SonicOS 7

Profile Objects

Administration Guide

SONICWALL®

Contents

1

Endpoint Security

With Endpoint Security, you can manage logs for your product subscriptions and licensed security products in one location. Security products include Capture Client, Content Filtering, Intrusion Prevention, App Control, Botnet/GeoIP Filtering, and Gateway Anti-Virus/Anti Spyware/Capture ATP.

When enabled, Capture Client leverages cloud sandbox file testing, comprehensive reporting, and enforcement for endpoint protection, while providing consistent assurance of client security, with easy-to-use and actionable intelligence and reporting.

Endpoint Security can secure your endpoints no matter where they are located and help you keep them clean of malware while enforcing access and content rules.

For configuring Endpoint Security, refer *Policy* > *Endpoint Security* section of SonicOS.

A default Endpoint Security Profile, **Endpoint Enforcement Default Profile**, is created by SonicOS. You can configure and edit this Endpoint Security profile, but you cannot delete it.

To add an Endpoint Security profile:

1. Navigate to **Object > Profile Objects > Endpoint Security** page.
2. Click **Add** icon on the top of the page.
3. Enter the name of the Endpoint Security Profile in the **Name** field.
4. Toggle the **Bypass Guest Endpoint Security Service** option to enable it. Enabling this option bypasses guest check for Endpoint Security when guest service is enabled on matched zone.
5. Toggle the **Capture Client Endpoint Security** option to enable it.
6. Click **Save**. The Endpoint Security profile is created.

To delete an Endpoint Security profile:

1. Navigate to **Object > Profile Objects > Endpoint Security** page.
2. Select the check box of an Endpoint Security profile which you want to delete and click **Delete** icon on the top of the page.

   OR

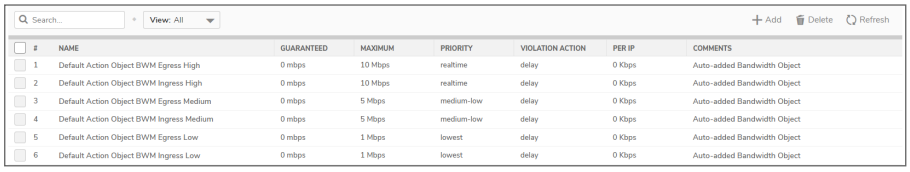
   Hover on the Endpoint Security profile and click **Delete** icon.

2

Bandwidth

Bandwidth management configuration is based on policies that specify bandwidth limitations for traffic classes. A complete bandwidth management policy consists of two parts: a classifier and a bandwidth rule.

A classifier specifies the actual parameters, such as priority, guaranteed bandwidth, and maximum bandwidth, and is configured in a bandwidth object. Classifiers identify and organize packets into traffic classes by matching specific criteria.

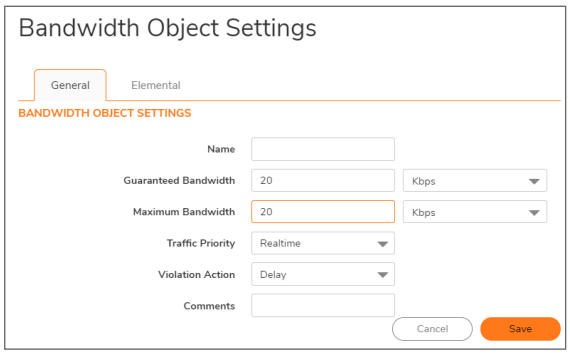


Configuring Bandwidth Objects

To add or configure a bandwidth object:

1. Navigate to **Object > Profile Objects > Bandwidth** page.
2. Do one of the following:
   - Click on the **Add** icon to create a new bandwidth object.
   - Hover on the bandwidth object which you want to edit and click the **Edit** icon.

   The following dialog screen is displayed:

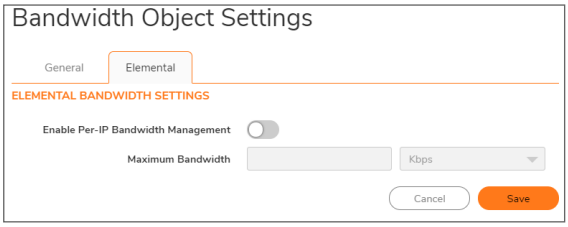


3. In the **Name** field, enter a descriptive name for this bandwidth object.

4. In the **Guaranteed Bandwidth** field, enter the amount of bandwidth that this bandwidth object will guarantee to provide for a traffic class. Type in the number and then select the rate, Kbps (kilobits per second) or Mbps (megabits per second) from the drop-down list.
5. In the **Maximum Bandwidth** field, enter the maximum amount of bandwidth that this bandwidth object will provide for a traffic class. Type in the number and then select the rate, Kbps or Mbps, from the drop-down list.

   NOTE: The actual allocated bandwidth may be less than this value when multiple traffic classes compete for a shared bandwidth.
6. From the **Traffic Priority** drop-down list, select the priority that this bandwidth object will provide for a traffic class. The highest priority is **0 Realtime**which is the default. The lowest priority is **7 Lowest**.

   When multiple traffic classes compete for shared bandwidth, classes with the highest priority are given precedence.
7. From the **Violation Action** drop-down list, select the action that this bandwidth object provides when traffic exceeds the maximum bandwidth setting:
   - **Delay** - specifies that excess traffic packets will be queued and sent when possible which is selected by default.
   - **Drop** - specifies that excess traffic packets will be dropped immediately.
8. In the **Comment** field, enter a text comment or description for this bandwidth object.
9. Click the **Elemental** tab.



10. Optionally select the **Enable Per-IP Bandwidth Management** option. This option is not selected by default. The Maximum Bandwidth fields become active.

    When **Enable Per-IP Bandwidth Management** is enabled, the maximum elemental bandwidth setting applies to each individual IP address under the parent traffic class.
11. Enter the **Maximum Bandwidth** value (number).
12. From the associated drop-down list, select the rate as either **Kbps** or **Mbps**.
13. Click **Save**.

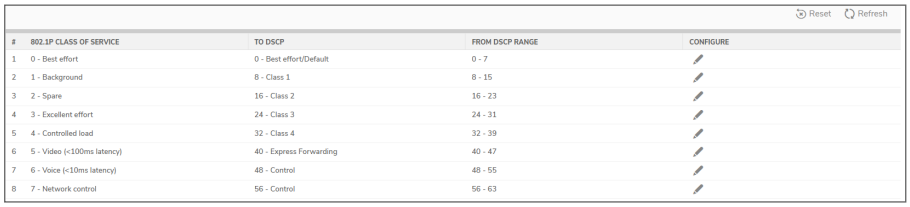
NOTE: Configuring bandwidth objects in an access rule is described in *Configuring BWM Settings with Advanced BWM* and *Configuring BWM Settings with Global BWM* in **Policy > Rules and Policies > Access Rules > Adding a Rule** chapter.

3

Quality of Service (QoS) Marking

Quality of Service (QoS) refers to various methods used to provide more predictable network behavior and performance. Predictability is especially vital to certain types of applications, such as Voice over IP (VoIP) and multimedia content, and to business applications such as order and credit-card processing. No amount of bandwidth can provide sufficient predictability, because no matter how large the amount, it is ultimately used to its capacity at some point in a network. QoS, when configured and implemented correctly, can greatly improve the management of traffic, and guarantee high levels of network service. This chapter shows the SonicOS user interface mapping table where the administrator can make changes in the mapping settings. The rest of the chapter explains in detail some of the techniques used to improve quality of service on networks.

The user interface gives the administrator the possibility of configuring mapping 802.1p to DSCP markings for QoS service across external systems. The table shown below gives the equivalences from one to the other, and a pencil icon for configuration. Select the icon in any row to bring up a dialog with options to select if changes to the mapping table are required. The choices are given in drop-down menus. Click **Reset** to apply the changes.



Topics:

Classification

Classification is necessary as a first step so that traffic in need of management can be identified. SonicOS uses Access Rules as the interface to classification of traffic. This provides fine controls using combinations of Address Object, Service Object, and Schedule Object elements, allowing for classification criteria as general as **all HTTP traffic** and as specific as **SSH traffic from hostA to serverB on Wednesdays at 2:12am**.

SonicWall network security appliances have the ability to recognize, map, modify, and generate the industry-standard external CoS designators, DSCP and 802.1p. For more information, see 802.1p and DSCP QoS.

After being identified, or classified, it can be managed. Management can be performed internally by SonicOS Bandwidth Management (BWM), which is perfectly effective as long as the network is a fully contained autonomous system. After external or intermediate elements are introduced, such as foreign network infrastructures with unknown configurations, or other hosts contending for bandwidth (for example, the Internet) the ability to offer guarantees and predictability are diminished. In other words, as long as the endpoints of the network and everything in between are within your management, BWM functions exactly as configured. After external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.

But all is not lost. After SonicOS classifies the traffic, it can **tag** the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags; and as a result, they too can participate in providing QoS.

ⓘ **NOTE:** Many service providers do not support CoS tags such as 802.1p or DSCP. Also, most network equipment with standard configurations is not be able to recognize 802.1p tags, and could drop tagged traffic.
Although DSCP does not cause compatibility issues, many service providers simply strip or ignore the DSCP tags, disregarding the code points.
If you wish to use 802.1p or DSCP marking on your network or your service provider's network, you must first establish that these methods are supported. Verify that your internal network equipment can support CoS priority marking, and that it is correctly configured to do so. Check with your service provider – some offer fee-based support for QoS using these CoS methods.

Marking

After the traffic has been classified, if it is to be handled by QoS capable external systems (for example, CoS aware switches or routers as might be available on a premium service provider's infrastructure, or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it rarely mistreats or discard the packet.

The other prevalent method of CoS marking is IEEE 802.1P. 802.1P occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16-bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1P only works with 802.1p capable equipment, and is not universally interoperable. Additionally, 802.1P, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1P across network boundaries (such as WAN links) was introduced in the form of **802.1P to DSCP mapping**.

802.1P to DSCP mapping allows 802.1P tags from one LAN to be mapped to DSCP values by SonicOS, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS appliance can then map the DSCP tags back to 802.1P tags for use on that LAN. For more information, see 802.1p and DSCP QoS.

Conditioning

The traffic can be conditioned (or managed) using any of the many policing, queuing, and shaping methods available. SonicOS provides internal conditioning capabilities with its Egress and Ingress Bandwidth Management (BWM). SonicOS's BWM is a perfectly effective solution for fully autonomous private networks with sufficient bandwidth, but can become somewhat less effective as more unknown external network elements and bandwidth contention are introduced. Refer to DSCP Marking: Example Scenario for a description of contention issues.

Topics:

- Site to Site VPN over QoS Capable Networks
- Site to Site VPN over Public Networks

Site to Site VPN over QoS Capable Networks

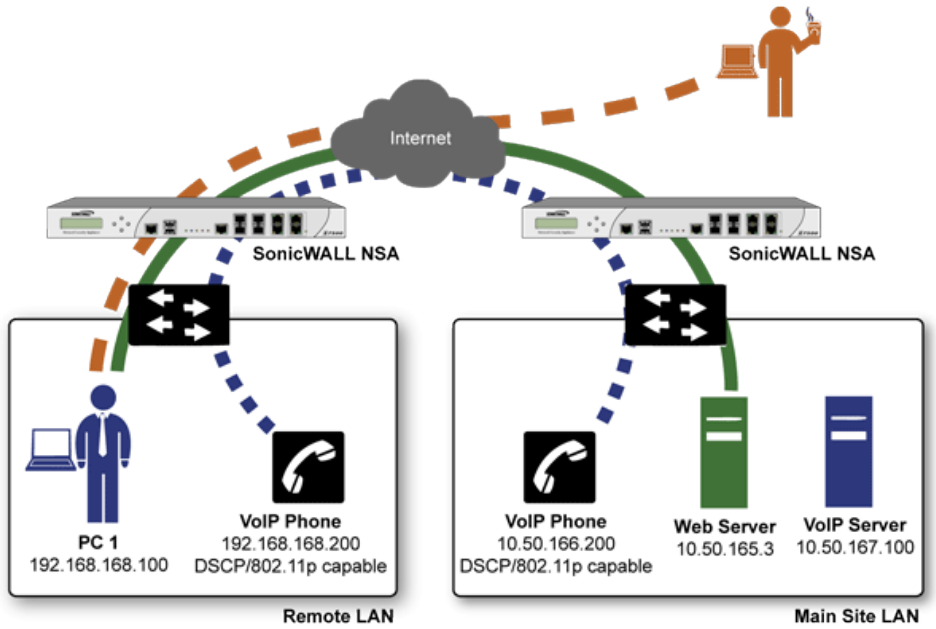
If the network path between the two end points is QoS aware, SonicOS can DSCP tag the inner encapsulate packet so that it is interpreted correctly at the other side of the tunnel, and it can also DSCP tag the outer ESP encapsulated packet so that its class can be interpreted and honored by each hop along the transit network. SonicOS can map 802.1p tags created on the internal networks to DSCP tags so that they can safely traverse the transit network. Then, when the packets are received on the other side, the receiving SonicWall appliance can translate the DSCP tags back to 802.1p tags for interpretation and honoring by that internal network.

