



SonicOSX 7

Match Objects

Administration Guide

SONICWALL®

Contents

Introduction to Match Objects for SonicOSX	6
Zones	7
How Zones Work	7
Predefined Zones	8
Security Types	9
Allow Interface Trust	10
Enabling SonicWall Security Services on Zones	10
Effect of Wireless and Non-Wireless Controller Modes	12
Effects of Enabling Non-Wireless Controller Mode	12
Effects of Enabling Wireless Controller Mode	12
The Zone Settings Table	12
Adding a New Zone	13
Configuring a Zone for Guest Access	15
Configuring a Zone for Open Authentication and Social Login	18
Configuring a Zone for Captive Portal Authentication with Radius	19
Configuring a Zone for a Customized Policy Message	20
Configuring a Zone for a Customized Login Page	22
Configuring the WLAN Zone	23
Configuring the RADIUS Server	25
Configuring DPI-SSL Granular Control per Zone	26
Enabling Automatic Redirection to the User-Policy Page	27
Deleting a Zone	28
Addresses	29
Types of Address Objects	29
About Address Groups	30
About UUIDs for Address Objects and Groups	31
Address Objects screen	32
Address Groups screen	32
Common Features	32
Common Functions	33
Common Column Headings	33
Sorting the Entries	35
Default Address Objects and Groups	36
Default Pref64 Address Object	36
Default Rogue Address Groups	36
Adding an Address Object	37

Editing Address Objects	39
Deleting Address Objects	39
Purging MAC or FQDN Address Objects	40
Creating Address Groups	40
Editing Address Groups	41
Deleting Address Groups	41
Working with Dynamic Address Objects	42
Key Features of Dynamic Address Objects	42
Enforcing the Use of Sanctioned Servers on the Network	44
Using MAC and FQDN Dynamic Address Objects	44
Services	51
About Default Service Objects and Groups	52
Predefined IP Protocols for Custom Service Objects	53
Adding Service Objects using Predefined Protocols	54
Adding Custom IP Type Services	56
Configuration Example	56
Editing Custom Service Objects	59
Deleting Custom Service Objects	59
Adding Custom Service Groups	59
Editing Custom Service Groups	60
Deleting Custom Service Groups	60
Countries	61
Country Objects	61
Country Groups	61
Add Country Groups	62
Applications	63
Application Objects	63
Application Groups	63
Add Application Groups	64
Web Categories	65
Web Category Objects	65
Web Category Groups	65
Add Web Category Groups	65
Websites	67
Website Objects	67
Website Groups	67
URI Lists	69
About URIs and the URI List	69
About Keywords and the Keyword List	70

Matching URI List Objects	70
Normal Matching	71
Wildcard matching	71
IPv6 Address Matching	71
IPv6 Wildcard Matching	72
Using URI List Objects	72
About URI List Groups	72
About CFS Action Objects	73
About the Passphrase Feature	73
About the Confirm Feature	73
About UUIDs for CFS Objects	74
Managing URI List Objects	75
About the URI List Objects Table	75
Configuring URI List Objects	75
Exporting a URI Lists	77
Editing a URI List Object	78
Deleting URI List Objects	79
Managing URI List Groups	79
About the URI List Groups Table	79
Adding URI List Groups	79
Editing a URI List Group	80
Deleting URI List Groups	80
Match Patterns	81
Match Patterns	81
Custom Match	82
Custom Match Objects	82
Custom Match Groups	83
Add Custom Match Groups	83
Schedules	84
Adding a Custom Schedule	84
Modifying Schedules	85
Deleting Custom Schedules	86
Dynamic Group	87
About the Dynamic External Address Group File	87
DEAG and DEAO Maximums	88
High Availability Requirements	88
Adding a Dynamic External Object	89
Editing Dynamic External Objects	90
Deleting Dynamic External Objects	91
Email Addresses	92
Configuring Email Address Objects	93

SonicWall Support	95
About This Document	96

Introduction to Match Objects for SonicOSX

Match objects represent the set of conditions which must be matched for actions to take place. Once logged into the firewall the Match Objects function for SonicOS/X is located at **OBJECT > Match Objects**. Within the Match Objects section, you define the object type, the match type (exact, partial, regex, prefix, or suffix), the input representation (text or hexadecimal), and the actual content to match. Match objects were referred to as application objects in previous releases of SonicOS/X. Match Objects are used in conjunction with Action Objects to create App rules.

The following topics are covered in this document

- [Zones](#)
- [Addresses](#)
- [Services](#)
- [Countries](#)
- [Applications](#)
- [Web Categories](#)
- [Websites](#)
- [URI Lists](#)
- [Match Patterns](#)
- [Custom Match](#)
- [Schedules](#)
- [Dynamic Group](#)
- [Email Addresses](#)

Zones

A zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. Zone-based security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or attack.

A network security zone is simply a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Security zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. For more information on configuring interfaces, navigate to **Network > Interfaces**.

SonicOSX zones allows you to apply security policies to the inside of the network. This allows you to do this by organizing network resources to different zones, and allowing or restricting traffic between those zones. This way, access to critical internal resources, such as payroll servers or engineering code servers, can be strictly controlled.

Zones also allow full exposure of the NAT table to allow you control over the traffic across the interfaces by controlling the source and destination addresses as traffic crosses from one zone to another. This means that NAT can be applied internally, or across VPN tunnels, which is a feature that users have long requested. Firewalls can also drive VPN traffic through the NAT policy and zone policy, because VPNs are now logically grouped into their own VPN zone.

How Zones Work

An easy way to visualize how security zones work is to imagine a large new building, with several rooms inside the building, and a group of new employees that do not know their way around the building. This building has one or more exits, which can be thought of as the WAN interfaces. The rooms within the building have one or more doors, which can be thought of as interfaces. These rooms can be thought of as zones inside each room are a number of people. The people are categorized and assigned to separate rooms within the building. People in each room going to another room or leaving the building, must talk to a door person on the way out of each room. This door person is the inter-zone/intra-zone security policy, and the door person's job to consult a list and make sure that the person is allowed to go to the other room, or to leave the building. If the person is allowed (for example, the security policy allows them in), they can leave the room through the door (the interface).

Upon entering the hallway, the person needs to consult with the hallway monitor to find out where the room is, or where the door out of the building is located. This hallway monitor provides the routing process because the monitor knows where all the rooms are located, and how to get in and out of the building. The monitor also knows the addresses of any of the remote offices, which can be considered the VPNs. If the building has more than one entrance/exit (WAN interfaces), the hallway monitor can direct people to use the secondary entrance/exit, depending upon how they have been told to do so (for example, only in an emergency, or to distribute the traffic in and out of the entrance/exits). This function can be thought of as WAN Load Balancing.

There are times that the rooms inside the building have more than one door, and times when there are groups of people in the room who are not familiar with one another. In this example, one group of people uses only one door, and another group uses the other door, even though groups are all in the same room. Because they also do not recognize each other, in order to speak with someone in another group, the users must ask the door person (the security policy) to point out which person in the other group is the one with whom they wish to speak. The door person has the option to not let one group of people talk to the other groups in the room. This is an example of when zones have more than one interface bound to them, and when intra-zone traffic is not allowed.

Sometimes, people want to visit remote offices, and people might arrive from remote offices to visit people in specific rooms in the building. These are the VPN tunnels. The hallway and doorway monitors check to see if this is allowed or not, and allow traffic through. The door person can also elect to force people to put on a costume before traveling to another room, or to exit, or to another remote office. This hides the true identity of the person, masquerading the person as someone else. This process can be thought of as the NAT policy.

Predefined Zones

① | **NOTE:** The predefined zones on your firewall depend on the device.

The predefined security zones on the SonicWall Security Appliance are not modifiable:

This Zone	Has this function
LAN	Consist of multiple interfaces, depending on your network design. Even though each interface has a different network subnet attached to it, when grouped together, they can be managed as a single entity.
WAN	Can consist of multiple interfaces. If you are using the Security Appliance's WAN failover capability, you need to add the second Internet interface to the WAN zone.
MGMT	Used for appliance management and includes only the MGMT interface. Interfaces in other zones can also be enabled for SonicOS management, but the MGMT zone/interface provides the added security of a separate zone just for management.
DMZ	Normally used for publicly accessible servers and can consist of one to four interfaces, depending on your network design.
VPN	A virtual zone used for simplifying secure, remote connectivity.
SSLVPN	Used for secure remote access using the SonicWall NetExtender client.
MULTICAST	Provides support for IP multicasting, which is a method for sending IN packets from a single source simultaneously to multiple hosts.

This Zone	Has this function
WLAN	<p>Provides support to SonicWall SonicPoints and SonicWaves. When assigned to the Opt port, it enforces SonicPoint Enforcement, automatically dropping all packets received from non-SonicPoint devices. The WLAN zone supports:</p> <ul style="list-style-type: none"> • Discovery Protocol (SDP) to automatically poll for and identify attached SonicPoints and SonicWaves • SonicWall Simple Provisioning Protocol to configure SonicPoints and SonicWaves using profiles • Wireless and guest service configurations

① | **NOTE:** Even though you can group interfaces together into one security zone, this does not preclude you from addressing a single interface within the zone.

Security Types

① | **NOTE:** The security types of a zone depend on the device.

Each zone has a security type, which defines the level of trust given to that zone.

Trusted	Provides the highest level of trust—meaning that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the Security Appliance. The LAN zone is always Trusted.
Management	Unique to the MGMT zone and MGMT interface and also provides the highest level of trust.
Encrypted	Used exclusively by the VPN and SSLVPN zones. All traffic to and from an Encrypted zone is encrypted.
Public	Offers a higher level of trust than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the Security Appliance and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN. By default, traffic from DMZ to LAN is denied, but traffic from LAN to ANY is allowed. This means only LAN-initiated connections have traffic between DMZ and LAN. The DMZ only has default access to the WAN, not the LAN.
Untrusted	Represents the lowest level of trust. It is used by both the WAN and the virtual Multicast zone. An Untrusted zone can be thought of as being on the WAN (unprotected) side of the Security Appliance. By default, traffic from Untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from every other zone type is permitted to Untrusted zones.
Wireless	Applied to the WLAN zone or any zone where the only interface to the network consists of SonicWall SonicPoint and SonicWave devices. Wireless security type is designed specifically for use with SonicPoints and SonicWaves. Placing an interface in a Wireless zone activates SDP (SonicWall Discovery Protocol) and SSPP (SonicWall Simple Provisioning Protocol) on that interface for automatic discovery and provisioning of SonicPoints and SonicWaves. Only traffic that

passes through a SonicPoint or SonicWaveis allowed through a Wireless zone; all other traffic is dropped.

Allow Interface Trust

The **Allow Interface Trust** setting in the **Add Zone** dialog automates the creation of Access Rules to allow traffic to flow between the interface of a zone instance. For example, if the LAN zone has both the **LAN** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

The screenshot shows the 'Zone Settings' dialog with the 'General' tab selected. The 'Name' field is set to 'LAN' and the 'Security Type' is set to 'Trusted'. The 'Allow Interface Trust' toggle switch is turned on and is highlighted with a red rectangular box. Below it, four other toggle switches are also turned on, each with a corresponding label.

Setting	Toggle State
Allow Interface Trust	On
Auto-generate Access Rules to allow traffic between zones of the same trust level	On
Auto-generate Access Rules to allow traffic to zones with lower trust level	On
Auto-generate Access Rules to allow traffic from zones with higher trust level	On
Auto-generate Access Rules to deny traffic from zones with lower trust level	On

Enabling SonicWall Security Services on Zones

You can enable SonicWall Security Services for traffic across zones. For example, you can enable SonicWall Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic. You can enable these SonicWall Security Services on zones:

Zone Settings

General Guest Services Wireless Radius Server

GENERAL SETTINGS

Name

Security Type

Allow Interface Trust

Auto-generate Access Rules to allow traffic between zones of the same trust level

Auto-generate Access Rules to allow traffic to zones with lower trust level

Auto-generate Access Rules to allow traffic from zones with higher trust level

Auto-generate Access Rules to deny traffic from zones with lower trust level

Enable Client AV Enforcement Service

Enable DPI-SSL Enforcement Service

Enable SSLVPN Access

Create Group VPN

Enable SSL Control

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Enable App Control Service

Enable SSL Client Inspection

Enable SSL Server Inspection

Enable Client AV Enforcement Service	Enforces anti-virus protection on multiple interfaces in the same Trusted and Public security types for WLAN zones.
Enable DPI-SSL Enforcement Service	Enforces enhanced NGAV (Next Generation AV) such as DPI-SSL Enforcement or SentinelOne AV enforcement in the same Trusted and Public security types for WLAN zones.
Enable SSLVPN Access	Enables SSLVPN secure remote access on the zone.
Create Group VPN	Creates a Group VPN policy for the zone, which is displayed in the VPN Policies table on Network > SSL VPN > Server Settings . You can customize the GroupVPN policy on Network > SSL VPN > Server Settings . If you have unselected Create Group VPN , the Group VPN policy is removed from Network > SSL VPN > Server Settings . For more information about creating VPN policies, see <i>SonicOS 7 Connectivity</i> .
Enable SSL Control	Enables SSL Control on the zone. All new SSL connections initiated from that zone are now subject to inspection. SSL Control must first be enabled globally Policy > Firewall > SSL Control . For more information about SSL Control, see <i>SonicOS 7 Security Configuration</i> .
Enable Gateway Anti-Virus Service	Enforces gateway anti-virus protection on multiple interfaces in the same Trusted and Public security types for WLAN zones.
Enable IPS	Enforces intrusion detection and prevention on multiple interfaces in the same Trusted and Public security types for WLAN zones.
Enable Anti-Spyware Service	Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted and Public security types for WLAN zones.
Enable App Control Service	Enforces application control policy services on multiple interfaces in the same Trusted and Public security types for WLAN zones.
Enable SSL Client	Enables granular DPI-SSL on a per-zone basis rather than globally for DPI-SSL clients.

Inspection

Enable SSL Server Inspection	Enable granular DPI-SSL on a per-zone basis rather than globally for DPI-SSL servers.
-------------------------------------	---

Effect of Wireless and Non-Wireless Controller Modes

Topics:

- [Effects of Enabling Non-Wireless Controller Mode](#)
- [Effects of Enabling Wireless Controller Mode](#)

Effects of Enabling Non-Wireless Controller Mode

Enabling Non-Wireless Controller Mode affects the **Object > Match Objects > Zones** page. Attempts to enable or delete the affected features are denied.

- The **Edit** and **Delete** icons for wireless zones become dimmed on the **Object > Match Objects > Zones** page.
- Internal wireless zones are disabled.

Effects of Enabling Wireless Controller Mode

Enabling Wireless Controller Mode affects the **Object > Match Objects > Zones** page. Attempts to enable or delete the affected features are denied.

- The **Edit** and **Delete** icons for VPN and SSL VPN zones become dimmed on the **Object > Match Objects > Zones** page.
- Any attempt to enable a zone with VPN and/or SSL VPN results in an error.

The Zone Settings Table

The **Zone Settings** table displays a listing of all the SonicWall Security Appliance's default predefined zones as well as any zones you create. The table displays the following status information about each zone configuration:

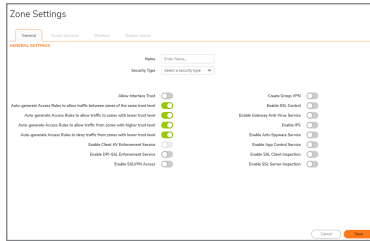
#	NAME	SECURITY T.	MEMBER INTERFACES	INTERFACE TRUST	CLIENT AV	GATEWAY AV	ANTI SPYWARE	IPS	APP CONTROL	SSL CONTROL	SSL VPN ACCESS	DPI SSL CLIENT	DPI SSL SERVER	CONFIGURE
1	LAN	Trusted	X0	✓	✓	✓	✓	✓	✓			✓		✎ ⚙
2	WAN	Untrusted	X1		✓	✓	✓	✓	✓					✎ ⚙
3	DMZ	Public		✓	✓	✓	✓	✓	✓			✓		✎ ⚙
4	VPN	Encrypted			✓	✓	✓	✓						✎ ⚙
5	SSLVPN	Salpas			✓	✓	✓	✓						✎ ⚙
6	MULTICAST	Untrusted												✎ ⚙

Name	Name of the zone. The predefined LAN, WAN, WLAN, VPN, SSLVPN, MGMT, MULTICAST, and Encrypted zone names cannot be changed.
Security Type	Security type: Trusted, Untrusted, Public, Wireless, or Encrypted.
Member Interfaces	Interfaces that are members of the zone.
Interface Trust	Check mark indicates the Allow Interface Trust setting is enabled for the zone.
Client AV	Check mark indicates SonicWall Client Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWall Client Anti-Virus manages an anti-virus client application on all clients on the zone.
Client CF	Check mark indicates Client Content Filtering services are enabled.
Gateway AV	Check mark indicates SonicWall Gateway Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWall Gateway Anti-Virus manages the anti-virus service on the firewall.
Anti-Spyware	Check mark indicates SonicWall Anti-Spyware detection and prevention is enabled for traffic through interfaces in the zone.
IPS	Check mark indicates SonicWall Intrusion Prevention Service is enabled for traffic coming in and going out of the zone.
App Control	Check mark indicates App Control Service is enabled for traffic coming in and going out the zone.
SSL Control	Check mark indicates SSL Control is enabled for traffic coming in and going out the zone. All new SSL connections initiated from that zone is now subject to inspection.
SSL VPN Access	Check mark indicates SSL VPN secure remote access is enabled for traffic coming in and going out the zone.
DPI-SSL Client	Check mark indicates granular DPI-SSL on a per-zone basis rather than a global basis for DPI-SSL clients.
DPI-SSL Server	Check mark indicates granular DPI-SSL on a per-zone basis rather than global basis for DPI-SSL servers.
Configure	Clicking the Edit icon displays the Zone Settings dialog. Clicking the Delete icon deletes the zone. The delete icon is dimmed for the predefined zones; you cannot delete these zones.

Adding a New Zone

To add a new zone:

1. Navigate to **Object > Match Objects > Zones.**
2. Click the **Add** icon.



3. Type a name for the new zone in the **Name** field.
4. From **Security Type**, select:

Trusted	Zones with the highest level of trust, such as internal LAN segments.
Public	Zones with a lower level of trust requirements, such as a DMZ interface.
Wireless	WLAN interface.
SSLVPN	Interfaces on which Content Filtering, Client AV enforcement, and Client CF services are enabled.

NOTE: Selecting this security type disables the **Enable SSLVPN Access** and **Create Group VPN** options on this dialog.

5. To allow intra-zone communications, select **Allow Interface Trust**. An Access Rule allowing traffic to flow between the interfaces of a Zone instance is created automatically. This option is not selected by default.
6. To have SonicOS automatically generate access rules to allow traffic between this zone and other zones of equal trust, select **Auto-generate Access Rules to allow traffic between zones of the same trust level**. For example, *CUSTOM_LAN -> CUSTOM_LAN* or *CUSTOM_LAN -> LAN*. This option is selected by default.

NOTE: For this option and the following Access Rules options, see *SonicOS Policies* for information about Access Rules.
7. To have SonicOS automatically generate access rules to allow traffic between this zone and other zones of lower trust, select **Auto-generate Access Rules to allow traffic to zones with lower trust level**. For example, *CUSTOM_LAN -> WAN* or *CUSTOM_LAN -> DMZ*. This option is selected by default.
8. To have SonicOS automatically generate access rules to allow traffic between this zone and other zones of higher trust, select **Auto-generate Access Rules to allow traffic from zones with higher trust level**. For example, *LAN -> CUSTOM_DMZ* or *CUSTOM_LAN -> CUSTOM_DMZ*. This option is selected by default.
9. To have SonicOS automatically generate access rules to deny traffic between this zone and zones of lower trust, select **Auto-generate Access Rules to deny traffic from zones with lower trust level**. For example, *WAN -> CUSTOM_LAN* or *DMZ -> CUSTOM_LAN*. This option is selected by default.
10. To enforce managed Client Anti-Virus protection on clients connected to multiple interfaces in the same Trusted, Public, or WLAN zones using the Client Anti-Virus client on your network hosts, select **Enable Client AV Enforcement Service**. This option is not selected by default.

