

USG SecuExtender (Windows)

The USG automatically loads the USG SecuExtender for Windows client program to your computer after a successful login to an SSL VPN tunnel with network extension support enabled.

Note: For information on using the USG SecuExtender for Mac client program, please see its User's Guide at the download library on the ZyXEL website.

The USG SecuExtender (Windows) lets you:

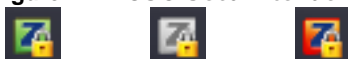
- Access servers, remote desktops and manage files as if you were on the local network.
- Use applications like e-mail, file transfer, and remote desktop programs directly without using a browser. For example, you can use Outlook for e-mail instead of the USG's web-based e-mail.
- Use applications, even proprietary applications, for which the USG does not offer SSL application objects.

The applications must be installed on your computer. For example, to use the VNC remote desktop program, you must have the VNC client installed on your computer.

24.1 The USG SecuExtender Icon

The USG SecuExtender icon color indicates the SSL VPN tunnel's connection status.

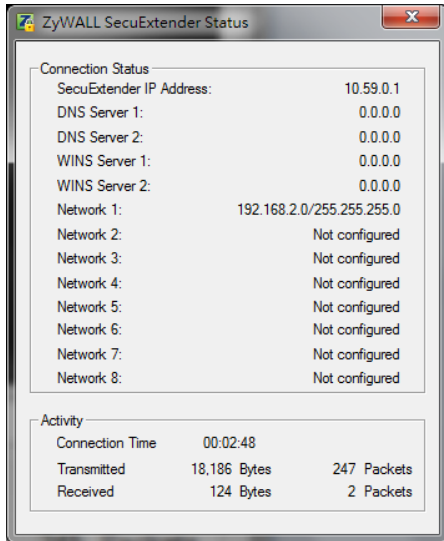
Figure 271 USG SecuExtender Icon



- Green: the SSL VPN tunnel is connected. You can connect to the SSL application and network resources. You can also use another application to access resources behind the USG.
- Gray: the SSL VPN tunnel's connection is suspended. This means the SSL VPN tunnel is connected, but the USG SecuExtender will not send any traffic through it until you right-click the icon and resume the connection.
- Red: the SSL VPN tunnel is not connected. You cannot connect to the SSL application and network resources.

24.2 Status

Right-click the USG SecuExtender icon in the system tray and select **Status** to open the **Status** screen. Use this screen to view the USG SecuExtender's connection status and activity statistics.

Figure 272 USG SecuExtender Status

The following table describes the labels in this screen.

Table 149 USG SecuExtender Status

LABEL	DESCRIPTION
Connection Status	
SecuExtender IP Address	This is the IP address the USG assigned to this remote user computer for an SSL VPN connection.
DNS Server 1/2	These are the IP addresses of the DNS server and backup DNS server for the SSL VPN connection. DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. Your computer uses the DNS server specified here to resolve domain names for resources you access through the SSL VPN connection.
WINS Server 1/2	These are the IP addresses of the WINS (Windows Internet Naming Service) and backup WINS servers for the SSL VPN connection. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.
Network 1~8	These are the networks (including netmask) that you can access through the SSL VPN connection.
Activity	
Connected Time	This is how long the computer has been connected to the SSL VPN tunnel.
Transmitted	This is how many bytes and packets the computer has sent through the SSL VPN connection.
Received	This is how many bytes and packets the computer has received through the SSL VPN connection.

24.3 View Log

If you have problems with the USG SecuExtender, customer support may request you to provide information from the log. Right-click the USG SecuExtender icon in the system tray and select **Log** to open a notepad file of the USG SecuExtender's log.

Figure 273 USG SecuExtender Log Example

```
#####
#####
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] Build Datetime: Feb 24 2009/
10:25:07
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG] rasphone.pbk: C:\Documents and
Settings\11746\rasphone.pbk
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG] SecuExtender.log:
C:\Documents and Settings\11746\SecuExtender.log
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] Check Parameters
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] Connect to 172.23.31.19:443/
10444
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] Parameter is OK
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] Checking System status...
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] Checking service (first) ...
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] SecuExtender Helper is running
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] System is OK
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG] Connect to 2887196435/443
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] Handshake LoopCounter: 0
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL] 611 bytes of handshake data
received
```

24.4 Suspend and Resume the Connection

When the USG SecuExtender icon in the system tray is green, you can right-click the icon and select **Suspend Connection** to keep the SSL VPN tunnel connected but not send any traffic through it until you right-click the icon and resume the connection.

24.5 Stop the Connection

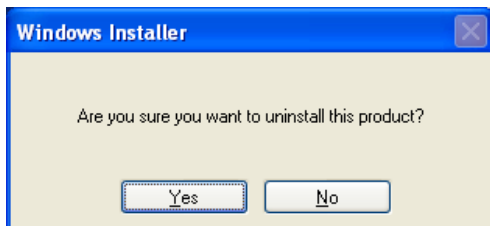
Right-click the icon and select **Stop Connection** to disconnect the SSL VPN tunnel.

24.6 Uninstalling the USG SecuExtender

Do the following if you need to remove the USG SecuExtender.

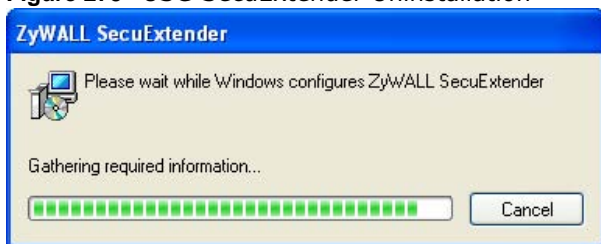
- 1 Click **start > All Programs > ZyXEL > USG SecuExtender > Uninstall ZyWALL SecuExtender**.
- 2 In the confirmation screen, click **Yes**.

Figure 274 Uninstalling the USG SecuExtender Confirmation



- 3 Windows uninstalls the USG SecuExtender.

Figure 275 USG SecuExtender Uninstallation

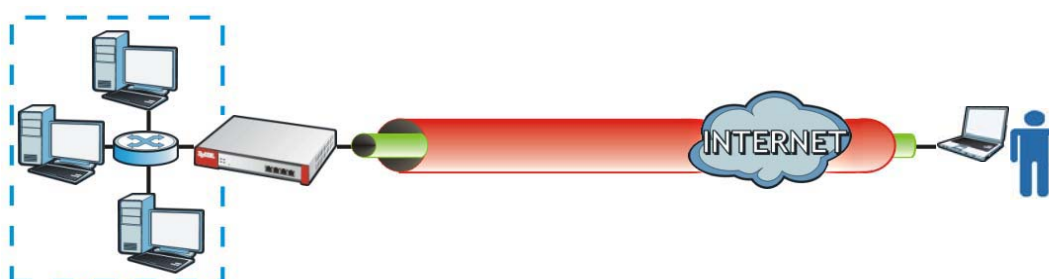


L2TP VPN

25.1 Overview

L2TP VPN uses the L2TP and IPsec client software included in remote users' Android, iOS, Windows or Mac OS X operating systems for secure connections to the network behind the USG. The remote users do not need their own IPsec gateways or third-party VPN client software.

Figure 276 L2TP VPN Overview



25.1.1 What You Can Do in this Chapter

- Use the **L2TP VPN** screen (see [Section 25.2 on page 396](#)) to configure the USG's L2TP VPN settings.
- Use the **VPN Setup Wizard** screen in **Quick Setup** ([Chapter 4 on page 49](#)) to configure the USG's L2TP VPN settings.

25.1.2 What You Need to Know

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPsec VPN tunnel is established first and then an L2TP tunnel is built inside it. See [Chapter 21 on page 332](#) for information on IPsec VPN.

IPsec Configuration Required for L2TP VPN

You must configure an IPsec VPN connection prior to proper L2TP VPN usage (see [Chapter 25 on page 395](#) for details). The IPsec VPN connection must:

- Be enabled.
- Use transport mode.
- Use **Pre-Shared Key** authentication.
- Use a VPN gateway with the **Secure Gateway** set to **0.0.0.0** if you need to allow L2TP VPN clients to connect from more than one IP address.

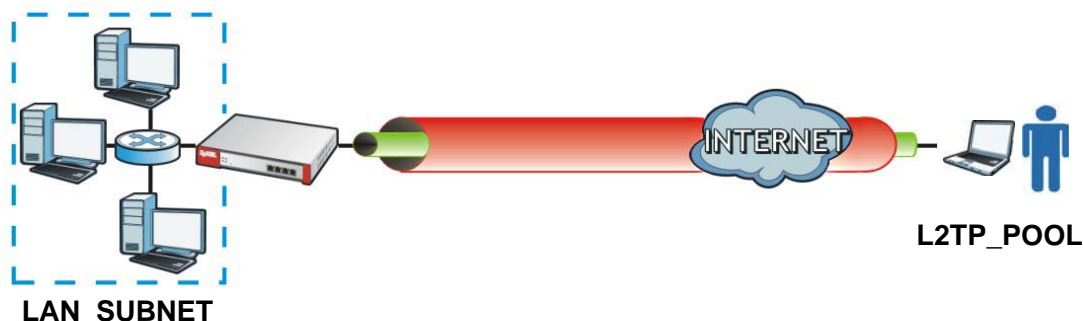
Using the Quick Setup VPN Setup Wizard

The **VPN Setup Wizard** is an easy and convenient way to configure the L2TP VPN settings. Click **Configuration > Quick Setup > VPN Setup > VPN Settings for L2TP VPN Settings** to get started.

Policy Route

The Policy Route for return traffic (from LAN to L2TP clients) is automatically created when USG adds a new L2TP connection, allowing users access the resources on a network without additional configuration. However, if some of the traffic from the L2TP clients needs to go to the Internet, you will need to create a policy route to send that traffic from the L2TP tunnels out through a WAN trunk. This task can be easily performed by clicking the Allow L2TP traffic through WAN checkbox at **Quick Setup > VPN Setup > Allow L2TP traffic through WAN**.

Figure 277 Policy Route for L2TP VPN



25.2 L2TP VPN Screen

Click **Configuration > VPN > L2TP VPN** to open the following screen. Use this screen to configure the USG's L2TP VPN settings.

Note: Disconnect any existing L2TP VPN sessions before modifying L2TP VPN settings. The remote users must make any needed matching configuration changes and re-establish the sessions using the new settings.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting, and other information.

Figure 278 Configuration > VPN > L2TP VPN

The following table describes the fields in this screen.