Site to Site VPN over Public Networks

SonicOS integrated BWM is very effective in managing traffic between VPN connected networks because ingress and egress traffic can be classified and controlled at both endpoints. If the network between the endpoints is non QoS aware, it regards and treats all VPN ESP equally. Because there is typically no control

over these intermediate networks or their paths, it is difficult to fully guarantee QoS, but BWM can still help to provide more predictable behavior.

SITE TO SITE VPN OVER PUBLIC NETWORKS



VoIP Traffic

Web Traffic

VoIP Traffic

LAN -> VPN	DSCP: 48	802.11p: 6	Inbound	Gar. 30%	Max: 60%	Pri: 0
LAN -> VPN	DSCP: 48	802.11p: 6	Outbound	Gar. 30%	Max: 60%	Pri: 0
VPN -> LAN	DSCP: 48	802.11p: 6	Inbound	Gar. 30%	Max: 60%	Pri: 0
VPN -> LAN	DSCP: 48	802.11p: 6	Outbound	Gar. 30%	Max: 60%	Pri: 0

Web Traffic (HTTP, HTTPS, NNTP, TCP4662

LAN -> VPN	DSCP: 8	802.11p: 1	Inbound	Gar. 5%	Max: 30%	Pri: 2
LAN -> VPN	DSCP: 8	802.11p: 1	Outbound	Gar. 5%	Max: 30%	Pri: 2
LAN -> WAN	DSCP: 0	802.11p: -	Inbound	Gar. 2%	Max: 30%	Pri: 7
LAN -> WAN	DSCP: 0	802.11p: -	Outbound	Gar. 2%	Max: 10%	Pri: 7

To provide end-to-end QoS, business-class service providers are increasingly offering traffic conditioning services on their IP networks. These services typically depend on the customer premise equipment to classify and tag the traffic, generally using a standard marking method such as DSCP. SonicOS has the ability to DSCP mark traffic after classification, as well as the ability to map 802.1p tags to DSCP tags for external network traversal and CoS preservation. For VPN traffic, SonicOS can DSCP mark not only the internal (payload) packets, but the external (encapsulating) packets as well so that QoS capable service providers can offer QoS even on encrypted VPN traffic.

The actual conditioning method employed by service providers varies from one to the next, but it generally involves a class-based queuing method such as Weighted Fair Queuing for prioritizing traffic, as well a congestion avoidance method, such as tail-drop or Random Early Detection.

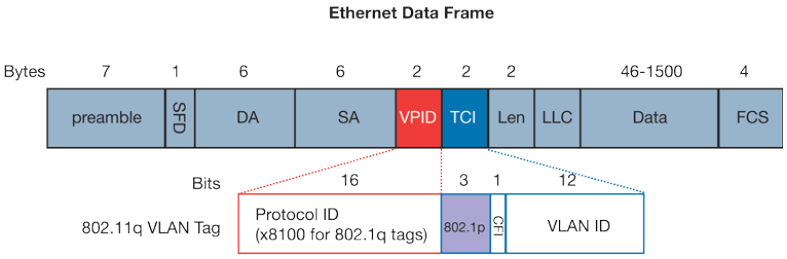
802.1p and DSCP QoS

Topics:

Enabling 802.1p

SonicOS supports layer 2 and layer 3 CoS methods for broad interoperability with external systems participating in QoS enabled environments. The layer 2 method is the IEEE 802.1p standard wherein 3-bits of an additional 16-bits inserted into the header of the Ethernet frame can be used to designate the priority of the frame, as illustrated in the following figure:

ETHERNET DATA FRAME



- **TPID**: Tag Protocol Identifier begins at byte 12 (after the 6 byte destination and source fields), is 2 bytes long, and has an Ether type of 0x8100 for tagged traffic.
- **802.1p**: The first three bits of the TCI (Tag Control Information – beginning at byte 14, and spanning 2 bytes) define user priority, giving eight (2^3) priority levels. IEEE 802.1p defines the operation for these 3 user priority bits.
- **CFI**: Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet networks and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- **VLAN ID**: VLAN ID (starts at bit 5 of byte 14) is the identification of the VLAN. It has 12-bits and allows for the identification of 4,096 (2^12) unique VLAN ID's. Of the 4,096 possible IDs, an ID of 0 is used to identify priority frames, and an ID of 4,095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

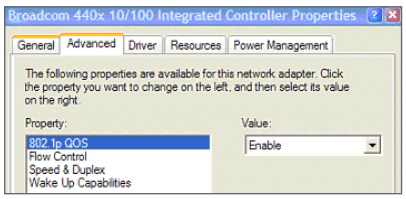
802.1p support begins by enabling 802.1p marking on the interfaces which you wish to have process 802.1p tags. 802.1p can be enabled on any Ethernet interface on any SonicWall appliance.

The behavior of the 802.1p field within these tags can be controlled by Access Rules. The default 802.1p Access Rule action of **None** will reset existing 802.1p tags to 0, unless otherwise configured (see Managing QoS Marking for details).

Enabling 802.1p marking will allow the target interface to recognize incoming 802.1p tags generated by 802.1p capable network devices, and will also allow the target interface to generate 802.1p tags, as controlled by Access Rules. Frames that have 802.1p tags inserted by SonicOS will bear VLAN ID 0.

802.1p tags will only be inserted according to Access Rules, so enabling 802.1p marking on an interface will not, at its default setting, disrupt communications with 802.1p-incapable devices.

802.1p requires the specific support by the networking devices with which you wish to use this method of prioritization. Many voice and video over IP devices provide support for 802.1p, but the feature must be enabled. Check your equipment's documentation for information on 802.1p support if you are unsure. Similarly, many server and host network cards (NICs) have the ability to support 802.1p, but the feature is usually disabled by default. On Win32 operating systems, you can check for and configure 802.1p settings on the **Advanced** view of the Properties page of your network card. If your card supports 802.1p, it is listed as **802.1p QoS**, **802.1p Support**, **QoS Packet Tagging** or something similar:

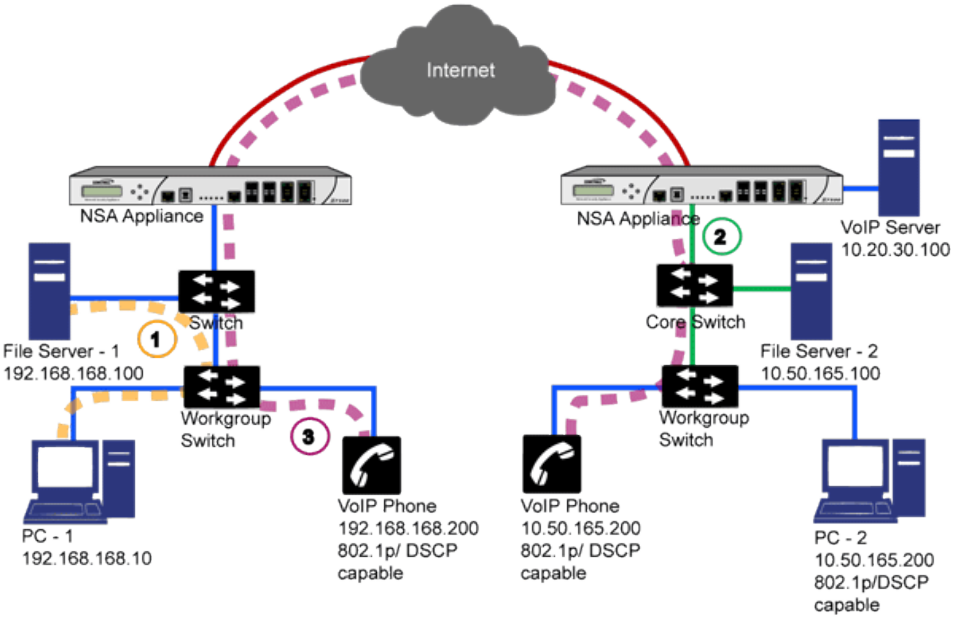


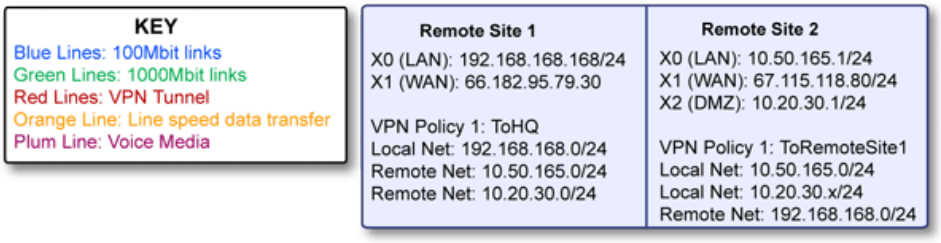
To process 802.1p tags, the feature must be present and enabled on the network interface. The network interface will then be able to generate packets with 802.1p tags, as governed by QoS capable applications. By default, general network communications will not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

ⓘ **NOTE:** If your network interface does not support 802.1p, it will not be able to process 802.1p tagged traffic, and will ignore it. Make certain when defining Access Rules to enable 802.1p marking that the target devices are 802.1p capable.
It should also be noted that when performing a packet capture (for example, with the diagnostic tool Ethereal) on 802.1p capable devices, some 802.1p capable devices will not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device will almost invariably show the header, but the host will be unable to process the packet.

Before moving on, it is important to introduce 'DSCP Marking' because of the potential interdependency between the two marking methods, as well as to explain why the interdependency exists. For more information, see Managing QoS Marking

DSCP MARKING: EXAMPLE SCENARIO





In the above scenario, we have **Remote Site 1** connected to 'Main Site' by an IPsec VPN. The company uses an internal 802.1p/DSCP capable VoIP phone system, with a private VoIP signaling server hosted at the Main Site. The Main Site has a mixed gigabit and Fast-Ethernet infrastructure, while Remote Site 1 is all Fast Ethernet. Both sites employ 802.1p capable switches for prioritization of internal traffic.

1. PC-1 at Remote Site 1 is transferring a 23 terabyte PowerPoint™ presentation to File Server 1, and the 100mbit link between the workgroup switch and the upstream switch is completely saturated.
2. At the Main Site, a caller on the 802.1p/DSCP capable VoIP Phone 10.50.165.200 initiates a call to the person at VoIP phone 192.168.168.200. The calling VoIP phone 802.1p tags the traffic with priority tag 6 (voice), and DSCP tags the traffic with a tag of 48.
    a. If the link between the Core Switch and the firewall is a VLAN, some switches will include the received 802.1p priority tag, in addition to the DSCP tag, in the packet sent to the firewall; this behavior varies from switch to switch, and is often configurable.
    b. If the link between the Core Switch and the firewall is not a VLAN, there is no way for the switch to include the 802.1p priority tag. The 802.1p priority is removed, and the packet (including only the DSCP tag) is forwarded to the firewall.

       When the firewall sent the packet across the VPN/WAN link, it could include the DSCP tag in the packet, but it is not possible to include the 802.1p tag. This would have the effect of losing all prioritization information for the VoIP traffic, because when the packet arrived at the

Remote Site, the switch would have no 802.1p MAC layer information with which to prioritize the traffic. The Remote Site switch would treat the VoIP traffic the same as the lower-priority file transfer because of the link saturation, introducing delay—maybe even dropped packets—to the VoIP flow, resulting in call quality degradation.

So how can critical 802.1p priority information from the Main Site LAN persist across the VPN/WAN link to Remote Site LAN? Through the use of QoS Mapping.

QoS Mapping is a feature which converts layer 2 802.1p tags to layer 3 DSCP tags so that they can safely traverse (in mapped form) 802.1p-incapable links; when the packet arrives for delivery to the next 802.1p-capable segment, QoS Mapping converts from DSCP back to 802.1p tags so that layer 2 QoS can be honored.