NOTE: This option is dimmed and unavailable until you select a security type from Security Type. For this option and the following Security Services options, see *SonicOS Security Configuration* for more information about these services.

11. To enforce enhanced NGAV (Next Generation AV) such as DPI-SSL Enforcement or SentinelOne AV enforcement, select **Enable DPI-SSL Enforcement Service**. This option is not selected by default. For more information about NGAV, see *SonicOS Security Configuration*.
12. To enable SSLVPN secure remote access on the zone, select **Enable SSLVPN Access**. This option is not selected by default.
 - ① | **NOTE:** This option is dimmed if **SSLVPN** is selected for **Security Type**.
13. To create a SonicWall Group VPN Policy for this zone automatically, select **Create Group VPN**. You can customize the Group VPN Policy in **Network > SSLVPN > Server Settings**. This option is not selected by default. This option is available until SSLVPN is selected for Security Type, but after the Security Type is changed to one of the other types, it remains dimmed and unavailable.
 - △ | **CAUTION:** Disabling Create Group VPN removes any corresponding Group VPN policy.
 - ① | **NOTE:** This option is dimmed if SSLVPN is selected for Security Type. For this and other connectivity options, see *SonicOS Connectivity* for more information.

Disabling Group VPN for WAN/WLAN VPN policies, deletes all VPN policies. Re-enabling the Create Group VPN option automatically creates a new, enabled VPN policy. Disabling VPN policies globally does not also delete auto-rules. If you do not want to VPN policies at all, globally disable VPN, and then delete all policies that correlate with VPN.

GroupVPN policies appear in the VPN Policies table located in **Network > SSLVPN > Server Settings**. WAN/WLAN GroupVPN policies are disabled by default when the firewall is booted with the factory default.
14. To enable SSL Control on the zone, select **Enable SSL Control**. All new SSL connections initiated from that zone are now subject to inspection. This option is not selected by default.
 - ① | **NOTE:** SSL Control must first be enabled globally on **Policy > Firewall > SSL Control**.
15. To enforce gateway anti-virus protection on your Security Appliance for all clients connecting to this zone, select **Enable Gateway Anti-Virus Service**. SonicWall Gateway Anti-Virus manages the anti-virus service on the Security Appliance. This option is not selected by default.
16. To enforce intrusion detection and prevention on multiple interfaces in the same Trusted, Public, or WLAN zones. select **Enable IPS**. This option is not selected by default.
17. To enforce anti-spyware detection and prevention on multiple interfaces in the same Trusted or Public security type for WLAN zones, select **Enable Anti-Spyware Service**. This option is not selected by default.
18. To enforce application control policy services on multiple interfaces in the same Trusted or Public security type for WLAN zones, select **Enable App Control Service**. This option is not selected by default. For more information about App Control, see *SonicOS Policies*.
19. To enable granular DPI-SSL on a per-zone basis rather than globally for DPI-SSL clients, select **Enable SSL Client Inspection**. This option is not selected by default.
20. To enable granular DPI-SSL on a per-zone basis rather than globally for DPI-SSL servers, select **Enable SSL Server Inspection**. This option is not selected by default.
21. Click **Save**. The new zone is now added to the Security Appliance.

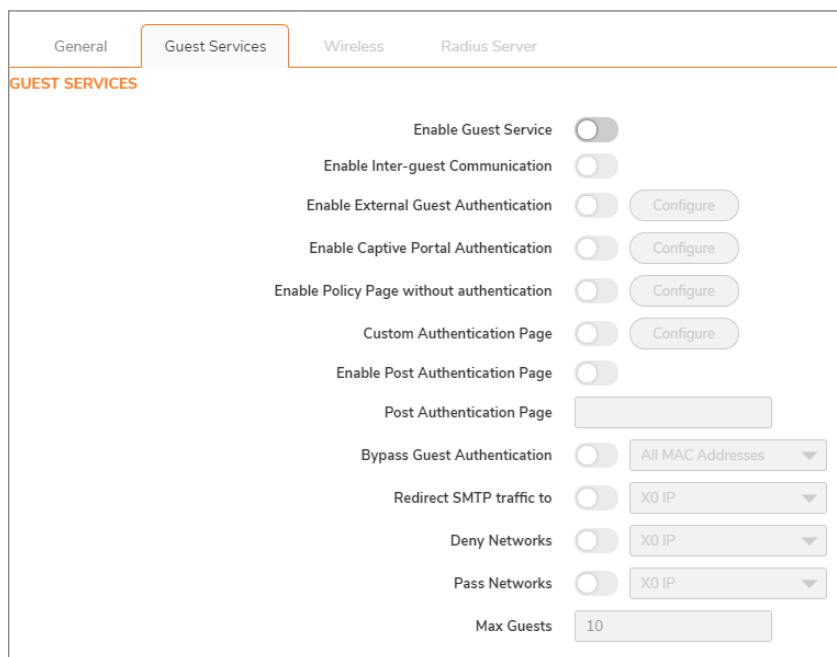
Configuring a Zone for Guest Access

- ① | **IMPORTANT:** You cannot configure an **Untrusted**, **Encrypted**, **SSL VPN**, or **Management** zone for guest access.

SonicWall User Guest Services provides an easy solution for creating wired and wireless guest passes and/or locked-down Internet-only network access for visitors or untrusted network nodes. This functionality can be extended to wireless or wired users on the WLAN, LAN, DMZ, or public/semi-public zone of your choice.

To configure Guest Services feature:

1. Navigate to **Object > Match Objects > Zones**.
2. Click **Edit** for the zone you wish to add Guest Services to. The **Zone Settings** dialog displays.
3. Click **Guest Services** tab.



4. Select **Enable Guest Services** option. All other options become available, but are not selected by default.
5. Select from the following configuration options for Guest Services:

Enable inter-guest communication	Allows guests to communicate directly with other users who are connected to this zone.
Bypass AV Check for Guests	Allows guest traffic to bypass Anti-Virus protection.
Bypass Client CF Check for Guests	Allows guest traffic to bypass Client CF enforcement.
Bypass DPI-SSL Enforcement Check for Guests	Allows guest traffic to bypass DPI-SSL enforcement.

Enable External Guest Authentication	<p>Requires guests connecting from the device or network you select to authenticate before gaining access. Selecting this option makes CONFIGURE available.</p> <p>① NOTE: When this option is selected, the following four options become dimmed and unavailable.</p>
Enable Captive Portal Authentication	<p>Allows you to create a customized login page with RADIUS authentication. Selecting this option makes Configure available. For information about configuring this option, see Configuring a Zone for Captive Portal Authentication with Radius.</p>
Enable Policy Page without authentication	<p>Directs users to a guest services usage policy page when they first connect to a SonicPoint or SonicWave in the WLAN zone. Guest users are authenticated by accepting the policy instead of providing a user name and password. Selecting this option makes Configure available. To set up an HTML customizable policy usage page, click Configure. For information about configuring this option, see Configuring a Zone for a Customized Policy Message.</p>
Custom Authentication Page	<p>Redirects users to a custom authentication page when they first connect to the network. Selecting this option makes Configure available. To set up the custom authentication page, click Configure. For information about configuring this option, see Configuring a Zone for a Customized Login Page.</p>
Post Authentication Page	<p>Directs users to the specified page immediately after successful authentication. Selecting this option makes its field available. Enter a URL for the post-authentication page in the field.</p>
Bypass Guest Authentication	<p>Allows the Guest Services feature to integrate into environments already using some form of user-level authentication. This feature automates the authentication process, allowing wireless users unrestricted wireless Guest Services without requiring authentication. When selected, this option's drop-down menu becomes available; select:</p> <ul style="list-style-type: none"> • All MAC Addresses (default) • An Address Object • An Address Group • Create new MAC object <p>① NOTE: This feature should only be used when unrestricted Guest Service access is desired, or when another device upstream is enforcing authentication.</p>
Redirect SMTP traffic to	<p>Redirects SMTP traffic incoming on this zone to an SMTP server you specify. When selected, this option's drop-down menu becomes available; select:</p> <ul style="list-style-type: none"> • An Address Object • Create new address object
Deny Networks	<p>Blocks traffic to the networks you name. When selected, this option's drop-down menu becomes available; select:</p> <ul style="list-style-type: none"> • An Address Object • An Address Object group • Create new address object

	<ul style="list-style-type: none"> • Create new address object group
Pass Networks	<p>Allows traffic through the Guest Service-enabled zone to the selected networks automatically. When selected, this option's drop-down menu becomes available; select:</p> <ul style="list-style-type: none"> • An Address Object • An Address Object group • Create new address object • Create new address object group
Max Guests	<p>Specifies the maximum number of guest users allowed to connect to this zone. The minimum number is 1, the maximum number is 4500, and the default setting is 10.</p>
Wireless Zone Guest Services Options	<p>Displays only for the WLAN zone or for a custom zone with a Security Type of Wireless.</p>
Enable Dynamic Address Translation	<p>Grants access to non-DHCP guests. This option is not selected by default.</p>

6. Click **Save** to apply these settings to this zone.

① **NOTE:** For information about creating Address Objects and Address Object Groups, see SonicOS **Match Objects > Addresses**.

Configuring a Zone for Open Authentication and Social Login

SonicOS supports Open Authentication (OAuth) and Social Login:

- OAuth assists users in sharing data between applications.
- Social Login simplifies the login process for various social media

Configuring a Zone for Captive Portal Authentication with RADIUS

To configure captive portal authentication with RADIUS:

1. On the **Zone Settings** dialog, click **Guest Services** tab.

The screenshot shows the 'Guest Services' tab in the 'Zone Settings' dialog. The 'GUEST SERVICES' section is active. The following options are visible:

- Enable Guest Service:
- Enable Inter-guest Communication:
- Enable External Guest Authentication: [Configure](#)
- Enable Captive Portal Authentication: [Configure](#)
- Enable Policy Page without authentication: [Configure](#)
- Custom Authentication Page: [Configure](#)
- Enable Post Authentication Page:
- Post Authentication Page:
- Bypass Guest Authentication: All MAC Addresses
- Redirect SMTP traffic to: X0 IP
- Deny Networks: X0 IP
- Pass Networks: X0 IP
- Max Guests: 10

2. Select **Enable Guest Services** option. The options become available.
3. Select **Enable Captive Portal Authentication**. **Configure** becomes available.
4. Click **Configure**.

The screenshot shows the 'CUSTOM PORTAL AUTHENTICATION SETTINGS' dialog. The following settings are visible:

- Internal Captive Portal Vendor URL:
- External Captive Portal Vendor URL:
- RADIUS SERVER ATTRIBUTES SETTINGS:
 - Captive Portal Welcome URL Source: From Radius
 - Custom Captive Portal Welcome URL Source:
 - Session Timeout Source: From Radius
 - Custom Session Timeout Source: Minutes
 - Idle Timeout Source: From Radius
 - Custom Idle Timeout Source: Minutes
- RADIUS AUTHENTICATION SETTINGS:
 - Radius Authentication Method: CHAP

Buttons: [Cancel](#) [Save](#)

5. In the **Custom Portal Authentication Settings** section:

- a. Enter the internal captive portal vendor's URL in the **Internal Captive Portal Vendor URI** field.
 - b. Enter the external captive portal vendor's URL in the **External Captive Portal Vendor URI** field.
6. In the **Radius Server Attributes Settings** section:
- a. Select the source for the captive portal welcome URL from **Captive Portal Welcome URL Source**:
 - **From Radius** (default); go to *Step c*
 - **Custom**; the next option becomes available
 - b. Enter the welcome URL in the **Custom Captive Portal Welcome URL** field.
 - c. Select the source for the session timeout limit from **Session Timeout Source**:
 - **From Radius** (default); go to *Step f*
 - **Custom**; the next option becomes available
 - d. Select the type of session timeout duration from **Custom Session Timeout**:
 - Minutes
 - Hours
 - Days (default)
 - e. Enter the limit in the field.
 - f. Select the source for the idle timeout from **Idle Timeout Source**:
 - From **Radius** (default); go to **Step 7**
 - **Custom**; the next option becomes available
 - g. Select the type of idle timeout duration from **Custom Session Timeout**:
 - Minutes
 - Hours
 - Days (default)
 - h. Enter the limit of the duration in the field.
7. In the **Radius Authentication Settings** section, select the authentication method from **Radius Authentication Method**:
- CHAP (default)
 - PAP – Encrypted
 - PAP – ClearText
8. Click **Save**.

Configuring a Zone for a Customized Policy Message

To configure a customized policy message:

1. On the **Zone Settings** dialog, click **Guest Services** tab.
2. Select **Enable Guest Services** option. The options become available.

3. Select **Enable Policy Page without authentication**. **Configure** becomes available.
4. Click **Configure**.

CUSTOM LOGIN PAGE SETTINGS

Guest Usage Policy

Idle Timeout

Auto Accept Policy Page

5. Enter your policy for guest usage in the **Guest Usage Policy** field. The text may include HTML formatting.
6. To preview your policy message, click **Preview**.
7. To specify an idle timeout, enter the timeout value in the **Idle Timeout** field.
8. Select the type of timeout:
 - Seconds
 - Minutes (default)
 - Hours
 - Days
9. Select **Auto Accept Policy Page**. This option is not selected by default.
10. Click **Save**.

Configuring a Zone for a Customized Login Page

To configure a customized login page:

1. On the **Zone Settings** dialog, click **Guest Services** tab.

The screenshot shows the 'Guest Services' tab in the Zone Settings dialog. The 'Enable Guest Service' toggle is turned on. Below it are several other options, each with a toggle and a 'Configure' button: 'Enable Inter-guest Communication', 'Enable External Guest Authentication', 'Enable Captive Portal Authentication', 'Enable Policy Page without authentication', and 'Custom Authentication Page'. 'Enable Post Authentication Page' is also present but not selected. Below these are 'Post Authentication Page' (text input), 'Bypass Guest Authentication' (toggle and dropdown menu), 'Redirect SMTP traffic to' (toggle and dropdown menu), 'Deny Networks' (toggle and dropdown menu), and 'Pass Networks' (toggle and dropdown menu). At the bottom is 'Max Guests' (text input with value 10).

2. Select **Enable Guest Services** option. The options become available.
3. Select **Custom Authentication Page** option.
4. Click **Configure** button.

The screenshot shows the 'CUSTOM LOGIN PAGE SETTINGS' dialog. It has four fields: 'Custom Header Content Type' (dropdown menu with 'URL' selected), 'Content' (text input with placeholder 'Enter content'), 'Custom Footer Content Type' (dropdown menu with 'URL' selected), and 'Content' (text input with placeholder 'Enter content').

5. For **Custom Header Content Type**, select:
 - URL
 - Text
6. Enter the URL or text in the **Content** field.
7. For **Custom Footer Content Type**, select:
 - URL
 - Text
8. Enter the URL or text in the **Content** field.
9. Click **Save**.

Configuring the WLAN Zone

1. Navigate to **Object > Match Objects > Zones**.
2. If you are configuring:
 - A new zone, click **Add**.
 - An existing zone, click the **Edit** icon for the WLAN zone.

The **Zone Settings** dialog displays

① **NOTE:** Depending on the zone, there also may be views available for **Guest Services**, **Wireless**, and **Radius Server**. How to configure the **General** view is described in [Adding a New Zone](#).

3. If creating a new zone, select **Wireless** from **Security Type**. **Guest Services**, **Wireless**, and **Radius Server** appear.
4. To automate the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance, select **Allow Interface Trust**. For example, if the LAN zone has both the LAN and X3 interfaces assigned to it, enabling **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other. This option is not selected by default.
5. Click **Wireless** tab.

The screenshot shows the 'Zone Settings' dialog with the 'Wireless' tab selected. The 'WIRELESS' section is highlighted in orange. Below it, the 'SONICPOINT/SONICWAVE SETTINGS' section contains several configuration options:

- Auto Provisioning SonicPoint N/Ni/Ne Provisioning Profile: (disabled)
- SonicPoint N/Ni/Ne Provisioning Profile: SonicPointN (dropdown)
- Auto Provisioning SonicPoint N Dual Radio Provisioning Profile: (disabled)
- SonicPoint N Dual Radio Provisioning Profile: SonicPointNDR (dropdown)
- Auto Provisioning SonicPoint ACe/ACi/N2 Provisioning Profile: (disabled)
- SonicPoint ACe/ACi/N2 Provisioning Profile: SonicPointACe/ACi/N2 (dropdown)
- Auto Provisioning SonicWave Provisioning Profile: (disabled)
- SonicWave Provisioning Profile: SonicWave (dropdown)
- Only allow traffic generated by a SonicPoint/SonicWave: (enabled)
- Prefer SonicPoint/SonicWave 2.4GHz Auto Channel Selection to be 1, 6 and 11 only: (disabled)
- Enforce SonicWave license activation from secure trusted license manager: (enabled)
- Disable SonicPoint/SonicWave management: (disabled)

6. In the **Wireless Settings** section, to require that all traffic that enters into the WLAN zone be authenticated through a SonicWall SSL VPN appliance, select **SSLVPN Enforcement**. Selecting this option makes the following two options available. This option is not selected by default.
7. From **SSL VPN** server, select an address object to direct traffic to the SonicWall SSL VPN appliance or create a new one. For information about creating Address Objects and Address Object Groups,

see *SonicOS Policies*.

8. From **SSL VPN service**, select the service or group of services to allow clients authenticated through the SSL VPN.
9. In the **SonicPoint/SonicWave Settings** section, select the **SonicPoint/SonicWave Provisioning Profile** to apply to all SonicPoints/SonicWaves connected to this zone. Whenever a SonicPoint/SonicWave connects to this zone, it is provisioned automatically by the settings in the SonicPoint/SonicWave Provisioning Profile, unless you have individually configured it with different settings. For information SonicPoint/SonicWave provisioning profiles, see *SonicOS Connectivity*.
 - ① **NOTE:** For the following four settings, optionally select Auto provisioning to allow SonicPoints/SonicWaves attached to the profile to be provisioned automatically when the profile is modified. This option is not selected by default.
10. Select the **SonicPointN/Ni/Ne Provisioning Profile** when you want to apply to all SonicPointN/Ni/Nes connected to this zone. Whenever a SonicPointN/Ni/Ne connects to this zone, it is automatically provisioned by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings. The default provisioning profile is **SonicPointN**.
11. Select **SonicPoint N Dual Radio Provisioning Profile** when you want to apply to all SonicPointNDRs connected to this zone. Whenever a SonicPointNDR connects to this zone, it is automatically provisioned by the settings in the SonicPointNDR Provisioning Profile, unless you have individually configured it with different settings. The default provisioning profile is SonicPointNDR.
12. Select SonicPointACe/ACi/N2 Provisioning Profile when you want to apply to all SonicPointACe/ACi/N2s connected to this zone. Whenever a SonicPointACe/ACi/N2 connects to this zone, it is automatically provisioned by the settings in the SonicPointACe/ACi/N2 Provisioning Profile, unless you have individually configured it with different settings. The default provisioning profile is **SonicPointACe/ACi/N2**.
13. Select **SonicWave Provisioning Profile** when you want to apply to all SonicPointNDRs connected to this zone. Whenever a SonicPointNDR connects to this zone, it is automatically provisioned by the settings in the SonicPointNDR Provisioning Profile, unless you have individually configured it with different settings. The default provisioning profile is SonicWave.
14. Select **Only allow traffic generated by a SonicPoint/SonicWave** to allow only traffic from SonicWall SonicPoints to enter the WLAN zone interface. This allows maximum security of your WLAN. This option is selected by default. Clear this option if you want to allow any traffic on your WLAN zone regardless of whether the traffic is from a wireless connection.
 - ① **TIP:** To allow any traffic on your WLAN zone regardless of whether it is from a wireless connection, clear **Only allow traffic generated by a SonicPoint / SonicPointN**.
 - ① **NOTE:** For Guest Services configuration information, see [Configuring a Zone for Guest Access](#). For RADIUS server configuration information, see [Configuring the RADIUS Server](#).
15. Optionally, select **Prefer SonicPoint/SonicWave 2.4Hz Auto Channel Selection to be 1.6 and 11 only**. This option is not selected by default.
 - ① **IMPORTANT:** Enable this option only when SonicPointN/AC 2.4Hz Auto Channel selection is preferred to be 1, 6, and 11.
16. Select **Enforce SonicWave license activation from secure trusted license manager**.
 - ⚠ **CAUTION:** This option enforces license activation from a secure trusted license manager; manual license keyset input is not allowed. Change this setting only under the direction of Technical Support.
17. Select **Disable SonicPoint/SonicWave management** to disable all management capabilities on this WLAN.
18. To:

- Configure the RADIUS server, go to [Configuring the RADIUS Server](#).
- Apply these settings to the WLAN zone, click **Save**.

