Under the **Wireless Settings** section, check the box to **Enable WLAN Radio**. In Client Bridge mode, after the radio is enabled, it acts as a client instead of an access point and does not provide wireless access to the client. Click **Apply** to have this setting take effect. The WLAN radio is disabled by default.

6 Select the following options:

SSID	Is filled with a default value of **sonicwall-** plus the last four characters of BSSID; for example, `sonicwall-C587`. The SSID can be changed to any alphanumeric value with a maximum of 32 characters.
Enable Short Guard Interval	Enable this to have a higher Tx/Rx rate if supported. It applies only to 802.11ac/n mode.
Enable Aggregation	Enables 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput. It applies only to 802.11ac/n mode.
Enable Wireless Client Connectivity Check and Auto Reconnect	Periodically checks the wireless client connectivity by pinging a user-defined IP address. In case of lost connection, performs an auto-reconnection.
Target remote IP to ping	If you enabled the connectivity check previously, enter a remote IP address to ping. Important: Make sure the specified IP address is pingable.

Client Bridge Advanced Radio Settings

To set the Advanced Radio Settings:

1 Set the **Antenna Diversity**. The default value is **Best**.

2 Select the Transmit Power from the drop-down menu:

- **Full Power** sends the strongest signal on the WLAN. For example, select **Full Power** if the signal is going from building-to-building.
- **Half (-3 dB)** is recommended for office-to-office within a building.
- **Quarter (-6 dB)** is recommended for short distance communications.
- **Eighth (-9 dB)** is recommended for shorter distance communications.
- **Minimum** is recommended for very short distance communications.

3 Specify the **Fragmentation Threshold (bytes)**. The minimum value can be **256** and the maximum is **2346**. The default is set to the maximum.

4 Set the **RTS Threshold (bytes)**. The minimum is **1** and the maximum is **2346**, which also the default.

5 Click **Accept** to save the settings.

You can click **RESTORE DEFAULT SETTINGS** to return to the factory default settings.

Access Point and Station

When two or more hosts have to be connected with one another over the 802.11 protocol, and the distance is too long for a direct connection to be established, a wireless repeater is used to bridge the gap.

SonicWall wireless security appliances have access point and bridge mode. While in **Access Point & Station** mode, one virtual access point is created as station and can connect to another access point. Other virtual access points works as normal access points. That is to say the unit configured as an **Access Point & Station** works in repeater mode. In this mode, we can also set the virtual interface which the station virtual access point used as a WAN interface.

The Wireless Distribution System (WDS) allows you to connect multiple access points. With WDS, access points communicate with one another without wires in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.

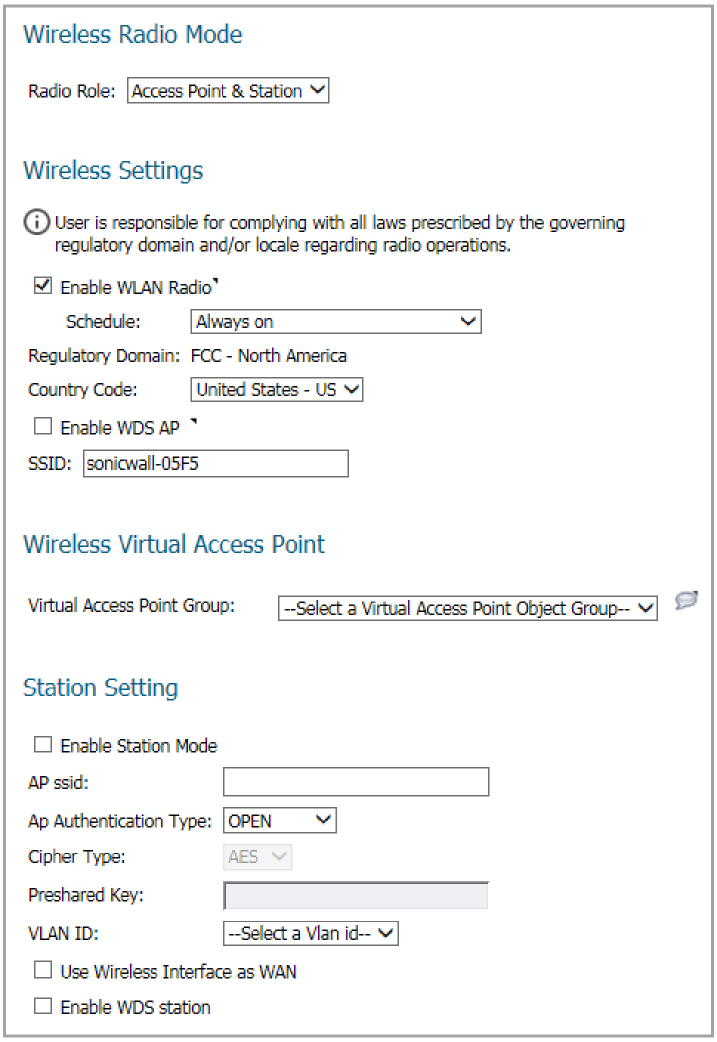
To configure the wireless appliance as an Access Point & Station, define the options as described in:

- Access Point & Station Wireless Settings
- Access Point & Station Wireless Virtual Access Point
- Station Settings

Access Point & Station Wireless Settings

> ⓘ **IMPORTANT:** When setting up the wireless appliance as an access point and station, you are responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

1. Select the **MANAGE** view.
2. Under **Connectivity**, select **Wireless > Base Settings**.
3. In the **Radio Role** field, chose **Access Point and Station** from the drop-down menu.



Wireless Radio Mode

Radio Role: Access Point & Station

Wireless Settings

ⓘ User is responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

☑ Enable WLAN Radio

Schedule: Always on

Regulatory Domain: FCC - North America

Country Code: United States - US

☐ Enable WDS AP

SSID: sonicwall-05F5

Wireless Virtual Access Point

Virtual Access Point Group: --Select a Virtual Access Point Object Group--

Station Setting

☐ Enable Station Mode

AP ssid:

Ap Authentication Type: OPEN

Cipher Type: AES

Preshared Key:

VLAN ID: --Select a Vlan id--

☐ Use Wireless Interface as WAN

☐ Enable WDS station

4 Check the box to **Enable WLAN Radio**. This provides clean wireless access to your mobile users. Click **Apply** to have this setting take effect. The WLAN radio is enabled by default.

5 In the **Schedule** field, select the time that WLAN radio is active from the drop-down menu. The Schedule list displays the schedule objects you create and manage in the **System Setup | Appliance > System Schedules** page in addition to the system-supplied options. The default value is **Always on**.

6 In the **Country Code** field, select the country in which the appliance is being used. The country code determines which regulatory domain the radio operation falls under.

7 Check the box to **Enable WDS AP**. This allows the WDS client to connect to this device as an access point.

8 Validate that the **SSID** field is filled in correctly. It is given a default value of **sonicwall-** plus the last four characters of the BSSID; for example, `sonicwall-C587`. The SSID can be changed to any alphanumeric value with a maximum of 32 characters.

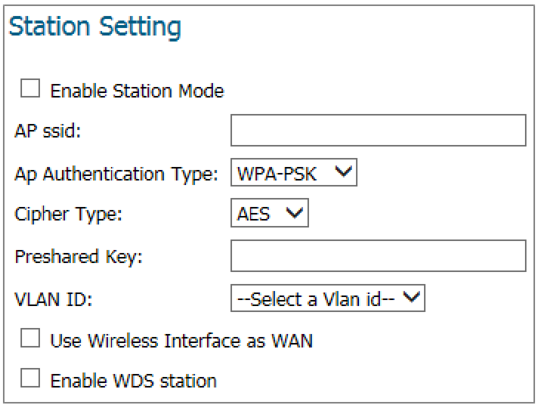
9 Click **ACCEPT** to save the settings.

Access Point & Station Wireless Virtual Access Point

If using wireless virtual access points, select a **Virtual Access Point Group** from the drop-down menu in the **Wireless Virtual Access Point** section. Or you can select a VAP group previously defined.

When done with all Access Point settings, click **Accept** to save the settings.

Station Settings



Station Setting

□ Enable Station Mode

AP ssid:

Ap Authentication Type: WPA-PSK

Cipher Type: AES

Preshared Key:

VLAN ID: --Select a Vlan id--

□ Use Wireless Interface as WAN

□ Enable WDS station

To configure the stations settings:

1 Check **Enable station Mode**.

2 Enter the **AP ssid** in the field provided.

3 Select the Ap Authentication Type from the drop-down menu. Choose from:

- OPEN
- WPA-PSK
- WPA2-PSK

4 Choose a **Cipher Type** from the drop-down menu.

5 Type in a **Preshared Key**.

6 Select a **VLAN ID** from the drop-down menu.

7 To **Use Wireless Interface as WAN**, check the box.

8 To **Enable WDS Station**, check the box.

9 Click **ACCEPT** to save the settings.

Configuring Wireless Security

On the **Connectivity | Wireless > Security** page, you configure the authentication and encryption settings for your wireless appliances. Different options are shown depending on the type of authentication you select.

Topics:

About Authentication

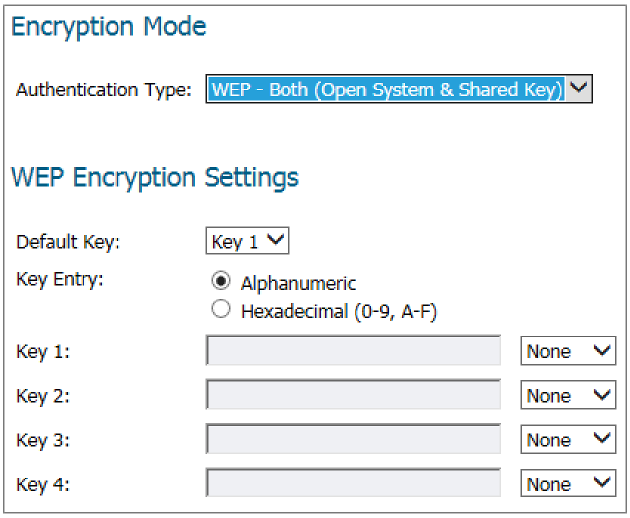
The authentication types are described in the following table:

Authentication Types

Type	Features and use
WEP (Wired Equivalent Protocol)	• Protects data over wireless networks • Provides no protection past the SonicWall appliances • Provides minimum protection for transmitted data • Uses a static key for encryption • Useful for older legacy devices, PDAs, wireless printers • Not recommended for deployments needing a high degree of security
WPA (Wi-Fi Protected Access)	• Good security (uses TKIP) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • No client software needed in most cases • Requires a separate authentication protocol, such as RADIUS to authenticate the users • Uses a dynamic key **NOTE:** This option is only visible when it has been enabled on the diagnostics page.
WPA2 (Wi-Fi Protected Access, v2)	• Best security (uses AES) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • Client software install might be necessary in some cases • Supports 802.11i WPA/WPA2 EAP authentication mode • No backend authentication needed after first log-in (allows for faster roaming) • supports two protocols for storing and generating keys: PSK (Pre-Shared Key) and EAP (Extensible Authentication Protocol) **NOTE:** EAP support is only available in Access Point Mode (selected on the **Connectivity | Wireless > Base Settings** page). EAP support is not available in Bridge Mode.
WPA2-AUTO	• Tries to connect using WPA2 security • If the client is not WPA2 capable, the connection defaults to WPA

Configuring the WEP Settings

The followings option can be set when one of the WEP options is selected for the **Authentication Type**.



Encryption Mode

Authentication Type: WEP - Both (Open System & Shared Key)

WEP Encryption Settings

Default Key: Key 1

Key Entry: ● Alphanumeric ○ Hexadecimal (0-9, A-F)

Key 1: None

Key 2: None

Key 3: None

Key 4: None

To configure wireless appliance for WEP authentication:

1 Navigate to the **Connectivity | Wireless > Security** page.

2 Select the appropriate authentication type from the **Authentication Type** drop-down menu.

- **WEP - Both (Open System & Shared Key)** (default): The **Default Key** assignments are not important as long as the identical keys are used in each field.
- **WEP - Open system**: In open-system authentication, the firewall allows the wireless client access without verifying its identity. All Web Encryptions Settings are grayed out an cannot be selected.
- **WEP -Shared key**: Uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed. If **Shared Key** is selected, then the **Default Key** assignment is important.

3 From the **Default Key** drop-down menu, select which key is the default key: **Key 1**, **Key 2**, **Key 3**, or **Key 4**.

4 From the **Key Entry** options, select if your keys are **Alphanumeric** or **Hexadecimal (0-9, A-F)**.

5 Enter up to four keys in the designated fields. For each key, select whether it us **64 bit**, **128 bit**, or **152 bit**. The higher the bit number, the more secure the key is. Refer to the following table to see how many characters each type of key requires.

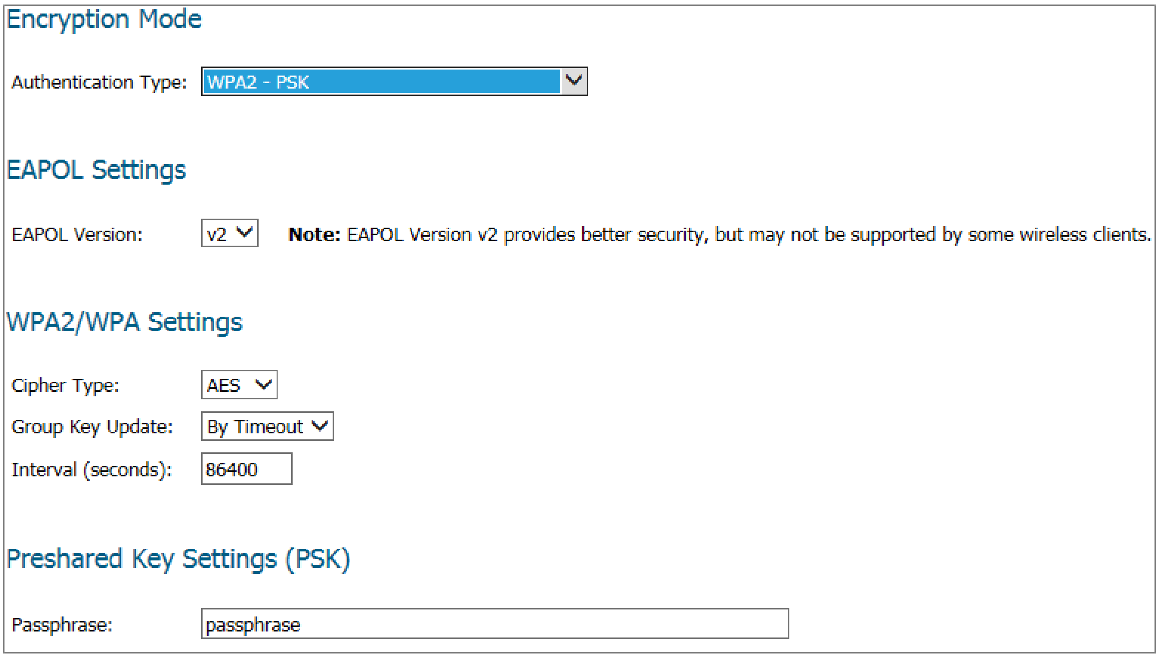
Key Types

Key Type	WEP - 64-bit	WEP - 128-bit	WEP - 152-bit
Alphanumeric	5 characters	13 characters	16 characters
Hexadecimal (0-9, A-F)	10 characters	26 characters	32 characters

6 Click **Accept**.

Configuring WPA2 PSK and WPA PSK Settings

The followings settings can be defined when one of the WPA PSK options is selected for the **Authentication Type**.



Encryption Mode

Authentication Type: WPA2 - PSK

EAPOL Settings

EAPOL Version: v2 **Note:** EAPOL Version v2 provides better security, but may not be supported by some wireless clients.

WPA2/WPA Settings

Cipher Type: AES

Group Key Update: By Timeout

Interval (seconds): 86400

Preshared Key Settings (PSK)

Passphrase: passphrase

To configure wireless appliance for WPA authentication with a preset shared key:

1 Navigate to the **Connectivity | Wireless > Security** page.

2 Select the appropriate authentication type from the **Authentication Type** drop-down menu.

- **WPA2 - PSK**: Connects using WPA2 and a preset authentication key.
- **WPA2 - Auto - PSK**: Automatically tries to connect using WPA2 and a preset authentication key, but falls back to WPA if the client is not WPA2-capable.

3 Select the **EAPOL Version** setting from the drop-down menu:

- **V2** (default)—Selects version 2. This provides better security than version 1, but might not be supported by some wireless clients.
- **V1**—Selects version 1 of the protocol.