Table 150 Configuration > VPN > L2TP VPN

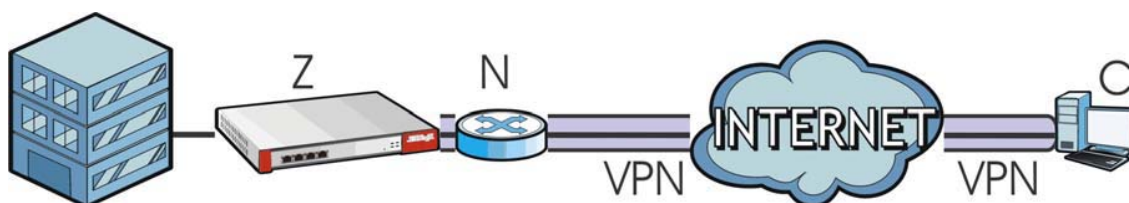
LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Enable L2TP Over IPSec	Use this field to turn the USG's L2TP VPN function on or off.
VPN Connection	Select the IPSec VPN connection the USG uses for L2TP VPN. All of the configured VPN connections display here, but the one you use must meet the requirements listed in IPSec Configuration Required for L2TP VPN on page 395 . Note: Modifying this VPN connection (or the VPN gateway that it uses) disconnects any existing L2TP VPN sessions.
IP Address Pool	Select the pool of IP addresses that the USG uses to assign to the L2TP VPN clients. Use Create new Object if you need to configure a new pool of IP addresses. This should not conflict with any WAN, LAN, DMZ or WLAN subnet even if they are not in use.
Authentication Method	Select how the USG authenticates a remote user before allowing access to the L2TP VPN tunnel. The authentication method has the USG check a user's user name and password against the USG's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these.
Authentication Server Certificate	Select the certificate to use to identify the USG for L2TP VPN connections. You must have certificates already configured in the My Certificates screen. The certificate is used with the EAP, PEAP, and MSCHAPv2 authentication protocols.

Table 150 Configuration > VPN > L2TP VPN (continued)

LABEL	DESCRIPTION
Allowed User	The remote user must log into the USG to use the L2TP VPN tunnel. Select a user or user group that can use the L2TP VPN tunnel. Use Create new Object if you need to configure a new user account. Otherwise, select any to allow any user with a valid account and password on the USG to log in.
Keep Alive Timer	The USG sends a Hello message after waiting this long without receiving any traffic from the remote user. The USG disconnects the VPN tunnel if the remote user does not respond.
First DNS Server, Second DNS Server	Specify the IP addresses of DNS servers to assign to the remote users. You can specify these IP addresses two ways. Custom Defined - enter a static IP address. From ISP - use the IP address of a DNS server that another interface received from its DHCP server.
First WINS Server, Second WINS Server	The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. Type the IP addresses of up to two WINS servers to assign to the remote users. You can specify these IP addresses two ways.
Apply	Click Apply to save your changes in the USG.
Reset	Click Reset to return the screen to its last-saved settings.

25.2.1 Example: L2TP and USG Behind a NAT Router

If the USG (Z) is behind a NAT router (N), then do the following for remote clients (C) to access the network behind the USG (Z) using L2TP over IPv4.



- 1 Create an address object in **Configuration > Object > Address** for the WAN IP address of the NAT router.



- 2 Go to **Configuration > VPN > IPsec VPN > VPN Connection** and click **Add** for **IPv4 Configuration** to create a new VPN connection.
- 3 Select **Remote Access (Server Role)** as the VPN scenario for the remote client.

- 4 Select the NAT router WAN IP address object as the **Local Policy**.

The screenshot shows the configuration page for an L2TP VPN connection. The 'General Settings' section has the 'Enable' checkbox checked and the 'Connection Name' set to 'L2TP-IPSec-NAT'. The 'VPN Gateway' section has 'Remote Access (Server Role)' selected. The 'Policy' section has 'NATrouterIP' selected for the local policy. The 'Phase 2 Setting' section has 'SA Life Time' set to 86400 seconds.

- 5 Go to **Configuration > VPN > L2TP VPN** and select the **VPN Connection** just configured.

The screenshot shows the configuration page for the L2TP VPN connection. The 'General Settings' section has the 'Enable L2TP Over IPSec' checkbox checked. The 'VPN Connection' is set to 'L2TP-IPSec-NAT'. The 'IP Address Pool' is set to 'LAN1_SUBNET'. The 'Authentication Method' is set to 'default'. The 'Allowed User' is set to 'any'. The 'Keep Alive Timer' is set to 60 seconds. The 'First DNS Server (Optional)' and 'Second DNS Server (Optional)' are both set to 'Custom Defined'. The 'First WINS Server (Optional)' and 'Second WINS Server (Optional)' are both empty. The 'Apply' button is highlighted.

BWM (Bandwidth Management)

26.1 Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

26.1.1 What You Can Do in this Chapter

Use the **BWM** screens (see [Section 26.2 on page 404](#)) to control bandwidth for services passing through the USG, and to identify the conditions that define the bandwidth control.

26.1.2 What You Need to Know

When you allow a service, you can restrict the bandwidth it uses. It controls TCP and UDP traffic. Use policy routes to manage other types of traffic (like ICMP).

Note: Bandwidth management in policy routes has priority over TCP and UDP traffic policies.

If you want to use a service, make sure both the security policy allow the service's packets to go through the USG.

Note: The USG checks security policies before it checks bandwidth management rules for traffic going through the USG.

Bandwidth management examines every TCP and UDP connection passing through the USG. Then, you can specify, by port, whether or not the USG continues to route the connection.

BWM Type

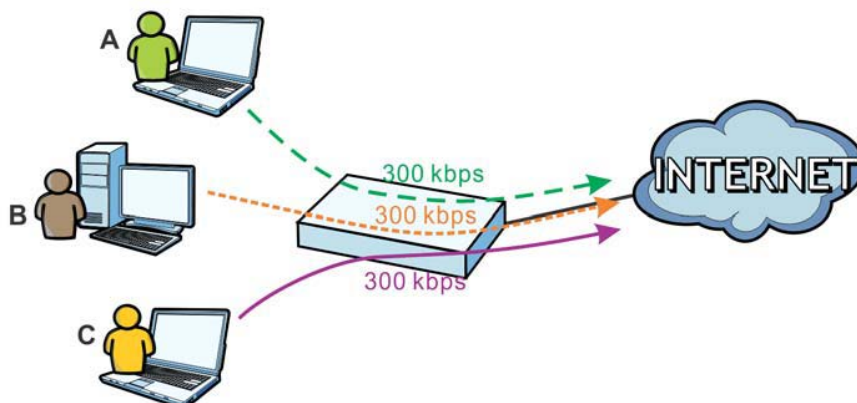
The USG supports three types of bandwidth management: **Shared**, **Per user** and **Per-Source-IP**.

The **Shared** BWM type is selected by default in a bandwidth management rule. All matched traffic shares the bandwidth configured in the rule.

If the BWM type is set to **Per user** in a rule, each user that matches the rule can use up to the configured bandwidth by his/her own.

Select the **Per-Source-IP** type when you want to set the maximum bandwidth for traffic from an individual source IP address.

In the following example, you configure a **Per user** bandwidth management rule for radius-users to limit outgoing traffic to 300 kbs. Then all radius-users (**A**, **B** and **C**) can send 300 kbps of traffic.



DiffServ and DSCP Marking

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

Connection and Packet Directions

Bandwidth management looks at the connection direction, that is, from which interface the connection was initiated and to which interface the connection is going.

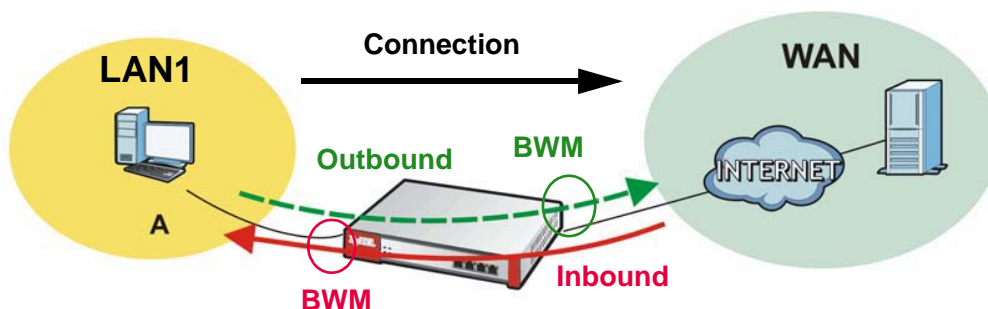
A connection has outbound and inbound packet flows. The USG controls the bandwidth of traffic of each flow as it is going out through an interface or VPN tunnel.

- The outbound traffic flows from the connection initiator to the connection responder.
- The inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.

- Outbound traffic goes from a LAN1 device to a WAN device. Bandwidth management is applied before sending the packets out a WAN interface on the USG.
- Inbound traffic comes back from the WAN device to the LAN1 device. Bandwidth management is applied before sending the traffic out a LAN1 interface.

Figure 279 LAN1 to WAN Connection and Packet Directions

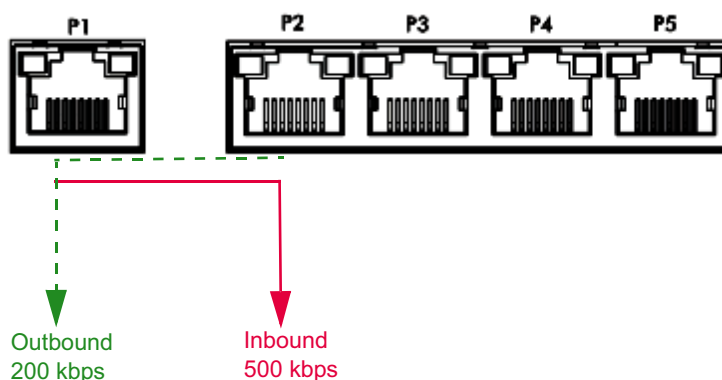


Outbound and Inbound Bandwidth Limits

You can limit an application's outbound or inbound bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to outbound or inbound traffic, each member of the out-going zone can send up to the limit. Take a LAN1 to WAN policy for example.

- Outbound traffic is limited to 200 kbps. The connection initiator is on the LAN1 so outbound means the traffic traveling from the LAN1 to the WAN. Each of the WAN zone's two interfaces can send the limit of 200 kbps of traffic.
- Inbound traffic is limited to 500 kbps. The connection initiator is on the LAN1 so inbound means the traffic traveling from the WAN to the LAN1.

Figure 280 LAN1 to WAN, Outbound 200 kbps, Inbound 500 kbps



Bandwidth Management Priority

- The USG gives bandwidth to higher-priority traffic first, until it reaches its configured bandwidth rate.
- Then lower-priority traffic gets bandwidth.
- The USG uses a fairness-based (round-robin) scheduler to divide bandwidth among traffic flows with the same priority.
- The USG automatically treats traffic with bandwidth management disabled as priority 7 (the lowest priority).

Maximize Bandwidth Usage

Maximize bandwidth usage allows applications with maximize bandwidth usage enabled to “borrow” any unused bandwidth on the out-going interface.

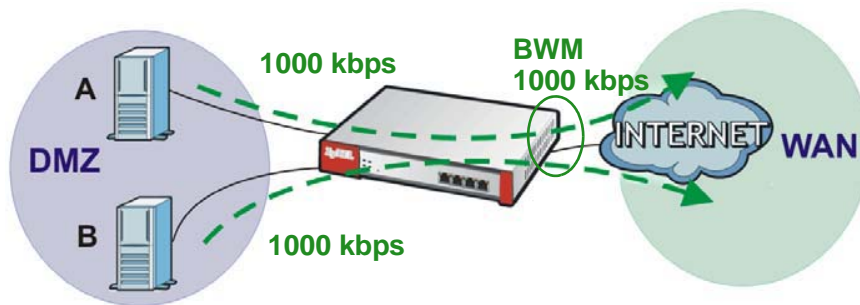
After each application gets its configured bandwidth rate, the USG uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

Unused bandwidth is divided equally. Higher priority traffic does not get a larger portion of the unused bandwidth.