Configuring the RADIUS Server

① | **NOTE:** The **Radius Server** tab is enabled or disabled based on the device.

1. Navigate to **Object > Match Objects > Zones**.
2. If you are configuring:
 - A new zone, click **Add**.
 - An existing zone, click the **Edit** icon for the WLAN zone.

The **Zone Settings** dialog displays.

① | **NOTE:** Depending on the zone, there also may be views available for **Guest Services**, **Wireless**, and **Radius Server**. How to configure the **General** view is described in [Adding a New Zone](#).

3. If creating a new zone, select **Wireless** from Security Type. **Guest Services**, **Wireless**, and **Radius Server** appear.
4. Click **Radius Server** tab.

Zone Settings

General Guest Services Wireless **Radius Server**

RADIUS SERVER

Enable Local Radius Server

Server Numbers Per Interface

Radius Server Port

Radius Server Client Password

Enable Local Radius Server TLS Cache

Cache Lifetime (h)

Database Access Settings

LDAP Server

Active Directory

ACTIVE DIRECTORY SETTINGS

Domain

Full Name

Admin User Name

Admin User Password

5. Select **Enable Local Radius Server**. The other options become available.
6. Enter the number of RADIUS servers numbers per interface in **Server Numbers Per Interface**. The minimum number is 1, the maximum is 512, and the default is 2.
7. Enter the port for the RADIUS server in the **Radius Server Port** field. The default is 1812.

8. Enter the password for the RADIUS client in the **Radius Client Password** field.
9. Optionally, select **Enable Local Radius Server TLS Cache** lifetime. This option is not selected by default. The **Cache Lifetime(h)** field becomes available.
 - Enter the lifetime, in hours, in the **Cache Lifetime(h)** field. The minimum and default is **1** hour; the maximum is 99999 hours.
10. Choose the database access method from **Database Access Settings**:

- **LDAP Server** – More options appear; go to Step 11.

LDAP SERVER SETTINGS

Name of IP Address	Enter name or IP Address
Base DN	Enter base DN
Identity DN	Enter identity DN
Identity DN Password	Enter identity DN Password
Enable LDAP TLS	<input type="checkbox"/>
LDAP Cache Cache	<input type="checkbox"/>
LDAP Cache Limit	Enter LDAP Cache Limit

- **Active Directory** – More options appear; go to Step 18.

ACTIVE DIRECTORY SETTINGS

Domain	Enter domain
Full Name	Enter full name
Admin User Name	Enter admin user name
Admin User Password	Enter admin user password

11. Enter the name or IP address of the LDAP server in the **Name or IP address** field.
12. Enter the base distinguished name in the **Base DN** field.
13. Enter the Identity distinguished name in the **Identity DN** field.
14. Enter the distinguished name password in the **Identity DN Password** field.
15. To enable LDAP Transport Layer Security (TLS), select **Enable Ldap TLS**. This option is not selected by default.
16. To enable LDAP cache, select **Enable Ldap Cache**. The Ldap Cache Lifetime(s) field becomes active.
 - Enter the lifetime, in seconds in the Ldap Cache Lifetime(s) field; the minimum is 1, the maximum is 99999, and the default is **86400**.
17. Go to Step 22.
18. Enter the domain name in the **Domain** field.
19. Enter the full name of the Active Directory in the **Full Name** field.
20. Enter the user name of the administrator user in the **Admin User Name** field.
21. Enter the password of the administrator user in the **Admin User Password** field.
22. Click **Save**.

Configuring DPI-SSL Granular Control per Zone

DPI-SSL granular control allows you to enable DPI-SSL on a per-zone basis rather than globally. You can enable both DPI-SSL Client and DPI-SSL Server per zone. For further information, see *SonicOS Security Configuration*.

Enabling Automatic Redirection to the User-Policy Page

SonicOS allows you to redirect a guest automatically to your guest-user policy page. If you enable this feature, also known as the zero-touch policy page redirection, the guest user is redirected automatically to your guest-user policy page. If you disable the feature, the guest must click **Accept**.

To enable automatic redirection to the user-policy page::

1. Navigate to **Object > Match Objects > Zones**.
2. Click either the:
 - **Add** icon to add a new zone.
 - **Edit** icon of an existing zone.

The **Zone Settings** dialog displays.

3. Type a name for the new zone in the **Name** field.
4. Select a **Security Type** from the drop-down.
5. Click **Guest Services** tab.

General Guest Services Wireless Radius Server

GUEST SERVICES

Enable Guest Service

Enable Inter-guest Communication

Enable External Guest Authentication Configure

Enable Captive Portal Authentication Configure

Enable Policy Page without authentication Configure

Custom Authentication Page Configure

Enable Post Authentication Page

Post Authentication Page

Bypass Guest Authentication All MAC Addresses

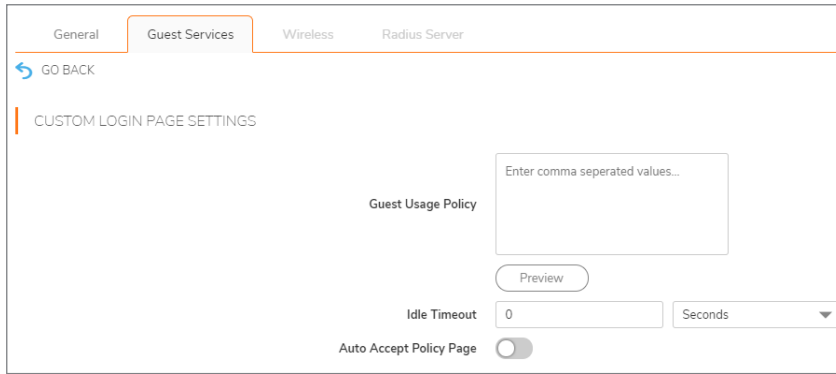
Redirect SMTP traffic to XO IP

Deny Networks XO IP

Pass Networks XO IP

Max Guests

6. Click **Enable Guest Services** option.
7. Click **Enable Policy Page without authentication** option.
8. Click **Configure** button. The **Custom Login Page Settings** dialog displays.



9. Select **Auto Accept Policy Page** option. This option is not selected by default.
10. Click **Save**.

Deleting a Zone

To delete a user-created zone:

1. Navigate to **Object > Match Objects > Zones**.
 - ① **NOTE:** The **Delete** icon is unavailable for predefined zones. You cannot delete these zones. Any zones that you create can be deleted.
2. Click the **Delete** icon in the zone's Configure column which you want to delete.

To delete one or more user-created zones:

1. Navigate to **Object > Match Objects > Zones**.
 - ① **NOTE:** The checkboxes are unavailable for predefined zones. You cannot delete these zones. Any zones that you create can be deleted.
2. Select the checkboxes of zones to delete and click **Delete Zones**.

Addresses

Address objects (AOs) allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. While more effort is involved in creating an address object than in simply entering an IP address, address objects were implemented to complement the management scheme of SonicOS, providing the following characteristics:

- **Zone Association** – When defined, host, MAC, and FQDN AOs require an explicit zone designation. In most areas of the interface (such as access rules) this is only used referentially. The functional application are the contextually accurate populations of address object drop-down menus and the area of VPN access definitions assigned to users and groups. When AOs are used to define VPN access, the access rule auto-creation process refers to the AO's zone to determine the correct intersection of VPN [zone] for rule placement. In other words, if the host AO, *192.168.168.200 Host*, belonging to the LAN zone was added to VPN access for the *Trusted Users* user group, the auto-created access rule would be assigned to the VPN LAN zone.
- **Management and Handling** – The versatile family of address objects types can be easily used throughout the SonicOS interface, allowing for handles (for example, when defining access rules) to be quickly defined and managed. The ability to simply add or remove members from address groups effectively enables modifications of referencing rules and policies without requiring direct manipulation.
- **Reusability** – Objects only need to be defined once, and can then be easily referenced as many times as needed.

For example, take an internal web server with an IP address of *67.115.118.80*. Rather than repeatedly typing in the IP address when constructing access rules or NAT policies, you can create a single entity called *My Web Server* as a host address object with an IP address of *67.115.118.80*. This address object, **My Web Server**, can then be easily and efficiently selected from a drop-down list in any configuration screen that employs address objects as a defining criterion.

Types of Address Objects

As there are multiple types of network address expressions, there are multiple address object types, as shown in the below table.

Type	Definition
Host	Defines a single host by its IP address and zone association. The netmask for a host address object is automatically set to 32-bit (<i>255.255.255.255</i>) to identify it as a single host. For example, <i>My Web Server</i> with an IP address of <i>67.115.118.110</i> and a default netmask of <i>255.255.255.255</i> .

Type	Definition
Range	Defines a range of contiguous IP addresses. No netmask is associated with range address objects, but internal logic generally treats each member of the specified range as a 32-bit masked host object. For example, <i>My Public Servers</i> with an IP address starting value of <i>67.115.118.66</i> and an ending value of <i>67.115.118.90</i> . All 25 individual host addresses in this range are included in this address object.
Network	Similar to range objects in that they include multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network address objects must be defined by the network's address and a corresponding netmask. For example, <i>My Public Network</i> with a network address of <i>67.115.118.64</i> and a netmask of <i>255.255.255.224</i> would include addresses from <i>67.115.118.64</i> through <i>67.115.118.95</i> . As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) cannot be assigned to a host.
MAC	Allows for the identification of a host by its hardware address or IPv4/IPv6 MAC (Media Access Control) address. MAC addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48-bit values that are expressed in 6-byte hex-notation. For example, <i>My Access Point</i> with a MAC address of <i>00:06:01:AB:02:CD</i> . MAC addresses are resolved to an IP address by referring to the ARP cache on the security appliance. MAC address objects are used by various components of wireless configurations throughout SonicOS, such as SonicPoint or SonicWave identification, and authorizing the BSSID (Basic Service Set Identifier, or WLAN MAC) of wireless access points detected during wireless scans. MAC address objects can also be used to allow hosts to bypass Guest Services authentication.
FQDN	Allows for the identification of a host by its IPv4/IPv6 Fully Qualified Domain Name (FQDN), such as <i>www.sonicwall.com</i> . FQDNs are resolved to their IP address (or IP addresses) using the DNS server configured on the security appliance. Wildcard entries are supported through the responses to queries sent to the DNS servers.

About Address Groups

SonicOS has the ability to group address objects and other address groups into address groups. Address groups can be defined to introduce further referential efficiencies. Address groups can contain any combination of host, range, or network address objects. For example, *My Public Group* can contain the host address object, *My Web Server*, and the range address object, *My Public Servers*, effectively representing IP addresses *67.115.118.66* to *67.115.118.90* and IP address *67.115.118.110*.

Dynamic address objects (MAC and FQDN) should be grouped separately, although they can safely be added to address groups of IP-based address objects, where they will be ignored when their reference is contextually irrelevant (for example, in a NAT policy).

Address groups are automatically created when certain features are enabled, such as a *Radius Pool* address group when the **Enable Local Radius Server** option is enabled in WLAN zone configuration, and are deleted when the feature is disabled.

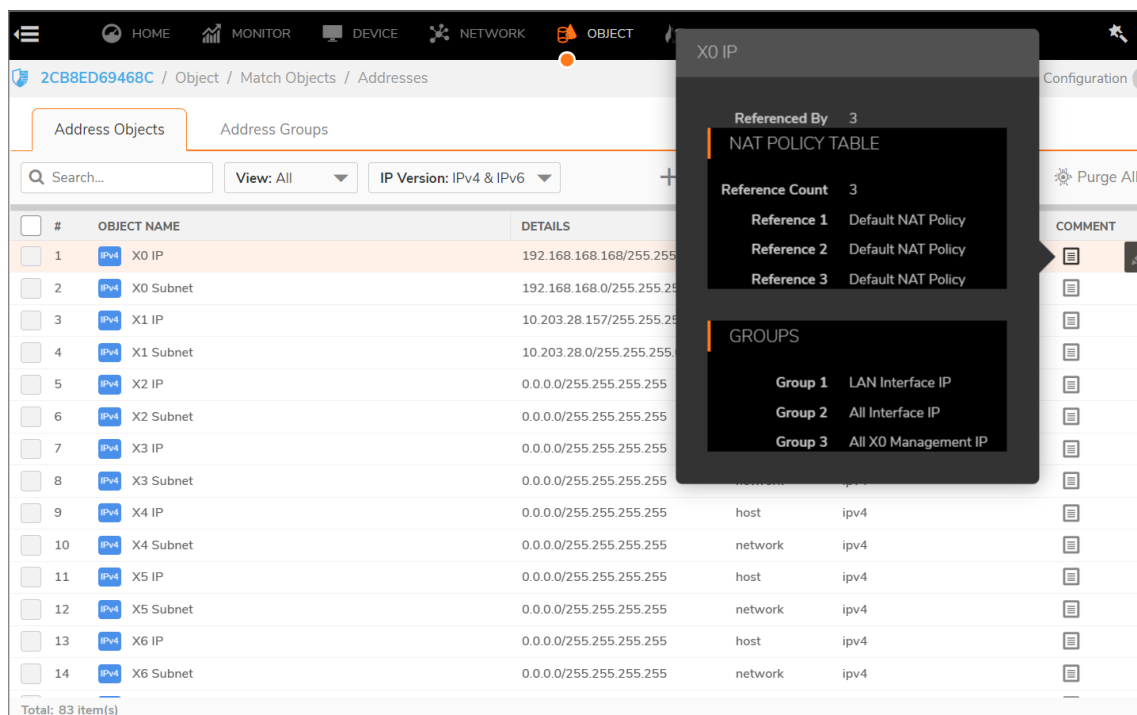
About UUIDs for Address Objects and Groups

A UUID (Universally Unique Identifier) is a 36-character string (32 alphanumeric characters and four hyphens) that is used to uniquely identify address objects and groups, among other entities, on SonicWall network security appliances. The SonicOS UUID is a system-generated, read-only internal value with these properties:

- A UUID is a unique representation of a SonicOS entity across the network.
- A UUID is generated at creation of an entity and removed at the deletion of the entity. It is not reused once it is removed.
- When an entity is modified, the UUID stays the same.
- UUIDs are regenerated after restarting the appliance with factory default settings.

By default, UUIDs are not displayed. UUID display is controlled by internal settings. For more information about internal settings, contact SonicWall Technical Support.

When displayed, UUIDs appear in the tables for each object or group type.



UUIDs facilitate the following functions:

- You can search for an address object or group by UUID with the global search function of the management interface.
- If an object or group object with a UUID is referenced by another entity with a UUID, you can display the reference count and referring entities by mousing over the **Comment** column on the **Addresses** page under **Object**.

Address Objects screen

Address Objects		Address Groups								
Q Search...		View: All	IP Version: IPv4 & IPv6	+ Add	Delete	Delete All	Resolve All	Purge All	Refresh	Display Options
#	OBJECT NAME	DETAILS	TYPE	IP VERSION	ZONE	COMMENT	CLASS	CONFIGURE		
1	X0 IP	192.168.168.168/255.255.255.255	host	ipv4	LAN		Default			
2	X0 Subnet	192.168.168.0/255.255.255.0	network	ipv4	LAN		Default			
3	X1 IP	10.203.28.157/255.255.255.255	host	ipv4	WAN		Default			
4	X1 Subnet	10.203.28.0/255.255.255.0	network	ipv4	WAN		Default			
5	X2 IP	0.0.0.0/255.255.255.255	host	ipv4			Default			
6	X2 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default			
7	X3 IP	0.0.0.0/255.255.255.255	host	ipv4			Default			
8	X3 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default			
9	X4 IP	0.0.0.0/255.255.255.255	host	ipv4			Default			
10	X4 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default			
11	X5 IP	0.0.0.0/255.255.255.255	host	ipv4			Default			
12	X5 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default			
13	X6 IP	0.0.0.0/255.255.255.255	host	ipv4			Default			
14	X6 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default			
15	X7 IP	0.0.0.0/255.255.255.255	host	ipv4			Default			
16	X7 Subnet	0.0.0.0/255.255.255.255	network	ipv4			Default			
17	X8 IP	0.0.0.0/255.255.255.255	host	ipv4			Default			

Total: 86 item(s)

Address Groups screen

Address Objects		Address Groups								
Q Search...		View: All	IP Version: IPv4 & IPv6	+ Add	Delete	Delete All	Resolve All	Purge All	Refresh	Display Options
#	GROUP NAME	DETAILS	TYPE	IP VERSION	ZONE	COMMENT	CLASS	CONFIGURE		
1	All Authorized Access Points	-	Group	ipv4	-		Default			
2	All Interface IP	-	Group	ipv4	-		Default			
3	All Interface IPv6 Addresses	-	Group	ipv6	-		Default			
4	All Rogue Access Points	-	Group	ipv4	-		Default			
5	All Rogue Devices	-	Group	ipv4	-		Default			
6	All SonicPoints	-	Group	ipv4	-		Default			
7	All U0 Management IP	-	Group	ipv4	-		Default			
8	All WAN IP	-	Group	ipv4	-		Default			
9	All X0 Management IP	-	Group	ipv4	-		Default			
10	All X1 Management IP	-	Group	ipv4	-		Default			
11	All X2 Management IP	-	Group	ipv4	-		Default			
12	All X3 Management IP	-	Group	ipv4	-		Default			
13	All X4 Management IP	-	Group	ipv4	-		Default			
14	All X5 Management IP	-	Group	ipv4	-		Default			
15	All X6 Management IP	-	Group	ipv4	-		Default			
16	All X7 Management IP	-	Group	ipv4	-		Default			
17	All X8 Management IP	-	Group	ipv4	-		Default			

Total: 79 item(s)

Common Features

The screen **Address Objects** and **Address Groups** contains these common functions and each table contains the same column headings.

View: All ▼
 IP Version: IPv4 & IPv6 ▼
 + Add
 Delete
 Delete All
 Resolve All
 Purge All
 Refresh

The bottom of each table displays the number of entries in the table.

75
 IPv6
 X9 IPv6 Primary Static Address

Total: 83 item(s)

Common Functions

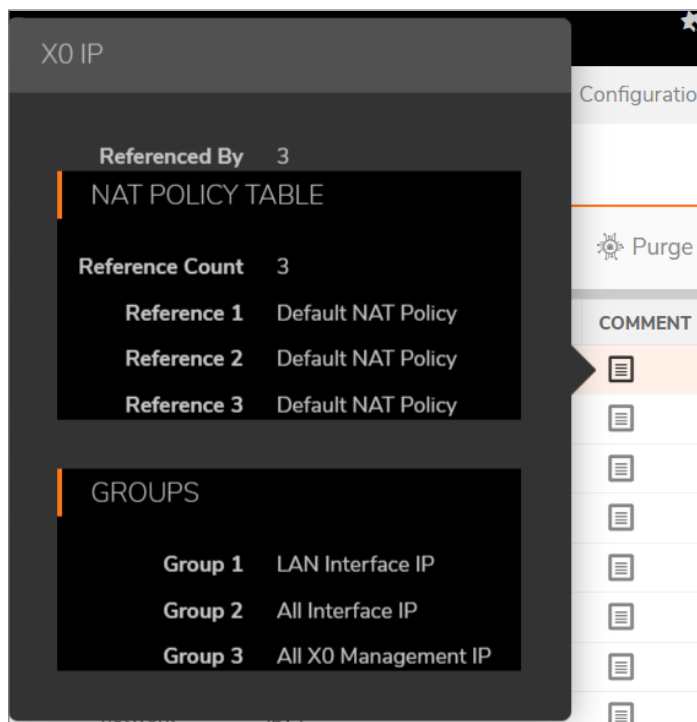
Function	Description
Search	Type in a search string to display only those entries containing the string. The search string is case insensitive.
View	Select Default to display only system-created default entries, Custom to display only custom entries, or All to display all entries. By default, the view type is selected as All .
IP Version	Select IPv4 to display only IPv4 entries, IPv6 to display only IPv6 entries, or IPv4 & IPv6 to display all entries. By default, the IP version is selected as IPv4 & IPv6 .
Add	Click to add an address object or address group.
Delete	Select Delete to delete selected custom entries from the table. Default entries cannot be deleted.
Delete All	Select Delete All to delete all custom entries from the table. Default entries cannot be deleted.
Resolve All	Select Resolve All to resolve all MAC or FQDN entries in the table.
Purge All	Select Purge All to remove out-of-date information from all MAC or FQDN entries. For MAC address objects, this is ARP information, and for FQDN address objects it is DNS TTL values.
Refresh	Click Refresh to refresh the table display.