4 In **WPA2/WPA Setting** section, specify these settings:

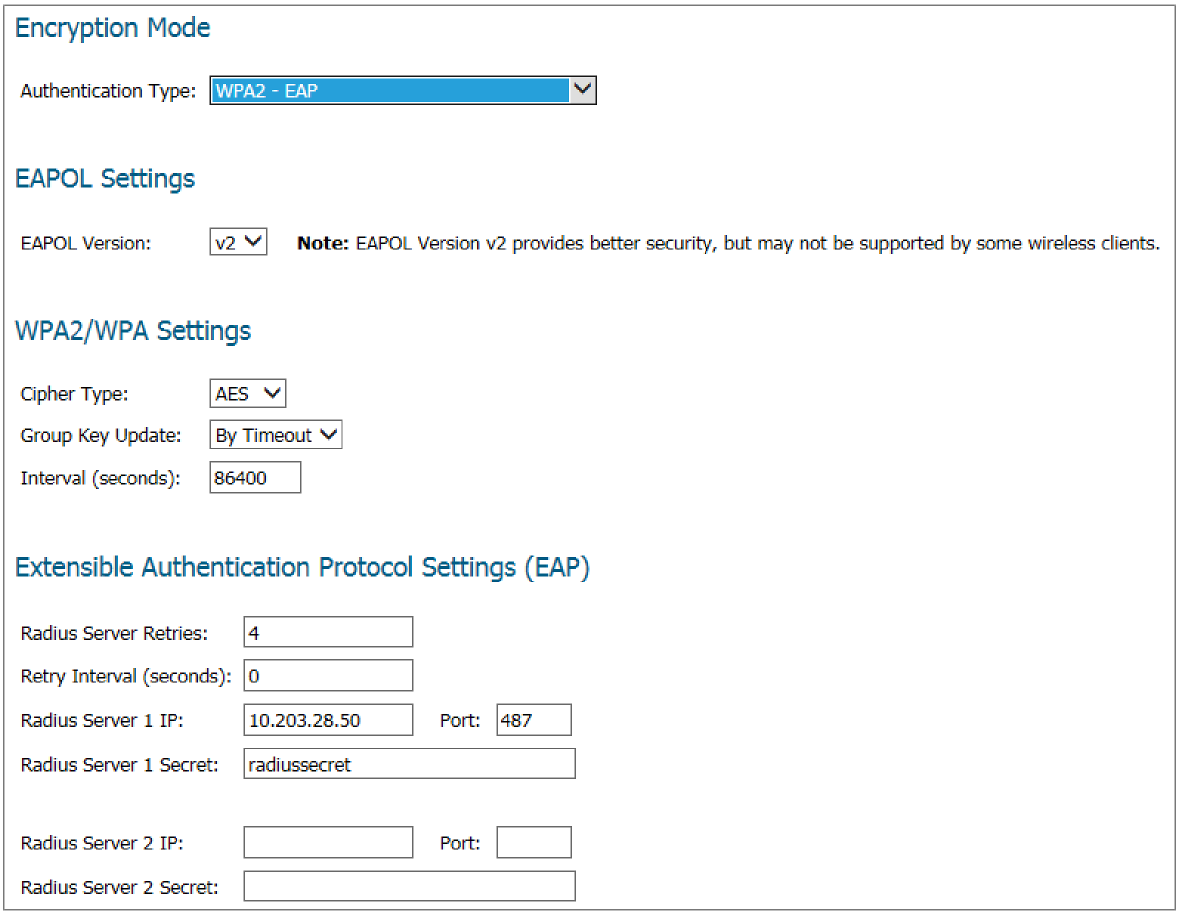
- **Cipher Type**—Select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis, but it is less secure and has lower throughput. AES and AUTO are also Cipher type options.
- **Group Key Update**—Specifies when the SonicWall security appliance updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds; this is the default. Select **Disabled** when using a static key.
- **Interval**—If you selected **By Timeout** in the **Group Key Update** field, enter the number of seconds before WPA automatically generates a new group key. The default is **86400** seconds. If you selected **Disabled** for **Group Key Update**, this option is not displayed.

5 In the **Passphrase** field, enter the passphrase from which the key is generated.

6 Click **ACCEPT** to save and apply your settings.

WPA2 EAP and WPA EAP Settings

The followings settings can be defined when one of the WPA EAP options is selected for the **Authentication Type**.



Encryption Mode

Authentication Type: WPA2 - EAP

EAPOL Settings

EAPOL Version: v2

Note: EAPOL Version v2 provides better security, but may not be supported by some wireless clients.

WPA2/WPA Settings

Cipher Type: AES

Group Key Update: By Timeout

Interval (seconds): 86400

Extensible Authentication Protocol Settings (EAP)

Radius Server Retries: 4

Retry Interval (seconds): 0

Radius Server 1 IP: 10.203.28.50 Port: 487

Radius Server 1 Secret: radiussecret

Radius Server 2 IP: Port:

Radius Server 2 Secret:

To configure wireless appliance for WPA authentication with a preset shared key:

1. Navigate to the **Connectivity | Wireless > Security** page.
2. Select the appropriate authentication type from the **Authentication Type** drop-down menu.
    - **WPA2 - EAP**: Connects using WPA2 an extensible authentication protocol.
    - **WPA2 - Auto - EAP**: Automatically tries to connect using WPA2 and an extensible authentication protocol, but falls back to WPA when the client is not WPA2-capable.

    ⓘ **NOTE:** EAP support is only available in Access Point mode, but not in Client Bridge mode.
3. Select the **EAPOL Version** setting from the drop-down menu:
    - **V1**—Selects the extensible authentication protocol over LAN version 1.
    - **V2**—Selects the extensible authentication protocol over LAN version 2. This provides better security than version 1, but might not be supported by some wireless clients.

4 In **WPA2/WPA Setting** section, specify these settings:

- **Cipher Type**—Select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis, but it is less secure and has lower throughput. AES and AUTO are also Cipher type options.
- **Group Key Update**—Specifies when the SonicWall security appliance updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds; this is the default. Select **Disabled** when using a static key.
- **Interval**—If you selected **By Timeout** in the **Group Key Update** field, enter the number of seconds before WPA automatically generates a new group key. The default is **86400** seconds. If you selected **Disabled** for **Group Key Update**, this option is not displayed.

5 In the **Extensible Authentication Protocol Settings (EAP)** section, specify these settings:

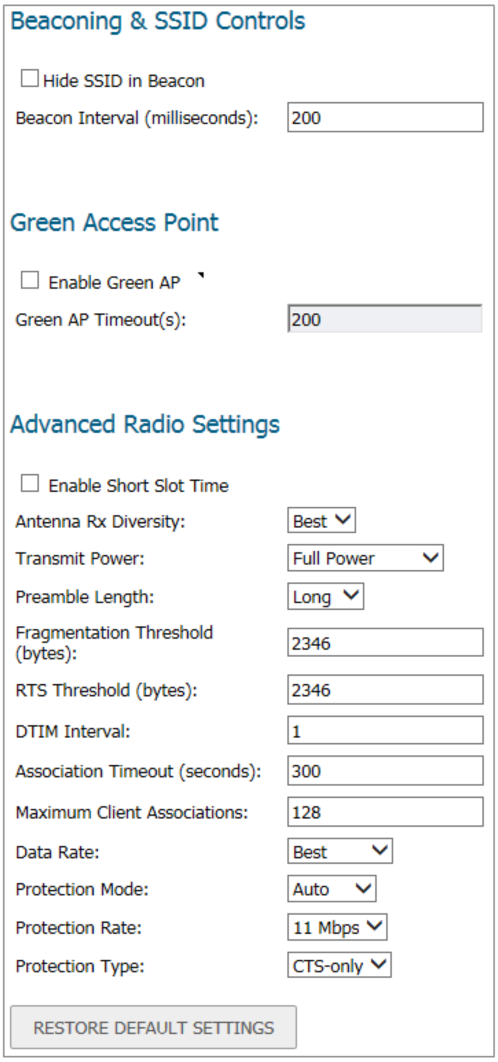
- **Radius Server Retries**—Enter the number of authentication retries the server attempts. The default is **4**.
- **Retry Interval (seconds)**—Enter the delay the server is to wait between retries. The default is **0** (no delay).
- **Radius Server 1 IP** and **Port**—Enter the IP address and port number for your primary RADIUS server.
- **Radius Server 1 Secret**—Enter the password for access to Radius Server.
- **Radius Server 2 IP** and **Port**—Enter the IP address and port number for your secondary RADIUS server, if you have one.
- **Radius Server 2 Secret**—Enter the password for access to Radius Server.

6 Click **Accept** to apply your WPA2 EAP settings.

32

Configuring Advanced Wireless Settings

On the Advanced Settings you can customize a range of features for your wireless appliance. This page is only accessible when the firewall is acting as an access point.



Beaconing & SSID Controls

☐ Hide SSID in Beacon

Beacon Interval (milliseconds):	200

Green Access Point

☐ Enable Green AP

Green AP Timeout(s):	200

Advanced Radio Settings

☐ Enable Short Slot Time

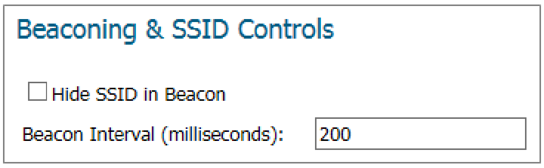
Antenna Rx Diversity:	Best
Transmit Power:	Full Power
Preamble Length:	Long
Fragmentation Threshold (bytes):	2346
RTS Threshold (bytes):	2346
DTIM Interval:	1
Association Timeout (seconds):	300
Maximum Client Associations:	128
Data Rate:	Best
Protection Mode:	Auto
Protection Rate:	11 Mbps
Protection Type:	CTS-only

Topics:

- Beaconing and SSID Controls
- Green Access Point
- Advanced Radio Settings

- Configurable Antenna Diversity

Beaconing and SSID Controls



Beaconing & SSID Controls

□ Hide SSID in Beacon

Beacon Interval (milliseconds): 200

To configure the Beaconing and SSID Controls:

1 Navigate to the **MANAGE**.

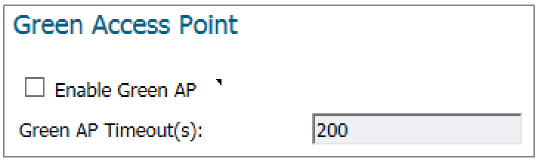
1 Select the **Connectivity | Wireless > Advanced Settings** page.

2 Select **Hide SSID in Beacon**, which suppresses broadcasting of the SSID name and disables responses to probe requests. Checking this option helps prevent your wireless SSID from being seen by unauthorized wireless clients. This setting is disabled by default.

3 Type a value, in milliseconds, for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently. The default interval is **200** milliseconds.

4 Click **ACCEPT** to apply your changes. Click **RESTORE DEFAULT SETTINGS** to return to the manufacturing defaults.

Green Access Point



Green Access Point

□ Enable Green AP

Green AP Timeout(s): 200

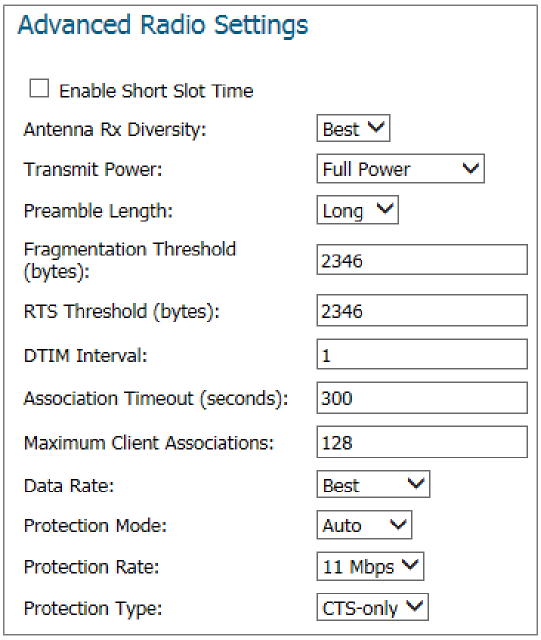
To configure power efficiency:

1 To increase power efficiency, select **Enable Green AP**. This setting is disabled by default.

2 Specify the number of time outs in the **Green AP Timeout(s)** field. The default is **200**.

3 Click **ACCEPT** to apply your changes. Click **RESTORE DEFAULT SETTINGS** to return to the manufacturing defaults.

Advanced Radio Settings



Advanced Radio Settings

☐ Enable Short Slot Time

Antenna Rx Diversity:	Best
Transmit Power:	Full Power
Preamble Length:	Long
Fragmentation Threshold (bytes):	2346
RTS Threshold (bytes):	2346
DTIM Interval:	1
Association Timeout (seconds):	300
Maximum Client Associations:	128
Data Rate:	Best
Protection Mode:	Auto
Protection Rate:	11 Mbps
Protection Type:	CTS-only

To configure advanced radio settings:

1 Select **Enable Short Slot Time** to increase performance if you only expect 802.11g traffic. 802.11b is not compatible with short slot time. This setting is disabled by default.

2 From the **Antenna Rx Diversity** drop-down menu select which antenna the wireless security appliance uses to send and receive data. For more information about antenna diversity, refer Configurable Antenna Diversity. The default is **Best**.

3 From the **Transmit Power** drop-down menu, select:

- **Full Power** to send the strongest signal on the WLAN. For example, select **Full Power** if the signal is going from building-to-building.
- **Half (-3 dB)** is recommended for office-to-office within a building.
- **Quarter (-6 dB)** is recommended for shorter distance communications.
- **Eighth (-9 dB)** is recommended for shorter distance communications.
- **Minimum** is recommended for very short distance communications.

4 From the **Preamble Length** drop-down menu, select **Short** or **Long**. **Short** is recommended for efficiency and improved throughput on the wireless network. The default is **Long**.

5 Specify the **Fragmentation Threshold (bytes)**. The minimum is 256; the maximum is 2346, and the default is **2346**.

You can fragment wireless frames to increase reliability and throughput in areas with RF interference or poor wireless coverage. Lower threshold numbers produce more fragments. Increasing the value means that frames are delivered with less overhead, but a lost or damaged frame must be discarded and retransmitted.

6 Specify the request-to-send (RTS) threshold in the **RTS Threshold (bytes)** field. The minimum is 1, the maximum is 2347, and the default is **2346**.

This field sets the threshold for a packet size (in bytes) at which a RTS is sent before packet transmission. Sending an RTS ensures that wireless collisions do not take place in situations where clients are in range of the same access point, but might not be in range of each other. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.

7 Specify the DTIM (Delivery of Traffic Indication Message) interval in the **DTIM Interval** field. The minimum is 1, the maximum is 256, and the default is **1**.

   For 802.11 power-save mode clients of incoming multicast packets, the DTIM interval specifies the number of beacon frames to wait before sending a DTIM. Increasing the DTIM Interval value allows you to conserve power more effectively.

8 Enter the number of seconds for client association in the **Association Timeout (seconds)** field. The default is **300** seconds, and the allowed range is from 60 to 36000 seconds. If your network is very busy, you can increase the timeout by increasing the number of seconds in this field.

9 Enter the **Maximum Client Associations** for each SonicPoint using this profile. The minimum value is 1; the maximum is 128, and the default is 128. This setting limits the number of stations that can connect wirelessly at one time.

10 From the **Data Rate** drop-down menu, select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate from the options that range from **1 Mbps** to **54 Mbps**.

11 From the **Protection Mode** drop-down menu, select the protection mode: **None**, **Always**, or **Auto**.

   Protection can decrease collisions, particularly where you have two overlapping SonicPoints. However, it can slow down performance. **Auto** is probably the best setting, as it engages only in the case of overlapping SonicPoints.

12 Choose the **Protection Rate** from the drop-down menu: **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**. The protection rate determines the data rate when protection mode is on. The slowest rate offers the greatest degree of protection, but also the slowest data transmission rate.

13 From the **Protection Type** drop-down menu, select the type of handshake used to establish a wireless connection: **CTS-only** (default) or **RTS-CTS**.

   ⓘ **NOTE:** 802.11b traffic is only compatible with **CTS**.

14 Click **ACCEPT** to apply your changes. Click **RESTORE DEFAULT SETTINGS** to return to the manufacturing defaults.

Configurable Antenna Diversity

The wireless SonicWall security appliances employ dual 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting, and both antennas act as potential receiving antenna. As radio signals arrive at both antennas on the secure wireless appliance, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal. To allow for external (higher gain uni-directional) antennas to be used, antenna diversity can be disabled.

The SonicWall NSA 220 and 250M wireless security appliances employ three antennas. The Antenna Diversity is set to **Best** by default, this is the only setting available for these appliances.

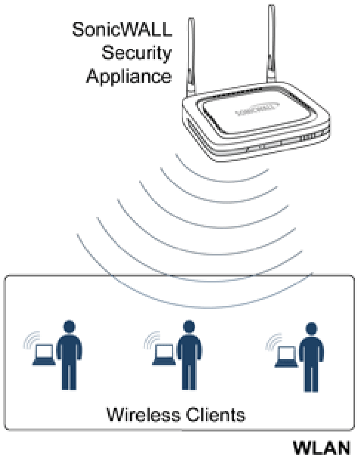
The **Antenna Diversity** setting determines which antenna the wireless security appliance uses to send and receive data. **Best** is the default setting. When selected, the wireless security appliance automatically selects the antenna with the strongest, clearest signal.

Wireless MAC Filter List

Wireless networking provides native MAC filtering capabilities that prevent wireless clients from authenticating and associating with the wireless security appliance. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card. The SonicOS wireless MAC Filter List allows you to configure a list of clients that are allowed or denied access to your wireless network. Without MAC filtering, any wireless client can join your wireless network if they know the SSID and other security parameters, thus allowing them to “break into” your wireless network.

A typical 289 MAC Filter List deployment scenario is illustrated below:

Typical SonicWall MAC Filter List Deployment



Topics:

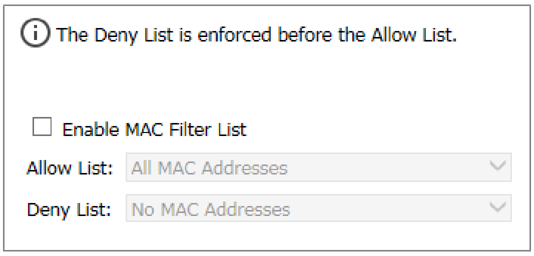
- Deployment Considerations
- Configuring the Wireless > MAC Filter List

Deployment Considerations

Consider the following when deploying the MAC Filter List:

- For the SonicPoint-N appliance, this feature requires the gateway to store the MAC Filer List settings.
- For the SonicWall TZ series appliance’s internal wireless, some members need to be added to the VAP structure to store the MAC Filter List settings and the complete function should be modified to set the configurations to the driver.
- The virtual access point can configure its MAC Filter List or inherit global settings configured on the **Connectivity | Wireless > MAC Filter List** page.