Bandwidth Management Behavior

The following sections show how bandwidth management behaves with various settings. For example, you configure DMZ to WAN policies for FTP servers **A** and **B**. Each server tries to send 1000 kbps, but the WAN is set to a maximum outgoing speed of 1000 kbps. You configure policy A for server **A**'s traffic and policy B for server **B**'s traffic.

Figure 281 Bandwidth Management Behavior



Configured Rate Effect

In the following table the configured rates total less than the available bandwidth and maximize bandwidth usage is disabled, both servers get their configured rate.

Table 151 Configured Rate Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	No	1	300 kbps
B	200 kbps	No	1	200 kbps

Priority Effect

Here the configured rates total more than the available bandwidth. Because server **A** has higher priority, it gets up to its configured rate (800 kbps), leaving only 200 kbps for server **B**.

Table 152 Priority Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	800 kbps	Yes	1	800 kbps
B	1000 kbps	Yes	2	200 kbps

Maximize Bandwidth Usage Effect

With maximize bandwidth usage enabled, after each server gets its configured rate, the rest of the available bandwidth is divided equally between the two. So server **A** gets its configured rate of 300 kbps and server **B** gets its configured rate of 200 kbps. Then the USG divides the remaining bandwidth ($1000 - 500 = 500$) equally between the two ($500 / 2 = 250$ kbps for each). The priority has no effect on how much of the unused bandwidth each server gets.

So server **A** gets its configured rate of 300 kbps plus 250 kbps for a total of 550 kbps. Server **B** gets its configured rate of 200 kbps plus 250 kbps for a total of 450 kbps.

Table 153 Maximize Bandwidth Usage Effect

POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	300 kbps	Yes	1	550 kbps
B	200 kbps	Yes	2	450 kbps

Priority and Over Allotment of Bandwidth Effect

Server **A** has a configured rate that equals the total amount of available bandwidth and a higher priority. You should regard extreme over allotment of traffic with different priorities (as shown here) as a configuration error. Even though the USG still attempts to let all traffic get through and not be lost, regardless of its priority, server **B** gets almost no bandwidth with this configuration.

Table 154 Priority and Over Allotment of Bandwidth Effect

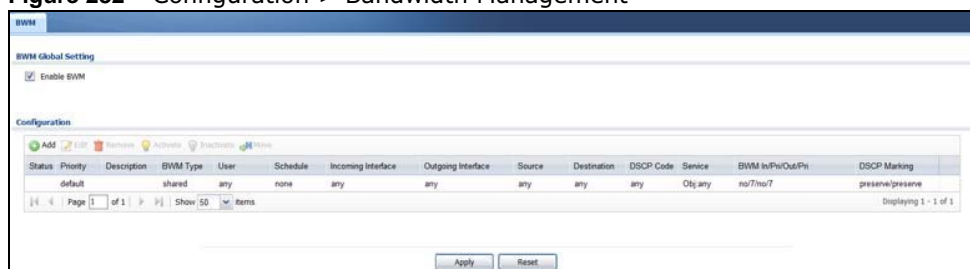
POLICY	CONFIGURED RATE	MAX. B. U.	PRIORITY	ACTUAL RATE
A	1000 kbps	Yes	1	999 kbps
B	1000 kbps	Yes	2	1 kbps

26.2 The Bandwidth Management Screen

The Bandwidth management screens control the bandwidth allocation for TCP and UDP traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions, similar to the sequence of rules used by firewalls, to specify how the USG handles the DSCP value and allocate bandwidth for the matching packets.

Click **Configuration > BWM** to open the following screen. This screen allows you to enable/disable bandwidth management and add, edit, and remove user-defined bandwidth management policies.

The default bandwidth management policy is the one with the priority of "default". It is the last policy the USG checks if traffic does not match any other bandwidth management policies you have configured. You cannot remove, activate, deactivate or move the default bandwidth management policy.

Figure 282 Configuration > Bandwidth Management

The following table describes the labels in this screen. See [Section 26.2.1 on page 406](#) for more information as well.

Table 155 Configuration > Bandwidth Management

LABEL	DESCRIPTION
Enable BWM	Select this check box to activate management bandwidth.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Move	To change an entry's position in the numbered list, select it and click Move to display a field to type a number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed.
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive. The status icon is not available for the default bandwidth management policy.
Priority	This field displays a sequential value for each bandwidth management policy and it is not associated with a specific setting. This field displays default for the default bandwidth management policy.
Description	This field displays additional information about this policy.
BWM Type	This field displays the below types of BWM: <ul style="list-style-type: none"> • Shared, when the policy is set for all matched traffic • Per User, when the policy is set for an individual user or a user group • Per-Source-IP, when the policy is set for a source IP
User	This is the type of user account to which the policy applies. If any displays, the policy applies to all user accounts.
Schedule	This is the schedule that defines when the policy applies. none means the policy always applies.
Incoming Interface	This is the source interface of the traffic to which this policy applies.
Outgoing Interface	This is the destination interface of the traffic to which this policy applies.
Source	This is the source address or address group for whom this policy applies. If any displays, the policy is effective for every source.
Destination	This is the destination address or address group for whom this policy applies. If any displays, the policy is effective for every destination.

Table 155 Configuration > Bandwidth Management

LABEL	DESCRIPTION
DSCP Code	<p>These are the DSCP code point values of incoming and outgoing packets to which this policy applies. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment.</p> <p>any means all DSCP value or no DSCP marker.</p> <p>default means traffic with a DSCP value of 0. This is usually best effort traffic</p> <p>The "af" options stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences.</p>
Service Type	<p>App and the service name displays if you selected Application Object for the service type. An Application Object is a pre-defined service.</p> <p>Obj and the service name displays if you selected Service Object for the service type. A Service Object is a customized pre-defined service or another service. Mouse over the service object name to view the corresponding IP protocol number.</p>
BWM In/Pri/Out/Pri	<p>This field shows the amount of bandwidth the traffic can use.</p> <p>In - This is how much inbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Inbound refers to the traffic the USG sends to a connection's initiator. If no displays here, this policy does not apply bandwidth management for the inbound traffic.</p> <p>Out - This is how much outgoing bandwidth, in kilobits per second, this policy allows the matching traffic to use. Outbound refers to the traffic the USG sends out from a connection's initiator. If no displays here, this policy does not apply bandwidth management for the outbound traffic.</p> <p>Pri - This is the priority for the incoming (the first Pri value) or outgoing (the second Pri value) traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The USG ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.</p>
DSCP Marking	<p>This is how the USG handles the DSCP value of the incoming and outgoing packets that match this policy.</p> <p>In - Inbound, the traffic the USG sends to a connection's initiator.</p> <p>Out - Outbound, the traffic the USG sends out from a connection's initiator.</p> <p>If this field displays a DSCP value, the USG applies that DSCP value to the route's outgoing packets.</p> <p>preserve means the USG does not modify the DSCP value of the route's outgoing packets.</p> <p>default means the USG sets the DSCP value of the route's outgoing packets to 0.</p> <p>The "af" choices stand for Assured Forwarding. The number following the "af" identifies one of four classes and one of three drop preferences.</p>
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

26.2.1 The Bandwidth Management Add/Edit Screen

The **Configuration > Bandwidth Management Add/Edit** screen allows you to create a new condition or edit an existing one.

802.1P Marking

Use 802.1P to prioritize outgoing traffic from a VLAN interface. The **Priority Code** is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest.

Table 156 Single Tagged 802.1Q Frame Format

			DA	SA	TPID	Priority	VID	Len/Etype	Data	FCS	IEEE 802.1Q customer tagged frame
--	--	--	----	----	------	----------	-----	-----------	------	-----	-----------------------------------

Table 157 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/Etype	Length and type of Ethernet frame
TPID	Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

The following table is a guide to types of traffic for the priority code.

Table 158 Priority Code and Types of Traffic

PRIORITY	TRAFFIC TYPES
0 (lowest)	Background
1	Best Effort
2	Excellent Effort
3	Critical Applications
4	Video, less than 100 ms latency and jitter
5	Voice, less than 10 ms latency and jitter
6	Internetnetwork Control
7 (highest)	Network Control

To access this screen, go to the **Configuration > Bandwidth Management** screen (see [Section 26.2 on page 404](#)), and click either the **Add** icon or an **Edit** icon.

Figure 283 Configuration > Bandwidth Management > Edit (For the Default Policy)

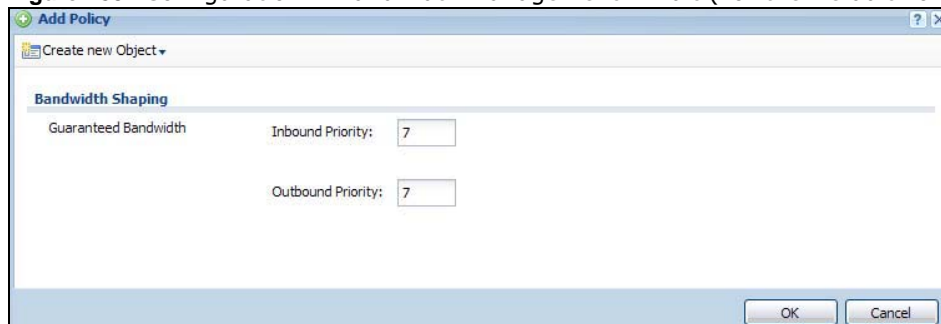


Figure 284 Configuration > Bandwidth Management > Add/Edit

The following table describes the labels in this screen.

Table 159 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
Create new Object	Use to configure any new settings objects that you need to use in this screen.
Configuration	
Enable	Select this check box to turn on this policy.
Description	Enter a description of this policy. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
Criteria	Use this section to configure the conditions of traffic to which this policy applies.

Table 159 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
BWM Type	This field displays the below types of BWM rule: <ul style="list-style-type: none"> • Shared, when the policy is set for all users • Per User, when the policy is set for an individual user or a user group • Per Source IP, when the policy is set for a source IP
User	Select a user name or user group to which to apply the policy. Use Create new Object if you need to configure a new user account. Select any to apply the policy for every user.
Schedule	Select a schedule that defines when the policy applies or select Create Object to configure a new one. Otherwise, select none to make the policy always effective.
Incoming Interface	Select the source interface of the traffic to which this policy applies.
Outgoing Interface	Select the destination interface of the traffic to which this policy applies.
Source	Select a source address or address group for whom this policy applies. Use Create new Object if you need to configure a new one. Select any if the policy is effective for every source.
Destination	Select a destination address or address group for whom this policy applies. Use Create new Object if you need to configure a new one. Select any if the policy is effective for every destination.
DSCP Code	Select a DSCP code point value of incoming packets to which this policy route applies or select User Defined to specify another DSCP code point. The lower the number the higher the priority with the exception of 0 which is usually given only best-effort treatment. any means all DSCP value or no DSCP marker. default means traffic with a DSCP value of 0. This is usually best effort traffic The " af " choices stand for Assured Forwarding. The number following the " af " identifies one of four classes and one of three drop preferences.
User-Defined DSCP Code	Use this field to specify a custom DSCP code point.
Service Type	Select Service Object if you want a specific service (defined in a service object) to which the policy applies.
Service Object	This field is available if you selected Service Object as the service type. Select a service or service group to identify the type of traffic to which this policy applies. any means all services.
DSCP Marking	Set how the USG handles the DSCP value of the incoming and outgoing packets that match this policy. Inbound refers to the traffic the USG sends to a connection's initiator. Outbound refers to the traffic the USG sends out from a connection's initiator. Select one of the pre-defined DSCP values to apply or select User Defined to specify another DSCP value. The " af " choices stand for Assured Forwarding. The number following the " af " identifies one of four classes and one of three drop preferences. Select preserve to have the USG keep the packets' original DSCP value. Select default to have the USG set the DSCP value of the packets to 0.
Bandwidth Shaping	Configure these fields to set the amount of bandwidth the matching traffic can use.