Common Column Headings

Column Heading	Description
Checkbox	Click to select a custom entry.
#	The number of the entry in the table. This number changes depending on whether the column is sorted by ascending or descending order. The Address Groups screen has a small triangle that allows you to expand or collapse the group entry. <p> <input type="checkbox"/> NOTE: Default address objects and default address groups cannot be deleted. </p>
Name	The unique name of the address object or address group entry. If an address group entry is expanded, this column shows: <ul style="list-style-type: none"> The unique name of each member of the address group. No Entries, if the address group does not contain members.
Details	Shows the details of the address object: applicable addresses or mask. For an address

Column Heading	Description
	group entry, this column is blank; an expanded entry, however, shows the details of the members of the group.
Type	Shows the address object type, such as Host , Network , Range , MAC Address , or FQDN . For an address group, the type is Group ; an expanded entry shows the type of each member.
IP Version	Shows the IP version of the address object or address group member: IPv4 , IPv6 , or Mixed .
Zone	Shows the assigned zone of the address object or address group member.
Class	Shows whether the address object or address group is Default (system defined) or Custom (user defined).
Comments	Mouse over the Comment icon to display pop-up information with details about the entry:

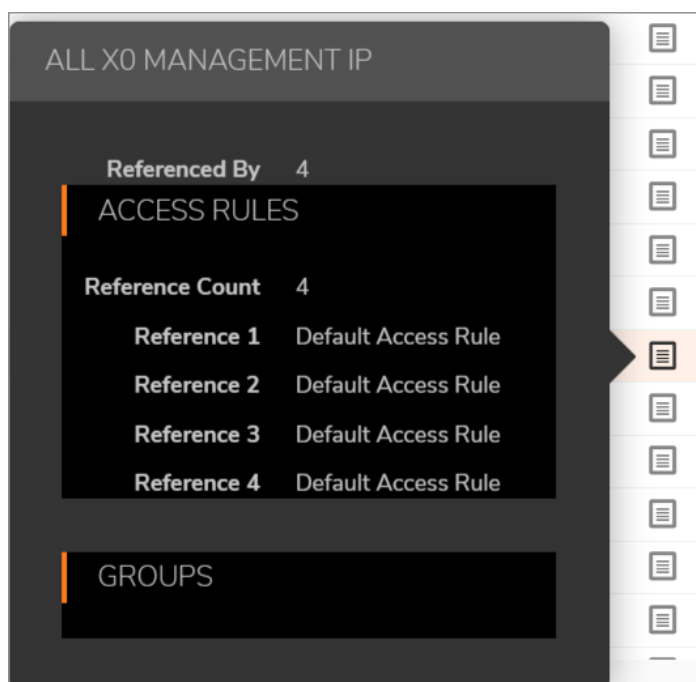
- **Address Object** - Displays this information:



- Name of the address object
- **Referenced By**: – What references the address object and the number of times it has been referenced. If the address object has not been referenced, this section will state *0*.
- **Groups** : – List of groups to which the address object belongs.
- **Configure** : – When you mouse over on the address object **Edit** and **Delete** icons for individual entries are displayed. Only custom address objects can be deleted; only custom entries and some default entries can be edited. If an entry cannot be edited or deleted, the icon(s) are dimmed.

Column Heading	Description
----------------	-------------

- **Address Group** - Displays this information:



- Name of the address group
- **Referenced By:** – What references the address group and the number of times it has been referenced. If the address group has not been referenced, this section will state 0.
- **Groups :** – List of groups to which the address group belongs.
- **Configure :** – When you mouse over on the address group **Edit** and **Delete** icons for individual entries are displayed. Only custom address groups can be deleted; only custom entries and some default entries can be edited. If an entry cannot be edited or deleted, the icon(s) are dimmed.

Sorting the Entries

The **Address Objects** and **Address Groups** screens display tables for easy viewing of address objects and address groups.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order (alphabetical A-Z or numeric starting from zero at the top).

Default Address Objects and Groups

The **Default** view displays the default address objects and address groups for your firewall. Selecting the **Default** view on one screen selects it for both screens. Default address objects entries cannot be modified or deleted although some default address groups can be. Therefore, on the:

- **Address Objects** screen, the **Edit** and **Delete** icons are dimmed.
- **Address Groups** screen, the **Edit** icon for most entries and the **Delete** icon for all but a few entries are dimmed. Those entries that can be edited or deleted have the requisite icons available.

Default Pref64 Address Object

To support the NAT64 feature, SonicOS provides the default network address object, *Pref64*. It is the original destination for a NAT64 policy and is always *pref64::/n*. You can create an address object of **Network** type to represent all addresses with *pref64::/n* to represent all IPv6 clients that can do NAT64; for example:

Name	<input type="text" value="pref64"/>
Zone Assignment	<input type="text" value="WAN"/>
Type	<input type="text" value="Network"/>
Network	<input type="text" value="64:ff9b::"/>
Netmask / Prefix Length	<input type="text" value="64"/>

A well-known prefix, *64:ff9b::/96*, is auto created by SonicOS. For further information about Pref64, see **Policy > NAT Rules** section.

Default Rogue Address Groups

SonicOS provides two default address groups for rogue wireless access points and devices.

- All Rogue Access Points
- All Rogue Devices

When Wireless Intrusion Detection and Prevention (WIDP) is enabled, SonicWave appliances can act as both an access point and as a sensor detecting any unauthorized access point connected to a SonicWall network. Detected rogue access points can be automatically added to the All Rogue Access Points address

group, and detected rogue devices added to the All Rogue Devices address group. For information about enabling options related to rogue access points, see *Configuring Advanced IDP* in the *SonicOS 7 Connectivity* administration documentation.

Adding an Address Object

An address object must be defined before configuring NAT policies, access rules, and services.

To add an address object:

1. Navigate to **Objects > Addresses > Address Objects** page.
2. On the **Address Objects** screen, click **Add** at the top of the page to display the Add Address Object dialog.

Address Object Settings

ADDRESS OBJECT SETTINGS

Name

Zone Assignment

Type

IP Address

Cancel Save

3. In the **Name** field, enter a descriptive, unique name for the network address object.
4. Select the zone for the address object from the **Zone Assignment** drop-down list.
5. Select one of the following from the **Type** drop-down list and fill in the associated fields that display when you select the **Type**:
 - **Host**, enter the IP address in the **IP Address** field.

ADDRESS OBJECT SETTINGS

Name

Zone Assignment

Type

IP Address

- **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

ADDRESS OBJECT SETTINGS

Name

Zone Assignment

Type

Starting IP Address

Ending IP Address

- **Network**, enter the network IP address and netmask (such as 255.255.255.0) or prefix length (such as 24) in the **Network** and **Netmask/Prefix Length** fields.

ADDRESS OBJECT SETTINGS

Name

Zone Assignment

Type

Network

Netmask / Prefix Length

- **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard '*') in the **FQDN Hostname** field. Optionally, select **Manually set DNS entries** and enter the time-to-live in seconds in the **TTL (120 ~ 86400s)** field. The minimum value is 120 and the maximum is 86400 seconds.

ADDRESS OBJECT SETTINGS

Name

Zone Assignment

Type

FQDN Hostname

Manually set DNS entries

TTL (120 ~ 86400s)

- **MAC**, enter the MAC address (such as 00:11:f5:1b:e3:cf) in the **MAC Address** field. By default, **Multi homed** option is selected.

ADDRESS OBJECT SETTINGS

Name

Zone Assignment

Type

MAC Address

Multi homed

6. Click **Save**.

Editing Address Objects

① | **NOTE:** Only custom address objects and certain default address objects can be edited.

To edit an address object:

1. Navigate to **Objects > Addresses > Address Objects** page.
2. In the **Configure** column on the Address object, click **Edit** icon. The Edit Address Object window is displayed, which has the same settings as the **Add Address Object** window (refer to [Adding an Address Object](#)).
3. Click **OK**.

Deleting Address Objects

① | **NOTE:** Only custom address objects can be deleted.

To delete a custom address object:

1. Navigate to **Objects > Addresses > Address Objects** page.
2. In the **Configure** column on the Address object, click **Delete** icon.
3. In the confirmation dialog box, click **OK** to delete the address object.

To delete one or more custom address objects:

1. Navigate to **Objects > Addresses > Address Objects** page.
2. Select the checkboxes for the entries to be deleted.
3. Click **Delete** at the top of the page.
4. In the confirmation dialog box, click **OK** to delete the address objects.

To delete all custom address objects:

1. Navigate to **Objects > Addresses > Address Objects** page.
2. Select **Delete All** at the top of the page.
3. In the confirmation dialog box, click **OK** to delete all the custom address objects.

Purging MAC or FQDN Address Objects

Purge is used to remove out-of-date ARP or DNS information from MAC or FQDN address objects.

To purge all MAC or FQDN address objects:

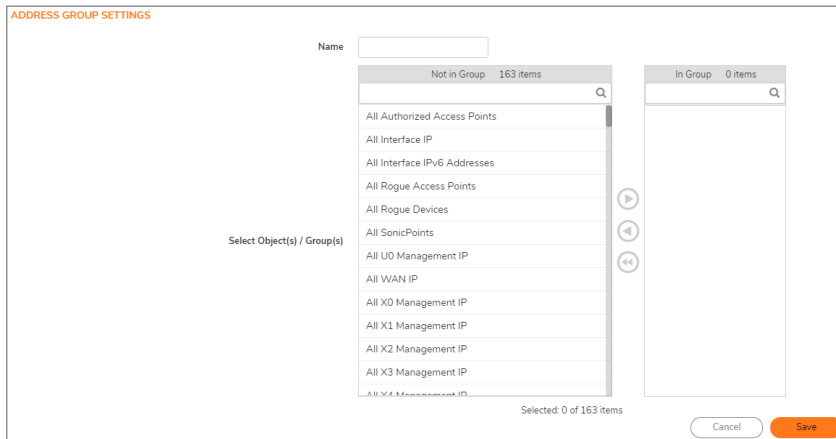
1. Navigate to **Objects > Addresses > Address Objects** page.
2. Click **Purge All** at the top of the page.

Creating Address Groups

As more and more address objects are added to the firewall, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the address group are applied to each address in the group. Address groups can contain other address groups as well as address objects.

To add an address group:

1. Navigate to **Objects > Addresses** page.
2. Click the **Address Groups** tab at the top of the page.
3. On the **Address Groups** screen, click **Add** to display the **Add Address Group** dialog.



4. Create a descriptive, unique name for the group in the **Name** field.
5. Select the desired address objects or groups from the list and then click the right arrow. The selected items move into the list on the right. Press the **Ctrl** or **Shift** key to select multiple items.
To remove an item from the group, select the item in the right column and click the left arrow. The selected item moves from the list on the right to the list on the left. To remove all the items from the

- group, click **un-select all items** icon.
6. Click **Save**.

Editing Address Groups

① | **NOTE:** Only custom and some default address groups can be edited; only custom address groups can be deleted.

To edit an address group:

1. Navigate to **Objects > Addresses** page.
2. Click the **Address Groups** tab at the top of the page.
3. In the **Configure** column on the Address Group, click **Edit** icon. The Edit Address Group window is displayed.
4. To change the name, edit the **Name** field.
5. Select the desired address objects or groups from the list and then click the right arrow. The selected items move into the list on the right. Press the **Ctrl** or **Shift** key to select multiple items.
To remove an item from the group, select the item in the right column and click the left arrow. The selected item moves from the list on the right to the list on the left. To remove all the items from the group, click **un-select all items** icon.
6. Click **Save**.

Deleting Address Groups

① | **NOTE:** Only custom address groups can be deleted.

To delete a custom address group:

1. Navigate to **Objects > Addresses > Address Groups** page.
2. In the **Configure** column on the Address Group, click **Delete** icon.
3. In the confirmation dialog box, click **OK** to delete the address group.

To delete one or more custom address groups:

1. Navigate to **Objects > Addresses > Address Groups** page.
2. Select the checkboxes for the entries to be deleted.
3. Click **Delete** at the top of the page.
4. In the confirmation dialog box, click **OK** to delete the address groups.

To delete all custom address groups:

1. Navigate to **Objects > Addresses > Address Groups** page.
2. Select **Delete All** at the top of the page.
3. In the confirmation dialog box, click **OK** to delete all the custom address groups.

Working with Dynamic Address Objects

From its inception, SonicOS has used address objects to represent IP addresses in most areas throughout the user interface. For information about address object types, refer [Types of Address Objects](#).

SonicOS supports two types of dynamic address objects:

- **MAC** – SonicOS resolves MAC AOs to an IP address by referring to the ARP cache on the firewall.
- **FQDN** – Fully Qualified Domain Names, such as 'www.reallybadWebsite.com', are resolved to their IP address (or IP addresses) using the DNS servers configured on the firewall. Wildcard entries using '*' are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

Key Features of Dynamic Address Objects

The term *Dynamic Address Object (DAO)* describes the underlying framework enabling MAC and FQDN AOs. By transforming AOs from static to dynamic structures, access rules can automatically respond to changes in the network.

The below table provides details and examples for DAOs.

DYNAMIC ADDRESS OBJECTS: FEATURES AND BENEFITS

Feature	Benefit
FQDN wildcard support	<p>FQDN address objects support wildcard entries, such as *.<i>somedomainname.com</i>, by first resolving the base domain name to all its defined host IP addresses, and then by constantly actively gleaning DNS responses as they pass through the firewall. For example, creating an FQDN AO for *.<i>myspace.com</i> will first use the DNS servers configured on the firewall to resolve <i>myspace.com</i> to 63.208.226.40, 63.208.226.41, 63.208.226.42, and 63.208.226.43 (as can be confirmed by nslookup <i>myspace.com</i> or equivalent). As most DNS servers do not allow zone transfers, it is typically not possible to automatically enumerate all the hosts in a domain. Instead, the firewall looks for DNS responses coming from sanctioned DNS servers as they traverse the firewall. So, if a host behind the firewall queries an external DNS server that is also a configured/defined DNS server on the firewall, the firewall parses the response to see if it matches the domain of any wildcard FQDN AOs.</p> <p>① NOTE: Sanctioned DNS servers are those DNS servers configured for use by firewall. The reason that responses from only sanctioned DNS servers are used in the wildcard learning process is to protect against the possibility of FQDN AO poisoning through the use of unsanctioned DNS servers with deliberately incorrect host entries. Future versions of SonicOS might offer the option to support responses from all DNS server. The use of sanctioned DNS servers can be enforced with the use of access rules, as described later in Enforcing the Use of Sanctioned Servers on the Network.</p>

Feature	Benefit
	<p>① NOTE: To illustrate, assume the firewall is configured to use DNS servers 4.2.2.1 and 4.2.2.2, and is providing these DNS servers to all firewalled client via DHCP. If firewalled client-A performs a DNS query against 4.2.2.1 or 4.2.2.2 for <i>vids.myspace.com</i>, the response is examined by the firewall and matched to the defined <i>*.myspace.com</i> FQDN AO. The result (63.208.226.224) is then added to the resolved values of the <i>*.myspace.com</i> DAO.</p> <p>① NOTE: If the workstation, client-A, in the example above had resolved and cached <i>vids.myspace.com</i> before the creation of the <i>*.myspace.com</i> AO, <i>vids.myspace.com</i> would not be resolved by the firewall because the client would use its resolver's cache rather than issuing a new DNS request. As a result, the firewall would not have the chance to learn about <i>vids.myspace.com</i> unless it was resolved by another host. On a Microsoft Windows workstation, the local resolver cache can be cleared using the command ipconfig /flushdns. This forces the client to resolve all FQDNs, thereby allowing the firewall to learn them as they are accessed.</p> <p>① NOTE: Wildcard FQDN entries resolve all hostnames within the context of the domain name, up to 256 entries per AO. For example, <i>*.sonicwall.com</i> resolves <i>www.sonicwall.com</i>, <i>software.sonicwall.com</i>, and <i>licensemanager.sonicwall.com</i>, to their respective IP addresses, but it does not resolve <i>sslvpn.demo.sonicwall.com</i> because it is in a different context; for <i>sslvpn.demo.sonicwall.com</i> to be resolved by a wildcard FQDN AO, the entry <i>*.demo.sonicwall.com</i> would be required, which would also resolve <i>sonicos-enhanced.demo.sonicwall.com</i>, <i>csm.demo.sonicwall.com</i>, <i>sonicos-standard.demo.sonicwall.com</i>, and so on.</p> <p>① NOTE: Wildcards only support full matches, not partial matches. In other words, <i>*.sonicwall.com</i> is a legitimate entry, but <i>w*.sonicwall.com</i>, <i>*w.sonicwall.com</i>, and <i>w*w.sonicwall.com</i> are not. A wildcard can only be specified once per entry, so <i>*.*.sonicwall.com</i>, for example, is not functional.</p>
FQDN resolution using DNS	FQDN address objects are resolved using the DNS servers configured on the firewall in the Network > DNS page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.
MAC address resolution using live ARP cache data	When a node is detected on any of the firewall's physical segments through the ARP (Address Resolution Protocol) mechanism, the firewall's ARP cache is updated with that node's MAC and IP address. When this update occurs, if a MAC address objects referencing that node's MAC is present, it will instantly be updated with the resolved address pairing. When a node times out of the ARP cache due to disuse (for example, the host is no longer L2 connected to the firewall) the MAC AO will transition to an unresolved state.
MAC address object multi-homing support	MAC AOs can be configured to support multi-homed nodes, where multi-homed refers to nodes with more than one IP address per physical interface. Up to 256 resolved entries are allowed per AO. This way, if a single MAC address resolves to

Feature	Benefit
	multiple IPs, all of the IP will be applicable to the access rules, etc., that refer to the MAC AO.
Automatic and manual refresh processes	MAC AO entries are automatically synchronized to the firewall's ARP cache, and FQDN AO entries abide by DNS entry TTL values, ensuring that the resolved values are always fresh. In addition to these automatic update processes, manual Refresh and Purge capabilities are provided for individual DAOs, or for all defined DAOs.

Enforcing the Use of Sanctioned Servers on the Network

Although not a requirement, it is recommended to enforce the use of authorized or sanctioned servers on the network. This practice can help to reduce illicit network activity, and will also serve to ensure the reliability of the FQDN wildcard resolution process. In general, it is good practice to define the endpoints of known protocol communications when possible. For example:

Create address groups of sanctioned servers (for example, SMTP, DNS)

- Create access rules in the relevant zones allowing only authorized SMTP servers on your network to communicate outbound SMTP; block all other outbound SMTP traffic to prevent intentional or unintentional outbound spamming.
- Create access rules in the relevant zones allowing authorized DNS servers on your network to communicate with all destination hosts using DNS protocols (TCP/UDP 53).
 - ① **IMPORTANT:** Be sure to have this rule in place if you have DNS servers on your network, and you will be configuring the restrictive DNS rule that follows.
- Create access rules in the relevant zones allowing firewalled hosts to only communicate via DNS (TCP/UDP 53) with sanctioned DNS servers; block all other DNS access to prevent communications with unauthorized DNS servers.
- Unsanctioned access attempts will then be viewable in the logs.