Configuring the Wireless > MAC Filter List



The Deny List is enforced before the Allow List.

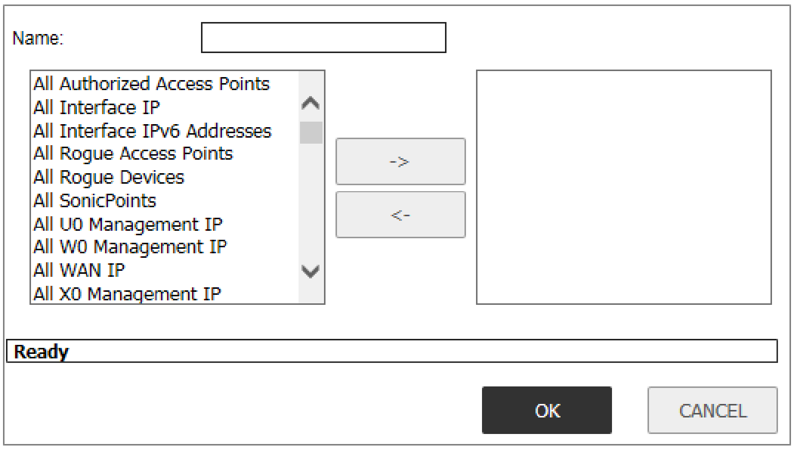
□ Enable MAC Filter List

Allow List: All MAC Addresses

Deny List: No MAC Addresses

To configure the MAC Filter List:

1. Select the **MANAGE** view.
2. Under **Connectivity**, select **Wireless > MAC Filter List**.
3. Click **Enable MAC Filter List**. This setting is disabled by default.
4. From the **Allow List** drop-down menu, select the address group you want to allow: **All MAC Addresses** (default), **Default ACL Allow Group**, or a group you created.
5. From the **Deny List** drop-down menu, select the address group you want to deny: No MAC Addresses (default), Default ACL Deny Group, or a group you created.
6. If you want to add new address objects to the allow and deny lists, select **Create New MAC Address Object Group...** from either the **Allow List** or **Deny List** drop-down menu.



Name:

   a. In the **Name:** text field, enter a name for the new group.
   b. In the left column, select the group(s) or individual address object(s) you want to allow or deny. You can use **Ctrl-click** to select more than one item at a time.
   c. Click the **Right Arrow ->** to add the items to the group.
   d. Click **OK**. The address displays in the drop-down menu for selection.
   e. Select the object, if wanted.
7. Click **Accept**.

34

Configuring Wireless IDS

Topics:

- About Wireless IDS
- Configuring IDS Settings

About Wireless IDS

Wireless Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWall wireless security appliances. They enable recognition of—and countermeasures against—the most common types of illicit wireless activity. Wireless IDS consists of three types of services:

- Sequence Number Analysis
- Association Flood Detection
- Rogue Access Point Detection

Access Point IDS

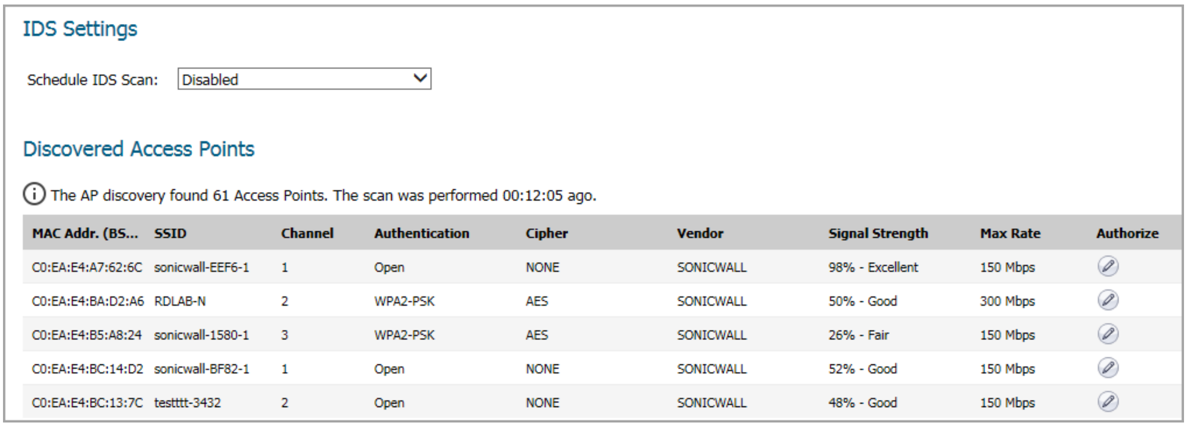
When the **Radio Role** of the wireless security appliance is set to **Access Point** mode, all three types of WIDS services are available, but Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation). Selecting **Scan Now** momentarily changes the Radio Role to allow the wireless security appliance to perform an active scan, and might cause a brief loss of connectivity for associated wireless clients. While in **Access Point** mode, the **Scan Now** function should only be used if no clients are actively associated, or if the possibility of client interruption is acceptable.

Rogue Access Points

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, afford-ability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. The real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. While this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The security appliance can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It does this in two ways: active scanning for access points on all 802.11a, 802.11g, and 802.11n channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

Configuring IDS Settings



IDS Settings

Schedule IDS Scan: Disabled

Discovered Access Points

ⓘ The AP discovery found 61 Access Points. The scan was performed 00:12:05 ago.

MAC Addr. (BS...	SSID	Channel	Authentication	Cipher	Vendor	Signal Strength	Max Rate	Authorize
C0:EA:E4:A7:62:6C	sonicwall-EEF6-1	1	Open	NONE	SONICWALL	98% - Excellent	150 Mbps	✎
C0:EA:E4:BA:D2:A6	RDLAB-N	2	WPA2-PSK	AES	SONICWALL	50% - Good	300 Mbps	✎
C0:EA:E4:B5:A8:24	sonicwall-1580-1	3	WPA2-PSK	AES	SONICWALL	26% - Fair	150 Mbps	✎
C0:EA:E4:BC:14:D2	sonicwall-BF82-1	1	Open	NONE	SONICWALL	52% - Good	150 Mbps	✎
C0:EA:E4:BC:13:7C	testttt-3432	2	Open	NONE	SONICWALL	48% - Good	150 Mbps	✎

Topics:

- IDS Settings
- Discovered Access Points

IDS Settings

To schedule when to run an IDS scan, choose an option from the **Schedule IDS Scan** drop-down menu:

- **Disabled**

  This is the default. IDS scans do not take place when selected.

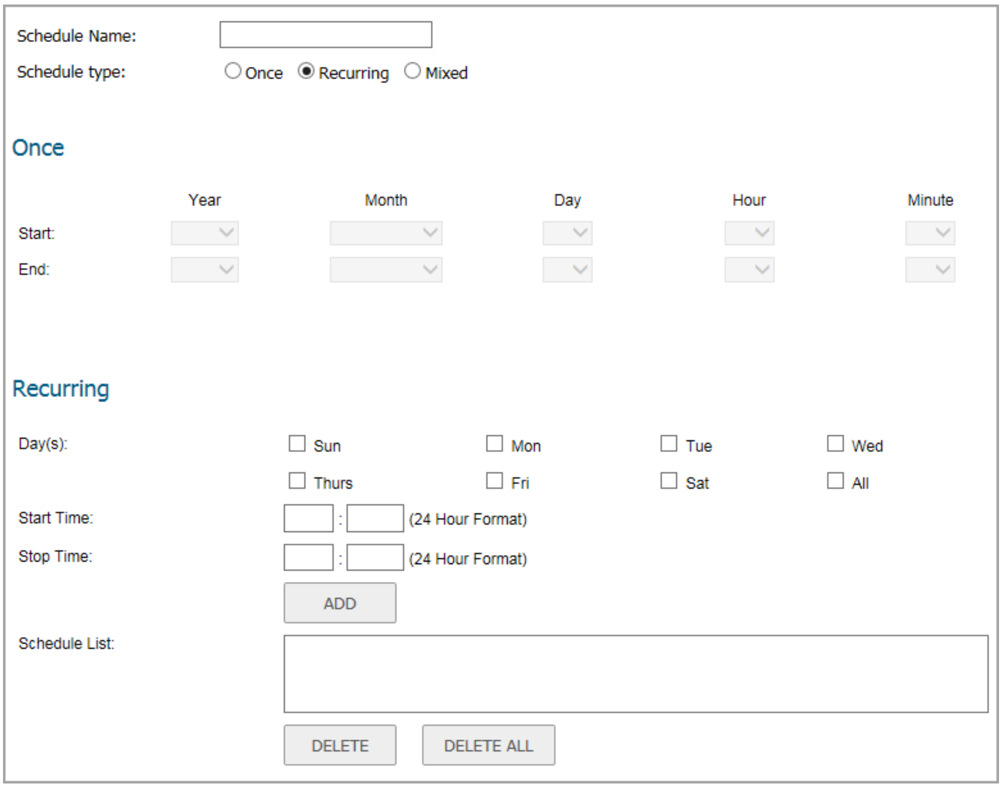
- **Create a new schedule...**

  The **Add Schedule** dialog displays and you can create a custom scheduled as described later in this section.

- **Work Hours**
- **M-T-W-TH-F 08:00 to 17:00**
- **After Hours**
- **M-T-W-TH-F 00:00 to 08:00**
- **M-T-W-TH-F 17:00 to 24:00**
- **SU-S 00:00 to 24:00**
- **Weekend Hours**

To add a new schedule to the Schedule ID Scan drop-down menu:

1 In the **Schedule IDS Scan** field, select **Create New Scheduled...**


Schedule type: ○ Once ● Recurring ○ Mixed

2 Type the **Schedule Name**.

3 Select Schedule type:

- With **Once**, you schedule a one-time event and only the fields in the **Once** section are active.
- With **Recurring**, you schedule a recurring event and only the fields in the **Recurring** section are active.
- With **Mixed**, you schedule a mixed event and all fields are active.

4 In the **Once** section, use the drop-down menus to schedule the start and end times for your IDS scan.

5 In the **Recurring** section:

a Pick the **Day(s)** for your scan.

b Enter a **Start Time**, using 24-hour format.

c Enter a **Stop Time**, using 24-hour format.

d Click **ADD** to add those parameters to the Schedule List.

e To delete an item from the list, highlight it and click **DELETE**. Click **DELETE ALL** to clear the Schedule List.

6 Click **OK** to add this schedule to the drop-down menu.

Discovered Access Points

Active scanning occurs when the wireless security appliance starts up and any time **Scan Now** is clicked at the bottom of the of the table. The appliance scans the environment and identifies other wireless devices in the vicinity. The Note above the table displays the number of Access Points found and the time, in days, hours, minutes, and seconds, since the last scan.

To refresh the entries in the **Discovered Access Points** table, click **Refresh**. To do an immediate scan, **Scan Now** (at the bottom of the table).

> **IMPORTANT:** The **Scan Now** feature causes a brief disruption in service when operating in Access Point Mode. This interruption manifests itself as follows:
>
> - Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
> - Persistent connections (protocols such as FTP) are impaired or severed.
>
> If this is a concern, wait to use **Scan Now** at a time when no clients are active or until the potential for disruption becomes acceptable.

When the wireless security appliance is operating in a Bridge Mode, the **Scan Now** feature does not cause any interruption to the bridged connectivity.

Settings

The **Discovered Access Points** table displays information on every access point that can be detected by all your SonicPoints or on a individual SonicPoint basis:

- **MAC Address (BSSID)**: The MAC address of the radio interface of the detected access point.
- **SSID**: The radio SSID of the access point.
- **Channel**: The radio channel used by the access point.
- **Authentication**: The type of authentication.
- **Cipher**: The cipher used.
- **Vendor**: The manufacturer of the access point. SonicPoints show a manufacturer of either SonicWall or Senao.
- **Signal Strength**: The strength of the detected radio signal.
- **Max Rate**: The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize**: Click the icon in the **Authorize** column to add the access point to the address object group of authorized access points.

Authorizing Access Points on Your Network

Access Points detected by the wireless security appliance are regarded as rogues until they are identified to the wireless security appliance as authorized for operation. To authorize an access point, click the **Authorize** icon.

35

Configuring Virtual Access Points with Internal Wireless Radio

A Virtual Access Point (VAP) is a multiplexed representation of a single physical access point—it presents itself as multiple discrete access points. To wireless LAN clients, each virtual access point appears to be an independent physical access point, when actually only one physical access point exists. Virtual access points allow you to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point and can be grouped and enforced on a single internal wireless radio.

The benefits of using the VAP includes:

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single physical access point to be used for multiple purposes to avoid channel collision problem. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, for example, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more wireless ISPs. However, in the US and Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. After the channels are utilized by existing access points, additional access points interfere with each other and reduce performance. VAPs conserve channels by allowing a single network to be used for multiple purposes.
- **Wireless LAN Infrastructure Optimization**—Shares the same Wireless LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

Topics:

Wireless Virtual AP Configuration Task List

A Wireless VAP deployment requires several steps to configure. The following section provides a brief overview of the steps involved:

1. **Network Zone** - The network zone is the backbone of your VAP configuration. Each zone you create has its own security and access control settings, and you can create and apply multiple zones to a single physical interface using wireless subnets. For more information on network zones, refer to the section on **Manage | Network > Zones** in *SonicOS 6.5 System Setup*.

2 **Wireless Interface** - The W0 interface (and its WLAN subnets) represent the physical connections between your SonicWall network security appliance and the internal wireless radio. Individual zone settings are applied to these interfaces and forwarded to the wireless radio. For more information on wireless interfaces, refer to the section on **Manage | Network > Interfaces** in *SonicOS 6.5 System Setup*.

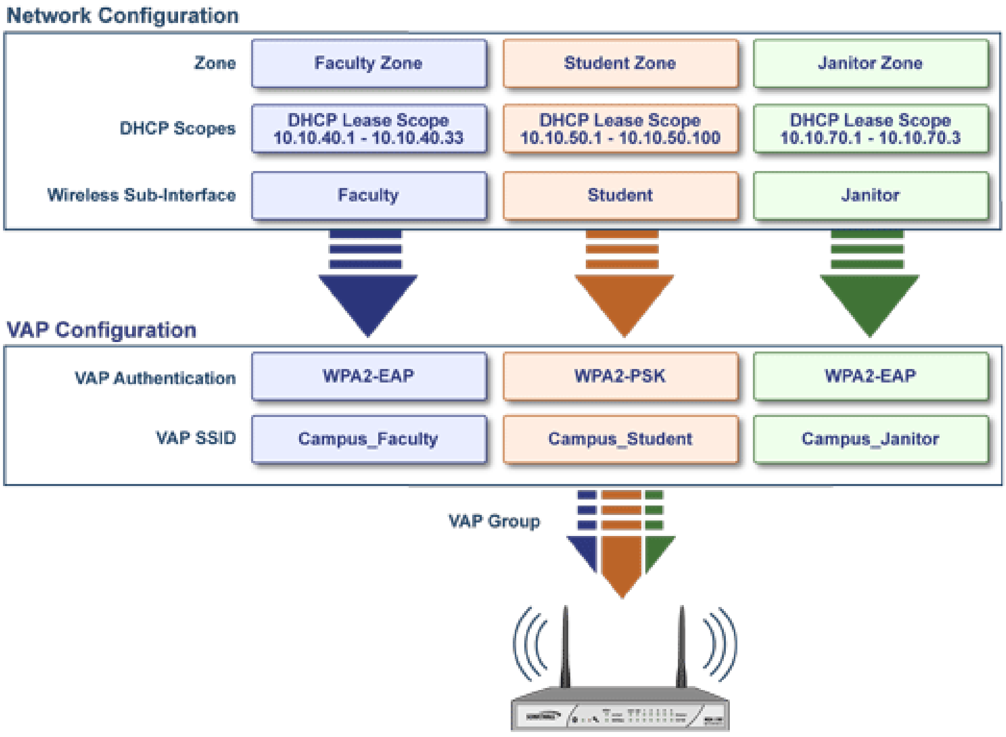
3 **DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as *Scopes*. The default ranges for DHCP scopes are often excessive for the needs of most wireless deployments, for instance, a scope of 200 addresses for an interface that only uses 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted. For more information on setting up the DHCP server, refer to the section on **Manage | Network > DHCP Server** in *SonicOS 6.5 System Setup*.

4 **Virtual Access Point Profiles** - The VAP Profile feature allows for creation of wireless configuration profiles which can be easily applied to new wireless Virtual Access Points as needed. Refer to **Virtual Access Point Profiles** for more information.

5 **Virtual Access Point** - The VAP Objects feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings. Refer to Virtual Access Points for more information.

6 **Virtual Access Point Group** - The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to a single internal wireless radio. Refer to Virtual Access Point Groups for more information.

7 **Assign VAP Group to Internal Wireless Radio**- The VAP Group is applied to the internal wireless radio and made available to users through multiple SSIDs. Refer to Enabling the Virtual Access Point Group for more information.