Table 159 Configuration > Bandwidth Management > Add/Edit

LABEL	DESCRIPTION
Inbound kbps	<p>Type how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use. Inbound refers to the traffic the USG sends to a connection's initiator.</p> <p>If you enter 0 here, this policy does not apply bandwidth management for the matching traffic that the USG sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7).</p> <p>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.</p>
Outbound kbps	<p>Type how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use. Outbound refers to the traffic the USG sends out from a connection's initiator.</p> <p>If you enter 0 here, this policy does not apply bandwidth management for the matching traffic that the USG sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7).</p> <p>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.</p>
Priority	<p>This field displays when the inbound or outbound bandwidth management is not set to 0. Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority.</p> <p>Traffic with a higher priority is given bandwidth before traffic with a lower priority.</p> <p>The USG uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority.</p> <p>The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration.</p>
Maximize Bandwidth Usage	<p>This field displays when the inbound or outbound bandwidth management is not set to 0 and the BWM Type is set to Shared. Enable maximize bandwidth usage to let the traffic matching this policy "borrow" all unused bandwidth on the out-going interface.</p> <p>After each application or type of traffic gets its configured bandwidth rate, the USG uses the fairness-based scheduler to divide any unused bandwidth on the out-going interface among applications and traffic types that need more bandwidth and have maximize bandwidth usage enabled.</p>
Maximum	<p>If you did not enable Maximize Bandwidth Usage, then type the maximum unused bandwidth that traffic matching this policy is allowed to "borrow" on the out-going interface (in Kbps), here.</p>
802.1P Marking	<p>Use 802.1P to prioritize outgoing traffic from a VLAN interface.</p>
Priority Code	<p>This is a 3-bit field within a 802.1Q VLAN tag that's used to prioritize associated outgoing VLAN traffic. "0" is the lowest priority level and "7" is the highest. See Table 158 on page 407. The setting configured here overwrites existing priority settings.</p>
Interface	<p>Choose a VLAN interface to which to apply the priority level for matching frames.</p>
Related Setting	
Log	<p>Select whether to have the USG generate a log (log), log and alert (log alert) or neither (no) when any traffic matches this policy.</p>
OK	<p>Click OK to save your changes back to the USG.</p>
Cancel	<p>Click Cancel to exit this screen without saving your changes.</p>

26.2.1.1 Adding Objects for the BWM Policy

Objects are parameters to which the Policy rules are built upon. There are three kinds of objects you can add/edit for the BWM policy, they are **User**, **Schedule** and **Address** objects. Click **Configuration > BWM > Add > Create New Object > Add User** to see the following screen.

Figure 285 Configuration >BWM > Create New Object > Add User

The screenshot shows the 'Add Policy' configuration window with the 'Add A User' sub-window open. The main window is titled 'Add Policy' and has a 'Create new Object' dropdown. The 'Configuration' section includes 'Enable' (checked), 'Description', and 'BWM Type' (Shared). The 'Criteria' section includes 'User' (any), 'Schedule' (none), 'Incoming Interface' (any), 'Outgoing Interface' (any), 'Source' (any), 'Destination' (any), 'DSCP Code' (any), 'Service Type' (Service Object), and 'Service Object' (any). The 'DSCP Marking' section includes 'Inbound Marking' (preserve) and 'Outbound Marking' (preserve). The 'Bandwidth Shaping' section includes 'Guaranteed Bandwidth' (Inbound: 0 kbps, Priority: 4) and 'Outbound' (0 kbps, Priority: 4). The '802.1P Marking' section includes 'Priority Code' (0) and 'Interface' (none). The 'Related Setting' section includes 'Log' (no). The 'Add A User' sub-window shows 'User Configuration' with fields for 'User Name', 'User Type' (user), 'Password', 'Rtype', 'Description', and 'Authentication Timeout Settings' (Lease Time: 1440 minutes, Reauthentication Time: 1440 minutes).

The following table describes the fields in the above screen.

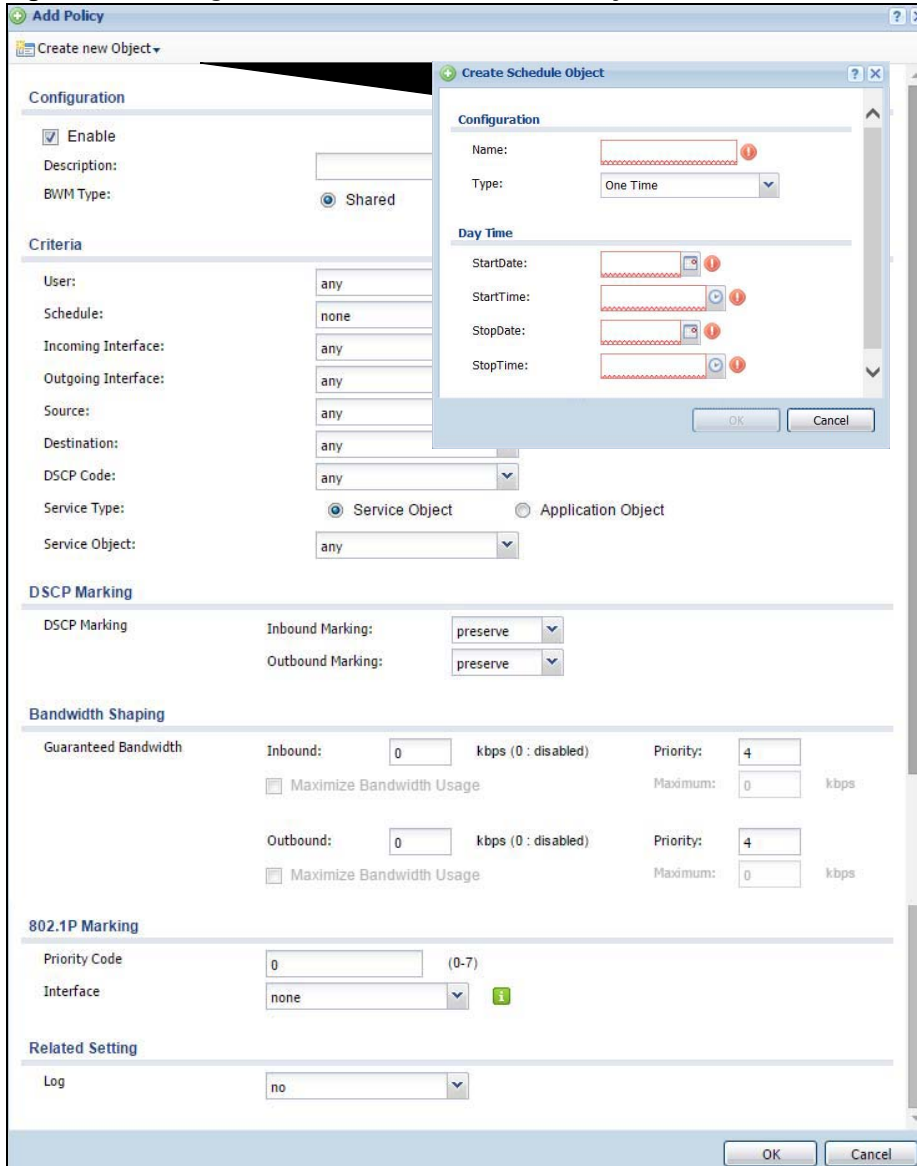
Table 160 Configuration > BWM > Create New Object > Add User

LABEL	DESCRIPTION
User Name	Type a user or user group object name of the rule.
User Type	Select a user type from the drop down menu. The user types are Admin, Limited admin, User, Guest, Ext-user, Ext-group-user.

Table 160 Configuration > BWM > Create New Object > Add User

LABEL	DESCRIPTION
Password	Type a password for the user object. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= ;: .! @\$&%#~ ` \ ()), and it can be up to eight characters long.
Retype	Retype the password to confirm.
Description	Enter a description for this user object. It is not used elsewhere. You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
Authentication Timeout Settings	Choose either Use Default setting option, which shows the default Lease Time of 1,440 minutes and Reauthentication Time of 1,440 minutes or you can enter them manually by choosing Use Manual Settings option.
Lease Time	This shows the Lease Time setting for the user, by default it is 1,440 minutes.
Reauthentication Time	This shows the Reauthentication Time for the user, by default it is 1,440 minutes.
OK	Click OK to save the setting.
Cancel	Click Cancel to abandon this screen.

Figure 286 Configuration > BWM > Create New Object > Add Schedule



The following table describes the fields in the above screen.

Table 161 Configuration > BWM > Create New Object > Add Schedule

LABEL	DESCRIPTION
Name	Enter a name for the schedule object of the rule.
Type	Select an option from the drop down menu for the schedule object. It will show One Time or Recurring .
Start Date	Click the icon menu on the right to choose a Start Date for the schedule object.
Start Time	Click the icon menu on the right to choose a Start Time for the schedule object.
Stop Date	Click the icon menu on the right to choose a Stop Date for schedule object.
Stop Time	Click the icon menu on the right to choose a Stop Time for the schedule object.

Figure 287 Configuration > BWM > Create New Object > Add Address

The screenshot shows the 'Add Policy' configuration window with the 'Create Address' dialog box open. The dialog box contains the following fields:

- Name:** A text input field with a red error indicator.
- Address Type:** A dropdown menu set to 'HOST'.
- IP Address:** A text input field set to '0.0.0.0'.

The background window shows the following configuration sections:

- Configuration:** Includes 'Enable' (checked), 'Description', and 'BWM Type' (set to 'Shared').
- Criteria:** Includes 'User', 'Schedule', 'Incoming Interface', 'Outgoing Interface', 'Source', 'Destination', 'DSCP Code', 'Service Type' (set to 'Service Object'), and 'Service Object'.
- DSCP Marking:** Includes 'Inbound Marking' and 'Outbound Marking', both set to 'preserve'.
- Bandwidth Shaping:** Includes 'Guaranteed Bandwidth' for 'Inbound' and 'Outbound', each with a 'Priority' of 4 and a 'Maximum' of 0 kbps. There are also checkboxes for 'Maximize Bandwidth Usage'.
- 802.1P Marking:** Includes 'Priority Code' (set to 0) and 'Interface' (set to none).
- Related Setting:** Includes 'Log' (set to no).

The following table describes the fields in the above screen.

Table 162 Configuration > BWM > Create New Object > Add Address

LABEL	DESCRIPTION
Name	Enter a name for the Address object of the rule.
Address Type	Select an Address Type from the drop down menu on the right. The Address Types are Host, Range, Subnet, Interface IP, Interface Subnet, and Interface Gateway.
IP Address	Enter an IP address for the Address object.
OK	Click OK to save the setting.
Cancel	Click Cancel to abandon the setting.