Using MAC and FQDN Dynamic Address Objects

MAC and FQDN DAOs provide extensive access rule construction flexibility. MAC and FQDN AOs are configured in the same way as static address objects, that is from the **Object > Addresses > Address Objects** page. Once created, their status can be viewed by a mouse-over of their appearance, and log events will record their addition and deletion.

Dynamic address objects lend themselves to many applications. The following are just a few examples of how they may be used.

Blocking All Protocol Access to a Domain using FQDN DAOs

There might be instances where you wish to block all protocol access to a particular destination IP because of non-standard ports of operations, unknown protocol use, or intentional traffic obscuration through encryption, tunneling, or both. An example would be a user who has set up an HTTPS proxy server (or other

method of port-forwarding/tunneling on trusted ports like 53, 80, 443, as well as nonstandard ports, like 5734, 23221, and 63466) on his DSL or cable modem home network for the purpose of obscuring his traffic by tunneling it through his home network. The lack of port predictability is usually further complicated by the dynamic addressing of these networks, making the IP address equally unpredictable.

Since these scenarios generally employ dynamic DNS (DDNS) registrations for the purpose of allowing users to locate the home network, FQDN AOs can be put to aggressive use to block access to all hosts within a DDNS registrar.

① **NOTE:** A DDNS target is used in this example for illustration. Non-DDNS target domains can be used just as well.

Assumptions

- The firewall is configured to use DNS server *10.50.165.3*, *10.50.128.53*.
- The firewall is providing DHCP leases to all firewalled users. All hosts on the network use the configured DNS servers above for resolution.
 - DNS communications to unsanctioned DNS servers optionally can be blocked with access rules, as described in [Enforcing the Use of Sanctioned Servers on the Network](#).
- The DSL home user is registering the hostname, *moosifer.dyndns.org*, with the DDNS provider DynDNS. For this session, the ISP assigned the DSL connection the address *71.35.249.153*.
 - A wildcard FQDN AO is used for illustration because other hostnames could easily be registered for the same IP address. Entries for other DDNS providers could also be added, as needed.

Step 1 – Create the FQDN Address Object:

1. Navigate to **Objects > Addresses > Address Objects** page.
2. Click **Add** and create the following FQDN address object:

The screenshot shows the 'ADDRESS OBJECT SETTINGS' form with the following fields and values:

- Name:** DynDNS.org entries
- Zone Assignment:** WAN
- Type:** FQDN
- FQDN Hostname:** *.dyndns.org
- Manually set DNS entries:**
- TTL (120 ~ 86400s):** 0

At the bottom right of the form are 'Cancel' and 'Save' buttons.

When first created, this entry will resolve only to the address for *dyndns.org*, for example, *63.208.196.110*. When a host behind the firewall attempts to resolve *moosifer.dyndns.org* using a sanctioned DNS server, the IP address(es) returned in the query response will be dynamically added to the FQDN AO.

Step 2 – Create the Access Rule:

1. Navigate to **Policies > Access Rules** page.
2. Click **Add** and create the access rule:

The screenshot shows the 'Adding Access Rule' configuration page. The 'Name' field is 'My Rule', 'Tags' is 'TODO', and 'Description' is 'Adding default rule'. The 'Action' is set to 'Allow', 'Type' is 'IPv4', 'Priority' is 'Auto Prioritize', and 'Schedule' is 'Work Hours'. The 'Enable' toggle is turned on. The 'Source / Destination' tab is selected, showing 'SOURCE' and 'DESTINATION' sections with dropdowns for 'Zone/Interface', 'Address', and 'Port/Services'. There are also 'USERS' and 'TCP / UDP' sections with dropdowns and input fields for inactivity timeouts. At the bottom, there is a 'Show Diagram' toggle and 'Cancel' and 'Save' buttons.

Any protocol access to target hosts within that FQDN will be blocked, and the access attempt will be logged.

Using an Internal DNS Server for FQDN-based Access Rules

It is common for dynamically configured (DHCP) network environments to work in combination with internal DNS servers for the purposes of dynamically registering internal hosts – a common example of this is Microsoft’s DHCP and DNS services. Hosts on such networks can easily be configured to dynamically update DNS records on an appropriately configured DNS server (for example, see the Microsoft Knowledgebase article *How to configure DNS dynamic updates in Windows Server 2003* at <http://support.microsoft.com/kb/816592/en-us>).

The following illustrates a packet dissection of a typical DNS dynamic update process, showing the dynamically configured host *10.50.165.249* registering its full hostname *bohuymath.moosifer.com* with the (DHCP provided) DNS server *10.50.165.3*.

```

19 2.100829 10.50.165.249 2420 10.50.165.3 53 DNS Dynamic update SOA moosifer.com
20 2.105100 10.50.165.3 53 10.50.165.249 2420 DNS Dynamic update response CNAME A 10.50.165.249
# Frame 19 (122 bytes on wire, 122 bytes captured)
# Ethernet II, Src: 00:00:00:1b:e3:cf (00:00:00:1b:e3:cf), Dst: 00:00:00:18:43:00 (00:00:00:18:43:00)
# Internet Protocol, Src: 10.50.165.249 (10.50.165.249), Dst: 10.50.165.3 (10.50.165.3)
# User Datagram Protocol, Src Port: 2420 (2420), Dst Port: 53 (53)
# Domain Name System (query)
  Transaction ID: 0x0bad
  Flags: 0x2800 (Dynamic update)
    0. .... = Response: Message is a query
    .010 1. .... = Opcode: Dynamic update (3)
    .... 0. .... = Truncated: Message is not truncated
    .... 0. .... = Recursion desired: Don't do query recursively
    .... 0. .... = Z: reserved (0)
    .... 0. .... = Non-authenticated data OK: Non-authenticated data is unacceptable
  Zones: 1
  Prerequisites: 2
  Updates: 0
  Additional RRs: 0
# Zone
  moosifer.com: type SOA, class IN
    Name: moosifer.com
    Type: SOA (Start of zone of authority)
    Class: IN (0x0001)
# Prerequisites
  bohuyuth.moosifer.com: type CNAME, class NONE
    Name: bohuyuth.moosifer.com
    Type: CNAME (Canonical name for an alias)
    Class: NONE (0x00fe)
    Time to live: 0 time
    Data length: 0
  bohuyuth.moosifer.com: type A, class IN, addr 10.50.165.249
    Name: bohuyuth.moosifer.com
    Type: A (host address)
    Class: IN (0x0001)
    Time to live: 0 time
    Data length: 4
    Addr: 10.50.165.249

```

In such environments, it could prove useful to employ FQDN AOs to control access by hostname. This would be most applicable in networks where hostnames are known, such as where hostname lists are maintained, or where a predictable naming convention is used.

Controlling a Dynamic Host's Network Access by MAC Address

Since DHCP is far more common than static addressing in most networks, it is sometimes difficult to predict the IP address of dynamically configured hosts, particularly in the absence of dynamic DNS updates or reliable hostnames. In these situations, it is possible to use MAC address objects to control a host's access by its relatively immutable MAC (hardware) address.

Like most other methods of access control, this can be employed either inclusively, for example, to deny access to/for a specific host or group of hosts, or exclusively, where only a specific host or group of hosts are granted access, and all other are denied. In this example, we will illustrate the latter.

Assuming you had a set of DHCP-enabled wireless clients running a proprietary operating system which precluded any type of user-level authentication, and that you wanted to only allow these clients to access an application-specific server (for example, 10.50.165.2) on your LAN. The WLAN segment is using WPA-PSK for security, and this set of clients should only have access to the 10.50.165.2 server, but to no other LAN resources. All other wireless clients should not be able to access the 10.50.165.2 server, but should have unrestricted access everywhere else.

Step 1 – Create the MAC Address Objects:

1. Navigate to **Objects > Addresses > Address Objects** page.
2. Click **Add** and create the following MAC address objects (multi-homing optional, as needed).

ADDRESS OBJECT SETTINGS

Name:

Zone Assignment:

Type:

MAC Address:

Multi homed:

ADDRESS OBJECT SETTINGS

Name:

Zone Assignment:

Type:

MAC Address:

Multi homed:

- Once created, if the hosts are present in the firewall's ARP cache, they will be resolved immediately, otherwise they will appear in an *unresolved* state in the **Address Objects** table until they are activated and are discovered through ARP:
- Create an address group for the handheld devices:

Step 2 – Create the Access Rules:

- Navigate to **Policies > Access Rules** page.
- Click **Add** and create four access rules with the settings shown in the below table.

SAMPLE ACCESS RULES

Setting	Access Rule 1	Access Rule 2	Access Rule 3	Access Rule 4
Allow / Deny	Allow	Deny	Allow	Deny
From Zone	WLAN	WLAN	WLAN	WLAN
To Zone	LAN	LAN	LAN	LAN
Service	MediaMoose Services	MediaMoose Services	Any	Any
Source	Handheld Devices	Any	Handheld Devices	Any
Destination	10.50.165.2	10.50.165.2	Any	Any
Users allowed	All	All	All	All
Schedule	Always on	Always on	Always on	Always on

- ① **NOTE:** The MediaMoose Services service is used to represent the specific application used by the handheld devices. The declaration of a specific service is optional, as needed.

Bandwidth Managing Access to an Entire Domain

Streaming media is one of the most profligate consumers of network bandwidth. But trying to control access, or manage bandwidth allotted to these sites is difficult because most sites that serve streaming media tend to do so off of large server farms. Moreover, these sites frequently re-encode the media and deliver it over HTTP, making it even more difficult to classify and isolate. Manual management of lists of servers is a difficult task, but wildcard FQDN address objects can be used to simplify this effort.

Step 1 – Create the FQDN Address Objects:

1. Navigate to **Objects > Addresses > Address Objects** page.
2. Click **Add** and create the following address object.

ADDRESS OBJECT SETTINGS

Name	All of YouTube
Zone Assignment	WAN
Type	FQDN
FQDN Hostname	*.youtube.com
Manually set DNS entries	<input type="checkbox"/>
TTL (120 ~ 86400s)	0

Upon initial creation, **.youtube.com* resolves to IP addresses *208.65.153.240*, *208.65.153.241*, *208.65.153.242*, but after an internal host begins to resolve hosts for all of the elements within the *youtube.com* domain, the learned host entries are added, such as the entry for the *v87.youtube.com* server (*208.65.154.84*).

Step 2 – Create the Bandwidth Object

1. Navigate to **Objects > Bandwidth** page.
2. Click **Add** and create the bandwidth object.

Bandwidth Object Settings

General
Elemental

BANDWIDTH OBJECT SETTINGS

Name

Guaranteed Bandwidth

Maximum Bandwidth

Traffic Priority

Violation Action

Comments

Cancel
Save

Step 3 – Create the Access Rule:

1. Navigate to **Policies > Access Rules** page.
2. Click **Add** and create the access rule:

Adding Access Rule

Name

Tags

Description

Action Allow Deny Discard

Type IPv4 IPv6

Priority

Schedule

Enable

Source / Destination
Security Profiles
Traffic Shaping
Logging
Optional Settings

SOURCE

Zone/Interface

Address

Port/Services

DESTINATION

Zone/Interface

Address

Port/Services

USERS

Include

Exclude

TCP / UDP

TCP Inactivity Timeout minutes

UDP Inactivity Timeout seconds

Show Diagram
Cancel Save

After the access rule is created, the Bandwidth Management icon appears within the Access Rule table, indicating that BWM is active and providing statistics. Move your mouse pointer over the icon to see the BWM settings.

Access to all *.youtube.com hosts, using any protocol, is now be cumulatively limited to speed that you have set, a low percentage of your total available bandwidth for all user sessions.

Services

Service Objects and Service Groups are configured under **Object > Services** page.

SonicOS supports an expanded IP protocol support to allow users to create service objects, service groups, and access rules based on these custom service protocols. For a list of pre-defined protocols, see [Predefined IP Protocols for Custom Service Objects](#). To add specific IP protocols required for your network, refer to [Adding Custom IP Type Services](#).

Services are used by the SonicWall security appliance to configure access rules for allowing or denying traffic to the network. The SonicWall security appliance includes predefined default service objects and default service groups. You can edit, but not delete, default service objects and default service groups.

You can create custom service objects and custom service groups to meet your specific business requirements.

The **View** drop-down list at the top of the page allows you to control the display of default and custom service objects and groups. Select **All** type to display both custom and default entries, select **Custom** to display only custom, or select **Default** to display only default service entries.

Service Objects		Service Groups									
Q Search...		View: All		+ Add		Delete		Refresh		Display Options	
<input type="checkbox"/>	#	NAME	PROTOCOL	PORT START	PORT END	CLASS	CONFIGURE				
<input type="checkbox"/>	▶ 1	HTTP	TCP	80	80	Default					
<input type="checkbox"/>	▶ 2	HTTP Management	TCP	80	80	Default					
<input type="checkbox"/>	▶ 3	HTTPS	TCP	443	443	Default					
<input type="checkbox"/>	▶ 4	HTTPS Management	TCP	443	443	Default					
<input type="checkbox"/>	▶ 5	HTTPS Redirect	TCP	0	0	Default					
<input type="checkbox"/>	▶ 6	RADIUS Accounting	UDP	1813	1813	Default					
<input type="checkbox"/>	▶ 7	SSO 3rd-Party API	TCP	0	0	Default					
<input type="checkbox"/>	▶ 8	IDENT	TCP	113	113	Default					
<input type="checkbox"/>	▶ 9	IMAP3	TCP	220	220	Default					
<input type="checkbox"/>	▶ 10	IMAP4	TCP	143	143	Default					
<input type="checkbox"/>	▶ 11	ISAKMP	UDP	500	500	Default					
<input type="checkbox"/>	▶ 12	LDAP	TCP	389	389	Default					
<input type="checkbox"/>	▶ 13	LDAP (UDP)	UDP	389	389	Default					
<input type="checkbox"/>	▶ 14	LDAPS	TCP	636	636	Default					
<input type="checkbox"/>	▶ 15	LPR (Unix Printer)	TCP	515	515	Default					
<input type="checkbox"/>	▶ 16	Megaco H.248 TCP	TCP	2944	2944	Default					
<input type="checkbox"/>	▶ 17	Megaco Text H.248 UDP	UDP	2944	2944	Default					

Total: 225 items

About Default Service Objects and Groups

Default service objects and groups are predefined in SonicOS and cannot be deleted, but can be edited. Only ports can be edited for default service objects. For default service groups, you can change the included or excluded services.

The **Service Objects** and **Service Groups** table display the following attributes of the service objects and service groups.

Name	The name of the service.
Protocol	The protocol of the service.
Port Start	The starting port number for the service.
Port End	The ending port number for the service.
Class	Indicates whether the entry is a Default (system) or Custom (user) service.
Comment	Move your mouse over the comment icon to display information about the service object or group. A popup displays the following: <ul style="list-style-type: none">• Referenced By – with a list of the types of rules or policies configured on the firewall which use the service object or group, along with the number of references to it for each type. The rule or policy type is displayed as a link when available, such as for Access Rules, NAT Policies, etc. You can click the link to go to the page to see the list of specific rules or policies using the service object or group.• Groups (Member of) – with a list of service groups or other types of groups that include the service object or group.
Configure	Displays the Edit , View and Delete icons for the service (default services cannot be deleted and their Delete icon is dimmed). The Edit icon displays the Edit Service dialog. Only ports can be edited for default service objects. For default service groups, you can change the included or excluded services.

Default service groups are groups of default service objects and/or other default service groups. Clicking on the triangle to the left of the group name displays all the individual default service objects and groups included in the group. For example, the **AD Directory Services** default group contains several service objects and service groups (refer to [AD Directory Services Group Details](#)). By grouping these multiple entries together, they can be referenced as a single service in rules and policies throughout SonicOS.

AD Directory Services Group Details

Service Objects		Service Groups					
#	NAME	PROTOCOL	COMMENT	PORT START	PORT END	CLASS	CONFIGURE
1	AD Directory Services					Default	
	LDAP	TCP		389	389	Default	
	LDAP (UDP)	UDP		389	389	Default	
	LDAPS	TCP		636	636	Default	
	NTP	UDP		123	123	Default	
	DCE EndPoint	TCP		135	135	Default	
	RPC Services	TCP		1025	5000	Default	
	RPC Services (ANA)	TCP		49152	65535	Default	
	AD NetBios Services					Default	
	Host Name Server					Default	
	Kerberos					Default	

Predefined IP Protocols for Custom Service Objects

ICMP (1)	Internet Control Message Protocol. A TCP/IP protocol used to send error and control messages.
IGMP (2)	Internet Group Management Protocol. The protocol that governs the management of multicast groups in a TCP/IP network.
TCP (6)	Transmission Control Protocol. The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.
UDP (17)	User Datagram Protocol. A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
6over4 (41)	Transmission of IPv6 over IPv4 domains without explicit tunnels. The 6over4 traffic is transmitted inside IPv4 packets whose IP headers have the IP protocol number set to 41.
GRE (47)	Generic Routing Encapsulation. A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP Internetwork.
ESP (50)	Encapsulated Security Payload. A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPsec.
AH (51)	Authentication Header. A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).
ICMPv6 (58)	Neighbor Discovery for Internet Message Control Protocol version 6. Neighbor Discovery defines five different ICMP packet types: A pair of Router Solicitation and Router Advertisement messages, a pair of Neighbor Solicitation and Neighbor Advertisements messages, and a Redirect message.
EIGRP (88)	Enhanced Interior Gateway Routing Protocol. Advanced version of

	IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
OSPF (89)	Open Shortest Path First. A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.
PIM (103)	<p>Protocol Independent Multicast). One of two PIM operational modes:</p> <ul style="list-style-type: none"> • PIM sparse mode (PIM-SM) tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. • PIM dense mode (PIM-DM) assumes all downstream routers and hosts want to receive a multicast datagram from a sender and floods multicast traffic throughout the network. Routers without downstream neighbors prune unwanted traffic. To minimize repeated flooding of datagrams and subsequent pruning, PIM DM uses a state refresh message sent by routers directly connected to the source. <p>① NOTE: The firewall can be configured only as a multicast proxy so multicast traffic can be passed through the up-/downstream interface. The firewall cannot act as a PIM router.</p>
L2TP (115)	Layer 2 Tunneling Protocol) A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPsec to provide virtual private network (VPN) connections from remote users to the corporate LAN.

Adding Service Objects using Predefined Protocols

You can add a custom service object for any of the predefined protocols, or service types:

PREDEFINED SERVICE TYPES

Protocol	IP Number
ICMP	1

IGMP	2
TCP	6
UDP	17
6over4	41
GRE	47
IPsec ESP	50
IPsec AH	51
ICMPv6	58
EIGRP	88
OSPF	89
PIM	103
L2TP	115

For definitions of these protocols, see [Predefined IP Protocols for Custom Service Objects](#).

All custom service objects you create are listed in the **Service Objects** table. You can group custom services by creating a custom service group for easy policy enforcement. If a protocol is not listed as a default service object, you can add a custom service object for it.

To add a custom service object using predefined protocols:

1. Navigate to **Object > Match Objects > Services > Service Objects** page.
2. Click the **Add** button. The **Service Objects** dialog displays.

3. Enter a descriptive name for the service object in the **Name** field.
 4. Select the type of IP protocol from the **Protocol** drop-down menu. The fields in the dialog may change.
 5. What you enter next depends on your IP protocol selection:
 - For **TCP** and **UDP** protocols, specify the **Port Range**.
 - For **ICMP**, **IGMP**, **OSPF**, and **PIM** protocols, select a Sub Type from the **Sub Type** drop-down menu.
- ① **NOTE:** PIM subtypes apply to both PIM-SM and PIM-DM except the following are for PIM SM only:
- **Type1: Register**
 - **Type2: Register Stop**

- **Type4: Bootstrap**
 - **Type8: Candidate RP Advertisement**
 - For the remaining protocols, you do not need to specify anything further.
6. Click **Save**.