Network Configuration

Zone	Faculty Zone	Student Zone	Janitor Zone
DHCP Scopes	DHCP Lease Scope 10.10.40.1 - 10.10.40.33	DHCP Lease Scope 10.10.50.1 - 10.10.50.100	DHCP Lease Scope 10.10.70.1 - 10.10.70.3
Wireless Sub-Interface	Faculty	Student	Janitor

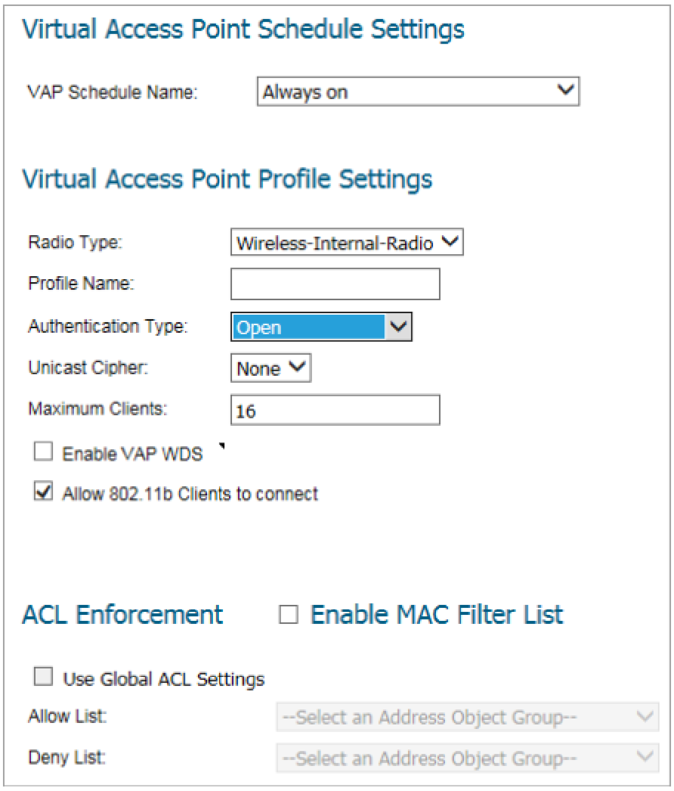
VAP Configuration

VAP Authentication	WPA2-EAP	WPA2-PSK	WPA2-EAP
VAP SSID	Campus_Faculty	Campus_Student	Campus_Janitor

Virtual Access Point Profiles

A Virtual Access Point Profile allows you to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **Manage | Wireless > Virtual Access Point** page. Select the profile name and click the **Edit** icon or click **ADD** to create a new Virtual Access Point Profile. Click **OK** when done.

TIP: This feature is especially useful for quick setup in situations where multiple virtual access points share the same authentication methods.



Virtual Access Point Schedule Settings

VAP Schedule Name: Always on

Virtual Access Point Profile Settings

Radio Type: Wireless-Internal-Radio

Profile Name:

Authentication Type: Open

Unicast Cipher: None

Maximum Clients: 16

□ Enable VAP WDS

☑ Allow 802.11b Clients to connect

ACL Enforcement □ Enable MAC Filter List

□ Use Global ACL Settings

Allow List: --Select an Address Object Group--

Deny List: --Select an Address Object Group--

Topics:

- Virtual Access Point Schedule Settings
- Virtual Access Point Profile Settings
- ACL Enforcement

Virtual Access Point Schedule Settings

Each Virtual Access Point can have its own schedule associated with it and by extension each profile can have a set schedule defined for it as well.

To associate a schedule with a Virtual Access Point Profile:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Virtual Access Point**.

3 Select **ADD** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.

4 In the **VAP Schedule Name** field, select the schedule you want from the options in the drop-down menu.

Virtual Access Point Profile Settings

To set the Virtual Access Point Profile settings:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Virtual Access Point**.

3 Select **ADD** if creating a new profile, or select a Virtual Access Point Profile and click on the **Edit** icon if editing an existing profile.

4 Set the **Radio Type**. It is set to **Wireless-Internal-Radio** by default. Retain this default setting if using the internal radio for VAP access; it is currently the only supported radio type.

5 In the **Profile Name** field, type a friendly name for this Virtual Access Point profile. Choose something descriptive and easy to remember as you apply this profile to new VAPs.

6 Select the **Authentication Type** from the drop-down menu. Choose from these options:

Authentication Type	Definition
Open	No authentication is specified.
Shared	A shared key is used to authenticate WEP encryptions settings
Both	If no shared key is configured, it is same as an open network. If shared key is configured, it means open authentication with encrypted data traffic.
WPA2-PSK	Best security used with trusted corporate wireless clients. Transparent authentication with Windows login. Supports fast-roaming feature. Uses pre-shared key for authentication.
WPA2-EAP	Best security used with trusted corporate wireless clients. Transparent authentication with Windows login. Supports fast-roaming feature. Uses extensible authentication protocol.
WPA2-AUTO-PSK	Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection defaults to WPA.Uses pre-shared key for authentication.
WPA2-AUTO-EAP	Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection defaults to WPA. Uses extensible authentication protocol.

The **Unicast Cipher** field is auto-populated based on what authentication type you selected.

ⓘ **NOTE:** Different setting appear on the page depending upon which option you select.

7 In the **Maximum Clients** field, type in the maximum number of concurrent client connections permissible for this virtual access point.

8 Check the box to **Enable VAP WDS** (wireless distribution system). By default, this option is not selected.

9 Check the box to **Allow 802.11b Clients to connect**. By default, this option is selected.

Depending on the **Authentication Type** selected, an additional section with options is added to the Add/Edit Virtual Access Point Profile page.

- If you selected **Both** or **Shared**, refer to WEP Encryption Settings for information on the settings.
- If you selected an option requiring a pre-shared key (PSK), refer to WPA-PSK > WPA2-PSK Encryption Settings for information on the settings.
- If you selected an option using the extensible authentication protocol (EAP), refer to WPA-EAP > WPA2-EAP Encryption Settings for information on the settings.

WEP Encryption Settings

If you selected **Both** or **Shared** in Step 6 of the prior procedure, the section called **WEP Encryption Settings** appears. WEP settings are commonly shared by virtual access points within a common physical access point.

In the **Encryption Key** field, select **Key 1**, **Key 2**, **Key 3** or **Key 4** from the drop-down menu.

WPA-PSK > WPA2-PSK Encryption Settings

If you selected an option in Step 6 that requires a pre-shared key—**WPA2-PSK** or **WPA2-AUTO-PSK**—the section called **WPA/WPA2-PSK Encryption Settings** appears. When these settings are defined, a preshared key is used for authentication. Input values in the following fields:

Field Name	Description
Pass Phrase	Type in the shared passphrase users need to enter when connecting with PSK-based authentication.
Group Key Interval	Type in the time period for which a Group Key is valid. The default value is 86400 seconds. Setting to low of a value can cause connection issues.

WPA-EAP > WPA2-EAP Encryption Settings

If you selected an option in Step 6 that requires EAP—**WPA2-EAP** or **WPA2-AUTO-EAP**—the section called **Radius Server Settings** appears. When these settings are defined, an external 802.1x/EAP capable RADIUS server is used for key generation and authentication. Input values in the following fields:

Field Name	Description
Radius Server Retries	Enter the number times a user can try to authenticate before access is denied. The default is 4.
Retry Interval (seconds)	Enter the time period during which retries are valid. The default is 0.
RADIUS Server 1	Input the name/location of the RADIUS authentication server.
Port	Input the port on which your primary RADIUS authentication server communicates with clients and network devices.
RADIUS Server 1 Secret	Enter the secret passcode for your primary RADIUS authentication server.
RADIUS Server 2	Input the name/location of your backup RADIUS authentication server.
Port	Input the port on which your backup RADIUS authentication server communicates with clients and network devices.
RADIUS Server 2 Secret	Enter the secret passcode for your backup RADIUS authentication server.
Group Key Interval	Input the time period (in seconds) during which the WPA/WPA2 group key is enforced. The default value is 86400.

ACL Enforcement

Each Virtual Access Point can support an individual Access Control List (ACL) to provide more effective authentication control. The Wireless ACL feature works in tandem with the wireless MAC Filter List currently available on SonicOS. Using the ACL Enforcement feature, users are able to enable or disable the MAC Filter List, set the Allow List, and set the Deny list.

Each VAP can have its own MAC Filter List settings or use the global settings. In Virtual Access Point (VAP) mode, each VAP of this group shares the same MAC Filter List settings.

To enable MAC Filter List enforcement:

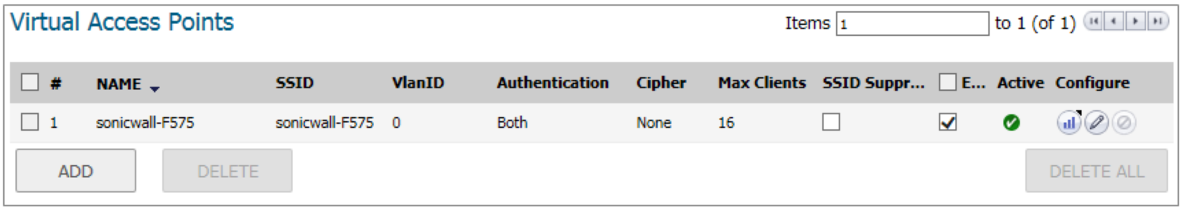
1. Check the box to **Enable MAC Filter List**. When the MAC filter list is enabled, the other settings are also enabled so you can set them.
2. Check the box if you want to **Use Global ACL Settings**. This associates the Virtual Access Point with the already existing MAC Filter List settings for the SonicWall network security appliance. Note you cannot edit the Allow or Deny Lists with this option enabled.
3. In the **Allow List**, select an option from the drop-down menu. This identified which MAC addresses you allow to have access.

   Choose **Create MAC Address Object Group** if you want to create a new address object group made up of those you want to have access. Refer to *SonicOS 6.5 Policies* for information on how to do that.
4. In the **Deny List**, select an option from the drop-down menu. This identified which MAC addresses that you deny access to.

   Choose **Create MAC Address Object Group** if you want to create a new address object group made up of those who should not have access. Refer to *SonicOS 6.5 Policies* for information on how to do that.
5. Click **OK** when done.

Virtual Access Points

The VAP Settings feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings. Virtual Access Points are configured from the **Connectivity | Wireless > Virtual Access Point** on the **MANAGE** view.



Virtual Access Points

Items 1 to 1 (of 1)

□	#	NAME	SSID	VlanID	Authentication	Cipher	Max Clients	SSID Suppr...	□ E...	Active	Configure
□	1	sonicwall-F575	sonicwall-F575	0	Both	None	16	□	☑	✓	

Topics:

- VAP General Settings
- VAP Advanced Settings

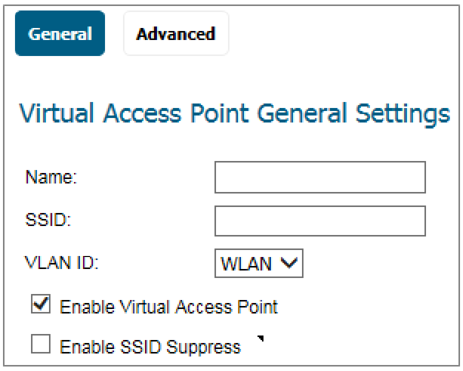
VAP General Settings

To define the Virtual Access Point General Settings:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Virtual Access Point**.

3 To edit an existing virtual access point, click the **Edit** icon for that access point. To create a new access point, click on **ADD** in the **Virtual Access Points** section.



Virtual Access Point General Settings

Name:

SSID:

VLAN ID: WLAN

☑ Enable Virtual Access Point

□ Enable SSID Suppress

4 In the **Name** field, create a friendly name for the access point.

5 In the **SSID** field, type in a unique name. This name a unique identifier attached to the packet header. It is case sensitive and can be up to 32 alphanumeric characters.

6 Select the **VLAN ID** from the drop-down menu.

7 Check the box to **Enable Virtual Access Point**.

8 Check the box to **Enable SSID Suppress** if you do not want your SSID to be seen by unauthorized wireless clients. When enabled, it suppresses the broadcasting of the SSID name and disables responses to probe requests.

9 Click **OK**.

VAP Advanced Settings

The **Advanced** option allows you to configure authentication and encryption settings for this virtual access point. The options listed are the same as those you define for a Virtual Access Point Profile.

To define the Virtual Access Point Advanced Settings:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Virtual Access Point**.

3 To edit an existing virtual access point, click the **Edit** icon for that access point. To create a new access point, click on **ADD** in the **Virtual Access Points** section.

4 Click **Advanced**.

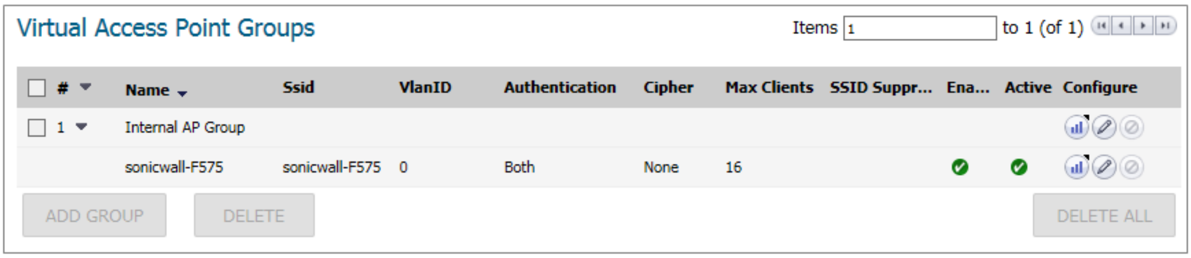
5 Under the heading **Virtual Access Point Advanced Settings**, choose a **Profile Name** from the drop-down menu. All the settings for that profile are auto-filled from the profile.

If you do not want to use a profile, leave the **Profile Name** set to **No Profile** and fill in the remaining fields as described in Virtual Access Point Profiles.

6 Click **OK**.

Virtual Access Point Groups

The Virtual Access Point Groups feature allows multiple VAP objects to be grouped and simultaneously applied to your internal wireless radio. Virtual Access Point Groups are configured from the **Connectivity | Wireless > Virtual Access Point** on the **MANAGE** view.



Virtual Access Point Groups

Items 1 to 1 (of 1)

□	#	Name	Ssid	VlanID	Authentication	Cipher	Max Clients	SSID Suppr...	Ena...	Active	Configure
□	1 ▾	Internal AP Group									
		sonicwall-F575	sonicwall-F575	0	Both	None	16		✓	✓	

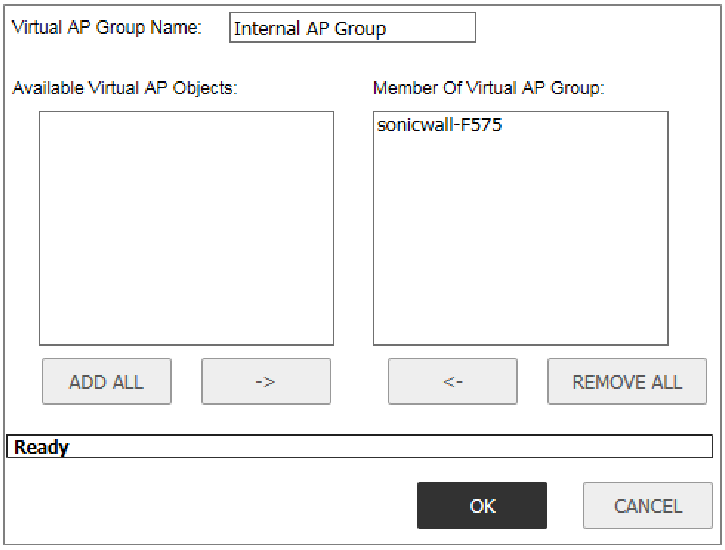
NOTE: Multiple virtual access points need to be set up before you can create a Virtual Access Point Group. If you have only one access point, it is automatically added to the default group Internal AP Group.

To create a Virtual Access Point Group:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Virtual Access Point**.

3 To edit an existing virtual access point group, click the **Edit** icon for that group.



Virtual AP Group Name: Internal AP Group

Available Virtual AP Objects:

Member Of Virtual AP Group: sonicwall-F575

Ready

4 To add an object to the group, select the object you want to add from the **Available Virtual AP Objects** list and click the right arrow.

5 To delete an object from the group, select the object you want to delete from the **Member of Virtual AP Group** list and click the left arrow.

6 Click **OK** when done.

Enabling the Virtual Access Point Group

After your virtual access points are configured and added to a VAP group, that group must be applied to the internal wireless radio and made available to the users.

To make the group available:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Base Settings**.

3 Scroll to **Wireless Virtual Access Point**.

4 In the **Virtual Access Point Group** field, select the **Internal AP Group** from the drop-down menu.

5 Click **ACCEPT** to up date the configuration.

Part 5

Connectivity | 3G/4G/Modem

36

3G/4G/Modem Overview

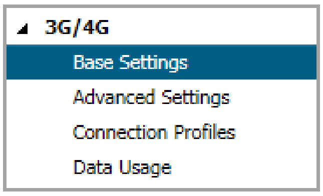
SonicWall network security appliances with a USB extension port can support either an external 3G/4G/LTE interface or analog modem interface.

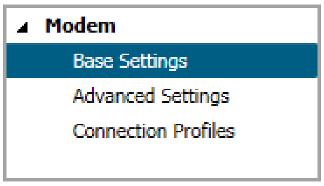
Topics:

- Device Detection and Selecting the Interface
- Understanding 3G/4G/LTE
- 3G/4G/LTE Prerequisites
- Enabling the U0/U1 Interface

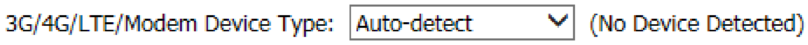
Device Detection and Selecting the Interface

By default, the appliance tries to detect the type of external interface that is connected. If it can successfully identify what kind it is, the left side navigation changes to show what was detected.