Content Filtering

27.1 Overview

Use the content filtering feature to control access to specific web sites or web content.

27.1.1 What You Can Do in this Chapter

- Use the **Filter Profile** screens ([Section Figure 289 on page 420](#)) to set up content filtering profiles.
- Use the **Trusted Web Sites** screens ([Section 27.4 on page 430](#)) to create a common list of good (allowed) web site addresses.
- Use the **Forbidden Web Sites** screens ([Section 27.5 on page 431](#)) to create a common list of bad (blocked) web site addresses.

27.1.2 What You Need to Know

Content Filtering

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filter policies for different addresses, schedules, users or groups and content filter profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filter profile.
- Use address and/or user/group objects to define to whose web access to apply the content filter profile.
- Apply a content filter profile that you have custom-tailored.

Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

- Category-based Blocking
The USG can block access to particular categories of web site content, such as pornography or racial intolerance.

- **Restrict Web Features**
The USG can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.
- **Customize Web Site Access**
You can specify URLs to which the USG blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the USG block access to URLs that contain particular keywords.

Content Filtering Configuration Guidelines

When the USG receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on the settings of the filtering profile specified by the policy. Some requests may not match any policy. The USG allows the request if the default policy is not set to block. The USG blocks the request if the default policy is set to block.

External Web Filtering Service

When you register for and enable the external web filtering service, your USG accesses an external database that has millions of web sites categorized based on content. You can have the USG block, block and/or log access to web sites based on these categories.

Keyword Blocking URL Checking

The USG checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the USG checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the USG would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

Finding Out More

- See [Section 27.6 on page 432](#) for content filtering background/technical information.

27.1.3 Before You Begin

- You must configure an address object, a schedule object and a filtering profile before you can set up a content security policy.
- You must have Content Filtering license in order to use the function.subscribe to use the external database content filtering (see the **Licensing > Registration** screens).

27.2 Content Filter Profile Screen

Click **Configuration > UTM Profile > Content Filter > Profile** to open the **Content Filter Profile** screen. Use this screen to enable content filtering, view and order your list of content filter policies, create a denial of access message or specify a redirect URL and check your external web filtering service registration status.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting and other information.

Figure 288 Configuration > UTM Profile > Content Filter > Profile

The screenshot shows the 'Content Filter Profile' configuration page. At the top, there are tabs for 'Profile', 'Trusted Web Sites', and 'Forbidden Web Sites'. Below the tabs are navigation icons for 'General Settings', 'Configuration Walkthrough', 'Troubleshooting', and 'Content Filter'. The 'General Settings' section includes a checkbox for 'Enable Content Filter Report Service' and a 'Report Server' link. Below this is a 'Content Filter Category Service Timeout' field set to 10 seconds. The 'Message to display when a site is blocked' section has fields for 'Denied Access Message' (pre-filled with 'Web access is restricted. Please contact the administrator.') and 'Redirect URL'. The 'Profile Management' section shows a table of profiles with columns for '#', 'Name', and 'Description'. The 'Content Filter Category Service License Status' section shows 'Licensed', 'Standard', and '2016-12-10'. At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 163 Configuration > UTM Profile > Content Filter > Profile

LABEL	DESCRIPTION
General Settings	
Enable Content Filter Report Service	Select this check box to have the USG collect category-based content filtering statistics.
Report Server	Click this link to choose where your USG is registered: myZyXEL.com or myZyXEL.com 2.0. Choose myZyXEL.com 2.0 for a model in this series.
Content Filter Category Service Timeout	Specify the allowable time period in seconds for accessing the external web filtering service's server.

Table 163 Configuration > UTM Profile > Content Filter > Profile (continued)

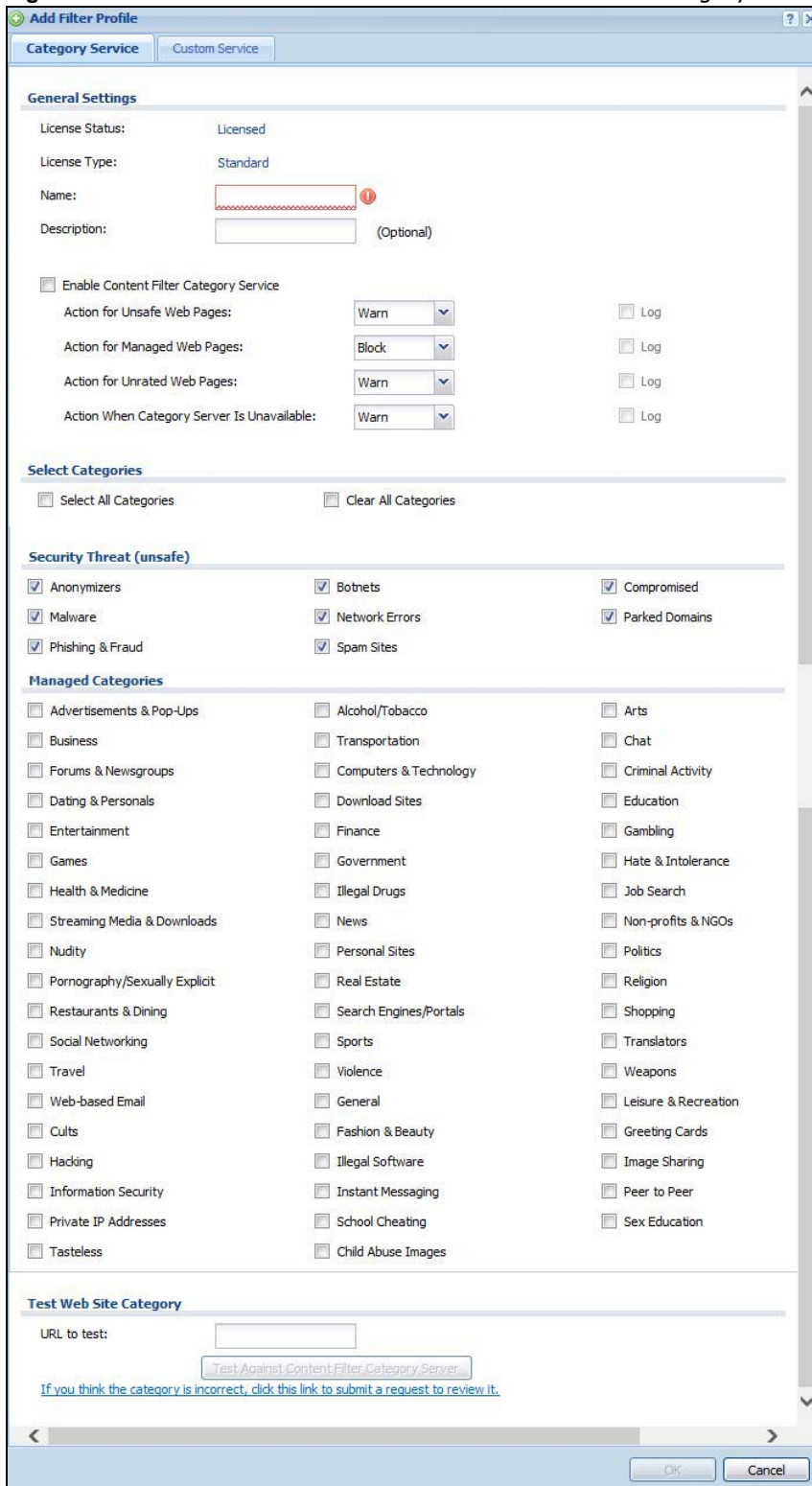
LABEL	DESCRIPTION
Denied Access Message	<p>Enter a message to be displayed when content filter blocks access to a web page. Use up to 127 characters (0-9a-zA-Z;/?:@&=+\$\._!~*')(%,"). For example, "Access to this web page is not allowed. Please contact the network administrator".</p> <p>It is also possible to leave this field blank if you have a URL specified in the Redirect URL field. In this case if the content filter blocks access to a web page, the USG just opens the web page you specified without showing a denied access message.</p>
Redirect URL	<p>Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message.</p> <p>Use "http://" or "https://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+\$\._!~*')(%). For example, http://192.168.1.17/blocked access.</p>
Profile Management	
Add	Click Add to create a new content filter rule.
Edit	Click Edit to make changes to a content filter rule.
Remove	Click Remove to delete a content filter rule.
Object Reference	Select an entry and click Object References to open a screen that shows which settings use the entry. Click Refresh to update information on this screen.
#	This column lists the index numbers of the content filter profile.
Name	This column lists the names of the content filter profile rule.
Description	This column lists the description of the content filter profile rule.
Reference	This displays the number of times an Object Reference is used in a rule.
License Status	<p>This read-only field displays the status of your content-filtering database service registration.</p> <p>Not Licensed displays if you have not successfully registered and activated the service.</p> <p>Expired displays if your subscription to the service has expired.</p> <p>Licensed displays if you have successfully registered the USG and activated the service.</p> <p>You can view content filter reports after you register the USG and activate the subscription service in the Registration screen.</p>
License Type	<p>This read-only field displays what kind of service registration you have for the content-filtering database.</p> <p>None displays if you have not successfully registered and activated the service.</p> <p>Standard displays if you have successfully registered the USG and activated the service.</p> <p>Trial displays if you have successfully registered the USG and activated the trial service subscription.</p>
Expiration Date	This field displays the date your service license expires.
Register Now	This link appears if you have not registered for the service or the service has expired. Click this link to go to the screen where you can register for the service.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

27.3 Content Filter Profile Add or Edit Screen

Click **Configuration > UTM > Content Filter > Profile > Add or Edit** to open the **Add Filter Profile** screen. Configure **Category Service** and **Custom Service** tabs.

27.3.1 Content Filter Add Profile Category Service

Figure 289 Content Filter > Profile > Add Filter Profile > Category Service



The following table describes the labels in this screen.