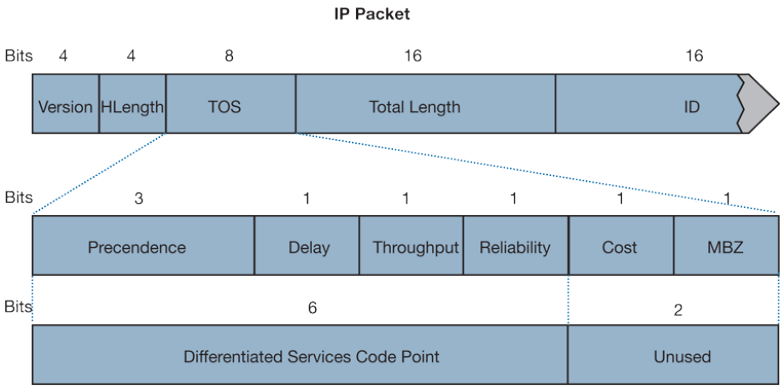
In our above scenario, the firewall at the Main Site assigns a DSCP tag (for example, value **48**) to the VoIP packets, as well as to the encapsulating ESP packets, allowing layer 3 QoS to be applied across the WAN. This assignment can occur either by preserving the existing DSCP tag, or by mapping the value from an 802.1p tag, if present. When the VoIP packets arrive at the other side of the link, the mapping process is reversed by the receiving SonicWall, mapping the DSCP tag back to an 802.1p tag.

3. The receiving SonicWall network security appliance at the Remote Site is configured to map the DSCP tag range 48-55 to 802.1p tag 6. When the packet exits the firewall, it will bear 802.1p tag 6. The Switch will recognize it as voice traffic, and will prioritize it over the file-transfer, guaranteeing QoS even in the event of link saturation.

DSCP Marking

DSCP (Differentiated Services Code Point) marking uses 6-bits of the 8-bit ToS field in the IP Header to provide up to 64 classes (or code points) for traffic. Since DSCP is a layer 3 marking method, there is no concern about compatibility as there is with 802.1p marking. Devices that do not support DSCP will simply ignore the tags, or at worst, they will reset the tag value to 0.

DSCP MARKING: IP PACKET



The above image depicts an IP packet, with a close-up on the ToS portion of the header. The ToS bits were originally used for Precedence and ToS (delay, throughput, reliability, and cost) settings, but were later repurposed by RFC2474 for the more versatile DSCP settings.

The below table displays the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

DSCP MARKING: COMMONLY USED CODE POINTS

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
0	Best effort	0 (Routine – 000)	-
8	Class 1	1 (Priority – 001)	-
10	Class 1, gold (AF11)	1 (Priority – 001)	T
12	Class 1, silver (AF12)	1 (Priority – 001)	D
14	Class 1, bronze (AF13)	1 (Priority – 001)	D, T
16	Class 2	2 (Immediate – 010)	-
18	Class 2, gold (AF21)	2 (Immediate – 010)	T
20	Class 2, silver (AF22)	2 (Immediate – 010)	D
22	Class 2, bronze (AF23)	2 (Immediate – 010)	D, T
24	Class 3	3 (Flash – 011)	-
26	Class 3, gold (AF31)	3 (Flash – 011)	T
27	Class 3, silver (AF32)	3 (Flash – 011)	D
30	Class 3, bronze (AF33)	3 (Flash – 011)	D, T
32	Class 4	4 (Flash Override – 100)	-
34	Class 4, gold (AF41)	4 (Flash Override – 100)	T
36	Class 4, silver (AF42)	4 (Flash Override – 100)	D
38	Class 4, bronze (AF43)	4 (Flash Override – 100)	D, T
40	Express forwarding	5 (CRITIC/ECP – 101)	-
46	Expedited forwarding (EF)	5 (CRITIC/ECP – 101)	D, T
48	Control	6 (Internet Control – 110)	-
56	Control	7 (Network Control – 111)	-

ⓘ | **TIP:** ECP: Elliptic Curve Group

DSCP marking can be performed on traffic to/from any interface and to/from any zone type, without exception. DSCP marking is controlled by Access Rules, from the **QoS** view, and can be used in conjunction with 802.1p marking, as well as with SonicOS's internal bandwidth management.

Topics:

- DSCP Marking and Mixed VPN Traffic
- Configure for 802.1p CoS 4 – Controlled load
- QoS Mapping
- Managing QoS Marking

DSCP Marking and Mixed VPN Traffic

Among their many security measures and characteristics, IPsec VPNs employ anti-replay mechanisms based upon monotonically incrementing sequence numbers added to the ESP header. Packets with

duplicate sequence numbers are dropped, as are packets that do not adhere to sequence criteria. One such criterion governs the handling of out-of-order packets. SonicOS provides a replay window of 64 packets, i.e. if an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet will be dropped.

This should be considered when using DSCP marking to provide layer 3 QoS to traffic traversing a VPN. If you have a VPN tunnel that is transporting a diversity of traffic, some that is being DSCP tagged high priority (for example, VoIP), and some that is DSCP tagged low-priority, or untagged/best-effort (for example, FTP), your service provider will prioritize the handling and delivery of the high-priority ESP packets over the best-effort ESP packets. Under certain traffic conditions, this can result in the best-effort packets being delayed for more than 64 packets, causing them to be dropped by the receiving SonicWall's anti-replay defenses.

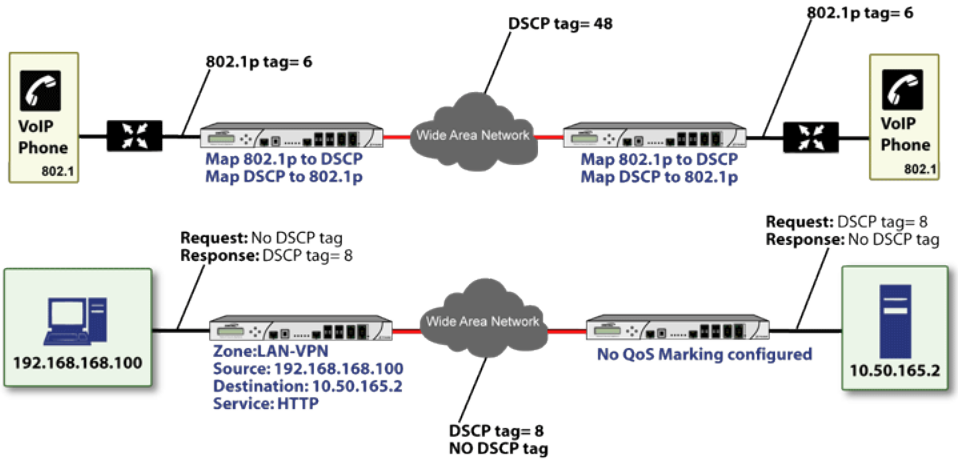
If symptoms of such a scenario emerge (for example, excessive retransmissions of low-priority traffic), it is recommended that you create a separate VPN policy for the high-priority and low-priority classes of traffic. This is most easily accomplished by placing the high-priority hosts (for example, the VoIP network) on their own subnet.

Configure for 802.1p CoS 4 – Controlled load

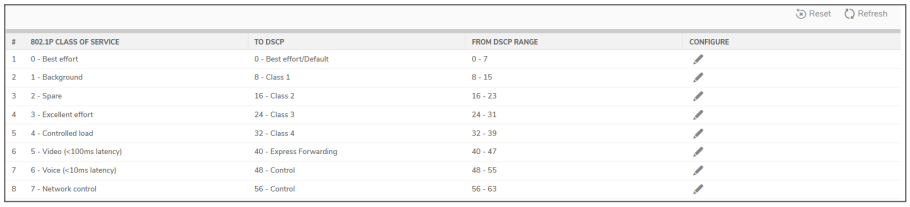
If you want to change the inbound mapping of DSCP tag 15 from its default 802.1p mapping of 1 to an 802.1p mapping of 2, it would have to be done in two steps because mapping ranges cannot overlap. Attempting to assign an overlapping mapping will give the error DSCP range already exists or overlaps with another range. First, you will have to remove 15 from its current end-range mapping to 802.1p CoS 1 (changing the end-range mapping of 802.1p CoS 1 to DSCP 14), then you can assign DSCP 15 to the start-range mapping on 802.1p CoS 2.

QoS Mapping

The primary objective of QoS Mapping is to allow 802.1p tags to persist across non-802.1p compliant links (for example, WAN links) by mapping them to corresponding DSCP tags before sending across the WAN link, and then mapping from DSCP back to 802.1p upon arriving at the other side, as shown in the below figure.

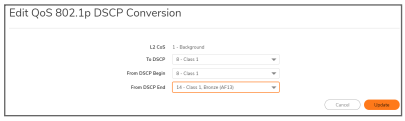


NOTE: Mapping will not occur until you assign **Map** as an action of the QoS view of an Access Rule. The mapping table only defines the correspondence that will be employed by an Access Rule's Map action.



For example, according to the default table, an 802.1p tag with a value of 2 will be outbound mapped to a DSCP value of 16, while a DSCP tag of 43 will be inbound mapped to an 802.1 value of 5.

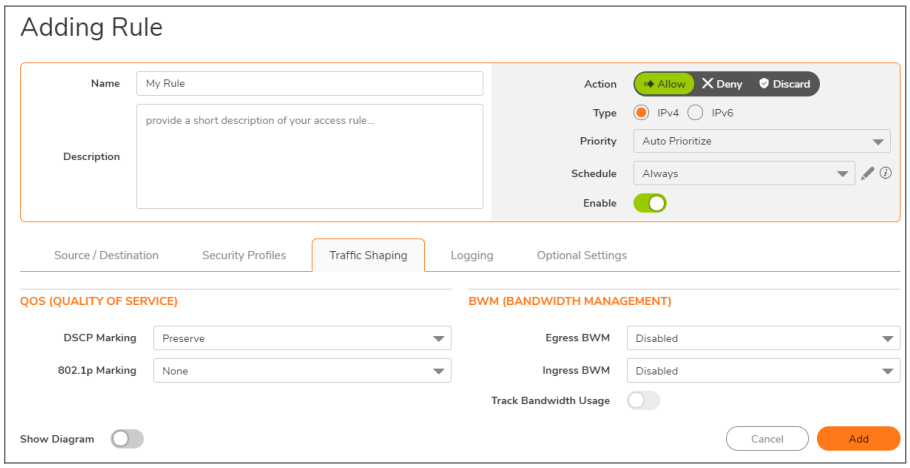
Each of these mappings can be reconfigured. If you wanted to change the outbound mapping of 802.1p tag 4 from its default DSCP value of 32 to a DSCP value of 43, you can click the Configure icon for 4 and select the new To DSCP value from the drop-down box:



You can restore the default mappings by clicking the **Reset** option.

Managing QoS Marking

QoS marking is configured from the **Traffc Shaping** tab of the **Add/Edit Rule** dialog of the **Policy > Rules and Policies > Access Rules > Add Rule** page.



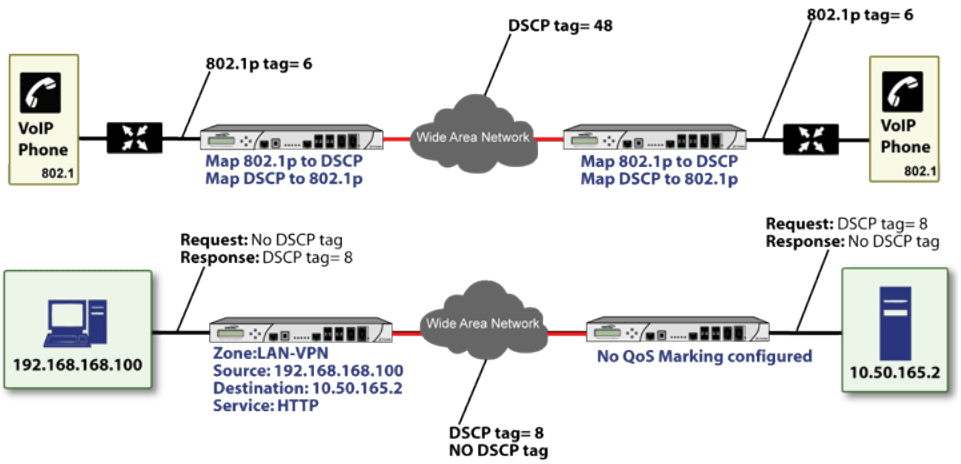
Both 802.1p and DSCP marking as managed by SonicOS Access Rules provide four actions: **None**, **Preserve**, **Explicit**, and **Map**. The default action for DSCP is **Preserve** and the default action for 802.1p is **None**.

The below table describes the behavior of each action on both methods of marking.

Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
None	When packets matching this class of traffic (as defined by the Access Rule) are sent out the egress interface, no 802.1p tag will be added.	The DSCP tag is explicitly set (or reset) to 0.	If the target interface for this class of traffic is a VLAN subinterface, the 802.1p portion of the 802.1q tag will be explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rule using the **Preserve**, **Explicit**, or **Map** action should be defined for this class of traffic.
Preserve	Existing 802.1p tag will be preserved.	Existing DSCP tag value will be preserved.	
Explicit	An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that will be presented.	An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that will be presented.	If either the 802.1p or the DSCP action is set to **Explicit** while the other is set to **Map**, the explicit assignment occurs first, and then the other is mapped according to that assignment.
Map	The mapping setting defined in the **Object > Profile Objects > QoS Marking** page will be used to map from a DSCP tag to an 802.1p tag	The mapping setting defined in the **Object > Profile Objects > QoS Marking** page will be used to map from an 802.1 tag to a DSCP tag. An additional checkbox will be presented to Allow **802.1p Marking to override DSCP values**. Selecting this checkbox will assert the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values.	If **Map** is set as the action on both DSCP and 802.1p, mapping will only occur in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP will be mapped from the 802.1p tag; if the packet is destined to a VLAN, then 802.1p will be mapped from the DSCP tag.

For example, refer below image which provides a bi-directional DSCP tag action.

BI-DIRECTIONAL DSCP TAG ACTION



HTTP access from a Web-browser on 192.168.168.100 to the Web server on 10.50.165.2 will result in the tagging of the inner (payload) packet and the outer (encapsulating ESP) packets with a DSCP value of 8. When the packets emerge from the other end of the tunnel, and are delivered to 10.50.165.2, they will bear a DSCP tag of 8. When 10.50.165.2 sends response packets back across the tunnel to 192.168.168.100 (beginning with the very first SYN/ACK packet) the Access Rule will tag the response packets delivered to 192.168.168.100 with a DSCP value of 8.

This behavior applies to all four QoS action settings for both DSCP and 802.1p marking.

One practical application for this behavior would be configuring an 802.1p marking rule for traffic destined for the VPN zone. Although 802.1p tags cannot be sent across the VPN, reply packets coming back across the VPN can be 802.1p tagged on egress from the tunnel. This requires that 802.1p tagging is active of the physical egress interface, and that the [Zone] > VPN Access Rule has an 802.1p marking action other than None.

After ensuring 802.1p compatibility with your relevant network devices, and enabling 802.1p marking on applicable SonicWall interfaces, you can begin configuring Access Rules to manage 802.1p tags.

The **Remote Site 1** network could have two Access Rules configured as in the below table.

REMOTE SITE 1: SAMPLE ACCESS RULE CONFIGURATION

Setting	Access Rule 1	Access Rule 2
General View		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VOIP	VOIP
Source	Lan Primary Subnet	Main Site Subnets
Destination	Main Site Subnets	Lan Primary Subnet
Users Allowed	All	All
Schedule	Always on	Always on

Setting	Access Rule 1	Access Rule 2
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
QoS View		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

The first Access Rule (governing **LAN > VPN**) would have the following effects:

- **VoI**P traffic (as defined by the Service Group) from **LAN Primary Subnet** destined to be sent across the VPN to **Main Site Subnets** would be evaluated for both DSCP and 802.1p tags.
    - The combination of setting both DSCP and 802.1p marking actions to **Map** is described in the table earlier in Managing QoS Marking.
    - Sent traffic containing only an 802.1p tag (for example, CoS = 6) would have the VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.
    - Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
    - Sent traffic containing only a DSCP tag (for example, CoS = 48) would have the DSCP value preserved on both inner and outer packets.
    - Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
    - Sent traffic containing only both an 802.1p tag (for example, CoS = 6) and a DSCP tag (for example, CoS = 63) would give precedence to the 802.1p tag and would be mapped accordingly. The VPN-bound inner (payload) packet DSCP would be tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.

Assuming returned traffic has been DSCP tagged (CoS = 48) by the firewall at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.

To examine the effects of the second Access Rule (VPN>LAN), we'll look at the Access Rules configured at the Main Site, as shown below:

MAIN SITE: SAMPLE ACCESS RULE CONFIGURATIONS

Setting	Access Rule 1	Access Rule 2
General View		
Action	Allow	Allow
From Zone	LAN	VPN
To Zone	VPN	LAN
Service	VOIP	VOIP
Source	Lan Subnets	Remote Site 1 Subnets
Destination	Remote Site 1 Subnets	Lan Subnets
Users Allowed	All	All

Setting	Access Rule 1	Access Rule 2
Schedule	Always on	Always on
Enable Logging	Enabled	Enabled
Allow Fragmented Packets	Enabled	Enabled
QoS View		
DSCP Marking Action	Map	Map
Allow 802.1p Marking to override DSCP values	Enabled	Enabled
802.1p Marking Action	Map	Map

VoIP traffic (as defined by the Service Group) arriving from **Remote Site 1 Subnets** across the VPN destined to **LAN Subnets** on the LAN zone at the Main Site would hit the Access Rule for inbound VoIP calls. Traffic arriving at the VPN zone will not have any 802.1p tags, only DSCP tags.

- Traffic exiting the tunnel containing a DSCP tag (for example, CoS = 48) would have the DSCP value preserved. Before the packet is delivered to the destination on the LAN, it will also be 802.1p tagged according to the **QoS Marking** settings (for example, CoS = 6) by the firewall at the Main Site.
- Assuming returned traffic has been 802.1p tagged (for example, CoS = 6) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been DSCP tagged (for example, CoS = 48) by the VoIP phone receiving the call at the Main Site, the return traffic will have the DSCP tag preserved on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been both 802.1p tagged (for example, CoS = 6) and DSCP tagged (for example, CoS = 14) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

Glossary

- **802.1p** – IEEE 802.1p is a Layer 2 (MAC layer) Class of Service mechanism that tags packets by using 3 priority bits (for a total of 8 priority levels) within the additional 16-bits of an 802.1q header. 802.1p processing requires compatible equipment for tag generation, recognition and processing, and should only be employed on compatible networks.
- **Bandwidth Management (BWM)** – Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWall employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.
- **Class of Service (CoS)** – A designator or identifier, such as a layer 2 or layer 3 tag, that is applied to traffic after classification. CoS information will be used by the Quality of Service (QoS) system to differentiate between the classes of traffic on the network, and to provide special handling (for example, prioritized queuing, low latency) as defined by the QoS system administrator.

- **Classification** – The act of identifying (or differentiating) certain types (or classes) of traffic. Within the context of QoS, this is performed for the sake of providing customized handling, typically prioritization or de-prioritization, based on the traffic's sensitivity to delay, latency, or packet loss. Classification within SonicOS uses Access Rules, and can occur based on any or all of the following elements: source zone, destination zone, source address object, destination address object, service object, schedule object.
- **Code Point** – A value that is marked (or tagged) into the DSCP portion of an IP packet by a host or by an intermediate network device. There are currently 64 Code Points available, from 0 to 63, used to define the ascending prioritized class of the tagged traffic.
- **Conditioning** – A broad term used to describe a plurality of methods of providing Quality of Service to network traffic, including but not limited to discarding, queuing, policing, and shaping.
- **DiffServ (Differentiated Services)** – A standard for differentiating between different types or classes of traffic on an IP network for the purpose of providing tailored handling to the traffic based on its requirements. DiffServ primarily depends upon Code Point values marked in the ToS header of an IP packet to differentiate between different classes of traffic. DiffServ service levels are executed on a Per Hop Basis at each router (or other DiffServ enabled network device) through which the marked traffic passes. DiffServ Service levels currently include at a minimum Default, Assured Forwarding, Expedited Forwarding, and DiffServ. Refer to DSCP Marking for more information.
- **Discarding** – A congestion avoidance mechanism that is employed by QoS systems in an attempt to predict when congestion might occur on a network, and to prevent the congestion by dropping over-limit traffic. Discarding can also be thought of as a queue management algorithm, since it attempts to avoid situations of full queues. Advanced discard mechanisms will abide by CoS markings so as to avoid dropping sensitive traffic. Common methods are:
    - **Tail Drop** – An indiscriminate method of dealing with a full queue wherein the last packets into the queue are dropped, regardless of their CoS marking.
    - **Random Early Detection (RED)** – RED monitors the status of queues to try to anticipate when a queue is about to become full. It then randomly discards packets in a staggered fashion to help minimize the potential of Global Synchronization. Basic implementations of RED, like Tail Drop, do not consider CoS markings.
    - **Weighted Random Early Detection (WRED)** – An implementation of RED that factors DSCP markings into its discard decision process.
- **DSCP (Differentiate Services Code Points)** – The repurposing of the ToS field of an IP header as described by RFC2747. DSCP uses 64 Code Point values to enable DiffServ (Differentiated Services). By marking traffic according to its class, each packet can be treated appropriately at every hop along the network.
- **Global Synchronization** – A potential side effect of discarding, the congestion avoidance method designed to deal with full queues. Global Synchronization occurs when multiple TCP flows through a congested link are dropped at the same time (as can occur in Tail Drop). When the native TCP slow-start mechanism commences with near simultaneity for each of these flows, the flows will again flood the link. This leads to cyclical waves of congestion and under-utilization.
- **Guaranteed Bandwidth** – A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Guaranteed Bandwidth can also be set to 0%.

- **Inbound (Ingress or IBWM)** – The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgments (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.
- **IntServ (Integrated Services)** – As defined by RFC1633. An alternative CoS system to DiffServ, IntServ differs fundamentally from DiffServ in that it has each device request (or reserve) its network requirements before it sends its traffic. This requires that each hop on the network be IntServ aware, and it also requires each hop to maintain state information for every flow. IntServ is not supported by SonicOS. The most common implementation of IntServ is RSVP.
- **Maximum Bandwidth** – A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic.The Maximum Bandwidth can be set to 0%, which will prevent all traffic.
- **Outbound (Egress or OBWM)** – Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.
- **Priority** – An additional dimension used in the classification of traffic. SonicOS uses 8 priority rings (0 = highest, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority ring.
- **Mapping** – With regard to SonicOS's implementation of QoS, mapping is the practice of converting layer 2 CoS tags (802.1p) to layer 3 CoS tags (DSCP) and back again for preserving the 802.1p tags across network links that do not support 802.1p tagging. The map correspondence is fully user-definable, and the act of mapping is controlled by Access Rules.
- **Marking** – Also known as **tagging** or **coloring** – The act of applying layer 2 (802.1p) or layer 3 (DSCP) information to a packet for the purpose of differentiation, so that it can be properly classified (recognized) and prioritized by network devices along the path to its destination.
- **Multi Protocol Label Switching (MPLS)** – A term that comes up frequently in the area of QoS, but which is natively unsupported by most customer premise IP networking devices, including SonicWall appliances. MPLS is a carrier-class network service that attempts to enhance the IP network experience by adding the concept connection-oriented paths (Label Switch Paths – LSPs) along the network. When a packet leaves a customer premise network, it is tagged by a Label Edge Router (LER) so that the label can be used to determine the LSP. The MPLS tag itself resides between layer 2 and layer 3, imparting upon MPLS characteristics of both network layers. MPLS is becoming quite popular for VPNs, offering both layer 2 and layer 3 VPN services, but remains interoperable with existing IPsec VPN implementation. MPLS is also very well known for its QoS capabilities, and interoperates well with conventional DSCP marking.
- **Per Hop Behavior (PHB)** – The handling that will be applied to a packet by each DiffServ capable router it traverses, based upon the DSCP classification of the packet. The behavior can be among such actions as discard, re-mark (re-classify), best-effort, assured forwarding, or expedited forwarding.
- **Policing** – A facility of traffic conditioning that attempts to control the rate of traffic into or out of a network link. Policing methods range from indiscriminate packet discarding to algorithmic shaping, to various queuing disciplines.

- **Queuing** – To effectively make use of a link's available bandwidth, queues are commonly employed to sort and separately manage traffic after it has been classified. Queues are then managed using a variety of methods and algorithms to ensure that the higher priority queues always have room to receive more traffic, and that they can be serviced (de-queued or processed) before lower priority queues. Some common queue disciplines include:
    - **FIFO (First In First Out)** – A very simple, undiscriminating queue where the first packet in is the first packet to be processed.
    - **Class Based Queuing (CBQ)** – A queuing discipline that takes into account the CoS of a packet, ensuring that higher priority traffic is treated preferentially.
    - **Weighted Fair Queuing (WFQ)** – A discipline that attempts to service queues using a simple formula based upon the packets' IP precedence and the total number of flows. WFQ has a tendency to become imbalanced when there is a disproportionately large number of high-priority flows to be serviced, often having the opposite of the desired effect.
    - **Token Based CBQ** – An enhancement to CBQ that employs a token, or a credit-based system that helps to smooth or normalize link utilization, avoiding burstiness as well as under-utilization. Employed by SonicOS BWM.
- **Resource Reservation Protocol (RSVP)** – An IntServ signaling protocol employed by some applications where the anticipated need for network behavior (for example, delay and bandwidth) is requested so that it can be reserved along the network path. Setting up this Reservation Path requires that each hop along the way be RSVP capable, and that each agrees to reserve the requested resources. This system of QoS is comparatively resource intensive, since it requires each hop to maintain state on existing flows. Although IntServ's RSVP is quite different from DiffServ's DSCP, the two can interoperate. RSVP is not supported by SonicOS.
- **Shaping** – An attempt by a QoS system to modify the rate of traffic flow, usually by employing some feedback mechanism to the sender. The most common example of this is TCP rate manipulation, where acknowledgements (ACKs) sent back to a TCP sender are queued and delayed so as to increase the calculated round-trip time (RTT), leveraging the inherent behavior of TCP to force the sender to slow the rate at which it sends data.
- **Type of Service (ToS)** – A field within the IP header wherein CoS information can be specified. Historically used, albeit somewhat rarely, in conjunction with IP precedence bits to define CoS. The ToS field is now rather commonly used by DiffServ's code point values.