You can manually specify which type of interface you want to configure on the **Connectivity | 3G/4G/Modem > Base Settings** page.

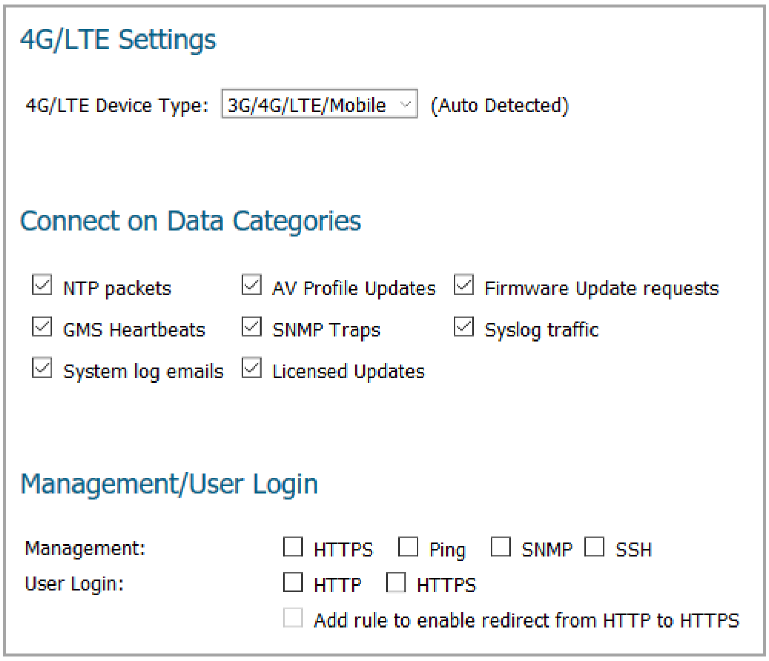


3G/4G/LTE/Modem Device Type: Auto-detect (No Device Detected)

The **3G/4G/LTE/Modem Device Type** drop-down menu provides these options:

- **Auto-detect** - Select this option and the appliance attempts to determine what kind of device is attached.
- **3G/4G/LTE/Mobile** - Select this option to manually configure a 3G/4G/LTE/Mobile interface.
- **Analog Modem** - Select this option to manually configure an analog modem interface.

When a device is connected after being detected or identified, the **Connectivity | 3G/4G/Modem > Base Settings** page displays configuration settings for it.



4G/LTE Settings

4G/LTE Device Type: 3G/4G/LTE/Mobile (Auto Detected)

Connect on Data Categories

☑ NTP packets ☑ AV Profile Updates ☑ Firmware Update requests

☑ GMS Heartbeats ☑ SNMP Traps ☑ Syslog traffic

☑ System log emails ☑ Licensed Updates

Management/User Login

Management: □ HTTPS □ Ping □ SNMP □ SSH

User Login: □ HTTP □ HTTPS

□ Add rule to enable redirect from HTTP to HTTPS

NOTE: A 3G/4G/LTE device can be connected/disconnected from the **MANAGE | System Setup | Network > Interfaces** page after clicking **MANAGE** for the U0 interface. See Enabling the U0/U1 Interface on page 310.

Understanding 3G/4G/LTE

SonicWall security appliances support 3G/4G/LTE Wireless WAN connections that utilize data connections over cellular networks. The 3G/4G/LTE connection can be used for:

- WAN Failover to a connection that is not dependent on wire or cable.
- Temporary networks where a preconfigured connection might not be available, such as at trade-shows and kiosks.
- Mobile networks, where the SonicWall appliance is based in a vehicle.
- Primary WAN connection where wire-based connections are not available and 3G/4G Cellular is.

To use the 3G/4G interface you must have a 3G/4G/LTE PC card or USB device and a contract with a wireless service provider. A 3G/4G/LTE service provider should be selected based primarily on the availability of supported hardware. SonicOS supports the devices listed online at: https://www.sonicwall.com/support/knowledge-base/?sol_id=170505473051240

SonicOS supports the following 3G/4G/LTE Wireless network providers (this list is subject to change):

- AT&T
- China Telecom
- H3G
- Orange
- Sprint PCS Wireless
- Telecom Italia Mobile
- Telefonica
- T-Mobile
- TDC Song
- Verizon Wireless
- Vodaphone

Topics:

- 3G/4G/LTE Connection Types
- SonicWave MiFi Extender
- 3G/4G/LTE Failover

3G/4G/LTE Connection Types

When the 3G/4G/LTE device is installed prior to starting the appliance, the device is listed in the Interface Settings table at **System Setup | Network > Interfaces** on the **MANAGE** view. The interface name is listed as **U0** or **U1** in the name column.

The 3G/4G/LTE Connection Types setting provides flexible control over WAN connectivity on SonicWall appliances with 3G/4G/LTE interfaces. The Connection Type is configured when you edit the profile on **Connectivity | 3G/4G > Connection Profiles.** The following connection types are offered on the **Parameters** tab of the 3G/4G Profile Configuration window:

- **Persistent Connection** – After the 3G/4G interface is connected to the 3G/4G service provider, it remains connected until the administrator disconnects it or a network event (such as the WAN becoming available) causes it to disconnect.
- **Connect on Data** – The 3G/4G interface connects automatically when the SonicWall appliance detects specific types of network traffic.
- **Manual Connection** – The 3G/4G interface is connected only when the administrator manually initiates the connection.

> △ CAUTION: **Although the 3G/4G connection can be manually enabled on the System Setup | Network > Interfaces page (by clicking MANAGE for the U0/U1 interface), this is not recommended; it can cause automatic connections to not function as expected. SonicWall recommends governing the 3G/4G interface using the connection types described previously.**

SonicWave MiFi Extender

In SonicOS 6.5, the SonicWave 3G/4G/LTE MiFi Extender feature allows SonicWall wireless access points to connect to 3G or 4G cellular networks to create a wireless hot spot that can be shared among mobile devices such as smart phones, laptops, and tablets. This WWAN solution allows multiple end users and mobile devices to share a 3G or 4G mobile broadband Internet connection.

To use this feature, plug a USB device into the SonicWave access point and it connects to the Internet over 3G/4G. In SonicOS, you bind a VLAN Interface to the USB modem.

This feature is supported on all SonicWall firewalls running SonicOS 6.5 and all SonicWave and access points with USB interfaces. A USB device that supports 3G, 4G, or the QMI protocol is required.

Use the following settings for the VLAN configuration:

- Set the Zone to WAN.
- Set the parent interface to the physical interface to which access points are connected.
- For a 3G USB modem, the IP Assignment should be Static, and assign a private IP address to it. Leave the gateway and DNS servers fields blank; they are filled automatically after the provisioning for the access point is completed.
- For 4G and QMI Modem, the IP Assignment should be DHCP. It gets the DHCP lease from the USB modem server after the modem is connected.

This feature uses 3G/4G connection profile settings configured on the MiFi Extender configuration page.

3G/4G/LTE Failover

IMPORTANT: You can manage the failover behavior of the 3G/4G/LTE device when the primary WAN interface goes down. For the 3G/4G/LTE interface to function as a backup interface, it can be configured as the Final Backup interface in the default load balancing group. Go to the **System Setup | Network > Failover & Load Balancing** page, and edit the group that contains the 3G/4G/LTE device.

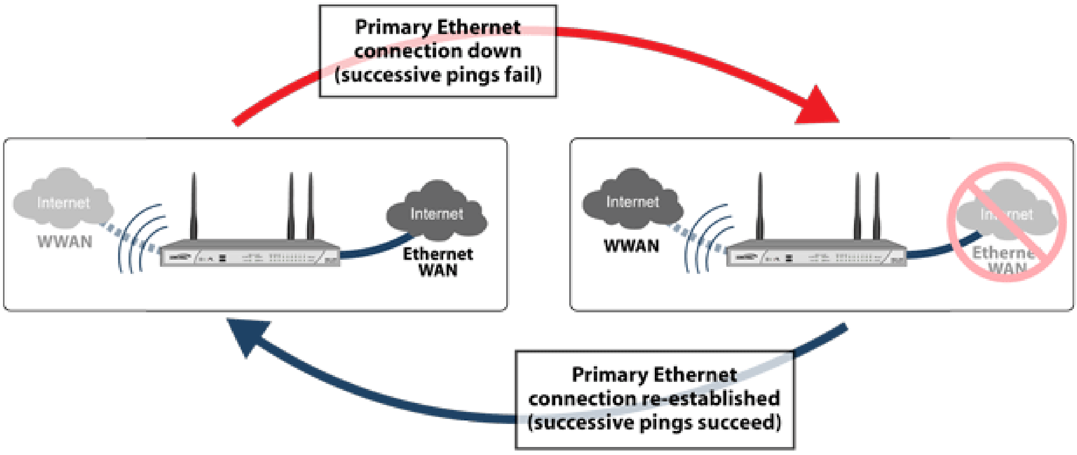
The following sections describe the three different methods of WAN-to-3G/4G/LTE failover. All of these sections assume that the U0/U1 interface is configured as the Final Backup interface in the load balancing group.

- 3G/4G/LTE Failover with Persistent Connection
- 3G/4G/LTE Failover with Connect on Data
- Manual Dial 3G/4G/LTE Failover

3G/4G/LTE Failover with Persistent Connection

The following figure depicts the sequence of events when the WAN Ethernet connection fails and the 3G/4G/LTE Connection Profile is configured for **Persistent Connection**.

3G/4G Failover Sequence of Events: Persistent Connection


Primary Ethernet connection down (successive pings fail)
Internet
WWAN
Internet
Ethernet WAN
Internet
WWAN
Internet
Ethernet WAN
Primary Ethernet connection re-established (successive pings succeed)

1 **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. The U0/U1 interface is never connected while the Ethernet WAN interface is available.

2 **Primary Ethernet connection fails** – The U0/U1 interface is initiated and remains in an *always-on* state while the Ethernet WAN connection is down.

If another Ethernet WAN interface is configured as part of the load balancing group, the appliance first fails over to the secondary Ethernet WAN before failing over to the U0/U1 interface. In this situation, failover to the U0/U1 interface only occurs when both the primary and secondary WAN paths are unavailable.

3 **Reestablishing Primary Ethernet Connectivity After Failover** – When the Ethernet WAN connection (either the primary WAN port or the secondary WAN port, if so configured) becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. This includes active connections and VPN connections. The U0/U1 interface connection is closed.

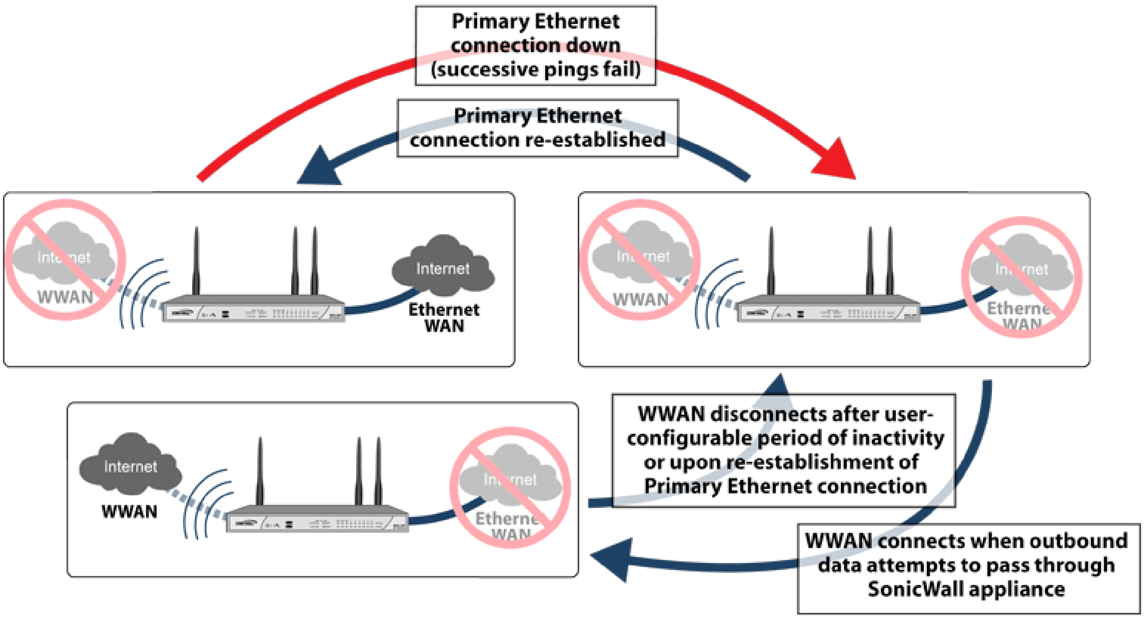
ⓘ **NOTE:** If the 3G/4G/LTE is configured as an Alternate WAN, even if **Preempt and failback to preferred interfaces when possible** is unchecked (**System Setup | Network > Edit Default LB Group**), the U0 connection disconnects when the Ethernet WAN becomes available.

△ CAUTION: **Do not configure a policy-based route that uses the U0/U1 interface when the U0/U1 interface is configured and up as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1 interface, the connection remains up until the Maximum Connection Time (if configured) is reached.**

3G/4G/LTE Failover with Connect on Data

The following illustration depicts the sequence of events that occur when the WAN Ethernet connection fails and the 3G/4G/LTE Connection Profile is configured for **Connect on Data**.

3G/4G Failover Sequence of Events: Connect on Data



Primary Ethernet connection down (successive pings fail)
Primary Ethernet connection re-established
Internet
WWAN
Internet
Ethernet WAN
Internet
WWAN
Internet
Ethernet WAN
WWAN disconnects after user-configurable period of inactivity or upon re-establishment of Primary Ethernet connection
Internet
WWAN
Internet
Ethernet WAN
WWAN connects when outbound data attempts to pass through SonicWall appliance

1 **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. 3G/4G/LTE is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies the U0/U1 interface as the destination interface).

2 **Primary Ethernet Connection Fails** – The U0/U1 interface connection is not established until outbound data attempts to pass through the SonicWall appliance.

3 **3G/4G Connection Established** – The U0/U1 interface connection is established when the device or a network node attempts to transfer data to the Internet. The U0/U1 interface stays connected until the Maximum Connection Time (if configured) is reached.

4 **Reestablishing WAN Ethernet Connectivity After Failover** – When an Ethernet WAN connection becomes available again or the inactivity timer (if configured) is reached, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. The U0/U1 interface connection is terminated.

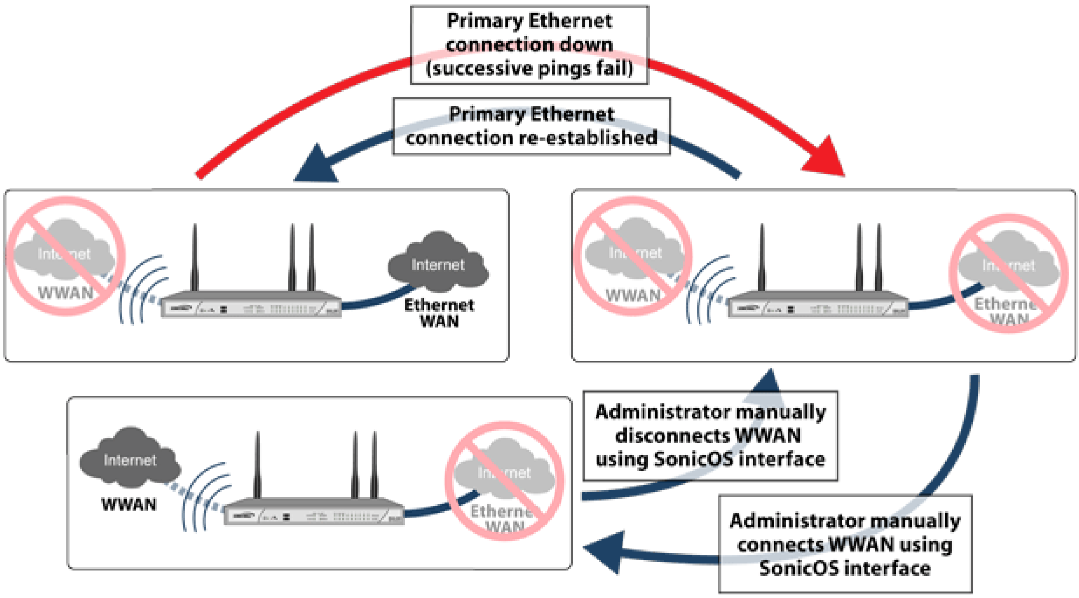
ⓘ **NOTE:** If the 3G/4G/LTE is configured as an Alternate WAN, even if **Preempt and failback to preferred interfaces when possible** is unchecked (**System Setup | Network > Edit Default LB Group**), the U0 connection disconnects when the Ethernet WAN becomes available.

△ CAUTION: **Do not configure a policy-based route that uses the U0/U1 interface when the U0/U1 interface is configured and up as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1 interface, the connection remains up until the Maximum Connection Time (if configured) is reached.**

Manual Dial 3G/4G/LTE Failover

△ CAUTION: **SonicWall does not recommend using a Manual Dial 3G/4G Connection Profile when the U0/U1 interface is intended to be used as a failover backup for the primary WAN interface. During a WAN failure the appliance loses WAN connectivity until the U0/U1 interface connection is manually initiated by the administrator. The following illustration depicts the sequence of events that occur when the WAN Ethernet connection fails, and the 3G/4G Connection Profile is configured for Manual Dial.**

3G/4G Failover Sequence of Events: Manual Dial


Primary Ethernet connection down (successive pings fail)
Primary Ethernet connection re-established
Internet
WWAN
Internet
Ethernet WAN
Internet
WWAN
Internet
Ethernet WAN
Administrator manually disconnects WWAN using SonicOS interface
Internet
WWAN
Internet
Ethernet WAN
Administrator manually connects WWAN using SonicOS interface

1 **Primary Ethernet Connection Available** - The Ethernet WAN is connected and used as the primary connection. 3G/4G/LTE is never connected while the Ethernet WAN connection is available.