Table 164 Configuration > UTM Profile> Content Filter > Profile > Add > Category Service

LABEL	DESCRIPTION
License Status	<p>This read-only field displays the status of your content-filtering database service registration.</p> <p>Not Licensed displays if you have not successfully registered and activated the service.</p> <p>Expired displays if your subscription to the service has expired.</p> <p>Licensed displays if you have successfully registered the USG and activated the service.</p> <p>You can view content filter reports after you register the USG and activate the subscription service in the Registration screen.</p>
License Type	<p>This read-only field displays what kind of service registration you have for the content-filtering database.</p> <p>None displays if you have not successfully registered and activated the service.</p> <p>Standard displays if you have successfully registered the USG and activated the standard content filtering service.</p> <p>Trial displays if you have successfully registered the USG and activated the trial service subscription.</p>
Name	<p>Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.</p>
Description	<p>Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.</p> <p>This field is optional.</p>
Enable Content Filter Category Service	<p>Enable external database content filtering to have the USG check an external database to find to which category a requested web page belongs. The USG then blocks or forwards access to the web page depending on the configuration of the rest of this page.</p>
Action for Unsafe Web Pages	<p>Select Pass to allow users to access web pages that match the unsafe categories that you select below.</p> <p>Select Block to prevent users from accessing web pages that match the unsafe categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page.</p> <p>Select Warn to display a warning message before allowing users to access web pages that match the unsafe categories that you select below.</p> <p>Select Log to record attempts to access web pages that match the unsafe categories that you select below.</p>

Table 164 Configuration > UTM Profile> Content Filter > Profile > Add > Category Service

LABEL	DESCRIPTION
Action for Managed Web Pages	<p>Select Pass to allow users to access web pages that match the other categories that you select below.</p> <p>Select Block to prevent users from accessing web pages that match the other categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page.</p> <p>Select Log to record attempts to access web pages that match the other categories that you select below.</p>
Action for Unrated Web Pages	<p>Select Pass to allow users to access web pages that the external web filtering service has not categorized.</p> <p>Select Block to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the Content Filter General screen along with the category of the blocked web page.</p> <p>Select Warn to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.</p> <p>Select Log to record attempts to access web pages that are not categorized.</p>
Action When Category Server Is Unavailable	<p>Select Pass to allow users to access any requested web page if the external content filtering database is unavailable.</p> <p>Select Block to block access to any requested web page if the external content filtering database is unavailable.</p> <p>Select Warn to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable.</p> <p>The following are possible causes for the external content filtering server not being available:</p> <ul style="list-style-type: none"> • There is no response from the external content filtering server within the time period specified in the Content Filter Server Unavailable Timeout field. • The USG is not able to resolve the domain name of the external content filtering database. • There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid"). <p>Select Log to record attempts to access web pages that occur when the external content filtering database is unavailable.</p>
Select Categories	
Select All Categories	Select this check box to restrict access to all site categories listed below.
Clear All Categories	Select this check box to clear the selected categories below.
Security Threat (unsafe)	These are the categories of web pages that are known to pose a threat to users or their computers.
Anonymizers	Sites and proxies that act as an intermediary for surfing to other Web sites in an anonymous fashion, whether to circumvent Web filtering or for other reasons. For example, blog.go2.tw, anonymizer.com, www.qu365.com.
Botnets	Sites that use bots (zombies) including command-and-control sites.
Compromised	Sites that have been compromised by someone other than the site owner in order to install malicious programs without the user's knowledge. Includes sites that may be vulnerable to a particular high-risk attack. For example, www.wokoo.net, movie.sx.zj.cn.

Table 164 Configuration > UTM Profile> Content Filter > Profile > Add > Category Service

LABEL	DESCRIPTION
Malware	Sites that install unwanted software on a user's computer with the intent to enable third-party monitoring or make system changes without the user's consent. For example, www.tqlkg.com, aladel.net.
Network Errors	Sites that do not resolve to any IP address.
Parked Domains	Sites that are inactive, typically reserved for later use. They most often do not contain their own content, may simply say "under construction," "purchase this domain," or display advertisements. For example, www.moemoon.com, artlin.net, img.sedoparking.com.
Phishing & Fraud	Sites that are used for deceptive or fraudulent purposes (e.g. phishing), such as stealing financial or other user account information. These sites are most often designed to appear as legitimate sites in order to mislead users into entering their credentials. For example, optimizedby.rmxads.com, 218.1.71.226/.../e3b.
Spam Sites	Sites that have been promoted through spam techniques. For example, img.tongji.linezing.com, banner.chinesegamer.net.
Managed Categories	These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content. You must have the Category Service content filtering license to filter these categories. See the next table for category details.
Test Web Site Category	
URL to test	You can check which category a web page belongs to. Enter a web site URL in the text box. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active.
If you think the category is incorrect	Click this link to see the category recorded in the USG's content filtering database for the web page you specified (if the database has an entry for it).
Test Against Content Filter Category Server	Click this button to see the category recorded in the external content filter server's database for the web page you specified.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

The following table describes the managed categories.

Table 165 Managed Category Descriptions

CATEGORY	DESCRIPTION
Advertisements & Pop-Ups	Sites that provide advertising graphics or other ad content files such as banners and pop-ups. For example, pagead2.google syndication.com, ad.yieldmanager.com.
Alcohol & Tobacco	Sites that promote or sell alcohol- or tobacco-related products or services. For example, www.drinks.com.tw, www.p9.com.tw, beer.ttl.com.tw.
Arts	Sites with artistic content or relating to artistic institutions such as theaters, museums, galleries, dance companies, photography, and digital graphic resources. For example, www.npm.gov.tw, www.nmh.gov.tw.
Business	Sites that provide business related information such as corporate Web sites. Information, services, or products that help businesses of all sizes to do their day-to-day commercial activities. For example, www.kinkos.com, www.proctorgamble.com, www.bbb.org.
Chat	Sites that enable web-based exchange of realtime messages through chat services or chat rooms. For example, me.sohu.com, blufiles.storage.live.com.

Table 165 Managed Category Descriptions (continued)

Child Abuse Images	Sites that portray or discuss children in sexual or other abusive acts. For example, a.uuzhijia.info.
Computers & Technology	Sites that contain information about computers, software, hardware, IT, peripheral and computer services, such as product reviews, discussions, and IT news. For example, www.informationsecurity.com.tw, blog.ithome.com.tw.
Criminal Activity	Sites that offer advice on how to commit illegal or criminal activities, or to avoid detection. These can include how to commit murder, build bombs, pick locks, etc. Also includes sites with information about illegal manipulation of electronic devices, hacking, fraud and illegal distribution of software. For example, www.hackbase.com, jia.hackbase.com, ad.adver.com.tw.
Cults	Sites relating to non-traditional religious practice typically known as "cults," that is, considered to be false, unorthodox, extremist, or coercive, with members often living under the direction of a charismatic leader. For example, www.churchofsatan.com, www.ccy.org.tw.
Dating & Personals	Sites that promote networking for interpersonal relationships such as dating and marriage. Includes sites for match-making, online dating, spousal introduction. For example, www.i-part.com.tw, www.imatchi.com.
Download Sites	Sites that contain downloadable software, whether shareware, freeware, or for a charge. Includes peer-to-peer sites. For example, www.hotdl.com, toget.pchome.com.tw, www.azroo.com.
Education	Sites sponsored by educational institutions and schools of all types including distance education. Includes general educational and reference materials such as dictionaries, encyclopedias, online courses, teaching aids and discussion guides. For example, www.tfam.museum, www.lksf.org, www.1980.org.tw..
Entertainment	Sites related to television, movies, music and video (including video on demand), such as program guides, celebrity sites, and entertainment news. For example, www.ctitv.com.tw, www.hboasia.com, www.startv.com.tw.
Fashion & Beauty	Sites concerning fashion, jewelry, glamour, beauty, modeling, cosmetics or related products or services. Includes product reviews, comparisons, and general consumer information. For example, women.sohu.com, baodian.women.sohu.com.
Finance	Sites related to banking, finance, payment or investment, including banks, brokerages, online stock trading, stock quotes, fund management, insurance companies, credit unions, credit card companies, and so on. For example, www.concords.com.tw, www.polaris.com.tw, www.bochk.com.
Forums & Newsgroups	Sites for sharing information in the form of newsgroups, forums, bulletin boards. For example, ck101.com, my.xuite.net, ptt.cc.
Gambling	Sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance. For example, www.taiwanlottery.com.tw, www.i-win.com.tw, www.hkjc.com.
Games	Sites relating to computer or other games, information about game producers, or how to obtain cheat codes. Game-related publication sites. For example, www.gamer.com.tw, www.wowtaiwan.com.tw, tw.lineage.gamania.com.
General	Sites that do not clearly fall into other categories, for example, blank Web pages. For example, bs.serving-sys.com, simg.sinajs.cn, i0.itc.cn.
Government	Sites run by governmental organizations, departments, or agencies, including police departments, fire departments, customs bureaus, emergency services, civil defense, counterterrorism organizations, military and hospitals. For example, www.ey.gov.tw, www.whitehouse.gov, www.npa.gov.tw.
Greeting cards	Sites that allow people to send and receive greeting cards and postcards. For example, www.e-card.com.tw, card.ivy.net.tw.

Table 165 Managed Category Descriptions (continued)

Hacking	Sites that promote or give advice about how to gain unauthorized access to proprietary computer systems, for the purpose of stealing information, perpetrating fraud, creating viruses, or committing other illegal activity related to theft of digital information. For example, www.hackbase.com , www.chinahacker.com .
Hate & Intolerance	Sites that promote a supremacist political agenda, encouraging oppression of people or groups of people based on their race, religion, gender, age, disability, sexual orientation or nationality. For example, www.racist-jokes.com , aryan-nations.org , whitepower.com .
Health & Medicine	Sites containing information pertaining to health, healthcare services, fitness and well-being, including information about medical equipment, hospitals, drugstores, nursing, medicine, procedures, prescription medications, etc. For example, www.lksf.org , www.ohayo.com.tw .
Illegal Drug	Sites with information on the purchase, manufacture, and use of illegal or recreational drugs and their paraphernalia, and misuse of prescription drugs and other compounds. For example, www.cannabis.net , www.amphetamines.com .
Illegal Software	Sites that illegally distribute software or copyrighted materials such as movies or music, software cracks, illicit serial numbers, illegal license key generators. For example, www.zhaokey.com.cn , www.tiansha.net .
Image Sharing	Sites that host digital photographs and images, online photo albums and digital photo exchanges. For example, photo.pchome.com.tw , photo.xuite.net , photobucket.com .
Information Security	Sites that provide legitimate information about data protection, including newly discovered vulnerabilities and how to block them. For example, www.informationsecurity.com.tw , www.itis.tw .
Instant Messaging	Sites that enable logging in to instant messaging services such as ICQ, AOL Instant Messenger, IRC, MSN, Jabber, Yahoo Messenger, and the like. For example, www.meebo.com , www.aim.com , www.ebuddy.com .
Job Search	Sites containing job listings, career information, assistance with job searches (such as resume writing, interviewing tips, etc.), employment agencies or head hunters. For example, www.104.com.tw , www.1111.com.tw , www.yes123.com.tw .
Leisure & Recreation	Sites relating to recreational activities and hobbies including zoos, public recreation centers, pools, amusement parks, and hobbies such as gardening, literature, arts & crafts, home improvement, home décor, family, etc. For example, tpbg.tfri.gov.tw , tw.fashion.yahoo.com , www.relaxtimes.com.tw .
News	Sites covering news and current events such as newspapers, newswire services, personalized news services, broadcasting sites, and magazines. For example, www.tvbs.com.tw , www.ebc.net.tw , www.iset.com.tw .
Non-profits & NGOs	Sites devoted to clubs, communities, unions, and non-profit organizations. Many of these groups exist for educational or charitable purposes. For example, www.tzuchi.org.tw , web.redcross.org.tw , www.lksf.org .
Nudity	Sites that contain full or partial nudity that are not necessarily overtly sexual in intent. Includes sites that advertise or sell lingerie, intimate apparel, or swimwear. For example, www.easyshop.com.tw , www.faster-swim.com.tw , image.baidu.com .
Peer-to-Peer	Sites that enable direct exchange of files between users without dependence on a central server. For example, www.eyny.com .
Personal Sites	Sites about or hosted by personal individuals, including those hosted on commercial sites. For example, blog.yam.com , www.wretch.cc , blog.xuite.net .
Politics	Sites that promote political parties or political advocacy, or provide information about political parties, interest groups, elections, legislation or lobbying. Also includes sites that offer legal information and advice. For example, www.kmt.org.tw , www.dpp.org.tw , cpc.people.com.cn .