Adding Custom IP Type Services

Using only the predefined IP protocol types, if the security appliance encounters traffic of any other IP protocol type it drops it as *unrecognized*. However, there exists a large and expanding list of other registered IP types, as governed by IANA (Internet Assigned Numbers Authority):

<http://www.iana.org/assignments/protocol-numbers>, so while the rigid practice of dropping less-common (unrecognized) IP Type traffic is secure, it is functionally restrictive.

SonicOS allows you to construct service objects representing any IP type, allowing access rules to then be written to recognize and control IP traffic of any type.

① **NOTE:** The generic service **Any** does not handle custom IP type service objects. In other words, simply defining a custom IP type service object for “IP Type 126” does not allow IP Type 126 traffic to pass through the default **LAN > WAN** Allow rule.

You need to create an access rule specifically containing the custom IP type service object to provide for its recognition and handling, as illustrated in [Configuration Example](#).

Configuration Example

Assume an administrator needs to allow RSVP (Resource Reservation Protocol - IP Type 46) and SRP (Spectralink™ Radio Protocol – IP type 119) from all clients on the WLAN zone (WLAN Subnets) to a server on the LAN zone (for example, *10.50.165.26*). You can define custom IP type service objects to handle these two services.

To define a custom IP type service and related configuration:

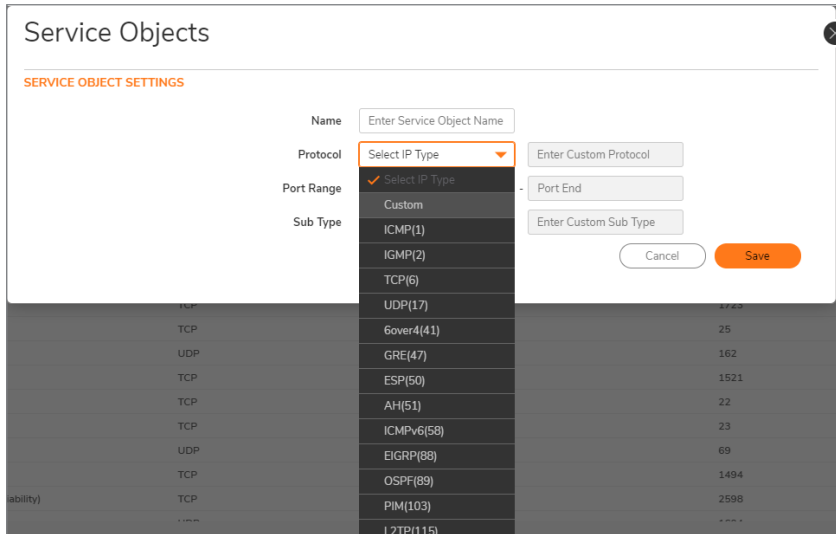
1. Navigate to **Object > Match Objects > Services > Service Objects** page.
2. Click the **Add** button. The **Service Objects** dialog displays.

Service Objects

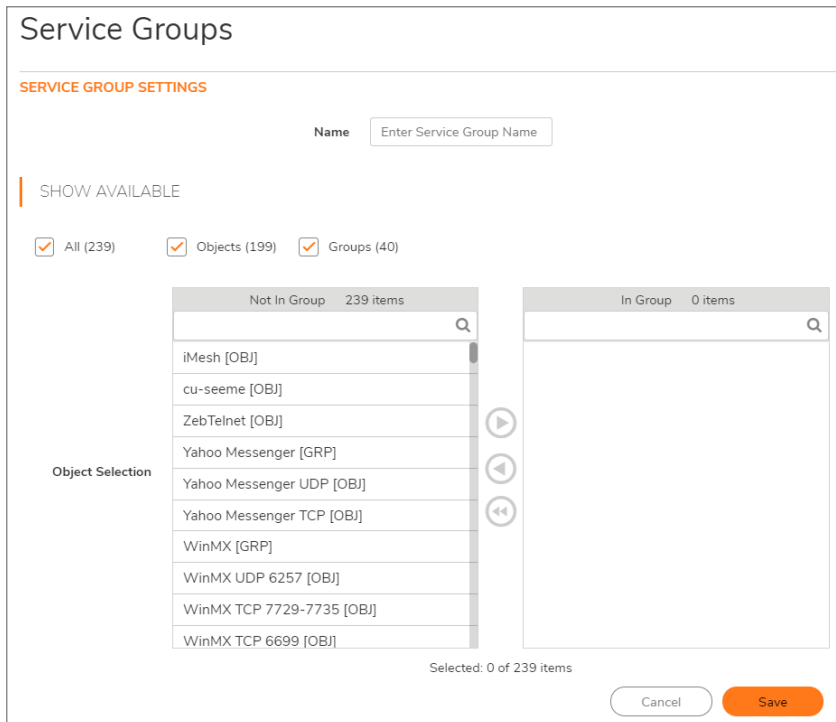
SERVICE OBJECT SETTINGS

Name	<input type="text" value="Enter Service Object Name"/>	
Protocol	<input style="width: 100px;" type="text" value="Select IP Type"/>	<input type="text" value="Enter Custom Protocol"/>
Port Range	<input type="text" value="Port Start"/>	- <input type="text" value="Port End"/>
Sub Type	<input style="width: 100px;" type="text" value="Select Sub IP Type"/>	<input type="text" value="Enter Custom Sub Type"/>

3. Enter a descriptive name for the service object in the **Name** field.
4. Select **Custom** IP type from the **Protocol** drop-down menu.



5. In the field to the right of the **Protocol** drop-down list, type in the protocol number for the **Custom IP Type**.
 - ① **NOTE:** The **Port Range** and **Sub Type** fields are not definable or applicable to a Custom IP Type.
 - ① **NOTE:** Attempts to define a custom protocol type service object for a predefined IP type is not permitted and results in an error message.
6. Click **Save**.
7. Repeat **Step 3 through Step 6** for each custom service to be defined.
8. Navigate to **Object > Match Objects > Services > Service Groups** page.
9. Click the **Add** button. The **Service Groups** dialog displays.



10. Enter a descriptive name for the service group in the **Name** field, such as *myServices*.
11. Select the custom service objects you just created from the list on the left, and then click the **Right Arrow** button to move them into the list on the right.
 - ① **NOTE:** Press **Ctrl** or **Shift** to select multiple service objects, and then click the **Right Arrow** button to move them all at one time.
12. Click **Save**.
13. Navigate to **Object > Match Objects > Services > Service Objects** page.
14. Click the **Add** button. The **Service Objects** dialog displays.
15. Create an address object for the host that the WLAN Subnets can access using *myServices*.
16. Select the custom service objects you just created from the list on the left, and then click the **Right Arrow** button to move them into the list on the right.
 - ① **NOTE:** Press **Ctrl** or **Shift** to select multiple service objects, and then click the **Right Arrow** button to move them all at one time.
17. Click **Save**.
18. Navigate to **Policy > Rules and Policies > Access Rules** page to create a **WLAN > LAN** rule.
19. Define an access rule allowing *myServices* from **WLAN Subnets** to the *10.50.165.26* address object.
 - ① **NOTE:** It may be necessary to create an access rule for bidirectional traffic; for example, an additional access rule from the **LAN > WLAN** allowing *myServices* from *10.50.165.26* to WLAN Subnets.
20. Click **Save**.
IP protocol 46 and 119 traffic will now be recognized and allowed to pass from WLAN Subnets to the host at *10.50.165.26*.

Editing Custom Service Objects

Click the **Edit** icon under **Configure** to edit the service object which includes the same configuration settings as the **Add Service** dialog. Refer to [Adding Service Objects using Predefined Protocols](#) or [Adding Custom IP Type Services](#).

Deleting Custom Service Objects

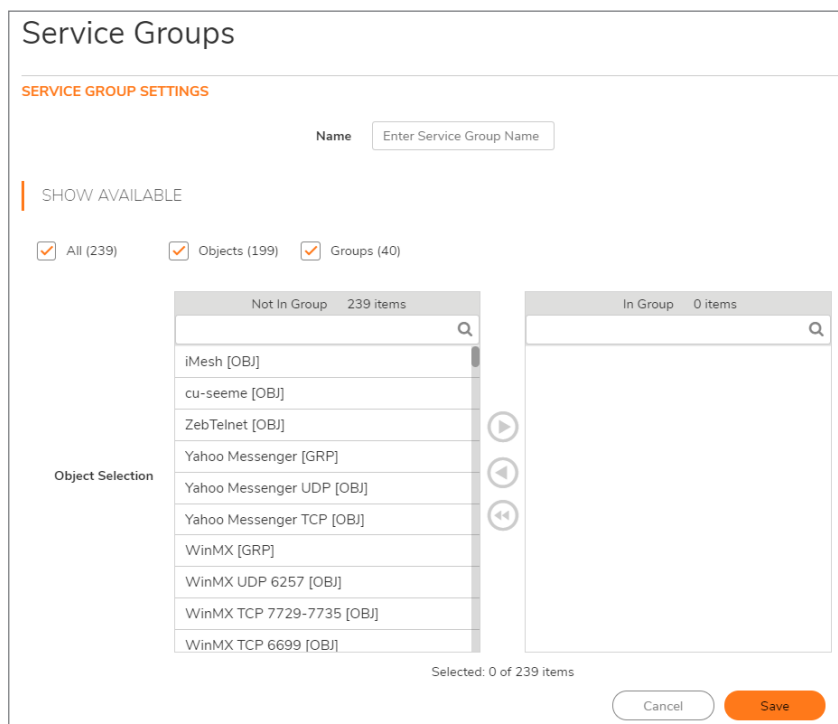
In the row for the service object you want to delete, click the **Delete** icon under **Configure** to delete an individual custom service object. To delete one or more custom service objects, select the checkboxes for the desired entries and click **Delete** at the top of the page.

Adding Custom Service Groups

You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a custom service group.

To create a custom service group:

1. Navigate to **Object > Match Objects > Service Groups** page.
2. Click the **Add** button. The **Service Groups** dialog displays.



3. Enter a name for the custom group in the **Name** field.
4. Select the custom service objects you just created from the list on the left, and then click the **Right Arrow** button to move them into the list on the right.
 - ① **NOTE:** Press **Ctrl** or **Shift** to select multiple service objects, and then click the **Right Arrow** button to move them all at one time.
5. Click **Save**.

Clicking the triangle to the left of a Custom service group name, expands the display to show all the individual Custom Services, Default Services, and Custom Services Groups included in the Custom service group entry.

#	NAME	PROTOCOL	COMMENT	PORT START	PORT END	CLASS	CONFIGURE
1	AD Directory Services					Default	[Edit] [Delete]
	LDAP	TCP		389	389	Default	
	LDAP (UDP)	UDP		389	389	Default	
	LDAPS	TCP		636	636	Default	
	NTP	UDP		123	123	Default	
	DCE EndPoint	TCP		135	135	Default	
	RPC Services	TCP		1025	5000	Default	
	RPC Services (IANA)	TCP		49152	65535	Default	
	AD NetBios Services					Default	
	Host Name Server					Default	
	Kerberos					Default	

Editing Custom Service Groups

Click the **Edit** icon in the **Configure** column to edit the custom service group, which includes the same configuration settings as the **Add Service Group** dialog.

You also can edit individual services of a custom service group by expanding the group, and clicking the **Edit** icon for the service.























Deleting Custom Service Groups

In the row for the service group you want to delete, click the **Delete** icon under **Configure** to delete an individual custom service group. To delete one or more custom service groups, select the checkboxes for the desired entries, click **Delete** at the top of the page.

Countries

The Country Objects screen provides a list of country objects that are available in the selection.

Country Objects

#	NAME	FLAG	CREATED	UPDATED	CLASS	GROUP REFERENCES
1	Afghanistan		2021-02-16 14:45		Default	
2	Aland Islands		2021-02-16 14:45		Default	
3	Albania		2021-02-16 14:45		Default	
4	Algeria		2021-02-16 14:45		Default	
5	American Samoa		2021-02-16 14:45		Default	
6	Andorra		2021-02-16 14:45		Default	
7	Angola		2021-02-16 14:45		Default	
8	Anguilla		2021-02-16 14:45		Default	
9	Anonymous Proxy/Private IP		2021-02-16 14:45		Default	
10	Antarctica		2021-02-16 14:45		Default	
11	Antigua and Barbuda		2021-02-16 14:45		Default	

Total: 253 item(s)

- **Export** - Exports the Country Objects Data to a CSV file.
- **Refresh** - Refreshes the list.
- **Column Selection** - Choose which columns to be shown in the list.

Country Groups

You can group any combination of Countries and then save your selections in the policy preferences.

Add Country Groups

Country Objects		Country Groups									
Q Search...		Used and Unused									
+ Add		Delete		Delete All		Export		Refresh		Column Selection	
#	NAME	FLAG	POLICY REFERENCES	CREATED	UPDATED	CLASS					
<input checked="" type="checkbox"/>	▶ 4	[?]		2021-03-26 17:46	2021-04-05 22:31	Custom					
<input type="checkbox"/>	▶ b	[?]		2021-04-05 17:50	2021-04-05 17:50	Custom					
<input type="checkbox"/>	▶ china	[?]		2021-03-01 15:28	2021-04-05 22:31	Custom					
<input type="checkbox"/>	▶ Contries 1	[?]		2021-02-19 17:55	2021-04-05 22:31	Custom					
<input type="checkbox"/>	▶ country1	[?]	Custom Security Policy_3	2021-04-05 17:50	2021-04-05 17:50	Custom					
<input type="checkbox"/>	▶ grp1	[?]		2021-04-05 20:20	2021-04-05 20:20	Custom					
<input type="checkbox"/>	▶ test_c1	[?]	Custom Security Policy_4	2021-04-05 17:24	2021-04-05 22:31	Custom					
<input type="checkbox"/>	▶ tt	[?]		2021-04-05 17:22	2021-04-05 22:31	Custom					

- **Add** - Add country group
 1. Click **Add** to add country group.
 2. Input a group name in the **Name** field.
 3. Select the countries which are not in the group by clicking on individual entries in the list.
 4. Click the arrow to move marked countries to the right view.
 5. Click **Save** to save the group.
- **Delete** - Check the box to delete a selected group.
- **Delete All** - Deletes all the groups in the list
- **Export** - Exports the Country Groups Data to a CSV file.
- **Refresh** - Refreshes the list.
- **Column Selection** - Choose which columns to be shown in the list.

Applications

The applications screen provides a list of applications that are available in the selection.

Application Objects

#	NAME	TYPE	CATEGORY	APPLICATION	RISK	TECHNOLOGY	TO CLIENT	TO SERVER	INCOMING	OUTGOING
1	00unblock	Application	PROXY-ACCESS			None				
2	00unblock - Browsing Activity	Component	PROXY-ACCESS	00unblock	3 / 5	Browser	✓			✓
3	100Bao	Application	P2P			None				
4	100Bao - Outbound Connection	Component	P2P	100Bao	4 / 5	Application		✓		✓
5	115Udown	Application	DOWNLOAD-APPS			None				
6	115Udown - DNS Query	Component	DOWNLOAD-APPS	115Udown	3 / 5	Application	✓	✓		✓
7	115Udown - File Sharing	Component	DOWNLOAD-APPS	115Udown	3 / 5	Application	✓	✓		✓
8	11st.co.kr	Application	BUSINESS-APPS			None				
9	11st.co.kr - Browsing Activity	Component	BUSINESS-APPS	11st.co.kr	1 / 5	Browser		✓		✓

Total: 5083 item(s)

- **Viewer** - Displays the application objects in a viewer.
- **Export** - Exports the Country Objects Data to a CSV file.
- **Refresh** - Refreshes the list.
- **Column Selection** - Choose which columns to be shown in the list.

Application Groups

You can group any combination of application groups and then save your selections in the policy preferences.

Add Application Groups

#	NAME	TYPE	CATEGORY	APPLICATION	RISK	TECHNOLOGY	TO CLIENT	TO SERVER	INCOMING	OUTGOING
1	app									
2	Application Tech App Group									
3	Browser Tech App Group									
4	Default App Object Group									
5	Elevated Risk App Group									
6	facebook									
7	FB									
8	Guarded Risk App Group									
9	High Risk App Group									
10	ICMP-based Protocol App Group									

Total: 22 item(s)

- **Viewer** - Displays the application groups in a viewer.
- **Add** - Adds application group
 1. Click **Add** to add application group.
 2. Input a group name in the **Name** field.
 3. Select the applications which are not in the group by clicking on individual entries in the list. Click **Browse** to choose from the application selector window and click **Select**.
 4. Click the arrow to move the applications to the right view.
 5. Click **Add** to save the group.
- **Delete** - Check the box to delete a selected group.
- **Delete All** - Deletes all the groups in the list
- **Export** - Exports the Application Groups Data to a CSV file.
- **Refresh** - Refreshes the list.
- **Column Selection** - Choose which columns to be shown in the list.

Web Categories

The applications screen provides a list of web categories that are available in the selection.

Web Category Objects

#	NAME	RATING ID	GROUP REFERENCE COUNT	GROUP REFERENCES	CREATED	UPDATED
8	Drugs/Illegal Drugs	8	1		2021-04-05 22:31	2021-04-05 22:32
9	Illegal Skills/Questionable Ski	9	1		2021-04-05 22:31	2021-04-05 22:32
10	Sex Education	10	1		2021-04-05 22:31	2021-04-05 22:32
11	Gambling	11	1		2021-04-05 22:31	2021-04-05 22:32
12	Alcohol/Tobacco	12	1		2021-04-05 22:31	2021-04-05 22:32
13	Chat/Instant Messaging (IM)	13	0		2021-04-05 22:32	2021-04-05 22:32
14	Arts/Entertainment	14	0		2021-04-05 22:32	2021-04-05 22:32
15	Business and Economy	15	0		2021-04-05 22:32	2021-04-05 22:32
16	Abortion/Advocacy Groups	16	0		2021-04-05 22:32	2021-04-05 22:32
17	Education	17	0		2021-04-05 22:32	2021-04-05 22:32

Total: 57 item(s)

- **Export** - Exports the Web Category Objects Data to a CSV file.
- **Refresh** - Refreshes the list.
- **Column Selection** - Choose which columns to be shown in the list.

Web Category Groups

You can group any combination of web category groups and then save your selections in the policy preferences.

Add Web Category Groups

#	NAME	RATING ID	POLICY REFERENCE COUNT	POLICY REFERENCES	CREATED	UPDATED
1	Default Web Category Object Group	0	0		2021-02-16 09:53	2021-04-05 22:32
2	Travel and Ads	0	0		2021-03-05 20:58	2021-04-05 22:32
3	custom_	0	0		2021-03-01 15:05	2021-04-05 22:32

- **Add** - Adds web category group
 1. Click **Add** to add application group.
 2. Input a group name in the **Name** field.
 3. Select the applications which are not in the group by clicking on individual entries in the list.
 4. Click the arrow to move the applications to the right view.
 5. Click **Save** to save the group.
- **Delete** - Check the box to delete a selected group.
- **Delete All** - Deletes all the groups in the list
- **Export** - Exports the web category Groups Data to a CSV file.
- **Refresh** - Refreshes the list.
- **Column Selection** - Choose which columns to be shown in the list.

Websites

The main screen provides a list of websites that are available in the selection.

#	NAME	CONTENT	GROUP REFERENCE COUNT	GROUP REFERENCES	CREATED	UPDATED
No Data						

Website Objects

- **Add**

To add a Website Object:

1. Click **Add**.
2. Input a Website Object name in the **Name** field.
3. Create the Website Object **Domain List** in the field provided.

① **NOTE:** To match URL `www.yahoo.com/*` input **www.yahoo.com** in the domain name field. To match URL `*.yahoo.*/*` input **yahoo** in the domain name field, and to match URL `*.yahoo.in/*` input **yahoo.in** in the domain name field. Multiple matches can be added, separated by a comma.

4. Click **Save** to save the object.
- **Delete** - Check the box to delete a selected object.
 - **Export** - Exports the Website Objects to a CSV file.
 - **Refresh** - Refreshes the list.
 - **Column Selection** - Choose which columns are shown in the list.

Website Groups

You can group any combination of websites or groups and then save your selections in the policy preferences.