2 **Primary Ethernet Connection Fails** - The U0/U1 interface connection is not established until the administrator manually enables the connection.

3 **3G/4G Connection Established** – A U0/U1 interface connection is established when the administrator manually enables the connection on the SonicWall appliance. The U0/U1 interface stays connected until you manually disable the connection.

4 **Reestablishing WAN Ethernet Connectivity After Failover** – Regardless of whether an Ethernet connection becomes available again, **all LAN-to-WAN traffic will still use the manually enabled 3G/4G connection** until the connection is manually disabled by you. After a manual disconnect, the available Ethernet connection is used.

3G/4G/LTE Prerequisites

Before configuring the 3G/4G/LTE interface, you must complete the following prerequisites:

- Purchase a 3G/4G/LTE service plan from a supported third-party wireless provider.
- Configure and activate your 3G/4G/LTE device.
- Insert the 3G/4G/LTE device into the SonicWall appliance **before** powering on the SonicWall security appliance.

  > ⓘ **IMPORTANT:** The 3G/4G/LTE device should only be inserted or removed when the SonicWall security appliance is powered off.

Enabling the U0/U1 Interface

When a 3G/4G/LTE USB modem is connected to a SonicWall security appliance, SonicOS detects the model and displays a U0 interface in the **MANAGE | System Setup | Network > Interfaces** page. This interface belongs to the WAN zone by default and can be used for Failover and Load Balancing. The U0 configuration settings include the device type, Connect on Data categories, and management/user login options. The U0 interface also provides a **MANAGE** button for accessing the Connection Manager.

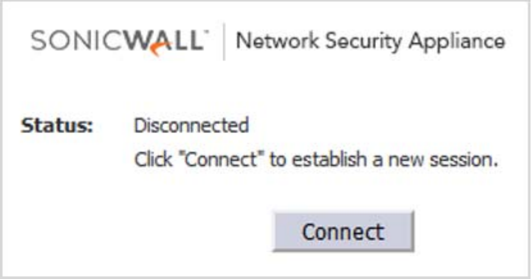
To use the modem, one needs to connect the USB device to the network by clicking **Connect** in the Connection Manager. Before the connection is established, U0's Connection Manager status is *Disconnected*.

> ⓘ **NOTE:** For all 3G/4G/LTE USB devices, a 3G/4G profile must be created before clicking **Connect**.

> △ CAUTION: **Repeatedly manually enabling the 3G/4G/LTE connection on the Network > Interfaces page (by clicking MANAGE for the U0/U1 interface) is not recommended. This can cause automatic connections to not function as expected. SonicWall recommends governing the 3G/4G/LTE interface using the connection types described in 3G/4G/LTE Connection Types.**

To manually initiate a connection on the U0/U1 external 3G/4G/LTE interface:

1 On the **Network > Interfaces** page, click **MANAGE** for the U0/U1 interface. The **U0/U1 Connection Status** dialog displays.

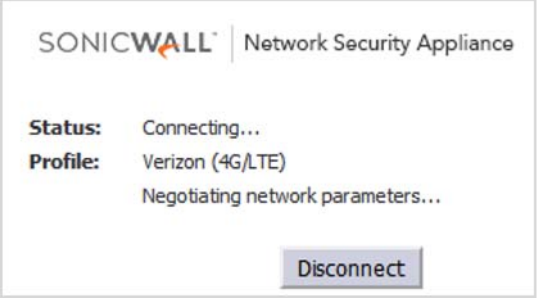


SONICWALL | Network Security Appliance

Status: Disconnected

Click "Connect" to establish a new session.

2 Click **Connect**. The WAN interface address and DNS address are assigned by the ISP's DHCP server. SonicOS uses this DHCP IP address for the U0 interface IP address.



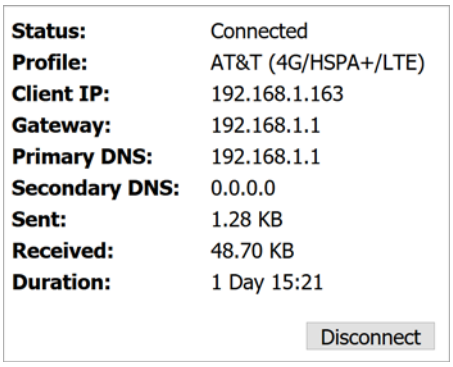
SONICWALL | Network Security Appliance

Status: Connecting...

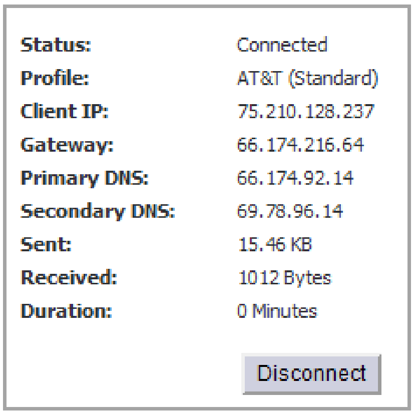
Profile: Verizon (4G/LTE)

Negotiating network parameters...

When the connection is active, the **U0/U1 Connection Status** (Connection Manager) displays statistics on the session. Images for a 4G/LTE device and a 3G (PPP) device are shown as follows.



Status:	Connected
Profile:	AT&T (4G/HSPA+/LTE)
Client IP:	192.168.1.163
Gateway:	192.168.1.1
Primary DNS:	192.168.1.1
Secondary DNS:	0.0.0.0
Sent:	1.28 KB
Received:	48.70 KB
Duration:	1 Day 15:21



Status:	Connected
Profile:	AT&T (Standard)
Client IP:	75.210.128.237
Gateway:	66.174.216.64
Primary DNS:	66.174.92.14
Secondary DNS:	69.78.96.14
Sent:	15.46 KB
Received:	1012 Bytes
Duration:	0 Minutes

NOTE: The DNS server address 192.168.1.1 is a temporary IP address. This address is the default internal DNS server address. Because this address might cause an IP address conflict, it cannot be used in SonicOS as a DNS server address. In the case of ATT Velocity/Huawei E3372 LTE devices, the device does not provide an AT command interface for fetching the real DNS server information. However, the LTE modem's internal web server has a valid DNS server. An HTTP communication channel is initiated by SonicOS to retrieve this valid DNS server address.

3 To end the connection, click **Disconnect**.

37

Configuring 3G/4G/Modem Base Settings

The first step to configuring a 3G/4G/LTE device or a modem is to define the Base Settings. As noted in 3G/4G/Modem Overview, the appliance tries to detect the type of device that is connected. If it can successfully identify the type, the left side navigation and the configuration pages change to show what was detected. Refer to Device Detection and Selecting the Interface if you want to manually select the device.

The following base settings need to be defined:

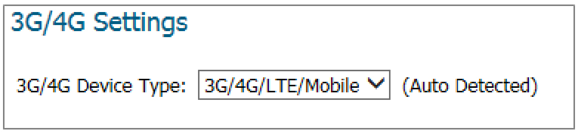
For 3G/4G/LTE Devices	For Modems
3G/4G/LTE Settings	Modem Settings
Connect on Data Categories	Connect on Data Categories
Management/User Login	Management/User Login

Topics:

- Settings
- Connect on Data Categories
- Management/User Login
- MiFi Extender Settings

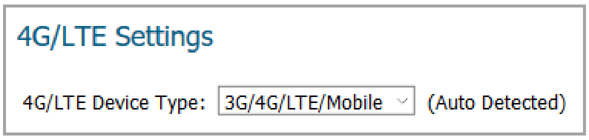
Settings

For the instructions provided in this section, the device has either been auto-detected by the appliance or it has been manually set. The following images show examples where the 3G/4G/LTE Device Type was auto-detected:



3G/4G Settings

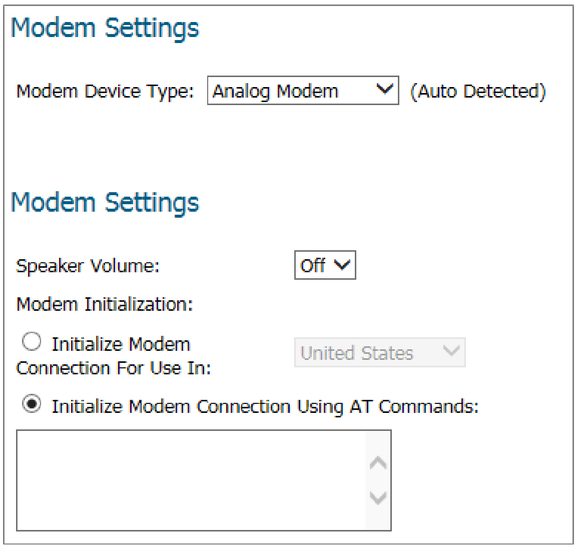
3G/4G Device Type: 3G/4G/LTE/Mobile (Auto Detected)



4G/LTE Settings

4G/LTE Device Type: 3G/4G/LTE/Mobile (Auto Detected)

This shows the same options for a modem. Note that there are two Modem Settings sections. The first one shows that the modem was auto-detected. The second one has options that needs to be set.



Modem Settings

Modem Device Type: Analog Modem (Auto Detected)

Modem Settings

Speaker Volume: Off

Modem Initialization:

○ Initialize Modem Connection For Use In: United States

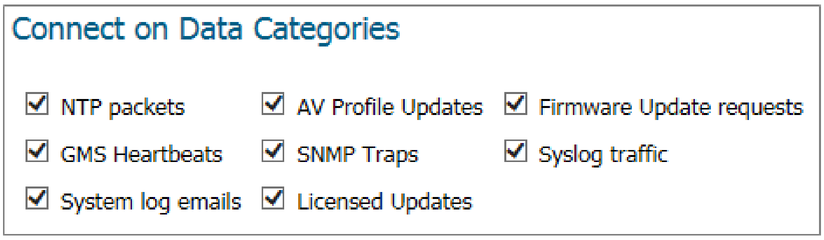
● Initialize Modem Connection Using AT Commands:

The **Modem Settings** section must be configured to enable management of the SonicWall appliance over the modem interface.

- **Speaker Volume** – Choose whether the speaker is **On** or **Off** (default).
- **Modem Initialization** – Choose one of the following options:
  - **Initialize Modem Connection For Use In** – Select the country from the drop-down menu.
  - **Initialize Modem Connection Using AT Commands** – Enter the appropriate AT commands in the field.

Connect on Data Categories

The **Connect on Data Categories** section displays if you select **3G/4G/LTE/Mobile** or **Analog Modem** as the device type. These settings allow you to configure the interface to automatically connect to the service provider when the SonicWall appliance detects specific types of traffic. The **Connect on Data Categories** are all selected by default.



Connect on Data Categories

☑ NTP packets ☑ AV Profile Updates ☑ Firmware Update requests

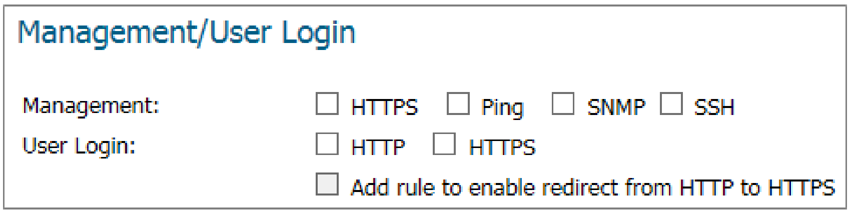
☑ GMS Heartbeats ☑ SNMP Traps ☑ Syslog traffic

☑ System log emails ☑ Licensed Updates

To configure the SonicWall appliance for Connect on Data operation, you must select **Connect on Data** as the **Connection Type** for the Connection Profile. Refer to Configuring 3G/4G/Modem Connection Profiles for more details.

Management/User Login

The **Management/User Login** section displays if you select **3G/4G/LTE/Mobile** or **Analog Modem** as the device type. The **Management/User Login** section must be configured to enable remote management of the SonicWall appliance over the interface.



Management/User Login

Management: □ HTTPS □ Ping □ SNMP □ SSH

User Login: □ HTTP □ HTTPS

□ Add rule to enable redirect from HTTP to HTTPS

In the **Management** field select any or all of the supported protocol(s): **HTTPS, Ping, SNMP**, **SSH**.

NOTE: Some ISPs do not allow HTTPS or Ping management on an IP address provided by the ISP.

In the **User Login** field **s**elect **HTTP** or **HTTPS** or both. However, remember that HTTP traffic is less secure than HTTPS.

If you select HTTPS for **Management** and/or **User Login**, the **Add rule to enable redirect from HTTP to HTTPS** option is selected automatically. If this option is enabled, the firewall converts HTTP requests automatically to HTTPS requests for added security. If you do not want the conversion, deselect the option.

NOTE: In previous releases of SonicOS, probe monitoring for the 3G/4G interface was configured on the **3G/4G > Settings** page. Now, probe monitoring is configured on the **System Setup | Network > Failover & Load Balancing** page. Refer to *SonicOS 6.5 System Setup* for more information.

MiFi Extender Settings

The 3G/4G/LTE MiFi Extender feature allows SonicWall SonicWave access points to connect to 3G or 4G cellular networks to create a wireless hot spot. Multiple end users and mobile devices can share a 3G or 4G mobile broadband Internet connection.

To use this feature, plug a USB device into the SonicWave access point. In SonicOS, you bind a VLAN Interface to the USB modem.

To configure the access point:

1. In the **MANAGE** view, navigate to **Connectivity | Access Points > Base Settings**.
2. Under **SonicPoint / SonicWave Objects**, click **Configure** for the access point you wish to use.
3. Click **3G/4G/LTE WWAN**.

   NOTE: You can click **3G/4G/LTE WWAN WIZARD** at the bottom of this page to have the wizard assist you in creating or selecting a VLAN interface and a 3G/4G/LTE connection profile.

4. Select **Enable 3G/4G/LTE Modem**.
5. Select the VLAN you created for the USB device from the **Bound to WAN VLAN Interface** drop-down menu.
6. To use a specific connection profile, select **Enable Connection Profile** and fill in the related fields. In many cases, the default connection profile can be used, in which case this step is optional.
7. Click **OK**.

The settings are pushed to the access point. You can view basic status in the **MANAGE** view on the **Connectivity | Access Points > 3G/4G/LTE WWAN** page.

When multiple access points and 3G/4G modems (at least two for each) are available, SonicOS can make use of them simultaneously and perform load balancing among them. First, assign a unique VLAN to each SonicPoint and modem pair. Then add these VLAN interfaces to a LB group on the **System Setup | Network > Failover & Load Balancing** page.

38

Configuring 3G/4G/Modem Advanced Settings

The **Advanced Settings** page is used to configure the following features for both 3G/4G/LTE devices and modems:

- Remotely Triggered Dial-Out Settings
- Bandwidth Management
- Connection Limit

Remotely Triggered Dial-Out Settings

The **Remotely Triggered Dial-Out** section enables you to remotely initiate a WAN modem connection. The following process describes how a Remotely Triggered Dial-Out call functions:

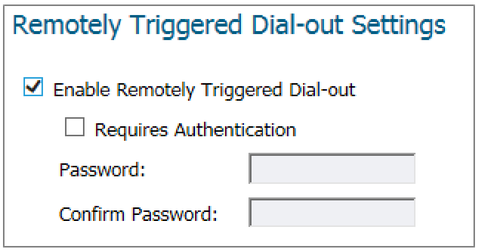
1. The network administrator initiates a modem connection to the SonicWall security appliance located at the remote office.
2. If the appliance is configured to authenticate the incoming call, it prompts the network administrator to enter a password. After the call is authenticated, the appliance terminates the call.
3. The appliance then initiates a modem connection to its dial-up ISP, based on the configured dial profile.
4. You access the appliance’s web management interface to perform the required tasks.

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The 3G/4G connection profile is configured for **dial-on-data**.
- The SonicWall Security Appliance is configured to be managed using **HTTPS**, so that the device can be accessed remotely.
- Although not required, you should enter a value in the **Enable Inactivity Disconnect** field. This field is located in the **Profile Configuration > Parameters** page. Access this by editing the profile for the device. If you do not enter a value in this field, dial-out calls remain connected indefinitely, and you have to manually terminate sessions by clicking **Disconnect**.

To configure Remotely Triggered Dial-Out:

1. On the **MANAGE** view, navigate to the **Advanced** page:
   - **Connectivity | 3G/4G > Advanced Settings**
   - **Connectivity | Modem > Advanced Settings**



Remotely Triggered Dial-out Settings

☑ Enable Remotely Triggered Dial-out

☐ Requires Authentication

Password:

Confirm Password:

2. Select **Enable Remotely Triggered Dial-Out**.
3. If you want to require authentication on the remote connection, check the box for **Requires Authentication** and type the password in the **Password** and **Confirm Password** fields.
4. Click **ACCEPT** to save your settings.

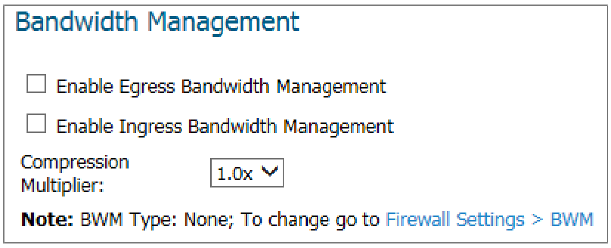
Bandwidth Management

The **Bandwidth Management** section allows you to enable egress or ingress bandwidth management services on the 3G/4G interface.