Table 165 Managed Category Descriptions (continued)

Pornography/Sexually Explicit	Sites that contain explicit sexual content. Includes adult products such as sex toys, CD-ROMs, and videos, adult services such as videoconferencing, escort services, and strip clubs, erotic stories and textual descriptions of sexual acts. For example, www.dvd888.com , www.18center.com , blog.sina.com.tw .
Private IP Addresses	Sites that are private IP addresses as defined in RFC 1918, that is, hosts that do not require access to hosts in other enterprises (or require just limited access) and whose IP address may be ambiguous between enterprises but are well defined within a certain enterprise. For example, 172.21.20.123, 192.168.35.62.
Real Estate	Sites relating to commercial or residential real estate services, including renting, purchasing, selling or financing homes, offices, etc. For example, www.sinyi.com.tw , www.yungching.com.tw , house.focus.cn .
Religion	Sites that deal with faith, human spirituality or religious beliefs, including sites of churches, synagogues, mosques and other houses of worship. For example, www.fgs.org.tw , www.twtaoism.net , www.fhl.net .
Restaurants & Dining	Sites that list, review, promote or advertise food, dining or catering services. Includes sites for recipes, cooking instruction and tips, food products, and wine advisors. For example, www.jogoya.com.tw , www.dintaifung.com.tw , www2.pizzahut.com.tw .
School Cheating	Sites that promote unethical practices such as cheating or plagiarism by providing test answers, written essays, research papers, or term papers. For example, www.zydk788.com , www.huafengksw.com .
Search Engines & Portals	Sites enabling the searching of the Web, newsgroups, images, directories, and other online content. Includes portal and directory sites such as white/yellow pages. For example, tw.yahoo.com , www.pchome.com.tw , www.google.com.tw .
Sex Education	Sites relating to sex education, including subjects such as respect for partner, abortion, gay and lesbian lifestyle, contraceptives, sexually transmitted diseases, and pregnancy. For example, apps.rockyou.com , www.howmama.com.tw , www.mombaby.com.tw .
Shopping	Sites for online shopping, catalogs, online ordering, auctions, classified ads. Excludes shopping for products and services exclusively covered by another category such as health & medicine. For example, shopping.pchome.com.tw , buy.yahoo.com.tw , www.tkec.com.tw .
Social Networking	Sites that enable social networking for online communities of various topics, for friendship, dating, or professional reasons. For example, www.facebook.com , www.flickr.com , www.groups.google.com .
Sports	Sites relating to sports teams, fan clubs, scores and sports news. Relates to all sports, whether professional or recreational. For example, www.yankees.com , www.mlb.com .
Streaming Media & Downloads	Sites that deliver streaming content, such as Internet radio, Internet TV or MP3 and live or archived media download sites. Includes fan sites, or official sites run by musicians, bands, or record labels. For example, www.youtube.com , pfp.sina.com.cn , my.xunlei.com .
Tasteless	Sites with offensive or tasteless content such as bathroom humor or profanity. For example, comedycentral.com , dilbert.com .
Translators	Sites that translate Web pages or phrases from one language to another. These sites may be used to attempt to bypass a filtering system. For example, translate.google.com.tw , www.smartlinkcorp.com , translation.paralink.com .
Transportation	Sites that provide information about motor vehicles such as cars, motorcycles, boats, trucks, RVs and the like. Includes manufacturer sites, dealerships, review sites, pricing, , online purchase sites, enthusiasts clubs, etc. For example, www.toyota.com.tw , www.ford.com.tw , www.sym.com.tw .

Table 165 Managed Category Descriptions (continued)

Travel	Sites that provide travel and tourism information or online booking of travel services such as airlines, accommodations, car rentals. Includes regional or city information sites. For example, www.startravel.com.tw, taipei.grand.hyatt.com.tw, www.car-plus.com.tw.
Unknown	Unknown For example, www.669.com.tw, www.appleballoon.com.tw, www.uimco.com.tw.
Violence	Sites that contain images or text depicting or advocating physical assault against humans, animals, or institutions. Sites of a particularly gruesome nature such as shocking depictions of blood or wounds, or cruel animal treatment. For example, crimescene.com, deathnet.com, michiganmilitia.com.
Weapons	Sites that depict, sell, review or describe guns and weapons, including for sport. For example, www.ak-47.net, warfare.ru.
Web-based Email	Sites that enable users to send and receive email through a web-accessible email account. For example, mail.163.com, mail.google.com, mail.yahoo.com.tw.

27.3.2 Content Filter Add Filter Profile Custom Service

Click **Configuration > UTM Profile > Content Filter > Filter Profile > Add or Edit > Custom Service** to open the **Custom Service** screen. You can create a list of good (allowed) web site addresses and a list of bad (blocked) web site addresses. You can also block web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

Figure 290 Configuration > UTM Profile > Content Filter > Filter Profile > Custom Service

Add Filter Profile

Category Service | **Custom Service**

General Settings

Name: ⓘ

Description: (Optional)

Enable Custom Service

Allow web traffic for trusted web sites only

Check Common Trusted/Forbidden List

Restricted Web Features

Block: ActiveX Java Cookies Web Proxy

Allow Java/ActiveX/Cookies/Web proxy to trusted web sites

Trusted Web Sites

Trusted Web Sites

Page 1 of 1 | Show 50 items | No data to display

Forbidden Web Sites

Forbidden Web Sites

Page 1 of 1 | Show 50 items | No data to display

Blocked URL Keywords

Blocked URL Keywords

Page 1 of 1 | Show 50 items | No data to display

Note: Use * as a wildcard to match any string in trusted/forbidden web sites and blocked URL keywords (for example, *.zyxel*.com).

The following table describes the labels in this screen.

Table 166 Configuration > UTM Profile > Content Filter > Profile > Custom Service

LABEL	DESCRIPTION
Name	Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the content filtering profile rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Enable Custom Service	Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names.

Table 166 Configuration > UTM Profile > Content Filter > Profile > Custom Service (continued)

LABEL	DESCRIPTION
Allow Web traffic for trusted web sites only	When this box is selected, the USG blocks Web access to sites that are not on the Trusted Web Sites list. If they are chosen carefully, this is the most effective way to block objectionable material.
Check Common Trusted/Forbidden List	Select this check box to check the common trusted and forbidden web sites lists. See Section 27.4 on page 430 and Section 27.5 on page 431 for information on configuring these lists.
Restricted Web Features	Select the check box(es) to restrict a feature. Select the check box(es) to restrict a feature. <ul style="list-style-type: none"> When you download a page containing ActiveX or Java, that part of the web page will be blocked with an X. When you download a page coming from a Web Proxy, the whole web page will be blocked. When you download a page containing cookies, the cookies will be removed, but the page will not be blocked.
Block ActiveX	ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Allow Java/ActiveX/Cookies/ Web proxy to trusted web sites	When this box is selected, the USG will permit Java, ActiveX and Cookies from sites on the Trusted Web Sites list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	This column displays the trusted web sites already added. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "*zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter "*.com" to allow all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter. "*" can be used as a wildcard to match any string. The entry must contain at least one "." or it will be invalid.
Forbidden Web Site List	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.

Table 166 Configuration > UTM Profile > Content Filter > Profile > Custom Service (continued)

LABEL	DESCRIPTION
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.
Forbidden Web Sites	<p>This list displays the forbidden web sites already added.</p> <p>Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "*bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", and do on. You can also enter just a top level domain. For example, enter "*.com" to block all .com domains.</p> <p>Use up to 127 characters (0-9a-z-). The casing does not matter. "*" can be used as a wildcard to match any string. The entry must contain at least one "." or it will be invalid.</p>
Blocked URL Keywords	This section allows you to block Web sites with URLs that contain certain keywords in the domain name or IP address.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the blocked URL keywords.
Blocked URL Keywords	<p>This list displays the keywords already added.</p> <p>Enter a keyword or a numerical IP address to block. You can also enter a numerical IP address.</p> <p>Use up to 127 case-insensitive characters (0-9a-zA-Z;/?:@&=+\$\._!~*()%). "*" can be used as a wildcard to match any string. Use " " to indicate a single wildcard character.</p> <p>For example enter *Bad_Site* to block access to any web page that includes the exact phrase Bad_Site. This does not block access to web pages that only include part of the phrase (such as Bad for example).</p>
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

27.4 Content Filter Trusted Web Sites Screen

Click **Configuration > UTM Profile > Content Filter > Trusted Web Sites** to open the **Trusted Web Sites** screen. You can create a common list of good (allowed) web site addresses. When you configure **Filter Profiles**, you can select the option to check the **Common Trusted Web Sites** list. Use this screen to add or remove specific sites from the filter list.

Figure 291 Configuration > UTM Profile > Content Filter > Trusted Web Sites

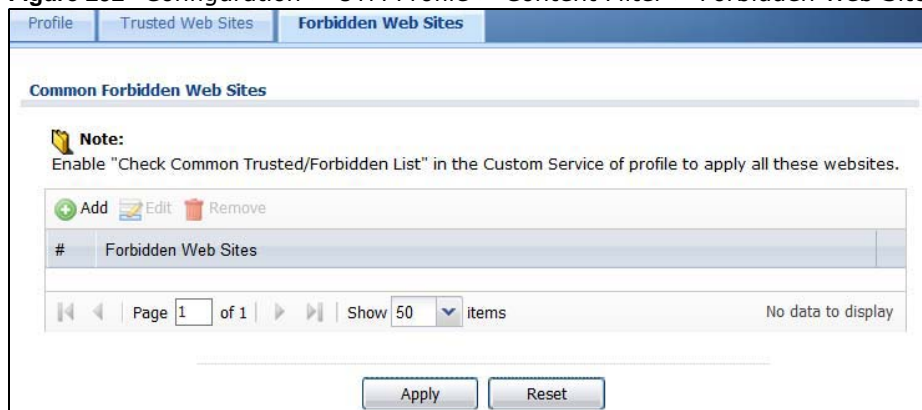
The following table describes the labels in this screen.

Table 167 Configuration > UTM Profile > Content Filter > Trusted Web Sites

LABEL	DESCRIPTION
Common Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the trusted web sites.
Trusted Web Site	This column displays the trusted web sites already added. Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

27.5 Content Filter Forbidden Web Sites Screen

Click **Configuration > UTM Profile > Content Filter > Forbidden Web Sites** to open the **Forbidden Web Sites** screen. You can create a common list of bad (blocked) web site addresses. When you configure **Filter Profiles**, you can select the option to check the **Common Forbidden Web Sites** list. Use this screen to add or remove specific sites from the filter list.

Figure 292 Configuration > UTM Profile > Content Filter > Forbidden Web Sites

The following table describes the labels in this screen.