#	NAME	CONTENT	POLICY REFERENCE COUNT	POLICY REFERENCES	CREATED	UPDATED
1	Default Website Object Group		0		2021-04-26 02:41	2021-04-26 02:41

- **Add**

To add a Website Group:

1. Click **Add**.
 2. Input a Website Group name in the **Name** field.
 3. From the Website Objects listed, move the objects you want in the group and remove any you don't want included.
 4. Click **Save** to save the group.
- **Delete** - Check the box to delete a selected object.
 - **Export** - Exports the Website Groups to a CSV file.
 - **Refresh** - Refreshes the list.
 - **Column Selection** - Choose which columns are shown in the list.

URI Lists

A **URI List Object** defines a list of URIs (Uniform Resource Identifiers) or domains that can be marked as allowed or forbidden. You can also export a URI list to an external file or import a file into a URI list.

When processing, URI lists have a higher priority than the category of a URI.

URI List Objects have the following requirements:

- Up to 128 URI List Objects are allowed.
- Each URI List Object supports up to 5000 URIs. The minimum number is 1.
- Up to 100 Keywords can be configured in each URI List Object. The minimum is zero.

About URIs and the URI List

Each **URI List Object** must have at least one URI in its **URI List**. You can manually add entries to the **URI List** by typing or pasting them in, or you can import a list of URIs from a text (*.txt*) file. The file can be created manually, or can be a file that was previously exported from the appliance. Each URI in the file is on its own line.

You can export the **URI List** contents into a text file that you can import later.

The URIs and **URI List** have the following requirements:

- Each URI can be up to 255 characters.
- The maximum combined length of all URIs in one **URI List** is 131,072 (1024*128) characters, including one character for each new line (carriage return) between the URIs.
- By definition, a URI is a string containing host and path. Port and other content are currently not supported, but you can use Keywords to match these.
- The host portion of a URI can be an IPv4 or IPv6 address string.
- Each URI can contain up to 16 tokens. A token in a URI is a string composed of the characters:
0 through 9
a through z
A through Z
\$ - _ + ! ' () , .
 - Each token can be up to 64 characters, including one character for each separator (. or /) surrounding the token.

- An asterisk (*) can be used as a wildcard representing a sequence of one or more valid tokens, not one or more characters.

Examples of valid URIs	Examples of invalid URIs
<ul style="list-style-type: none"> • <i>news.example.com</i> • <i>news.example.com/path</i> • <i>news.example.com/path/abc.txt</i> • <i>news.*.com/*.txt</i> • <i>10.10.10.10</i> • <i>10.10.10.10/path</i> • <i>[2001:2002::2003]/path</i> • <i>[2001:2002::2003:*.2004]/path/*.txt</i> 	<p>Using the wildcard character (*) incorrectly can result in invalid URIs such as:</p> <ul style="list-style-type: none"> • <i>example*.com</i> • <i>exa*ple.com</i> • <i>example.*.*.com</i> <p>NOTE: The wildcard character represents a sequence of one or more tokens, not one or more characters.</p>

About Keywords and the Keyword List

A URI List Object uses its URI List to match URIs when scanning web traffic. It uses a token-based match algorithm, which means *torrent.com* does not match *seedtorrent.com*. The Keyword List makes URI matching more flexible, allowing the URI List Object to match traffic by matching other portions of a URI.

If a web traffic URI string (host+path+queryString) has any sub-string in the keyword list, the URI List Object gets a match. For example, if “sports” and “news” are in the keywords list, the URI List Object can match *www.extremesports.com*, *news.google.com/news/headlines?ned=us&hl=en*, or *www.yahoo.com/?q=sports*.

As with the URI List, you can manually add entries to the **Keyword List** by typing or pasting them in, or you can import a list of keywords from a text (*.txt*) file. The file can be created manually, or can be a file that was previously exported from the appliance. Each keyword in the file is on its own line.

You can export the **Keyword List** contents into a text file that you can import later.

Keyword and Keyword List requirements:

- Each keyword can contain up to 255 printable ASCII characters.
- The maximum combined length of keywords in one **Keyword List** is limited to 1024 * 2, including one character for each new line (carriage return) between the keywords.

Matching URI List Objects

The matching process for **URI List Objects** is based on tokens. A valid token sequence is composed of one or more tokens, joined by a specific character, like “.” or “/”. A URI represents a token sequence. For example, the URI *www.example.com* is a token sequence consisting of *www*, *example*, and *com*, joined by a “.”. Generally, if a URI contains one of the URIs in a URI List Object, then the URI List Object matches that URI.

Normal Matching

If a list object contains a URI such as *example.com*, then that object matches URIs defined as:

```
[<token sequence>(./)]example.com[(./)<token sequence>]
```

For example, the URI List Object matches any of the following URIs:

- *example.com*
- *www.example.com*
- *example.com.uk*
- *www.example.com.uk*
- *example.com/path*

The URI List Object does not match the URI, *specialexample.com*, because *specialexample* is identified as a different token than *example*.

Wildcard matching

Wildcard matching is supported. An asterisk (*) is used as the wildcard character, and represents a valid sequence of tokens. If a list object contains a URI such as *example.*.com*, then that list object matches URIs defined as:

```
[<token sequence>(./)]example.<token sequence>.com[(./)<token sequence>]
```

For example, the URI List Object *example.*.com* matches any of the following URIs:

- *example.exam1.com*
- *example.exam1.exam2.com*
- *www.example.exam1.com/path*

The URI List Object does not match the URI:

- *example.com*

This is because the wildcard character (*) represents a valid token sequence that isn't present in *example.com*.

IPv6 Address Matching

IPv6 address string matching is also supported. While an IPv4 address can be handled as a normal token sequence, an IPv6 address string needs to be handled specially. If a URI List Object contains a URI such as *[2001:2002::2008]*, then that URI List Object matches URIs defined as:

```
[2001:2002::2008][/<token sequence>]
```

For example, the URI List Object matches any of the following URIs:

- *[2001:2002::2008]*
- *[2001:2002::2008]/path*

- `[2001:2002::2008]/path/abc.txt`

IPv6 Wildcard Matching

Wildcard matching in the IPv6 address string is supported. If a list object contains a URI such as `[2001:2002*:2008]/*abc.mp3`, then that list object matches URIs defined as:

`[2001:2002:<token sequence>:2008]/<token sequence>/abc.mp3`

For example, the URI List Object matches any of the following URIs:

- `[2001:2002:2003::2007:2008]/path/abc.txt`
- `[2001:2002:2003:2004:2005:2006:2007:2008]/path/path2/abc.txt`

Using URI List Objects

Currently, URI List Objects can be used in these fields:

- Allowed URI List of a CFS profile
- Forbidden URI List of a CFS profile
- Web Excluded Domains of Websense

CFS URI List Objects are used in these fields differently. When used in an Allowed or URI Forbidden List of a CFS profile, the CFS URI List Object acts normally. For example, if the URI List Object contains a URI such as `example.com/path/abc.txt`, then that list object matches URIs defined as:

`[<token sequence>(./)] example.com/path/abc.txt[(./)<token sequence>]`

When used by the Web Excluded Domains of Websense, only the host portion of the URI takes effect. For example, if the URI List Object contains the same URI as above, `example.com/path/abc.txt`, then that list object matches all domains containing the token sequence `example.com`. The path portion in the URI is ignored.

About URI List Groups

Starting in SonicOS 6.5.2, URI List Groups are supported for flexible and convenient management of URI List Objects, including CFS profile allowed and forbidden lists or for a Websense exclusion list. You can assign multiple URI List Objects to one group, and refer to that group directly within other modules. The URI List Group supports nested inclusion, allowing one URI List Group to contain other URI List Groups. A URI List Group can be used anywhere that a URI List Object can be used.

You can configure up to 128 URI List Groups, and the maximum length of a URI List Group name is 49 characters. You can assign up to 128 URI List Objects and/or URI List Groups to a URI List Group. The maximum number of unique URIs is 5000, and the maximum number of unique keywords is 100.

About CFS Action Objects

The CFS Action Object defines what happens after a packet is filtered by CFS and matches a CFS policy. Navigate to **Policy > Security Services > Content Filter** to configure CFS general settings. Navigate to **Policy > Rules and Policies > Content Filter Rules** to configure CFS policies.

About the Passphrase Feature

The Passphrase feature, in conjunction with the Confirm feature, restricts web access based on a passphrase or password. You can configure the passphrase operation for special URI categories or domains in the Forbidden URI List. To access the forbidden URIs, users are asked to enter the correct password or else web access is blocked.

① **IMPORTANT:** Passphrase only works for HTTP requests. HTTPS requests cannot be redirected to a Passphrase page.

For information about the Confirm feature, see [About the Confirm Feature](#).

How the Passphrase operation works:

1. The user attempts to access a restricted website.
2. A Passphrase page displays on the user's browser.
3. The user must enter the passphrase or password and then submit it.
4. CFS validates the submitted passphrase/password with the website's password:
 - If the passphrase/password matches, web access is allowed. No further confirmations are needed, and users can continue to access websites of the same category for the Active Time period set for the Confirm feature. The default is 60 minutes.
 - If the passphrase/password does not match, access is blocked, and a Block page is sent to the user.

① **NOTE:** Users have three chances to enter the passphrase/password. The site is blocked if all chances fail.

If the user selects **Cancel**, the site is blocked immediately.

About the Confirm Feature

The Confirm feature (also known as Consent) restricts web access by requiring a confirmation from the user before allowing access. You can configure the Confirm operation for special URL categories or domains, and the users need to confirm the web request when they first visit the sites.

① **IMPORTANT:** Confirm only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm (Consent) page.

How the Confirm operation works:

1. The user attempts to access a blocked website.
2. A popup dialog appears, requesting confirmation.
3. Users must select **Continue** or **Close**.
 - If a user confirms to access this category of websites, user is redirected to the first confirmed website. No further confirmations are needed, and users can continue to access websites of the same category for the Active Time period that is set for the Confirm feature. The default is 60 minutes.
 - If a user chooses **Close**, user is shown the Block page and is blocked from that category of website for the period of the Active Time setting.

About UUIDs for CFS Objects

SonicOS 6.5.3 (and higher) automatically generates and binds UUIDs (Universally Unique Identifiers) for these Content Filter objects and groups during their creation:

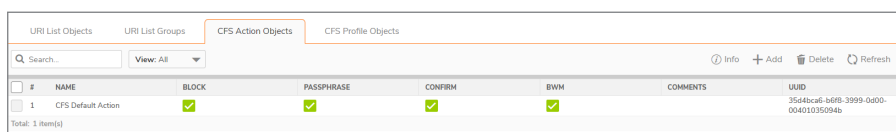
- URI List Object
- URI List Group
- CFS Action Object
- CFS Profile Object

SonicOS also generates and binds UUIDs to Content Filter Policies during creation.

A UUID consists of 32 hexadecimal digits displayed in five-character groups that are separated by hyphens. A UUID is generated at the creation of an object and remains the same thereafter, even when the object is modified or after rebooting the firewall. The UUID is removed when the object is deleted and is not reused once removed. UUIDs are regenerated after restarting the appliance with factory default settings.

By default, UUIDs are not displayed. UUID display is controlled by internal settings. For more information about internal settings, contact SonicWall Technical Support.

When displayed, UUIDs appear in the CFS object tables for each object or group type.



#	NAME	BLOCK	PASSPHRASE	CONFIRM	BWM	COMMENTS	UUID
1	CFS Default Action	✓	✓	✓	✓		3544bcab-b6f8-3999-0a00-00401035094b

CFS object UUIDs facilitate the following functions:

- You can search for a CFS object by UUID with the global search function of the management interface.
- If an object with a UUID is referenced by another entity with a UUID, you can display the reference count and referring entity by mousing over the balloon in the **Comment** column.

When a CFS Action Object, CFS Profile Object, URI List Object, or URI List Group is used by a Content Filter Policy, you can display the reference count and referenced policy by mousing over the balloon in the Comment column on the object's page under **Object**.

Managing URI List Objects

Topics:

- [About the URI List Objects Table](#)
- [Configuring URI List Objects](#)
- [Exporting a URI Lists](#)
- [Editing a URI List Object](#)
- [Deleting URI List Objects](#)

About the URI List Objects Table

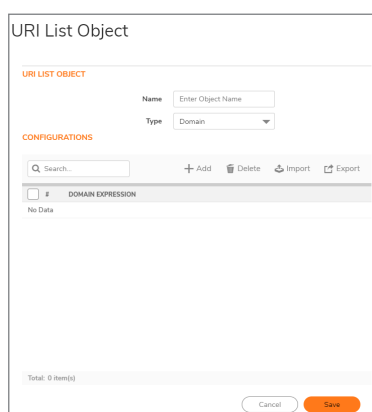
To view the URI List Objects, navigate to **Object > Match Objects > ContentFilter/URL > URL List Objects**.

Name	Name of the URI List Object.
URI List	Specifies the URIs in the URI List Object.
Keyword List	Specifies the Keywords configured in the URI List Object.
Configure	Contains the Edit and Delete icons for each entry in the table.

Configuring URI List Objects

To configure URI List Objects:

1. Navigate to **Object > Match Objects > URI Lists**.
2. At the top of the page, click **Add**.



The screenshot shows the 'URI List Object' configuration form. It includes a 'Name' field with the placeholder 'Enter Object Name', a 'Type' dropdown menu set to 'Domain', and a 'CONFIGURATIONS' section with a search bar and buttons for '+ Add', 'Delete', 'Import', and 'Export'. Below these is a table with a header '# DOMAIN EXPRESSION' and a 'No Data' message. At the bottom, there is a 'Total: 0 item(s)' label and 'Cancel' and 'Save' buttons.

3. Enter a descriptive name for the URI List Object in the **Name** field.
4. You can either add the URIs or import them from a file.

To add URIs:

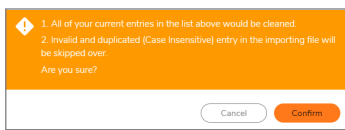
- a. Click **ADD** to manually add URIs.



- b. Enter a URI and then click **OK**. See [About URIs and the URI List](#) for information about URI requirements.
- c. Repeat the process until you have added all the URIs for the list.

To import a list of URIs from a text file:

- a. Click **Import**.

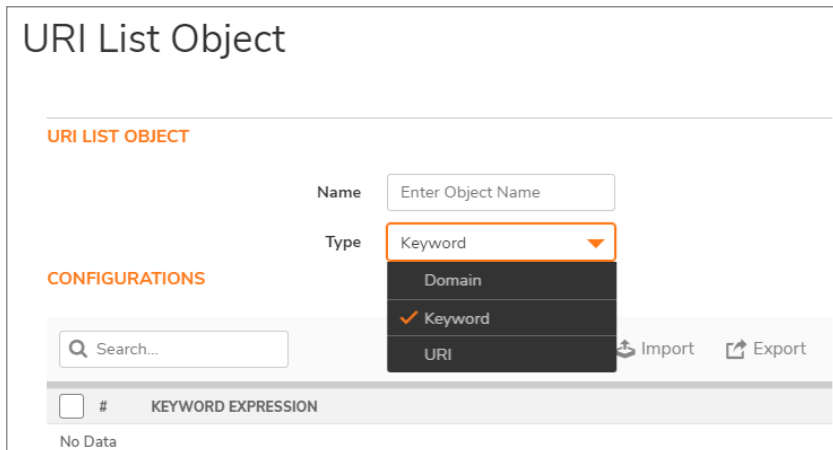


ⓘ IMPORTANT: The text file must conform to the conditions stated in [About URIs and the URI List](#). Only the first 2000 valid URIs in the file are imported. Invalid URIs are skipped and do not count toward the maximum of 2000 URIs per **URI List Object**.

URIs in the text file can be separated by any of these separators, which are added by pressing **Enter** or **Return** on your keyboard:

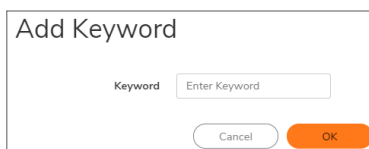
Separator	Style
\r\n	Windows style, new line separator
\r	MAC OS style, new line separator
\n	UNIX style, new line separator

- b. Click **Confirm**.
 - c. On the **File Upload** dialog, select the file and click **Open**. The URI List table is populated, and any URIs that were already added via the **ADD** button are replaced by the URIs in the imported file.
5. When finished adding URIs to the **URI List**, optionally select **Keyword** from the **Type** drop-down to add some keywords.

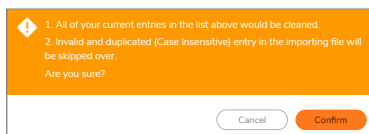


IMPORTANT: For information about keywords and the **Keyword List**, refer to [About Keywords and the Keyword List](#).

- Click **ADD** to manually add keywords.



- Type or paste a keyword into the field, then click **OK**.
- Add more keywords until all the keywords for the list have been input.
- To import a keyword list from a text file instead of adding keywords manually, click **Import**.

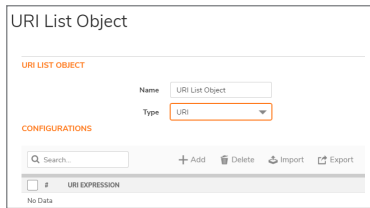


- Click **Confirm**. The dialog displays.
- On the **File Upload** dialog, select the file and click **Open**. The Keyword List table is populated. Any keywords that were already added via the **ADD** button are replaced by the keywords in the imported file.
- When finished adding URIs and keywords, click **OK** in the **Add CFS URI List Object** dialog.
- Click **Add** to populate the **URI List Objects** table or click **CANCEL** to close the **URI List Object** dialog.

Exporting a URI Lists

To export a URI List Object:

- Navigate to **Object > Match Objects > URI Lists**.
- In the **Configure** column, click the **Edit** icon for the list object to be exported. The **URI List Object** dialog displays.



3. To export the URI List, click the **URI List** button and then click **EXPORT**. The **Opening customizedUriList.rtf** dialog displays.
4. You can either open the file or save it. If you:
 - Open the file, all the entries are on one line.
 - Save the file, it is downloaded to your Downloads folder with the file name, **customizedUriList.rtf**; new line characters are added after each entry.
5. Click **OK**.
6. To export the Keyword List, click the **Keyword List** button and then click **EXPORT**. The **Opening customizedKeywordList.rtf** dialog displays.
7. You can either open the file or save it. If you:
 - Open the file, all the entries are on one line.
 - Save the file, it is downloaded to your Downloads folder with the file name, **customizedKeywordList.rtf**; new line characters are added after each entry.
8. Click **OK**.

Editing a URI List Object

To edit a URI List Object:

1. Navigate to **Object > Match Objects > URI Lists**.
2. In the **Configure** column, click the **Edit** icon for the list object to be edited.
3. Select either URI List or Keyword List by clicking the button. You can:
 - Delete an entry in the URI List table or Keyword List table by clicking on the entry's Delete icon.
 - Select the entries in the table and click **Delete** button. Click **OK** in the confirmation message. When you click OK in the **URI List Object** dialog, a message indicates that there must be at least one entry left in the URI List table (this is not required for the Keyword List table). Either:
 - Add one or more entries to the table.
 - Import entries from a file.
 - Click **Cancel** and try a different approach.
 - Edit an entry by clicking the **Edit** icon. The Edit URI or Edit Keyword dialog displays, depending on which screen you selected for this step.
 - Make changes to the URI or the keyword.
 - Click **SAVE**. The URI List table or Keyword List table is updated.
4. Click **OK** in the **URI List Object** dialog.

Deleting URI List Objects

To delete URI List Objects:

1. Navigate to **Object > Match Objects > ContentFilter/URL > URI List Objects**
2. Do one of these:
 - Click the **Delete** icon in the **Configure** column for the list object to be deleted.
 - Click the checkbox for one or more list objects to be deleted. Click the **Delete** button.

Managing URI List Groups

Topics:

- [About the URI List Groups Table](#)
- [Adding URI List Groups](#)
- [Editing a URI List Group](#)
- [Deleting URI List Objects](#)

About the URI List Groups Table

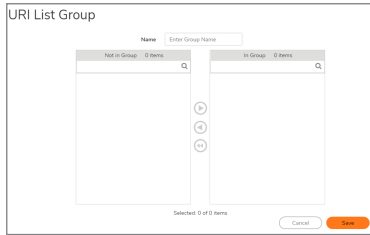
Name	Name of the URI List Group.
URI List	Specifies the URIs in the URI List Group.
Keyword List	Specifies the Keywords configured in the URI List Group.
Configure	Contains the Edit and Delete icons for each entry in the table.