4

Content Filter

SonicWall Content Filtering Service (CFS) version 4.0 delivers content filtering enforcement for educational institutions, businesses, libraries, and government agencies. With content filter objects, you can control the websites students and employees can access using their IT-issued computers while behind the organization's firewall.

NOTE: For information about upgrading from an older version to CFS 4.0, see the *SonicWall Content Filtering Service Upgrade Guide*. Also, for applying these objects in CFS policies, see the *Policy > Rules and Policies > Content Filter Rules* section of the *SonicOS Security Configuration* technical documentation.

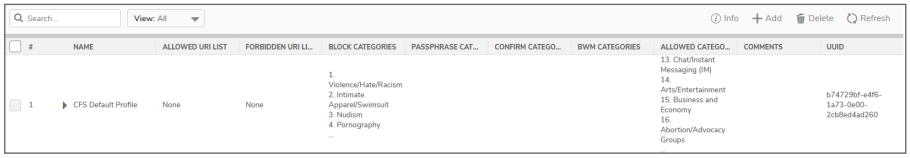
Topics:

Managing CFS Profile Objects

Topics:

About CFS Profile Objects

A CFS Profile Object defines the action triggered for each HTTP/HTTPS connection.

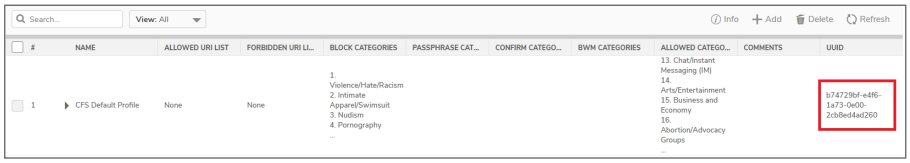


Name	Name of the CFS Profile Object; the name of the default CFS Profile Object is **CFS Default Profile**. The default object can be edited, but not deleted.
Allowed URI List	Name of the URI List Object listed in the Allowed List.
Forbidden URI List	Name of the URI List Object listed in the Forbidden List.
Block Categories	Names of all the categories blocked by the CFS Profile Object.
Passphrase Categories	Names of all the categories requiring a passphrase by this CFS Profile Object.
Confirm Categories	Names of all the categories requiring confirmation by this CFS Profile Object.
BWM Categories	Names of all the categories governed by bandwidth management by this CFS Profile Object.
Allowed Categories	Names of all the categories allowed by the CFS Profile Object.
Comments	Comments which you have added during creation of CFS Profile Object.
UUID	A UUID (Universally Unique Identifier) is a 36-character string (32 alphanumeric characters and four hyphens) that is used to uniquely identify profile objects and groups, among other entities, on SonicWall network security appliances. The SonicOS UUID is a system-generated and read-only internal value.

About UUIDs for CFS Profile Objects

SonicOS 6.5.3 (and higher) automatically generates and binds UUIDs (Universally Unique Identifiers) for the Content Filter objects.

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.

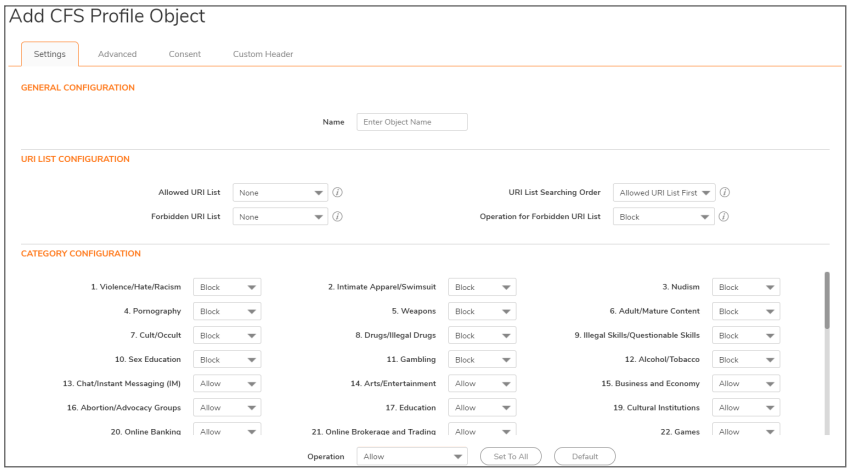


Configuring CFS Profile Objects

A default CFS Profile Object, **CFS Default Profile**, is created by SonicOS. You can configure and edit this CFS Profile Object, but you cannot delete it.

To configure CFS Profile Objects:

1. Navigate to **Object > Profile Objects > Content Filter** page.
2. Click the **Add** button at the top of the page. The **Add CFS Profile Object** dialog displays.



3. On the **Settings** screen, enter the name of the CFS Profile Object in the **Name** field.
4. From the **Allowed URI List** drop-down menu, choose the URI List Object that contains URIs for which unrestricted access is allowed; treat this list as a white list:
   - None (default).
   - Name of the URI List Object.
   - Create new URI List object; choosing this option displays the Add CFS URI List Object dialog. For how to create a URI List Object, see *Objects > Match Objects > URI Lists* section of SonicOS.
5. From the **Forbidden URI List** drop-down menu, choose the URI List Object that contains URIs for which access is not allowed at all; treat this list as a black list:
   - None (default).
   - Name of the URI List Object.
   - Create new URI List object; choosing this option displays the Add CFS URI List Object dialog. For how to create a URI List Object, see *Objects > Match Objects > URI Lists* section of SonicOS.
6. From the **URI List Searching Order** drop-down menu, choose which URI list is searched first during filtering:
   - Allowed URI List First (default)
   - Forbidden URI List First

7. From the **Operation for Forbidden URI** List drop-down menu, choose the action to be taken when a URI on the Forbidden List is encountered:

Block (default)	The block page configured for the CFS Action Object is displayed to the user accessing the site.
Confirm	The confirm page configured for the CFS Action Object is displayed to the user accessing the site. The user must confirm access permission.
Passphrase	The passphrase page configured for the CFS Action Object is displayed to the user accessing the site. The user must enter a valid password to enter the site.

8. The **Category Configuration** section lists all the categories of URIs, such as Arts & Entertainment, Business, Education, Travel, Weapons, and Shopping. You can configure the action to be taken for all URIs in each category instead of individually. As you scroll down the list, choose the action from the drop-down menu for each category:
   - Allow
   - Block
   - BWM
   - Confirm
   - Passphrase

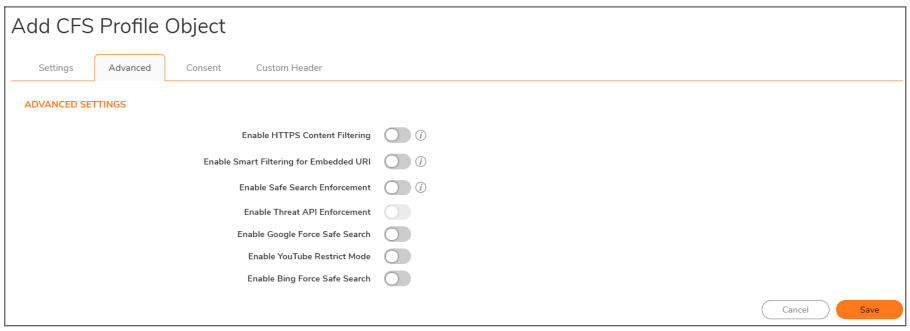
   ⓘ | **NOTE:** By default, Categories 1-12 and 59 are blocked; the remaining categories are allowed.

   - To change all categories to the same action:
     1. Choose the action from the **Operation** drop-down menu.
     2. Click the **Set To All** button.
   - To reset all the categories to its default action, click the **Default** button.
9. To enable Smart Filtering and Safe Search options, click the **Advanced** tab. For information about configuring the options on this screen, go to Advanced Screen.
10. To set up web usage consent, click the **Consent** tab. For information about configuring the options on this screen, go to Consent Screen.
11. To configure Custom Header insertion, click the **Custom Header** tab. For information about configuring the options on this screen, go to Custom Header Screen.
12. Click **Add**. The **CFS Profile Objects** table is updated.

Topics:

Advanced Screen

This screen is one of the four screens in **Add CFS Profile Object** dialog. To open the dialog, navigate to **Object > Profile Objects > Content Filter**page and click the **Add** button at the top of the page. Then click **Advanced** tab.



ⓘ | **NOTE:** By default, none of the options are selected.

1. To enable content filtering for HTTPS sites, select the **Enable HTTPS Content Filtering** option. This policy-based HTTPS content filtering option is available in SonicOS 6.5.3 or higher. It replaces the global HTTPS content filtering option in previous versions on the **Policy > Security Services > Content Filter** page.

   ⓘ | **NOTE:** When DPI-SSL client inspection is enabled and Content Filter is selected for inspection, then that inspection takes precedence and the policy-based HTTPS content filtering setting is ignored. Specifically, when the **Enable SSL Client Inspection** and **Content Filter** options are enabled on the **Policy > DPI-SSL** page, then the **Enable HTTPS Content Filtering** option in the CFS policy is ignored. In this case, DPI-SSL will decrypt the connection and send it as plain text to CFS later for filtering.

   HTTPS content filtering is IP based and does not inspect the URL, but uses other methods to obtain the URL rating. When this option is enabled, CFS performs URL rating lookup in this order:

   a. Searches the client *hello* for the Server Name, which CFS uses to obtain the URL rating.
   b. If the Server Name is not available, searches the SSL certificate for the Common Name, which CFS uses to obtain the URL rating.
   c. If neither Server Name nor Common Name is available, CFS uses the IP address to obtain the URL rating.

   While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS filtered pages will be silently blocked.

2. To detect the embedded URL inside Google Translate (*https://translate.google.com*) and filter the embedded URI, select the **Enable Smart Filtering for Embedded URI** option.

   ⓘ | **IMPORTANT:** This feature requires enabling Client DPI-SSL with content filter.

   ⓘ | **NOTE:** This feature takes effect only on Google Translate, which works on currently rated embedded web sites.

3. To enforce Safe Search when searching on any of the following websites, select the **Enable Safe Search Enforcement** option:
   - *www.yahoo.com*
   - *www.ask.com*
   - *www.dogpile.com*
   - *www.lycos.com*

   NOTE: This enforcement cannot be configured at the policy level as the function employs DNS redirection to HTTPS sites. For HTTPS sites, client DPI-SSL with content filter must be enabled.
4. To enable Threat API, select the **Enable Threat API Enforcement** option.

   NOTE: After SonicOS receives the initial threat list and creates a Threat URI List Object, the Threat URI List Object is referenced by **Enable Threat API Enforcement**.
5. To override the Safe Search option for Google inside each CFS Policy and its corresponding CFS Action, select the **Enable Google Force Safe Search** option.

   NOTE: Typically, Safe Search happens automatically and is powered by Google, but when this option is enabled, SonicOS rewrites the Google domain in the DNS response to the Google Safe Search virtual IP address.

   NOTE: This feature takes effect only after the DNS cache of the client host is refreshed.
6. To access YouTube in Restrict (Safe Search) mode, select the **Enable YouTube Restrict Mode** option.

   NOTE: YouTube provides a new feature to screen videos that may contain inappropriate content flagged by users and other signals. When this feature is enabled, SonicOS rewrites the DNS response for the YouTube domain to its Safe Search virtual IP address.

   NOTE: This feature takes effect only after the DNS cache of the client host is refreshed.
7. To override the Safe Search option for Bing inside each CFS Policy and its corresponding CFS Action, select the **Enable Bing Force Safe Search** option.