NOTE: For information on configuring Bandwidth Management, refer to **Firewall Settings** in *SonicOS 6.5 Security Configuration*.

To configure bandwidth management:

1. On the **MANAGE** view, navigate to the **Advanced** page:
   - **Connectivity | 3G/4G > Advanced Settings**
   - **Connectivity | Modem > Advanced Settings**



Bandwidth Management

☐ Enable Egress Bandwidth Management

☐ Enable Ingress Bandwidth Management

Compression Multiplier: 1.0x

Note: BWM Type: None; To change go to Firewall Settings > BWM

2. Check the box to **Enable Egress Bandwidth Management**.
3. Check the box to **Enable Ingress Bandwidth Management**.
4. Select the **Compression Multiplier** from the drop-down menu:

   1.0x (default), **1.5x 2.0x**, **2.5x**, **3.0x**, **3.5x**, **4.0x**

   The Compression Multiplier applies to both egress and ingress bandwidths.
5. Click **ACCEPT** to save your settings.

The note under Bandwidth Management, also tells you what bandwidth management type was selected and provides a link to change it if you want.

Connection Limit

The **Connection Limit** section allows you to set a host/node limit on the 3G/4G or modem connection. This feature is especially useful for deployments where the device is used as an overflow or in load-balanced situations to avoid over-taxing the connection.

In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is **0**, which allows an unlimited number of nodes.

39

Configuring 3G/4G/Modem Connection Profiles

Use the **Connection Profiles** page to configure 3G/4G/LTE and modem connection profiles. You can also set the primary and alternate profiles.

Topics:

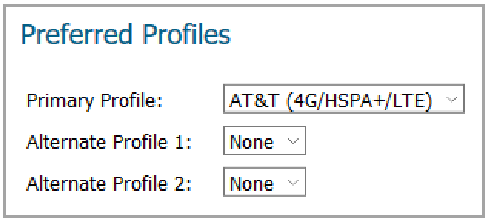
- Preferred Profiles
- Connection Profiles

Preferred Profiles

To set the preferred profiles:

1 On the **MANAGE** view, navigate to the **Connection Profiles** page:

- **Connectivity | 3G/4G > Connection Profiles**
- **Connectivity | Modem > Connection Profiles**

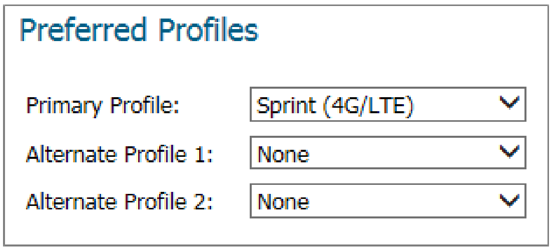


Preferred Profiles

Primary Profile: AT&T (4G/HSPA+/LTE)

Alternate Profile 1: None

Alternate Profile 2: None



Preferred Profiles

Primary Profile: Sprint (4G/LTE)

Alternate Profile 1: None

Alternate Profile 2: None

2 In the **Preferred Profiles** section, select the **Primary Profile** from the drop-down menu.

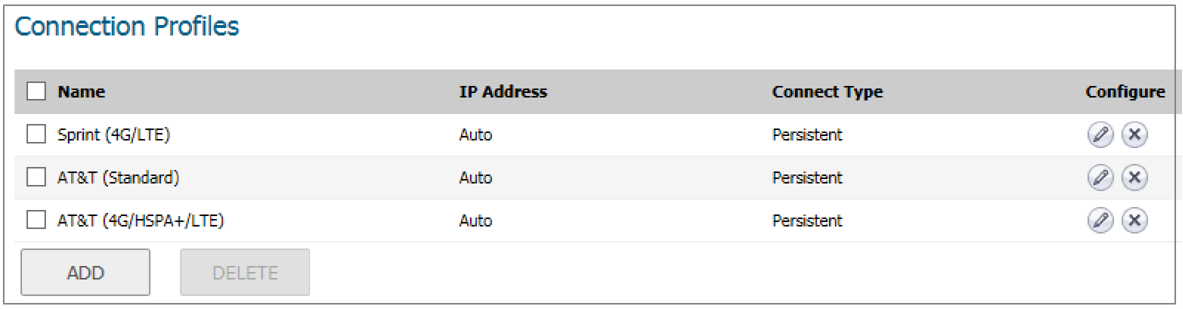
> ⓘ | **NOTE:** The options for modems are different than those listed for 3G/4G/LTE devices.

3 If wanted, select up **Alternate Profile 1** and **Alternate Profile 2** from the drop-down menus.

4 Click **ACCEPT** so save your settings.

Connection Profiles

To create a connection profile, click **ADD**, or to edit an existing click the **Edit** icon in the **Configuration** column of the table.



Connection Profiles

□ Name	IP Address	Connect Type	Configure
□ Sprint (4G/LTE)	Auto	Persistent	
□ AT&T (Standard)	Auto	Persistent	
□ AT&T (4G/HSPA+/LTE)	Auto	Persistent	

Perform the steps in the following sections:

For Modems:	For 3G/4G Devices:	For LTE Devices
General Settings	General Settings	General Settings
ISP Address		
Parameters Settings	Parameters Settings	Parameters Settings
	IP Address Settings	IP Address Settings
Schedule Settings	Schedule Settings	Schedule Settings
	Data Limiting	Data Limiting
Advanced	Advanced	

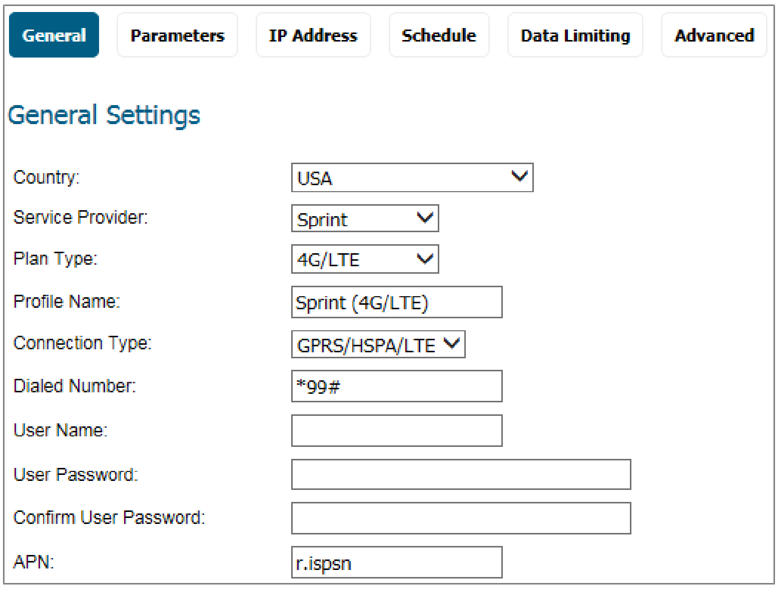
NOTE: Depending on your selection for **3G/4G/Modem Device Type** in the **Base Settings** page, not all options might be available.

General Settings

When you add or update a Connection Profile, the default view shows the **General Settings** to configure for the service provider. After selecting your country, service provider, and plan type, the rest of the fields are automatically field for most service providers.

To configure general connection settings:

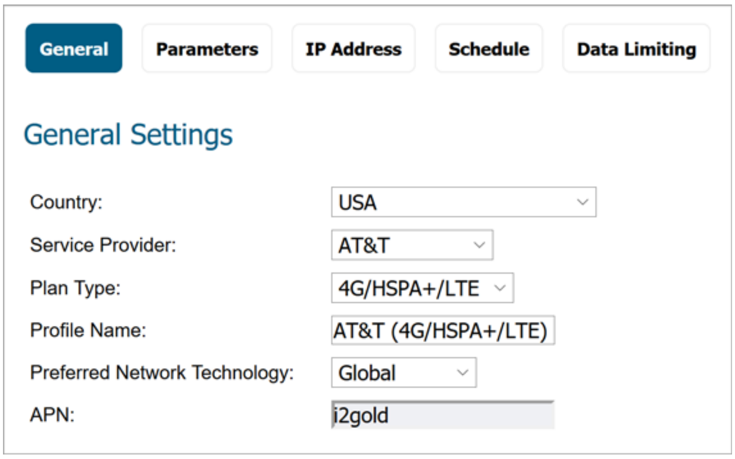
PPP Modem Settings



General Settings

Country:	USA
Service Provider:	Sprint
Plan Type:	4G/LTE
Profile Name:	Sprint (4G/LTE)
Connection Type:	GPRS/HSPA/LTE
Dialed Number:	*99#
User Name:	
User Password:	
Confirm User Password:	
APN:	r.ispsn

LTE Modem Settings



General Settings

Country:	USA
Service Provider:	AT&T
Plan Type:	4G/HSPA+/LTE
Profile Name:	AT&T (4G/HSPA+/LTE)
Preferred Network Technology:	Global
APN:	i2gold

1 Select the **Country** where the SonicWall appliance is deployed.

2 Select the **Service Provider** that you created an account with.

ⓘ **NOTE:** Only service providers supported in the country you selected are displayed.

3 From the **Plan Type** drop-down menu, select the plan you subscribed to. If your specific plan type is:

- Listed in the drop-down menu (many basic plans are labeled simply as **standard**), the rest of the fields in the **General** tab are automatically provisioned. Verify that these fields are correct, and then skip to Parameters Settings.
- Not listed in the drop-down menu, select **Other**.

4 Enter a name for the profile in the **Profile Name** field.

5 For an LTE modem, select the **Preferred Network Technology**. Choose from:

- **Global**
- **LTE/CDMA**
- **GSM/UMTS**

6 For an LTE modem, enter the **APN** value.

7 For a PPP modem, verify that the appropriate **Connection Type** is selected.

> **NOTE:** This field is automatically provisioned for most service providers.

8 For a PPP modem, verify that the **Dialed Number** is correct.

> **NOTE:** The dialed number is ***99#** for most Service Providers.

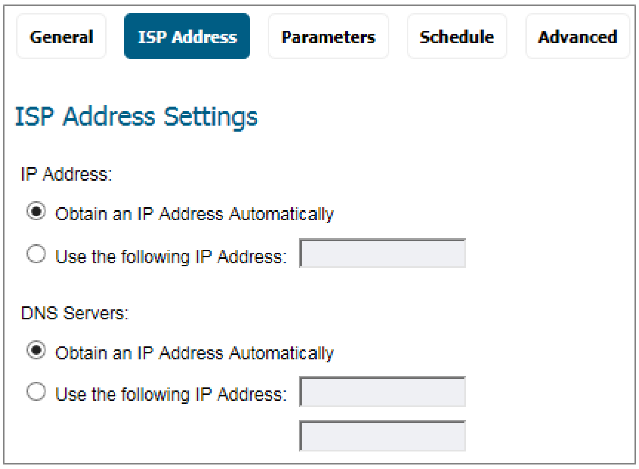
9 For a PPP modem, enter your username and password in the **User Name**, **User Password**, and **Confirm User Password** fields, respectively, if required by your provider.

ISP Address

The ISP Address settings are shown for modems only. This allows you to define how the modem communicates with the rest of your infrastructure.

To configure the ISP Address:

1 Select **ISP Address**.



ISP Address Settings

IP Address:

● Obtain an IP Address Automatically

○ Use the following IP Address:

DNS Servers:

● Obtain an IP Address Automatically

○ Use the following IP Address:

2 Under **IP Address**, choose one of the following:

- **Obtain an IP Address Automatically**
- **Use the following IP Address** and type the address in the field.

3 Under **DNS Servers**, choose one of the following:

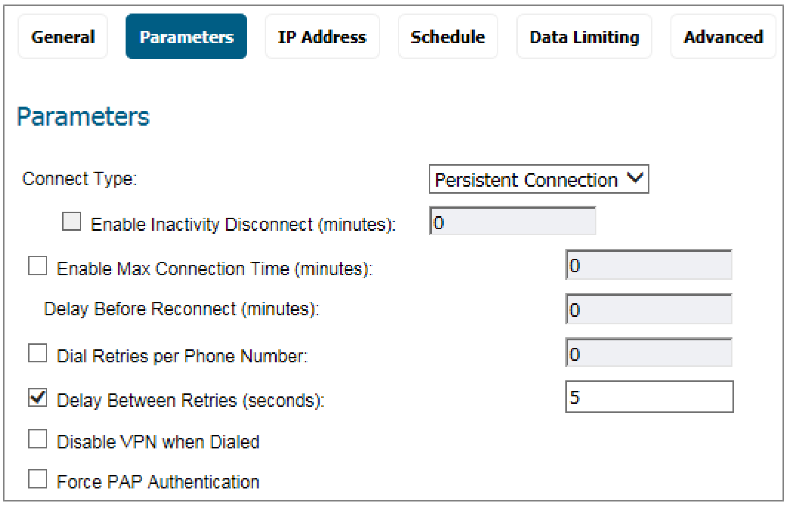
- **Obtain an IP Address Automatically**
- **Use the following IP Address** and type a primary address in the first field and a secondary address in the next field.

Parameters Settings

The **Parameters** settings allows you to define conditions under which the service connects. The three connection types are **Persistent Connection, Connect on Data**, and **Manual Connection**. The mechanics of these connection types are described in Understanding 3G/4G/LTE.

To configure the Parameter settings:

1 Click **Parameters**.



Parameters

Connect Type: Persistent Connection

□ Enable Inactivity Disconnect (minutes): 0

□ Enable Max Connection Time (minutes): 0

Delay Before Reconnect (minutes): 0

□ Dial Retries per Phone Number: 0

☑ Delay Between Retries (seconds): 5

□ Disable VPN when Dialed

□ Force PAP Authentication

2 In the **Connection Type** drop-down menu, select whether the connection profile is a **Persistent Connection**, **Connect on Data**, or **Manual Connection**.

> **NOTE:** To configure the SonicWall appliance for remotely triggered dial-out, the **Connection Type** must be **Connect on Data**.

3 Check the box to **Enable Inactivity Disconnect (minutes)** and enter the number of minutes a connection can be inactive before it is disconnected. Note that this option is not available if the **Connection Type** is **Persistent Connection**.

4 Check the box to **Enable Max Connection Time (minutes)** and enter the number of minutes the connection stays connected, whether the session is inactive or not.

5 Enter a value in the **Delay Before Reconnect (minutes)** to have the SonicWall appliance automatically reconnect after the specified number of minutes.

6 Check the **Dial Retries per Phone Number** box and enter a number in the field to specify the number of times the SonicWall appliance is to attempt to reconnect.

7 Check the **Delay Between Retries (seconds)** box and enter a number in the field to specify the number of seconds between retry attempts.

8 Select **Disable VPN when Dialed** to disable VPN connections over the 3G/4G interface.

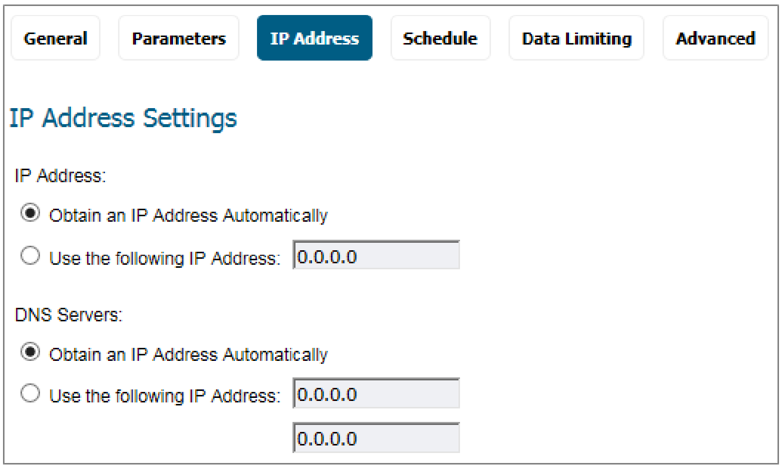
9 Check the box to **Force PAP Authentication**.

IP Address Settings

Use **IP Address Settings** to configure dynamic or static IP addressing for a 3G/4G/LTE interface. In most cases, you want to **Obtain an IP Address Automatically**; however, you can configure manual IP addresses for both your gateway IP address and one or more DNS server IP addresses if this is required by your service provider.

To configure IP addressing:

1 Select **IP Address**.



IP Address Settings

IP Address:

● Obtain an IP Address Automatically

○ Use the following IP Address: 0.0.0.0

DNS Servers:

● Obtain an IP Address Automatically

○ Use the following IP Address: 0.0.0.0

0.0.0.0

By default, 3G/4G connection profiles are configured to obtain IP addresses and DNS server addresses automatically.

2 To specify a static IP address, select the **Use the following IP Address** radio box and enter the IP address in the field.

3 To manually enter DNS server addresses, select **Use the following IP Address** and enter the IP addresses of the primary and secondary DNS servers in the fields.