Adding URI List Groups

To add a URI List Group:

1. Navigate to **Object > Match Objects > URI List Groups** tab.
2. At the top of the page, click **Add**.

The **URI List Group** dialog displays. A list of all configured URI List Objects and URI List Groups is displayed on the left side of the dialog.



3. Enter a descriptive name for the URI List Group in the **Name** field.
4. Click on an item in the list on the left that you want to include in the URI List Group.
5. Click the right arrow button to move the selected item into the field on the right.
6. Click **Save** to create the URI List Group using the list on the right.

Editing a URI List Group

To edit a URI List Group:

1. Navigate to **Object > Match Objects > URI List Groups** tab.
2. In the **Configure** column, click the **Edit** icon for the group to be edited.
3. Click on an item in either side and use the left or right arrow button to move it to the other side. Items on the right are part of the URI List Group. You can click un-select all items icon to move all items from the right to the left side, if you want to remove all of them from the URI List Group.
4. Click **Save**.

Deleting URI List Groups

To delete URI List Groups:

1. Navigate to **Object > Match Objects > URI List Groups** tab.
2. Do one of these:
 - Click the **Delete** icon in the **Configure** column for the group to be deleted.
 - Click the checkbox for one or more groups to be deleted. Click the **Delete** button.

Match Patterns

The Match Patterns screen provides a list of match patterns that are available in the selection.

Match Patterns

Q Search... * Used and Unused ▾						
+ Add 🗑️ Delete 📄 Export 🔄 Refresh ⚙️ Column Selection						
<input type="checkbox"/>	#	NAME	OBJECT TYPE	MATCH TYPE	NEGATIVE MATCHING	REPRESENTA...
<input type="checkbox"/>	▼ 1	Obj 1	ActiveX Class ID	Exact Match	Disable	Alphanumeric
OBJECT CONTENT						
Content entry Match 1, Match 5						

- **Add**

To add a match pattern:

1. Click **Add** to add match pattern.
 2. Input a name in the **Object Name** field.
 3. From the drop-down list, select **Match Object Type** and **Match Type**.
 4. Choose **Alphanumeric** or **Hexadecimal** from the input representation.
 5. To add Object content, input **Content Name** in the text field and click **Add**.
 6. Click **Save** to save the group.
- **Delete** - Check the box to delete a selected group.
 - **Export** - Exports the Match Patterns Data to a CSV file.
 - **Refresh** - Refreshes the list.
 - **Column Selection** - Choose which columns are shown in the list.

Custom Match

The Custom Match screen provides a list of country objects that are available in the selection.

Custom Match Objects

- **Add**

To add Custom Match Objects :

1. Click **Add** to add custom match objects.
 2. Input a Policy name in the **Policy Name** field.
 3. From the drop-down list, select Policy Type, Match Object Included, Mail from Included and other fields and click **Add**.
- **Delete** - Check the box to delete a selected group.
 - **Export** - Exports the Custom Match Objects Data to a CSV file.
 - **Refresh** - Refreshes the list.
 - **Column Selection** - Choose which columns to be shown in the list.

Custom Match Groups

You can group any combination of custom match groups and then save your selections in the policy preferences.

Add Custom Match Groups

Custom Match Objects		Custom Match Groups							
Q Search...		Used and Unused		+ Add Delete Export Refresh Column Selection					
<input type="checkbox"/>	#	NAME	POLICY TYPE	MATCH PATT...	CLASS	POLICY REFERENCE COUNT	POLICY REFERENCES	CREATED	UPDATED
<input type="checkbox"/>	▶ 1	17hfgbshn				0		2021-04-10 01:46	2021-04-10 01:46
<input type="checkbox"/>	▶ 2	custom group1				0		2021-04-10 01:46	2021-04-10 01:46

- **Add**

To add a Custom Match group:

1. Click **Add** to add custom match group.
 2. Input a group name in the **Name** field.
 3. Select the custom match items which are not in the group by clicking on individual entries in the list.
 4. Click the arrow to move marked custom match groups to the right view.
 5. Click **Add** to add the group.
- **Delete** - Check the box to delete a selected group.
 - **Delete All** - Deletes all the groups in the list
 - **Export** - Exports the Custom Match groups Data to a CSV file.
 - **Refresh** - Refreshes the list.
 - **Column Selection** - Choose which columns to be shown in the list.

Schedules

SonicOS uses schedule objects in conjunction with its security features and policies. To create schedule objects, navigate to **Object > Match Objects > Schedules**. You can apply schedule objects for a specific security feature or policy (rule). For example, if you add an access rule **Policy > Rules and Policies > Access Rules** page, the **Add Rule** dialog lists all the available predefined schedule objects as well as the schedule objects that you have created in the **Schedules** page. A schedule can include multiple day and time increments for rule enforcement with a single schedule.

The **Schedules** page allows you to create and manage default and custom schedule objects for enforcing schedule times for a variety of SonicWall Security Appliance features.

#	NAME	DAYS OF WEEK	TIME	COMMENT	START TIME	END TIME
1	Work Hours					
2	After Hours					
3	Weekend Hours					
4	AppFlow Report Hours					
5	App Visualization Report Hours					
6	TSR Report Hours					
7	Cloud Backup Hours					
8	Guest Cycle Quota Update					

NOTE: You can modify default schedules, but you cannot delete them.

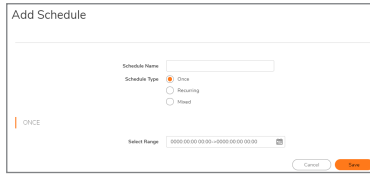
The **Schedules** table displays all predefined and custom schedules. The default schedules consist of:

Work Hours	After Hours
Weekend Hours	AppFlow Report Hours
App Visualization Report Hours	TSR Report Hours
Cloud Backup Hours	Guest Cycle Quota Update

Adding a Custom Schedule

To create custom schedules:

1. Navigate to **Object > Match Objects > Schedules**.
2. Click **Add**. The **Add Schedule** dialog displays.



3. Enter a descriptive name for the schedule in the **Schedule Name** field.
4. Choose one of the following radio buttons for **Schedule Type**:

Once	For a one-time schedule between the configured Start and End times and dates. When selected, the fields under Once become available, and the fields under Recurring become dimmed.
Recurring	For a schedule that occurs repeatedly during the same configured hours and days of the week, with no start or end date. When selected, the fields under Recurring become available, and the fields under Once become dimmed.
Mixed	For a schedule that occurs repeatedly during the same configured hours and days of the week, between the configured start and end dates. When selected, all fields on the page become active.

① | **NOTE:** Time must be in 24-hour format, for example, 17:00 for 5 p.m.

5. If the fields under **Once** are available, configure the:
 - Starting date and time by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down menu in the **Start** row. The hour is represented in 24-hour format.
 - Ending date and time by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down menu in the **End** row. The hour is represented in 24-hour format.
6. If the fields under **Recurring** are available:
 - Select the checkboxes for the days of the week to apply to the schedule or select **All**.
 - Enter the time of day for the schedule to begin in the **Start Time** field.
 - Enter the time of day for the schedule to stop in the **Stop Time** field.
7. Click **Add** to add the schedule to the **Schedule List**.
8. Click **Save**. The **Schedule** is created.

Modifying Schedules

To modify both default and custom schedules:

1. Navigate to **Object > Match Objects > Schedules**.
2. Mouse over on the Schedule which you want to edit and click **Edit** icon. The **Edit Schedule** dialog displays.

3. You can change any component of the schedule, such as time(s), type, and/or days, except the name of default schedules cannot be changed and the field is dimmed. To make changes, follow the procedure in [Adding a Custom Schedule](#).
4. Click **Save**.

Deleting Custom Schedules

You can delete custom schedules, but you cannot delete default schedules.

1. Navigate to **Object > Match Objects > Schedules**.
2. Mouse over on the Schedule which you want to delete and click **Delete** icon.

To delete multiple schedule objects:

1. Navigate to **Object > Match Objects > Schedules**.
2. In the Schedules table, select multiple custom schedules and click **Delete** at top of the page.

Dynamic Group

Dynamic Groups are comprised of Dynamic External Address Groups (DEAG) and Dynamic External Address Objects (DEAO). A Dynamic External Address Group is an Address Group whose members are dynamic. Dynamic External Address Objects are intermediate, internal objects that are dynamically created and placed under a Dynamic External Address Group when a Dynamic External Address Group file is downloaded. The Dynamic External Objects feature eliminates the need for manually modifying an Address Group to add or remove members.

#	NAME	TYPE	ZONE	PROTOCOL	PERIODIC DOWNLOAD INT...	URL	SERVER
1	Group1	address_group	DMZ	https	5-minutes	https://sonicw7.eng.sonicwall.co	external-objects
2	Group2	address_group	DMZ	https	15-minutes	https://10.203.28.157/sonicw7	external-objects

Popup tooltips appear when you move your mouse over many of the fields in a DEAG entry. Multiple Dynamic External Address Groups can be configured and you can use these DEAGs in access rules or policies. For example, if you want to maintain a group for all partner IP addresses on which certain access rules are enforced, you can create a Dynamic External Address Group / Dynamic External Object.

The creation of a Dynamic External Object consists of two parts:

- Creation of the Dynamic External Address Group file on an FTP server or on a web page at a specific URL
- Configuration of the Dynamic External Address Group on the **Object > Dynamic Group** page in SonicOS including downloading and using the information in the DEAG file.

About the Dynamic External Address Group File

The Dynamic External Address Group file (DEAG file) contains a list of IP addresses or Fully Qualified Domain Names (FQDNs) that define the DEAOs which are members of the DEAG. The DEAG file resides externally, on a server for FTP access or on a web page at a specific URL for HTTPS access. The list of IP addresses or FQDNs can be modified at the external location and the associated DEAOs and DEAG in SonicOS are dynamically updated with those changes, if configured to periodically download the file.

The DEAG file can contain a text list of either IP addresses or FQDNs formatted as follows:

- A list of IP addresses, one per line. It can include subnets specified in CIDR format.
- A list of FQDNs, one per line. An FQDN is a character string such as **www.example.com**. It cannot contain any wildcard (*) characters.
- A mixed list of FQDNs and IP addresses/subnets, one per line. This is only supported for FQDN type DEAGs. A non-FQDN type DEAG will not accept FQDNs in the DEAG file.

However, it is not recommended to mix and match IP addresses and FQDNs in the DEAG file, because the IP addresses in this list will also be treated as FQDNs and SonicOS will attempt to resolve them. A better way to mix these input types is to create individual DEAGs of FQDN type and non-FQDN type and then add both DEAGs to a separate address group for use in access rules.

For every DEAG, a DEAO with the IP address *0.0.0.0* is automatically created. For example, if there is only one DEAG, the maximum number of IP addresses in the DEAG file is one less than the maximum number of DEAOs allowed, as defined in [DEAG and DEAO Maximums](#).

DEAG and DEAO Maximums

Maximum DEAGs:

- The maximum number of DEAGs, including both IP address and FQDN types, is 25% of the total number of address groups supported by the device.
- The maximum number of DEAGs that can be created cannot exceed the number of address groups remaining before exceeding the total number supported on the firewall.
For example, if a device supports 1024 Address Groups and you are using only 20 Address Groups, then 256 DEAGs (25% of 1024) can be created. However, if you have already manually created 1000 Address Groups, then only 24 DEAGs can be created.

Maximum DEAOs:

- The maximum number of *IP address type* DEAOs is 25% of the total number of address objects supported by the device.
- The maximum number of *FQDN type* DEAOs is 50% of the total number of address objects supported by the device.
- The maximum number of DEAOs that can be created cannot exceed the number of address objects remaining before exceeding the total number supported on the firewall.

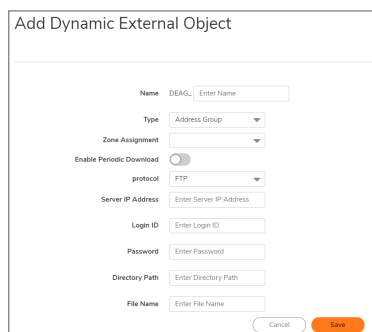
High Availability Requirements

When deployed as a High Availability pair, both the active and standby firewalls must have a connection to the server or URL to download the file that contains the list of IP addresses or FQDNs. This requires configuring the monitoring IP address on the standby unit.

Adding a Dynamic External Object

To add a Dynamic External Object:

1. Navigate to **Objects > Match Objects > Dynamic Group** page.
2. Click the **Add** button. The **Add Dynamic External Object** dialog displays.



3. Enter a unique, descriptive name for the dynamic external address group in the **Name** field. “DEAG_” is automatically prepended to the name when saved.
4. The **Type** field is set to *Address Group*, with no other options.
5. In the **Zone Assignment** drop-down list, select the zone for the Dynamic External Address Group.
6. Select the **Enable Periodic Download** option for ongoing, periodic downloads of the Dynamic Address Group File.
7. If **Enable Periodic Download** is enabled, select the number of minutes or hours between downloads in the Download interval field. You can select one of:
 - 5 minutes
 - 15 minutes
 - 1 hour
 - 24 hours
8. Select the type of protocol to use for downloading the DEAG file from the **Protocol** drop-down list. The choices are FTP or HTTPS. The remaining fields in the dialog are different for FTP and HTTPS.
9. If you selected **FTP** as the **protocol**, specify the following:
 - **Server IP Address** – the IP address of the FTP server where the DEAG file resides
Refer to [About the Dynamic External Address Group File](#) for information about the DEAG file.
 - **Login ID** – the user name for logging into the FTP server
 - **Password** – the password for logging into the FTP server
 - **Directory Path** – the folder in which the DEAG file resides on the FTP server
 - **File Name** – the name of the DEAG file on the FTP server
10. If you selected **HTTPS** as the **protocol**, specify the following:

- **URL Name** – the URL which has the list of IP addresses or FQDNs

The screenshot shows a configuration window titled "Add Dynamic External Object". It contains the following fields and controls:

- Name:** A text input field with the value "DEAG_" and a placeholder "Enter Name".
- Type:** A dropdown menu with "Address Group" selected.
- Zone Assignment:** A dropdown menu.
- Enable Periodic Download:** A toggle switch that is currently turned off.
- protocol:** A dropdown menu with "HTTPS" selected.
- URL:** A text input field with the value "https://10.203.28.157/sonic".

At the bottom right of the dialog, there are two buttons: "Cancel" and "Save".

The URL Name should start with *https://* and follow with the page name. This page contains the list of IP addresses or FQDNs.

11. Click **Save**.

Based on the configuration, the firewall reads the list of IP addresses or FQDNs from the file or URL. Then SonicOS automatically creates the following:

- Address group with the name provided in the **Add Dynamic External Object** dialog. This address group is read-only, meaning that you cannot edit or delete it.
- Address objects for every valid unique IP address or FQDN in the file. These address objects are also read-only.

The individual address objects are then added to the Dynamic External Address Group / Dynamic External Object. You can use this in access rules and policies.

Editing Dynamic External Objects

Mouse over on the Dynamic External Object which you want to edit and click **Edit** icon. The Configuration settings are same as the **Add Dynamic External Object** dialog.

You cannot change the **Name** of the DEAG or the Zone Assignment when editing the Dynamic External Object.

Deleting Dynamic External Objects

To delete Dynamic External Objects:

1. Navigate to **Objects > Match Objects > Dynamic Group** page.
 2. Do one of the following:
 - Mouse over on the Dynamic External Object which you want to delete and click **Delete** icon.
 - Click the checkbox for one or more objects to be deleted and click **Delete** at top of the page.
- ① **NOTE:** If a Dynamic External Address Group is in use, such as when an access rule is using it, the deletion attempt will fail.

Email Addresses

Application control allows the creation of custom email address lists as email address objects. You can only use email address objects with App Rules policies when the **Policy Type** is **SMTP Client**. Email address objects can represent individual users or the entire domain. You can also create an email address object that represents a group by adding a list of individual addresses to the object. This provides a way to easily include or exclude a group of users when creating an App Rules policy of type SMTP client. For more information, refer to **Policy > App Rules**.

For example, you can create an email address object to represent the support group:

E-mail Address Object Settings

E-mail User Object Name

Match Type ?

Content ? + 🗑️ ↻

<input type="checkbox"/> #	CONTENT
<input type="checkbox"/> 1	dawn@sonicwall.com
<input type="checkbox"/> 2	mike@sonicwall.com
<input type="checkbox"/> 3	john@sonicwall.com

Cancel
Save

After you define the group in an email address object, you can create an SMTP client policy that includes or excludes the group.

Navigate to **Policy > App Rules > Add**, the settings exclude the support group from a policy that prevents executable files from being attached to outgoing email. You can use the email address object in either the **Mail from Included**, **Mail from Excluded**, **RCPT to Included**, or **RCPT to Excluded** fields of the SMTP client policy. The **Mail from** fields refer to the sender of the email. The **RCPT to** fields refer to the intended recipient.

Add App Rule

Policy Name	Support Group	Users/Groups Included	All
Policy Type	SMTP Client	Users/Groups Excluded	None
Address Source	Any	Schedule	Always On
Address Destination	Any	Enable flow reporting	<input type="checkbox"/>
Service Source	Any	Enable Logging	<input checked="" type="checkbox"/>
Service Destination	SMTP (Send E-Mail)	Log individual object content	<input type="checkbox"/>
Exclusion Address	None	Log Redundancy Filter (seconds)	<input checked="" type="checkbox"/>
Match Object Included	Custom Object - HTT...	Use Global Settings	1
Action Object	Reset/Drop	Connection Side	Client Side
Mail from Included	SupportGroup	Direction	<input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Mail from Excluded	None		Incoming
Rcpt to Included	Any		
Rcpt to Excluded	None		

Although App Rules cannot extract group members directly from Outlook Exchange or similar applications, you can use the member lists in Outlook to create a text file that lists the group members. Then, when you create an email address object for this group, click **Upload** icon to import the list from your text file. Ensure that each email address is on a line by itself in the text file.

E-mail Address Object Settings

E-mail User Object Name	Enter Object Name	<div style="border: 1px solid black; padding: 5px; font-size: 0.8em;"> Uploading new Object. Values will overwrite any existing Object Values. Values should be separated by a new line in imported file. </div>
Match Type	Exact Match	
Content	Enter Object Content	<input type="button" value="i"/> <input type="button" value="+"/> <input type="button" value="trash"/> <input type="button" value="upload"/>
	<input type="checkbox"/> # CONTENT No Data	

Configuring Email Address Objects

To configure email address object settings:

1. Navigate to **Object > Match Objects > Email Addresses**.
2. Click **Add** at the top of the page. The **E-mail Address Object Settings** dialog displays.

3. Enter a descriptive name for the email address object in the **Email User Object Name** field.
4. For **Match Type**, select one of:
 - **Exact Match** – To exactly match the email address that you provide.
 - **Partial Match** – To match any part of the email address.
 - **Regex Match** – To use a regular expression to match the email address.
5. In the **Content** field, enter the email id and click **Add** icon.
 - For example, to match on a domain, select **Partial Match** in the previous step and then type **@** followed by the domain name in the **Content** field, for example, type: **@sonicwall.com**. To match on an individual user, select **Exact Match** in the previous step and then type the full email address in the **Content** field, for example: **jsmith@sonicwall.com**.
 - Importing a list of elements from a text file by clicking **Upload** icon. Each element in the file must be on a line by itself.
By defining an email address object with a list of users, you can use App Rules to simulate groups.
6. Click **Save**.
The Email Address Object is created and displayed in the table.

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

SonicOSX Match Objects Administration Guide

Updated - May 2021

Software Version - 7

232-005340-00 Rev A

Copyright © 2021 SonicWall Inc. All rights reserved.

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

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

End User Product Agreement

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

Open Source Code

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

General Public License Source Code Request

Attn: Jennifer Anderson

1033 McCarthy Blvd

Milpitas, CA 95035