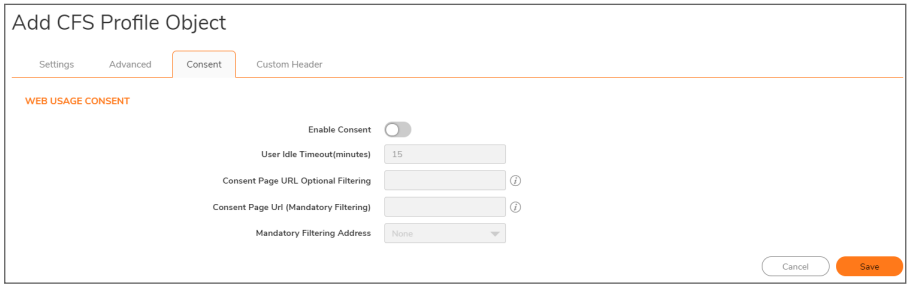
   NOTE: When this feature is enabled, SonicOS rewrites the DNS response for the Bing domain to its Safe Search virtual IP address.

   NOTE: This feature takes effect only after the DNS cache of the client host is refreshed.
8. Click **Save**.

Consent Screen

This screen is one of the four screens in **Add CFS Profile Object** dialog. To open the dialog, navigate **Object > Profile Objects > Content Filter**page and click the **Add** button at the top of the page. Then click **Consent** tab.

NOTE: Consent only works for HTTP requests. HTTPS requests cannot be redirected to a Confirm (consent) page.



1. To enable consent, which displays the Consent (Confirm) page when a user visits a site requiring consent before access, select the **Enable Consent** option. This option is not selected by default. When this option is selected, the other options become available.
2. To remind users that their time has expired by displaying the Consent page, enter the idle-time duration in the **User Idle Timeout(minutes)** field. The minimum idle time is 1 minute, the maximum is 9999 minutes, and the default is **15** minutes.
3. In the **Consent Page URL (optional filtering)** field, enter the URL of the website where a user is redirected if they go to a website requiring consent. The Consent page must:
    - Reside on a web server and be accessible as a URI by users on the network.
    - Contain links to the following two pages in the SonicWall appliance, which, when selected, tell the firewall the type of access the user wishes to have:
        - Unfiltered access: *<appliance's LAN IP address>/iAccept.html*
        - Filtered access: *<appliance's LAN IP address>/iAcceptFilter.html*
4. In the **Consent Page URL (mandatory filtering)** field, enter the website URL where the user is redirected if they go to a website requiring mandatory filtering. The Consent page must:
    - Reside on a web server and be accessible as a URI by users on the network.
    - Contain a link to the *<appliance's LAN IP address>/iAcceptFilter.html* page in the SonicWall appliance, which tells the firewall that the user accepts filtered access.
5. From the **Mandatory Filtering Address** drop-down menu, choose an Address Object that contains the configured IP addresses requiring mandatory filtering.
6. Click **Save**.

Custom Header Screen

Starting in SonicOS 6.5.1, you can configure the firewall as a web proxy server to control web service, such as preventing users from signing in to some web services using any accounts other than the accounts provided, or restricting the content viewable by users. The web proxy server adds a custom header to all traffic matched by the Content Filtering policy, and the header identifies the domains whose users can access the web services or the content that users can access. Encrypted HTTPS traffic is supported if DPI-SSL is enabled.

This screen is one of the four screens in **Add CFS Profile Object** dialog. To open the dialog, navigate **Object > Profile Objects > Content Filter**page and click the **Add** button at the top of the page. Then click **Custom Header Screen** tab.

This feature requires the following:

- Content Filter Service is enabled.
- Custom header insertion is enabled in the matched CFS profile object.
- DPI-SSL is enabled for custom header insertion with encrypted HTTPS requests.

To configure a CFS custom header and enable custom header insertion:

1. Navigate to **Object > Profile Objects > Content Filter**tab.
2. Click **Add** at the top of the page.
3. In the **Add/Edit CFS Profile Object** dialog, click **Custom Header** tab to display the Custom Header Insertion options.
4. Enable the **Enable Custom Header Insertion** option.
5. Click **Add** icon to configure the **Domain**, **Key**, and **Value** for the custom header entry.

Domain is used to check whether the host in an HTTP request is matched to an entry during packet handling. **Key** and **Value** are used to generate the right header for the entry when building runtime data for custom header insertion.

The Domain can contain:

- Each domain name can contain up to 16 tokens separated by periods (.).
- The domain name cannot start or end with separators.
- Each token can contain up to 128 printable ASCII characters.
- Tokens in a domain name can only contain the characters: *0-9a-zA-z$-_+!'(),*.
- IPv4/IPv6 addresses can be defined as a domain name, e.g. “[2001:2002:2003::2005:2006]”.

6. Click **Save**.

Editing a CFS Profile Object

To edit a CFS Profile Object:

1. Navigate to **Object > Profile Objects > Content Filter**page.
2. Hover on the CFS Profile Object to be edited and click the **Edit** icon. The **Edit CFS Profile Object** dialog displays. This dialog is the same as the **Add CFS Profile Object** dialog.
3. To make your changes, follow the appropriate procedures in Configuring CFS Profile Objects.

Deleting CFS Profile Objects

To delete CFS Profile Objects:

1. Navigate to **Object > Profile Objects > Content Filter**page.
2. Do one of the following:
    - Hover on the Profile object to be deleted and click the **Delete** icon.
    - Click the checkbox for one or more Profile objects to be deleted and click the **Delete** icon on top of the page.

Applying Content Filter Objects

After you finish configuring your Content Filter Objects, you need to apply them to Content Filter policies. Configuring Content Filters is done on the **Policy Security Services > Content Filter** page (see the *Configuring Content Filtering Service* section of the *SonicOS Security Configuration* technical documentation).

5

DHCP Option

A SonicWall network security appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. **Network > DHCP Server** includes settings for configuring the appliance's DHCP server, Lease Scopes, and DHCP Leases.

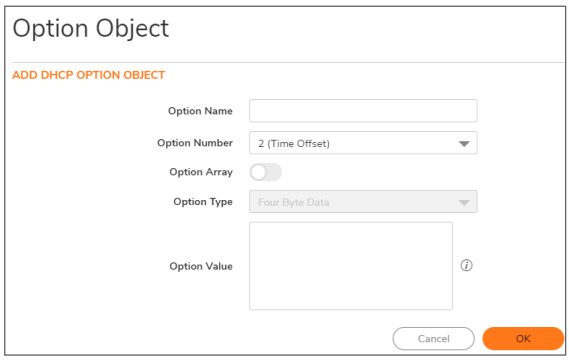
The SonicWall DHCP server Option feature provides support for DHCP Options, also known as vendor extensions, as defined primarily in RFCs 2131 and 2132. DHCP Options allow users to specify additional DHCP parameters in the form of predefined, vendor-specific information that is stored in the options field of a DHCP message. When the DHCP message is sent to clients on the network, it provides vendor-specific configuration and service information. For more information on RFC-Defined DHCP Option Numbers, see:

- IPv4 Options: RFC-Defined DHCPV4 Option Numbers
- IPv6 Options: RFC-Defined DHCPV6 Option Numbers

Configuring DHCP Option Objects

You can create DHCP Option objects in one of these ways:

1. Navigate to **Object > Profile Objects > DHCP Option** page, and click **Add** to create IPv4 and IPv6 DHCP Option Objects. The Add DHCP Option Object dialog displays.



2. Type a name for the option object in the **Option Name** field.

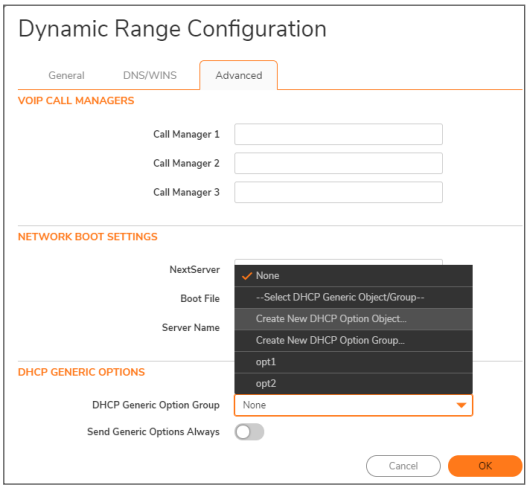
3. From **Option Number**, select the option number that corresponds to your DHCP option. For a list of option numbers, names, and descriptions, refer to:
    - For IPv4, see RFC-Defined DHCPV4 Option Numbers
    - For IPv6, see RFC-Defined DHCPV6 Option Numbers
4. If:
    - Only one option type is available, for example, for **Option Number 2 (Time Offset)**, **Option Array** is dimmed. Go to **Step 7**.
    - There are multiple option types available, for example, for **77 (User Class Information)**, **Option Type** becomes available and lists allowable types of the option, such as **IP Address**, **Two-Byte Data**, **String**, **Boolean**, and so on. Select the option type.
5. Type the option value, for example, an IP address, in the **Option Value** field. If Option Array is checked, multiple values may be entered, separated by a semi-colon (;).
6. Click **OK**. The object displays in the **Option Objects** table.

DHCPV4 OPTION OBJECTS TABLE

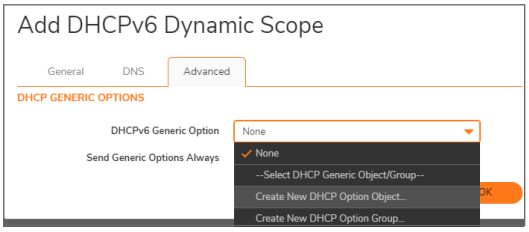
DHCPV6 OPTION OBJECTS TABLE

OR

- Navigate to **Network > DHCP Server > DHCP Server Lease Scopes** tab,
    - To create IPv4 Option object, click **Add Static** or **Add Dynamic** option. In the dialog, click **Advanced** tab and select **Create New DHCP Option Object** from the **DHCP Generic Option Group** drop-down.



- To create IPv6 Option object, select **IPv6** tab and click **Add Static** or **Add Dynamic** option. In the dialog, click **Advanced** tab and select **Create New DHCP Option Object** from the **DHCP Generic Option** drop-down.



- Follow Steps from 2 through Step 6 from the above section. The object displays in the **Option Objects** table.

RFC-Defined DHCPV4 Option Numbers

Option Number	Name	Description
2	Time Offset	Time offset in seconds from UTC
3	Routers	N/4 router addresses
4	Time Servers	N/4 time server addresses
5	Name Servers	N/4 IEN-116 server addresses
6	DNS Servers	N/4 DNS server addresses
7	Log Servers	N/4 logging server addresses
8	Cookie Servers	N/4 quote server addresses
9	LPR Servers	N/4 printer server addresses
10	Impress Servers	N/4 impress server addresses
11	RLP Servers	N/4 RLP server addresses
12	Host Name	Hostname string, such as (Server Unicast)
13	Boot File Size	Size of boot file in 512-byte chunks
14	Merit Dump File	Client to dump and name of file to dump to
15	Domain Name	DNS domain name of the client
16	Swap Server	Swap server addresses
17	Root Path	Path name for root disk
18	Extension File	Patch name for more BOOTP info
19	IP Layer Forwarding	Enable or disable IP forwarding
20	Src route enabler	Enable or disable source routing
21	Policy Filter	Routing policy filters
22	Maximum DG Reassembly Size	Maximum datagram reassembly size
23	Default IP TTL	Default IP time-to-live

Option Number	Name	Description
24	Path MTU Aging Timeout	Path MTU aging timeout
25	MTU Plateau	Path MTU plateau table
26	Interface MTU Size	Interface MTU size
27	All Subnets Are Local	All subnets are local
28	Broadcast Address	Broadcast address
29	Perform Mask Discovery	Perform mask discovery
30	Provide Mask to Others	Provide mask to others
31	Perform Router Discovery	Perform router discovery
32	Router Solicitation Address	Router solicitation address
33	Static Routing Table	Static routing table
34	Trailer Encapsulation	Trailer encapsulation
35	ARP Cache Timeout	ARP cache timeout
36	Ethernet Encapsulation	Ethernet encapsulation
37	Default TCP Time to Live	Default TCP time to live
38	TCP Keepalive Interval	TCP keepalive interval
39	TCP Keepalive Garbage	TCP keepalive garbage
40	NIS Domain Name	NIS domain name
41	NIS Server Addresses	NIS server addresses
42	NTP Servers Addresses	NTP servers addresses
43	Vendor Specific Information	Vendor specific information
44	NetBIOS Name Server	NetBIOS name server
45	NetBIOS Datagram Distribution	NetBIOS datagram distribution
46	NetBIOS Node Type	NetBIOS node type
47	NetBIOS Scope	NetBIOS scope
48	X Window Font Server	X window font server
49	X Window Display Manager	X window display manager
50	Requested IP address	Requested IP address
51	IP Address Lease Time	IP address lease time
52	Option Overload	Overload “sname” or “file”
53	DHCP Message Type	DHCP message type
54	DHCP Server Identification	DHCP server identification
55	Parameter Request List	Parameter request list
56	Message	DHCP error message
57	DHCP Maximum Message Size	DHCP maximum message size
58	Renew Time Value	DHCP renewal (T1) time
59	Rebinding Time Value	DHCP rebinding (T2) time
60	Client Identifier	Client identifier