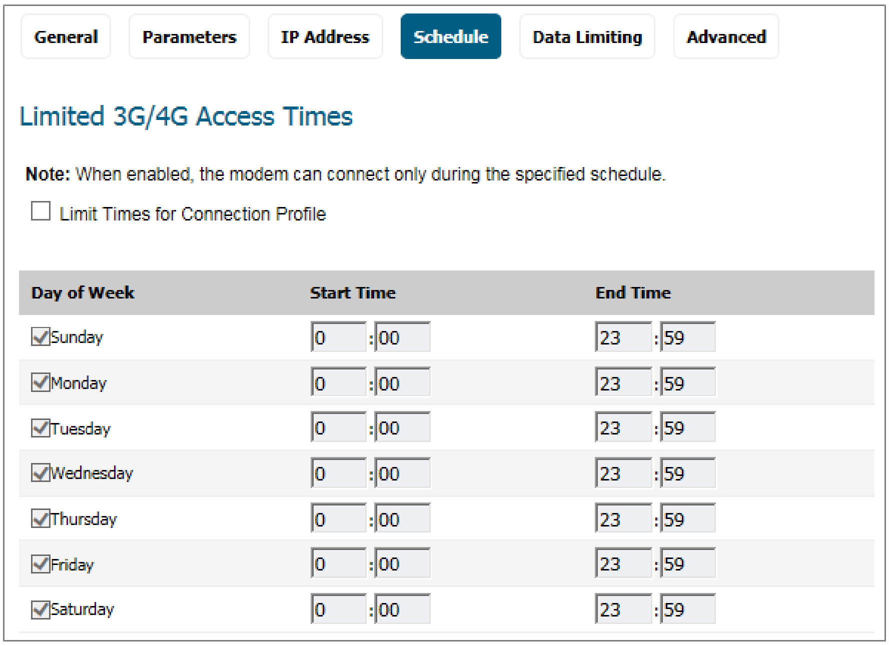
Schedule Settings

Use **Schedule** to limit connections to specified times during specific days of the week. This feature is useful for data plans where access is limited during certain times of day, such as plans with free night/weekend minutes.

NOTE: When this feature is enabled, if the checkbox for a day is **not** selected, 3G/4G/LTE access is denied for that entire day.

To configure an access schedule:

1 Click **Schedule**.



Limited 3G/4G Access Times

Note: When enabled, the modem can connect only during the specified schedule.

☐ Limit Times for Connection Profile

Day of Week	Start Time	End Time
☑ Sunday	0 : 00	23 : 59
☑ Monday	0 : 00	23 : 59
☑ Tuesday	0 : 00	23 : 59
☑ Wednesday	0 : 00	23 : 59
☑ Thursday	0 : 00	23 : 59
☑ Friday	0 : 00	23 : 59
☑ Saturday	0 : 00	23 : 59

2 Select **Limit Times for Connection Profile** to enable the scheduling feature for this interface.

3 Select the checkbox for each **Day of Week** you wish to allow access on.

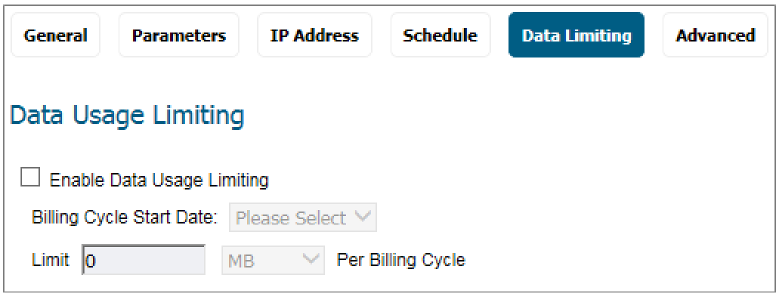
4 Enter the desired **Start Time** and **End Time** (in 24-hour format) for each day of the week.

Data Limiting

Data Limiting is only available for 3G/4G/LTE devices. Use it to limit data usage on a monthly basis. This feature gives you the ability to track usage based on your 3G/4G/LTE provider's billing cycle and disconnect when a given limit is reached.

To limit data usage:

1 Click on **Data Limiting**.



Data Usage Limiting

□ Enable Data Usage Limiting

Billing Cycle Start Date: Please Select

Limit 0 MB Per Billing Cycle

ⓘ **TIP:** If your 3G/4G/LTE account has a monthly data or time limit, enabling Data Usage Limiting is strongly recommended.

2 Check the box to **Enable Data Usage Limiting** and have the 3G/4G/LTE interface become automatically disabled when the specified data or time limit has been reached for the month.

3 Select the day of the month to start tracking the monthly data or time usage in the **Billing Cycle Start Date** drop-down menu.

4 Enter a value in the **Limit** field and select the appropriate limiting factor: either **GB**, **MB**, **KB**, or **minutes**.

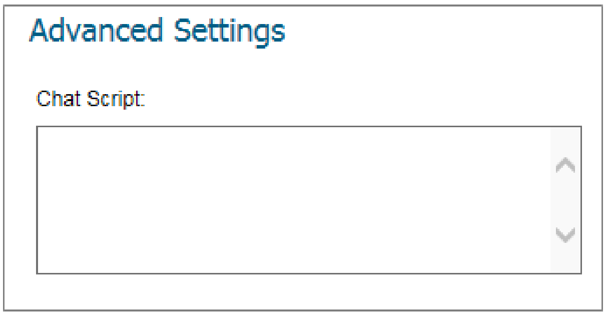
Advanced

Use **Advanced** to manually configure a chat script used during the 3G/4G connection process.

ⓘ **TIP:** Configuring a chat script is only necessary when you need to add commands or special instructions to the standard dial-up connection script.

To configure a chat script:

1 Click **Advanced**.



Advanced Settings

Chat Script:

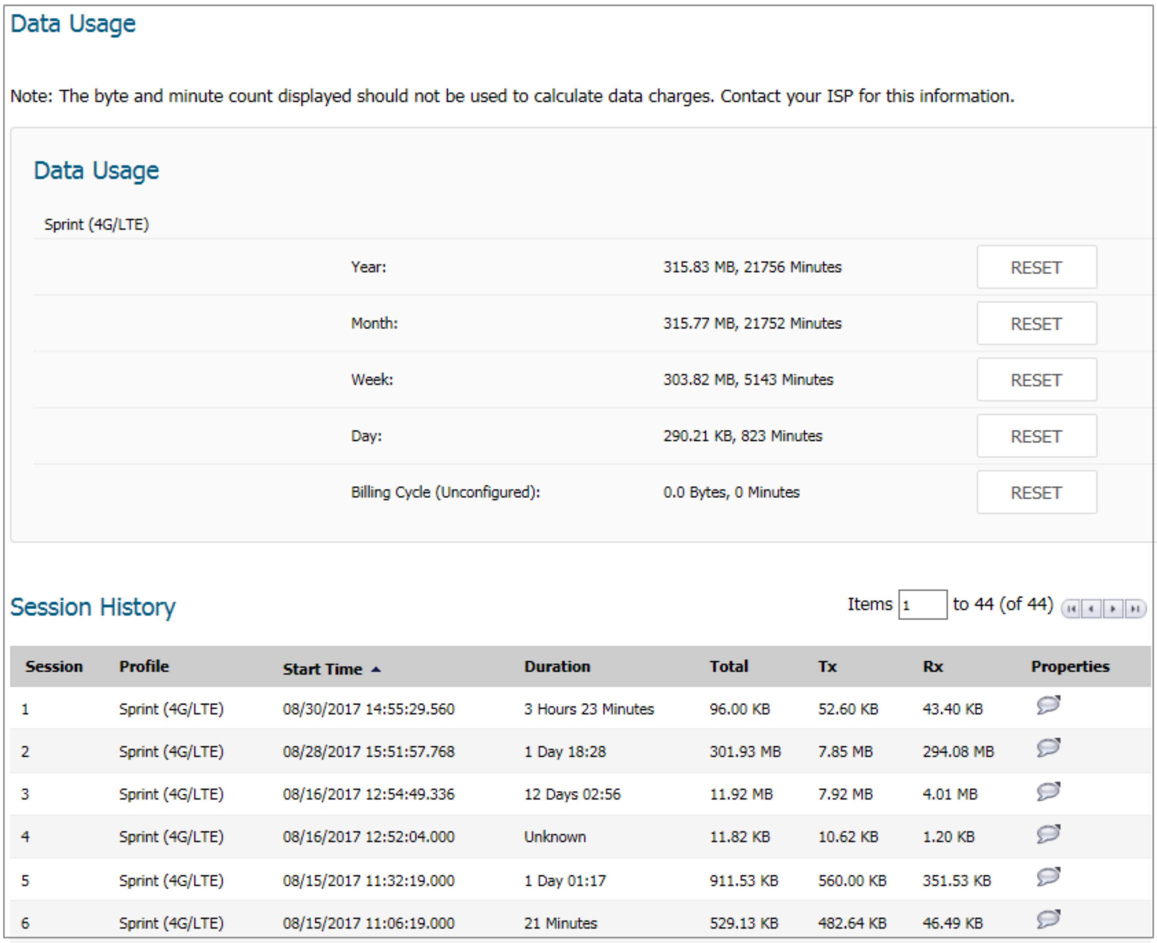
2 Enter the connection chat script in the **Chat Script** field.

3 Click **OK**.

40

Monitoring 3G/4G Data Usage

Navigate to **Connectivity | 3G/4G > Data Usage on the MANAGE** view to monitor **Data Usage** and view **Session History**.



Data Usage

Note: The byte and minute count displayed should not be used to calculate data charges. Contact your ISP for this information.

Data Usage

Sprint (4G/LTE)

Year:	315.83 MB, 21756 Minutes	RESET
Month:	315.77 MB, 21752 Minutes	RESET
Week:	303.82 MB, 5143 Minutes	RESET
Day:	290.21 KB, 823 Minutes	RESET
Billing Cycle (Unconfigured):	0.0 Bytes, 0 Minutes	RESET

Session History

Items 1 to 44 (of 44)

Session	Profile	Start Time ▲	Duration	Total	Tx	Rx	Properties
1	Sprint (4G/LTE)	08/30/2017 14:55:29.560	3 Hours 23 Minutes	96.00 KB	52.60 KB	43.40 KB	💬
2	Sprint (4G/LTE)	08/28/2017 15:51:57.768	1 Day 18:28	301.93 MB	7.85 MB	294.08 MB	💬
3	Sprint (4G/LTE)	08/16/2017 12:54:49.336	12 Days 02:56	11.92 MB	7.92 MB	4.01 MB	💬
4	Sprint (4G/LTE)	08/16/2017 12:52:04.000	Unknown	11.82 KB	10.62 KB	1.20 KB	💬
5	Sprint (4G/LTE)	08/15/2017 11:32:19.000	1 Day 01:17	911.53 KB	560.00 KB	351.53 KB	💬
6	Sprint (4G/LTE)	08/15/2017 11:06:19.000	21 Minutes	529.13 KB	482.64 KB	46.49 KB	💬

The **Data Usage** table displays the current data usage and online time for the current **Year, Month, Week, Day**, and **Billing Cycle**. Billing cycle usage is only calculated if the **Enable Data Usage Limiting** option is enabled on the 3G/4G Connection Profile.

Click **Reset** to reset any of the data usage categories.

ⓘ **NOTE:** The **Data Usage** table is only an estimate of the current usage and should not be used to calculate actual charges. Contact your Service Provider for accurate billing information.

The **Session History** table displays a summary of information about 3G/4G/LTE sessions. To view additional details about a specific session, place your mouse cursor over the **Comment** icon in the **Properties** column. To clear the table, click **Clear**.

Part 6

Connectivity | Appendixes

41

Virtual Access Point Sample Configuration

This section provides Virtual Access Point configuration examples based on real-world, wireless needs.

Topics:

- Configuring a VAP for School Faculty Access
- Deploying VAPs to the Wireless Radio

Configuring a VAP for School Faculty Access

You can use a VAP for a set of users who are commonly in the office, on campus, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users would already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services. This section contains the following:

- Configuring a Zone
- Creating a New Wireless Subnet
- Creating a Wireless VAP Profile
- Creating the Wireless VAP
- Create More > Deploy Current VAPs

Configuring a Zone

In this section you create and configure a new corporate wireless zone with SonicWall firewall security services and enhanced WiFiSec/WPA2 wireless security. Refer to *SonicOS 6.5 System Setup* for more details about Zones.

1. Log into the management interface of your SonicWall network security appliance.
2. Select the **MANAGE** view.
3. Under **System Setup**, select **Network > Zones**.
4. Click **Add...** to add a new zone.

General Settings Tab

1. In the **General** tab, enter a friendly name such as “WLAN_Faculty” in the **Name** field.
2. Select **Wireless** from the **Security Type** drop-down menu.

3 Select the **Allow Interface Trust** checkbox to allow communication between faculty users.

4 Select the checkboxes for all of the security services you would normally apply to faculty on the wireless LAN.

Wireless Settings Tab

1 Select the **Only allow traffic generated by a SonicPoint/SonicWave** checkbox.

2 Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).

3 Click **OK** to save these changes.

Your new zone now appears at the bottom of the **Network > Zones** page, although you might notice it is not yet linked to a Member Interface. This is your next step.

Creating a New Wireless Subnet

In this section you create and configure a new wireless subnet on your current WLAN. This wireless subnet is linked to the zone you created previously, in the Configuring a Zone.

To create a new wireless subnet:

1 Under the **MANAGE** view, select the **System Setup | Network > Interfaces** page.

1 In the **Add Interface** field, select **Virtual Interface**.

2 In the **Zone** drop-down menu, select the zone you created previously. In this case, we have chosen **WLAN_Faculty**.

3 Enter a **VLAN Tag** for this interface. The VLAN allows the internal wireless radio to identify which traffic belongs to this subnet. In this case, we choose 100 as our subnet VLAN tag.

4 Select **W0** interface from the **Parent Interface**.

5 Enter the desired **IP Address** for this subinterface.

6 Click **OK** to add this subinterface.

Your WLAN Subnet interface now appears in the Interface Settings list.

Creating a Wireless VAP Profile

In this section, you create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but facilitates greater ease of use when configuring multiple VAPs.

To create a wireless VAP profile:

1 Select the **MANAGE** view.

2 Under **Connectivity**, select **Wireless > Virtual Access Point**.

3 Click the **ADD** in the **Virtual Access Point Profiles** section.

4 Select a **VAP Schedule Name** from the drop-down menu.

5 Enter a **Profile Name** such as “Corporate-WPA2” for this VAP Profile.

6 Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This employs an automatic user authentication based on your current RADIUS server settings (set in the following paragraphs).

7. In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP needs to support.
8. In the **Radio Server Settings** section, enter your current RADIUS server information. This information is used to support authenticated login to the new subnet.
9. Click **OK** to create this VAP Profile.

Creating the Wireless VAP

In this section, you create and configure a new Virtual Access Point and associate it with the wireless subnet you created previously, in Creating a New Wireless Subnet.

To create a wireless VAP:

General

1. Navigate to **Connectivity | Wireless > Virtual Access Point** page.
2. Click **ADD** in the **Virtual Access Points** section.
3. Enter a friendly name in the **Name** field.
4. Enter an **SSID** name for the VAP. In this case we chose **Campus_Faculty**. This is the name users see when choosing a wireless network to connect with.
5. Select the **VLAN ID** from the drop-down menu. The one you created should be listed there. In this case we chose the VLAN tag for WLAN_Faculty subnet.
6. Select the checkbox to **Enable Virtual Access Point**.
7. Select the checkbox to **Enable SSID Suppress** to hide this SSID from users.
8. Click **OK** to add this VAP.

   Your new VAP now appears in the Virtual Access Points list.

Advanced

1. Click **Advanced** to edit encryption settings.
2. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** drop-down menu. We created and chose a “Corporate-WPA2” profile, which uses **WPA2-AUTO-EAP** as the authentication method. If you have not set up a VAP Profile, continue with steps 2 through 4. Otherwise, continue to Create More > Deploy Current VAPs.
3. In the **Advanced** tab, select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This employs an automatic user authentication based on your current RADIUS server settings (Set in the following paragraphs).
4. In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP supports.
5. In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information is used to support authenticated login to the wireless subnet.

Create More > Deploy Current VAPs

Now that you have successfully set up a wireless subnet for faculty access, you can choose to add more custom VAPs, or to deploy this configuration to your internal wireless radio.

ⓘ **TIP:** Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously by following the steps in the Deploying VAPs to the Wireless Radio.

Deploying VAPs to the Wireless Radio

In the following section you group your new VAPs, associating them with the internal wireless radio. Users are not able to access your VAPs until you complete this process:

- Grouping Multiple VAPs
- Associating a VAP Group with your Wireless Radio

Grouping Multiple VAPs

In this section, you add multiple VAPs into a single group to be associated with your physical access points.

1. Navigate to **Connectivity | Wireless > Virtual Access Point** on the **MANAGE** view.
2. Click **Edit** for the **Internal AP Group**.
3. Select the desired VAPs from the list and click **->** to add them to the group. Optionally, click **Add All** to add all VAPs to a single group.
4. Press **OK** to save changes and create the group.
5. To setup 802.11g WEP or 802.11a WEP/WPA encryption, or to enable MAC address filtering, edit the Virtual Access Point or Virtual Access Point profile and go to the **Advanced** tab. If any of your VAPs use encryption, you must configure these settings before your wireless VAPs function.
6. Click **OK** to save changes and create this Wireless Provisioning Profile.

Associating a VAP Group with your Wireless Radio

After your VAPs are configured and added to **Internal AP Group**, that group must be specified in the **Wireless > Settings** page in order for the VAPs to be available through your internal wireless radio.

1. Navigate to **Connectivity | Wireless > Base Settings**.
2. In the Wireless Virtual Access Point section, select the **Internal AP Group** from the **Virtual Access Point Group** drop-down menu.
3. Click **ACCEPT** to continue and associate this VAP group with your internal wireless radio.

ⓘ **NOTE:** If you are setting up guest services for the first time, be sure to make necessary configurations as described in *SonicOS 6.5 System Setup* under **Users > Guest Services**.

42

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 MySonicWall
- 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

Legend

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

⚠ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ⓘ **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

SonicOS 6.5 Connectivity Administration
Updated - July 2020
Software Version - 6.5.4
232-001809-04 Rev E

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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. SonicWall Inc. 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/#tab-id-3.

Open Source Code

SonicWall 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
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035