Option Number	Name	Description
61	Client Identifier	Client identifier
62	Netware/IP Domain Name	Netware/IP domain name
63	Netware/IP sub Options	Netware/IP sub options
64	NIS+ V3 Client Domain Name	NIS+ V3 client domain name
65	NIS+ V3 Server Address	NIS+ V3 server address
66	TFTP Server Name	TFTP server name
67	Boot File Name	Boot file name
68	Home Agent Addresses	Home agent addresses
69	Simple Mail Server Addresses	Simple mail server addresses
70	Post Office Server Addresses	Post office server addresses
71	Network News Server Addresses	Network news server addresses
72	WWW Server Addresses	WWW server addresses
73	Finger Server Addresses	Finger server addresses
74	Chat Server Addresses	Chat server addresses
75	StreetTalk Server Addresses	StreetTalk server addresses
76	StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses
77	User Class Information	User class information
78	SLP Directory Agent	Directory agent information
79	SLP Service Scope	Service location agent scope
80	Rapid Commit	Rapid commit
81	FQDN, Fully Qualified Domain Name	Fully qualified domain name
82	Relay Agent Information	Relay agent information
83	Internet Storage Name Service	Internet storage name service
84	Undefined	N/A
85	Novell Directory Servers	Novell Directory Services servers
86	Novell Directory Server Tree Name	Novell Directory Services server tree name
87	Novell Directory Server Context	Novell Directory Services server context
88	BCMCS Controller Domain Name List	CMCS controller domain name list
89	BCMCS Controller IPv4 Address List	BCMCS controller IPv4 address list
90	Authentication	Authentication
91- 92	Undefined	N/A
93	Client System	Client system architecture
94	Client Network Device Interface	Client network device interface
95	LDAP Use	Lightweight Directory Access Protocol
96	Undefined	N/A
97	UUID/GUID-based Client Identifier	UUID/GUID-based client identifier

Option Number	Name	Description
98	Open Group's User Authentication	Open group's user authentication
99 - 108	Undefined	N/A
109	Autonomous System Number	Autonomous system number
110 - 111	Undefined	N/A
112	NetInfo Parent Server Address	NetInfo parent server address
113	NetInfo Parent Server Tag	NetInfo parent server tag
114	URL:	URL
115	Undefined	N/A
116	Auto Configure	DHCP auto-configuration
117	Name Service Search	Name service search
118	Subnet Collection	Subnet selection
119	DNS Domain Search List	DNS domain search list
120	SIP Servers DHCP Option	SIP servers DHCP option
121	Classless Static Route Option	Classless static route option
122	CCC, CableLabs Client Configuration	CableLabs client configuration
123	GeoConf	GeoConf
124	Vendor-Identifying Vendor Class	Vendor-identifying vendor class
125	Vendor Identifying Vendor Specific	Vendor-identifying vendor specific
126 - 127	Undefined	N/A
128	TFTP Server IP Address	TFTP server IP address for IP phone software load
129	Call Server IP Address	Call server IP address
130	Discrimination String	Discrimination string to identify vendor
131	Remote Statistics Server IP Address	Remote statistics server IP address
132	802.1Q VLAN ID	IEEE 802.1Q VLAN ID
133	802.1Q L2 Priority	IEEE 802.1Q layer 2 priority
134	Diffserv Code Point	Diffserv code point for VoIP signalling and media streams
135	HTTP Proxy For Phone Applications	HTTP proxy for phone-specific applications
136 - 149	Undefined	N/A
150	TFTP Server Address, Etherboot, GRUB Config	TFTP server address, Etherboot, GRUB configuration
151 - 174	Undefined	N/A
175	Ether Boot	Ether Boot
176	IP Telephone	IP telephone
177	Ether Boot PacketCable and CableHome	Ether Boot PacketCable and CableHome

Option Number	Name	Description
178 - 207	Undefined	N/A
208	pxelinux.magic (string) = 241.0.116.126	pxelinux.magic (string) = 241.0.116.126
209	pxelinux.configfile (text)	pxelinux.configfile (text)
210	pxelinux.pathprefix (text)	pxelinux.pathprefix (text)
211	pxelinux.reboottime	pxelinux.reboottime
212 - 219	Undefined	N/A
220	Subnet Allocation	Subnet allocation
221	Virtual Subnet Allocation	Virtual subnet selection
222 - 223	Undefined	N/A
224 - 257	Private Use	Private use

RFC-Defined DHCPV6 Option Numbers

Option Number	Name	Description
12	Server Unicast	Hostname string, such as (Server Unicast)
21	SIP Servers Domain Name List	Enables listing of SIP Servers domain names
22	SIP Servers IPv6 Address List	Enables listing of SIP Servers IPv6 Addresses
23	DNS Recursive Name Server	Enables listing of DNS Recursive Name servers
24	Domain Search List	Enables listing of domain names for searching
27	Network Information Service (NIS) Servers	Enables listing of Network Information Service (NIS) servers
28	Network Information Service V2 (NIS+) Servers	Enables listing of Network Information Service V2 (NIS+) servers
29	Network Information Service (NIS) Domain Name	Enables listing of Network Information Service (NIS) domain names
30	Network Information Service V2 (NIS+) Domain Name	Enables listing of Network Information Service V2 (NIS+) domain names
31	Simple Network Time Protocol (SNTP) Servers	Enables listing of Simple Network Time Protocol (SNTP) servers
32	Information Refresh Time	Information refresh time

Editing DHCP Option Objects

Mouse over on the DHCP OptionObject which you want to edit and click **Edit** icon. The Configuration settings are same as the **Add DHCP Option Object** dialog. For more information, see Configuring DHCP Option Objects.

You cannot change the **Name** of the DHCP Option Object.

Deleting DHCP Option Objects

To delete DHCP Option Objects:

1. Navigate to**Object > Profile Objects > DHCP Option** page.
2. Do one of the following:
   - Mouse over on the DHCP Option which you want to delete and click **Delete** icon.
   - Click the checkbox for one or more objects to be deleted and click **Delete** icon at top of the page.

6

AWS

Before setting up AWS objects or groups, be sure to configure the firewall with the AWS credentials that it needs to use. You can configure these in **Network > System > AWS Configuration** page. In addition, the Test Configuration button is available there to validate the settings before proceeding. See *Configuring AWS Credentials* in the *SonicOS System Setup* administration documentation for more information.

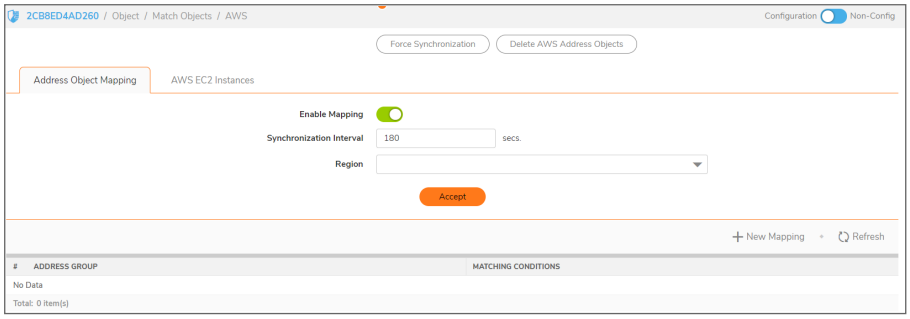
If AWS is not yet configured, the **Object > Profile Objects > AWS** page displays a link to the configuration page. Click on that to open the **Network > System > AWS Configuration** page.

AWS Objects

The **AWS** page is used to map the IP addresses of EC2 Instances running in the AWS Cloud with address objects and address groups configured on the firewall.

New address objects are created for Instance IP addresses, address groups for all addresses of an Instance and those Instance address groups can be added to existing address groups. Those objects, as with any other address objects and address groups, can then be used in firewall policies and features to permit or block access, route traffic and so on.

The **Profile Objects > AWS** page allows a SonicOS administrator to specify sets of EC2 Instance properties. If any of the Instances in one of the monitored regions matches a set of properties, address objects and address groups are created so that, effectively an address group representing the Instance is added to the custom, pre-existing address group specified in the relevant mapping. This address group can be used in firewall policies and, thus, those policies can shape the interaction with EC2 Instances running on AWS.



Topics:

About Address Object Mapping with AWS

EC2 Instances are virtual machines (VMs) running on AWS. Each instance can be one of a number of different available types, depending on the resources required for that instance by the customer. The virtual machine is an instance of a particular Amazon Machine Image (AMI), essentially a template and a specification for VMs that are created from it. All EC2 Instances have a number of properties including:

- Instance type
- AMI used in their creation
- Running state
- ID used for identification
- ID of the Virtual Private Cloud (VPC) where the Instance is located
- A set of user defined tags

You can use any or all of those properties to map matching Instances to address groups that a SonicOS administrator has previously configured on the firewall. Those address groups can be used in Route, VPN and Firewall Policies which can affect how the firewall interacts with AWS hosted machines.

In order to map EC2 Instances to firewall address groups, the Administrator configures any number of mappings between sets of instance properties and pre-existing address groups. If an EC2 Instance, in any of the monitored AWS Regions, matches a set of specified properties, one or more address objects and a single address group are created to represent that Instance and that address group is added to the target address group of the relevant mapping.

EC2 Instances can have multiple private and public IP addresses depending on the number of virtual network interfaces and the use of Elastic IP Addresses. When an Instance matches the properties specified in a mapping, address objects are created for each of its IP addresses, both public and private. Those address objects are then added into one address group which represents the EC2 Instance as a whole. It is that “Instance address group” that is then added to the mapping's target address group, an existing address group used in the configuration of the various firewall policies. Any one EC2 Instance may match the criteria

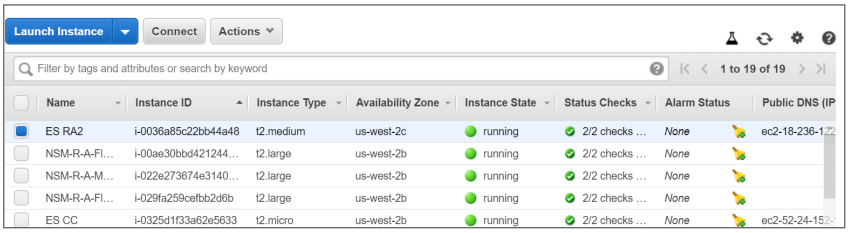
of more than one mapping, in which case the Instance address group is added to more than one target address group. There are no limits.

Tagging an EC2 Instance on AWS

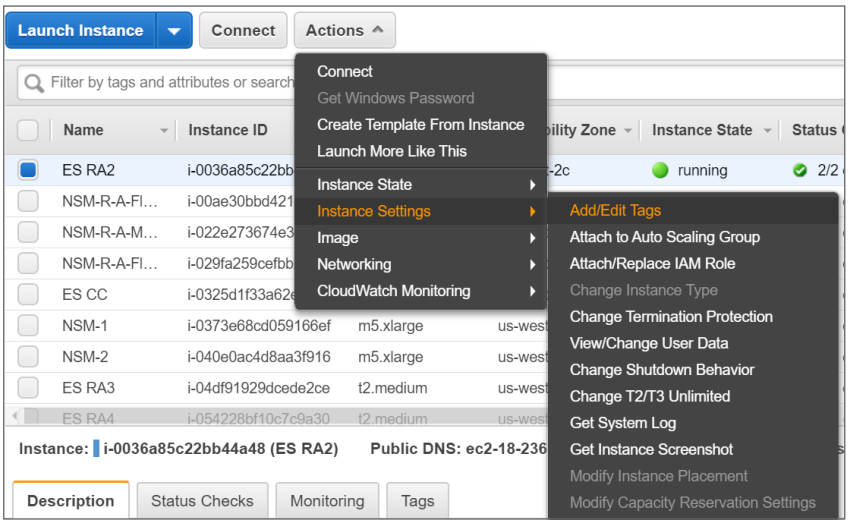
There are multiple ways to tag an EC2 Instance. This section describes how to do so manually.

To manually add a tag to an existing EC2 Instance:

1. On the AWS Console, navigate to the EC2 Dashboard and turn to the Instances page.
2. Select the Instance that you wish to tag by selecting the check box in the first column of the table.

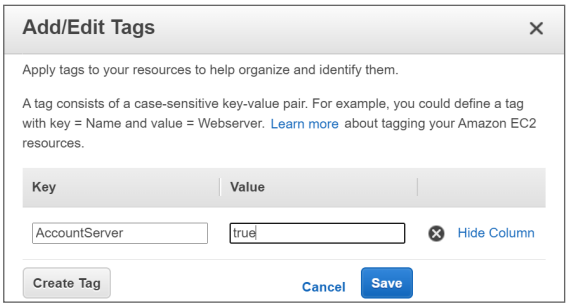


3. With the Instance selected, click on the **Actions** button to launch the popup menu.
4. Select **Instance Settings** and then select **Add/Edit Tags**.

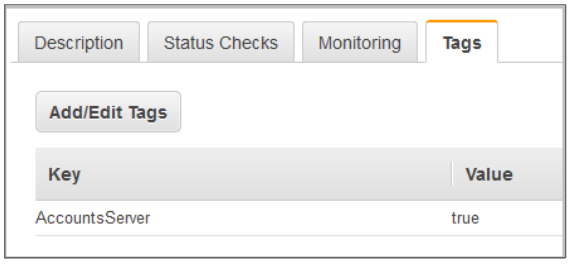


The **Add/Edit** Tags dialog is displayed.

5. In the **Add/Edit** Tags dialog, enter descriptive values in the **Key** and **Value** fields.



6. Click **Save** to tag the Instance with this key and value.
7. Verify the tag on the Instances page under the EC2 Dashboard. With the Instance still selected, view the associated tags by clicking the **Tags** tab in the panel at the bottom of the page. This provides confirmation that the EC2 Instance has been tagged.

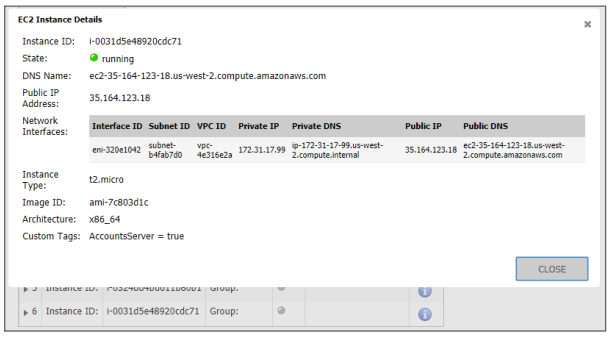


You can now use that tag when defining address object mappings in the SonicOS management interface.

Viewing Instance Properties in SonicOS

The **Profile Objects > AWS** page provides a way to define mappings between sets of EC2 Instance properties and firewall address groups. Address objects and an address group are created for any EC2 Instance that matches the set of specified properties, and the address group is added to the mapping's targeted address group.

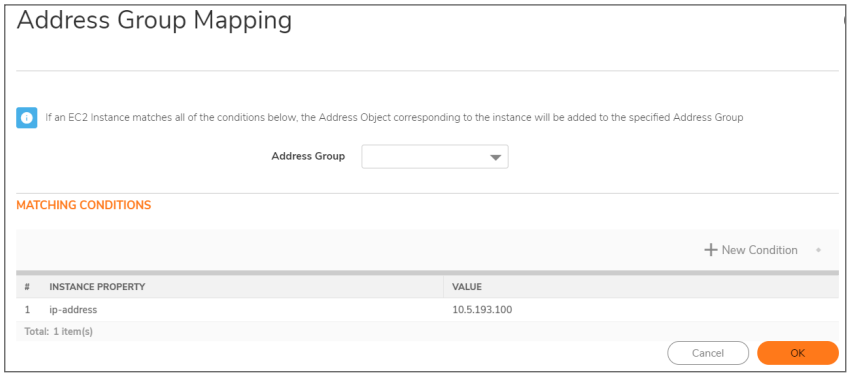
For any EC2 Instance, you can view the values of the different properties that can be used in a mapping by clicking the **Information** button in the row for the Instance. This launches a popup dialog that displays the various properties including the Instance's ID, running state, AMI, type, the VPC ID and the different IP addresses. The user defined or custom tags, and their values, are also listed.



Creating a New Address Object Mapping

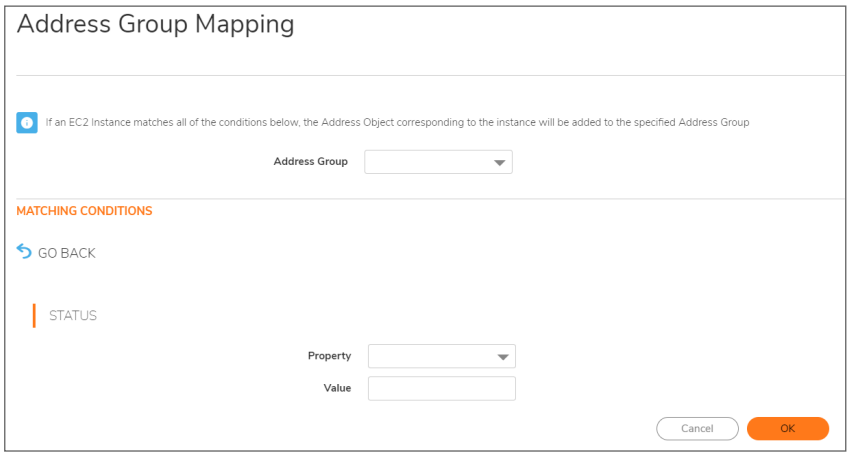
To create a new address object mapping:

1. Navigate to the **Object > Profile Objects > AWS** page.
2. Click the **New Mapping** button. This pops up a dialog enabling you to specify the details of the mapping.



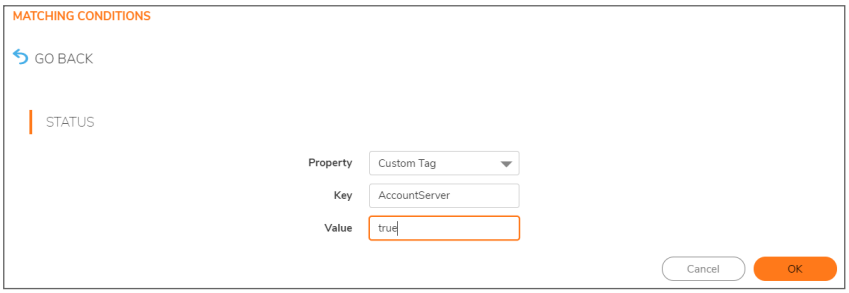
3. In the **Address Group** drop-down list, select the existing address group to which the address groups representing any matched EC2 Instances will be added.

   Only custom address groups are shown in the selection control. If you have added a custom tag to an address group, you can use this custom tag to add a new condition to the mapping.
4. Click the **New Condition** button. The Mapping Condition options are displayed.

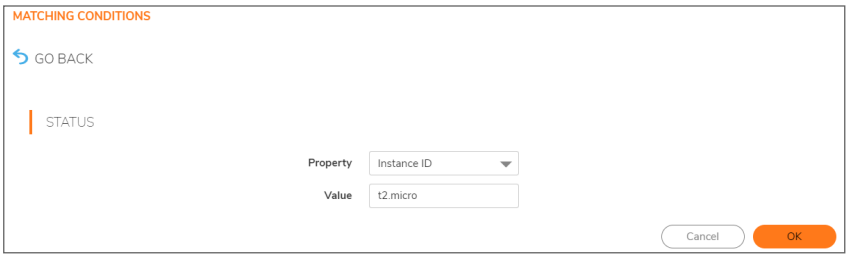


5. Choose the desired property from the **Property** drop-down list. For example, select **Custom Tag**.
6. In the **Key** field, enter the key for the tag.

7. In the **Value** field, enter the value that you wish to match against, such as true.



8. Click **OK**.
9. Back in the **Address Group Mapping** dialog, optionally add another mapping condition by clicking the **New Condition** button again.
10. Select the desired property from the **Property** drop-down list.
11. Fill in the displayed fields as needed.



12. Click **OK**.
13. Back in the **Address Group Mapping** dialog, review the whole mapping condition you are about to create.

    Any EC2 Instance in the regions of interest that match our specified conditions (in this example, having a custom tag of *AccountsServer = true* and of type *t2.micro*) will have address objects created for each of their IP addresses. Those address objects are added to an address group, representing the EC2 Instance as a whole and that address group is added to the address group targeted in the mapping. In this example, that is the address group called *AccountsDeptServers*.
14. Optionally edit or delete particular conditions by clicking on the corresponding button in the **Manage** column of the row.
15. When ready, click **OK**.
16. In the **Object > Profile Objects > AWS** page, click **Accept** to save the mapping.

Enable Mapping

You can create any number of address object mappings, however, they will not take effect until you enable mapping.

To enable mapping:

1. On the **Object > Profile Objects > AWS** page, select the **Enable Mapping** option.
2. Click the **Accept** button.

Configuring Synchronization

The **Synchronization Interval** determines how often the firewall should check for changes and make any necessary updates to the relevant address objects and address groups.

Synchronization is needed because the address object mappings and the AWS regions being monitored can be changed or reconfigured at any time, while the IP addresses and running state of the EC2 instances may be changed on AWS.

To configure the Synchronization Interval:

1. On the **Object > Profile Objects > AWS** page, enter the desired number of seconds into the **Synchronization Interval** field.
2. Click **Accept**.

To force synchronization:

1. On the **Object > Profile Objects > AWS** page, click on either the **Force Synchronization** or the **Delete AWS Address Objects** button.

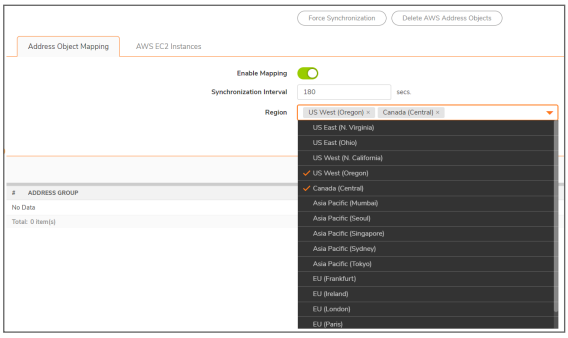
   This is useful if you are aware of changes and in a hurry to see the address objects updated accordingly.
2. Click **Accept**.
3. Click the **Refresh** button so that the page reflects the latest data.

Configuring Regions to Monitor

EC2 Instances are tied to particular AWS Regions. SonicOS only monitors those AWS regions of particular interest. By default, this setting is initialized to the AWS region chosen as the Default Region during AWS Configuration and used if sending firewall logs to AWS CloudWatch Logs. However, it is possible to select multiple regions to monitor and the mappings will be applied across each of those selected.

To select one or more regions to monitor:

1. On the **Object > Profile Objects > AWS** page, click on the **Region** drop-down list and select the checkbox for each region of interest.



2. Click **Accept**.

Verifying AWS Address Objects and Groups

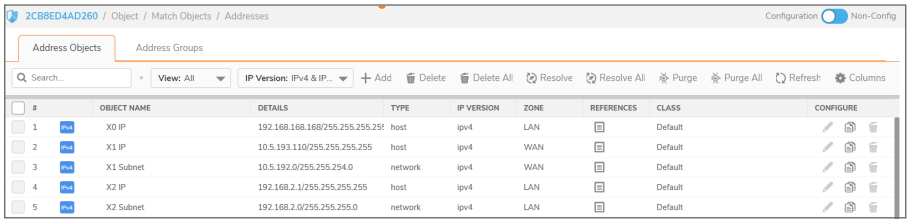
With mappings in place, a **Synchronization Interval** set, **Region** specified and, most importantly, **Mapping** enabled, you can view address objects and address groups representing the matched EC2 Instances and their IP addresses.

For example, on the AWS page itself, the address group and the Mapped address groups are shown in the EC2 Instances table.

Expanding the relevant row reveals the address objects corresponding to an Instance's public and private IP addresses.

Navigating to the **Object > Match Objects > Addresses** page in SonicOS and viewing the Address Object screen shows those same host address objects. VPN is used for the zone of private IP addresses and WAN is used for a public address zone.

A naming convention is used for the Instance address group and the address objects for each of the IP addresses, based on the Instance ID and, for the address objects, a suffix depending on whether the address is public or private.



Viewing the **Address Groups** screen and expanding the rows of interest shows that the original *AccountsDeptServers* address group now has an address group, representing an EC2 Instance, as a member.

The EC2 Instance address group itself contains the address objects that were created for each of its IP addresses.

7

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

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

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.

SonicOS Profile Objects Administration Guide
Updated - February 2021
Software Version - 7
232-005342-10 Rev B

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