Table 168 Configuration > UTM Profile > Content Filter > Forbidden Web Sites

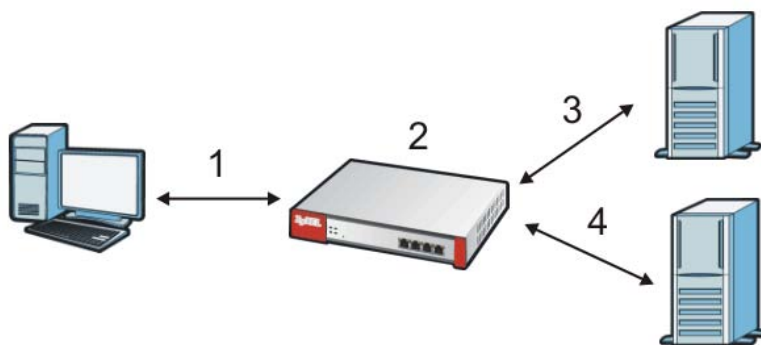
LABEL	DESCRIPTION
Common Forbidden Web Sites	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list.
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
#	This displays the index number of the forbidden web sites.
Forbidden Web Sites	This list displays the forbidden web sites already added. Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are also blocked. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", and do on. You can also enter just a top level domain. For example, enter .com to block all .com domains. Use up to 127 characters (0-9a-z-). The casing does not matter.
Apply	Click Apply to save your changes back to the USG.
Cancel	Click Reset to return the screen to its last-saved settings.

27.6 Content Filter Technical Reference

This section provides content filtering background information.

External Content Filter Server Lookup Procedure

The content filter lookup process is described below.

Figure 293 Content Filter Lookup Procedure

- 1 A computer behind the USG tries to access a web site.
- 2 The USG looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the USG's cache. The USG blocks, blocks and logs or just logs the request based on your configuration.
- 3 Use the **Content Filter Cache** screen to configure how long a web site address remains in the cache as well as view those web site addresses. All of the web site address records are also cleared from the local cache when the USG restarts.
- 4 If the USG has no record of the web site, it queries the external content filter database and simultaneously sends the request to the web server.
- 5 The external content filter server sends the category information back to the USG, which then blocks and/or logs access to the web site based on the settings in the content filter profile. The web site's address and category are then stored in the USG's content filter cache.

Anti-Spam

28.1 Overview

The anti-spam feature can mark or discard spam (unsolicited commercial or junk e-mail). Use the white list to identify legitimate e-mail. Use the black list to identify spam e-mail. The USG can also check e-mail against a DNS black list (DNSBL) of IP addresses of servers that are suspected of being used by spammers.

28.1.1 What You Can Do in this Chapter

- Use the **Profile** screens ([Section 28.3 on page 436](#)) to turn anti-spam on or off and manage anti-spam policies.
- Use the **Mail Scan** screen ([Section 28.4 on page 439](#)) to enable and configure the mail scan functions.
- Use the **Black/White List** screens ([Section 28.5 on page 441](#)) to set up a black list to identify spam and a white list to identify legitimate e-mail.
- Use the **DNSBL** screens ([Section 28.7 on page 446](#)) to have the USG check e-mail against DNS Black Lists.

28.1.2 What You Need to Know

White List

Configure white list entries to identify legitimate e-mail. The white list entries have the USG classify any e-mail that is from a specified sender or uses a specified header field and header value as being legitimate (see [E-mail Headers on page 435](#) for more on mail headers). The anti-spam feature checks an e-mail against the white list entries before doing any other anti-spam checking. If the e-mail matches a white list entry, the USG classifies the e-mail as legitimate and does not perform any more anti-spam checking on that individual e-mail. A properly configured white list helps keep important e-mail from being incorrectly classified as spam. The white list can also increase the USG's anti-spam speed and efficiency by not having the USG perform the full anti-spam checking process on legitimate e-mail.

Black List

Configure black list entries to identify spam. The black list entries have the USG classify any e-mail that is from or forwarded by a specified IP address or uses a specified header field and header value as being spam. If an e-mail does not match any of the white list entries, the USG checks it against the black list entries. The USG classifies an e-mail that matches a black list entry as spam and immediately takes the configured action for dealing with spam. If an e-mail matches a blacklist entry, the USG does not perform any more anti-spam checking on that individual e-mail. A properly

configured black list helps catch spam e-mail and increases the USG's anti-spam speed and efficiency.

SMTP and POP3

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of e-mail messages between servers. E-mail clients (also called e-mail applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve e-mail. E-mail clients also generally use SMTP to send messages to a mail server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many e-mail applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

The USG's anti-spam feature checks SMTP (TCP port 25) and POP3 (TCP port 110) e-mails by default. You can also specify custom SMTP and POP3 ports for the USG to check.

E-mail Headers

Every email has a header and a body. The header is structured into fields and includes the addresses of the recipient and sender, the subject, and other information about the e-mail and its journey. The body is the actual message text and any attachments. You can have the USG check for specific header fields with specific values.

E-mail programs usually only show you the To:, From:, Subject:, and Date: header fields but there are others such as Received: and Content-Type:. To see all of an e-mail's header, you can select an e-mail in your e-mail program and look at its properties or details. For example, in Microsoft's Outlook Express, select a mail and click **File > Properties > Details**. This displays the e-mail's header. Click **Message Source** to see the source for the entire mail including both the header and the body.

E-mail Header Buffer Size

The USG has a 5 K buffer for an individual e-mail header. If an e-mail's header is longer than 5 K, the USG only checks up to the first 5 K.

DNSBL

A DNS Black List (DNSBL) is a server that hosts a list of IP addresses known or suspected of having sent or forwarded spam. A DNSBL is also known as a DNS spam blocking list. The USG can check the routing addresses of e-mail against DNSBLs and classify an e-mail as spam if it was sent or forwarded by a computer with an IP address in the DNSBL.

Finding Out More

See [Section 28.8 on page 448](#) for more background information on anti-spam.

28.2 Before You Begin

- Before using the Anti-Spam features (IP Reputation, Mail Content Analysis and Virus Outbreak Detection) you must activate your Anti-Spam Service license.

- Configure your zones before you configure anti-spam.

28.3 The Anti-Spam Profile Screen

Click **Configuration > UTM Profile > Anti-Spam** to open the **Anti-Spam Profile** screen. Use this screen to turn the anti-spam feature on or off and manage anti-spam policies. You can also select the action the USG takes when the mail sessions threshold is reached.

Click on the icons to go to the OneSecurity.com website where there is guidance on configuration walkthroughs, troubleshooting and other information.

Figure 294 Configuration > UTM Profile > Anti-Spam > Profile

The following table describes the labels in this screen.

Table 169 Configuration > UTM Profile > Anti-Spam > Profile

LABEL	DESCRIPTION
General Settings	
Action taken when mail sessions threshold is reached	An e-mail session is when an e-mail client and e-mail server (or two e-mail servers) connect through the USG. Select how to handle concurrent e-mail sessions that exceed the maximum number of concurrent e-mail sessions that the anti-spam feature can handle. See the chapter of product specifications for the threshold. Select Forward Session to have the USG allow the excess e-mail sessions without any spam filtering. Select Drop Session to have the USG drop mail connections to stop the excess e-mail sessions. The e-mail client or server will have to re-attempt to send or receive e-mail later when the number of e-mail sessions is under the threshold.
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.

Table 169 Configuration > UTM Profile > Anti-Spam > Profile

LABEL	DESCRIPTION
Object Reference	Select an entry and click Object References to open a screen that shows which settings use the entry. Click Refresh to update information in this screen.
Priority	This is the index number of the anti-spam rule. Anti-spam rules are applied in turn.
Name	The name identifies the anti-spam rule.
Description	This is some optional extra information on the rule.
Scan Options	This shows which types (protocols) of traffic to scan for spam.
Reference	This shows how many objects are referenced in the rule.
License	
License Status	This read-only field displays the status of your anti-spam scanning service registration. Not Licensed displays if you have not successfully registered and activated the service. Expired displays if your subscription to the service has expired. Licensed displays if you have successfully registered the USG and activated the service.
License Type	This read-only field displays what kind of service registration you have for the anti-spam scanning. None displays if you have not successfully registered and activated the service. Standard displays if you have successfully registered the USG and activated the service with your iCard's PIN number. Trial displays if you have successfully registered the USG and activated the trial service subscription.
Expiration Date	This field displays the date your service license expires.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.3.1 The Anti-Spam Profile Add or Edit Screen

Click the **Add** or **Edit** icon in the **Configuration > UTM Profile > Anti-Spam > Profile** screen to display the configuration screen as shown next. Use this screen to configure an anti-spam policy that controls what traffic direction of e-mail to check, which e-mail protocols to scan, the scanning options, and the action to take on spam traffic.

Figure 295 Configuration > UTM Profile > Anti-Spam > Profile > Add

The following table describes the labels in this screen.

Table 170 Configuration > UTM Profile > Anti-Spam > Profile > Add

LABEL	DESCRIPTION
General Settings	
Name	Enter a descriptive name for this anti-spam rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description for the anti-spam rule to help identify the purpose of rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. This field is optional.
Log	Select how the USG is to log the event when the DNSBL times out or an e-mail matches the white list, black list, or DNSBL. no: Do not create a log. log: Create a log on the USG. log alert: An alert is an e-mailed log for more serious events that may need more immediate attention. Select this option to have the USG send an alert.
Scan Options	
Check White List	Select this check box to check e-mail against the white list. The USG classifies e-mail that matches a white list entry as legitimate (not spam).
Check Black List	Select this check box to check e-mail against the black list. The USG classifies e-mail that matches a black list entry as spam.
Check IP Reputation (SMTP Only)	Select this to use IP reputation to identify Spam or Unwanted Bulk Email by the sender's IP address.

Table 170 Configuration > UTM Profile > Anti-Spam > Profile > Add (continued)

LABEL	DESCRIPTION
Check Mail Content	Select this to identify Spam Email by content, such as malicious content.
Check Virus Outbreak	Select this to scan emails for attached viruses.
Check DNSBL	Select this check box to check e-mail against the USG's configured DNSBL domains. The USG classifies e-mail that matches a DNS black list as spam.
Actions for Spam Mail	Use this section to set how the USG is to handle spam mail.
SMTP	Select how the USG is to handle spam SMTP mail. Select drop to discard spam SMTP mail. Select forward to allow spam SMTP mail to go through. Select forward with tag to add a spam tag to an SMTP spam mail's mail subject and send it on to the destination.
POP3	Select how the USG is to handle spam POP3 mail. Select forward to allow spam POP3 mail to go through. Select forward with tag to add a spam tag to an POP3 spam mail's mail subject and send it on to the destination.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving your changes.

28.4 The Mail Scan Screen

Click **Configuration > UTM Profile > Anti-Spam > Mail Scan** to open the **Mail Scan** screen. Use this screen to enable and configure the Mail Scan functions. You must first enable the Mail Scan functions on this screen before selecting them in the **Configuration > UTM Profile > Anti-Spam > Profile > Add/Edit** screen.

Figure 296 Configuration > UTM Profile > Anti-Spam > Mail Scan

The screenshot shows the 'Mail Scan' configuration page with the following sections and fields:

- Sender Reputation:**
 - Enable Sender Reputation Checking (SMTP only)
- Mail Content Analysis:**
 - Enable Mail Content Analysis
 - Mail Content Spam Tag: [Spam] (Optional)
 - Mail Content X-Header: X- [] : [] (Optional)
- Virus Outbreak Detection:**
 - Enable Virus Outbreak Detection
 - Virus Outbreak Tag: [Virus] (Optional)
 - Virus Outbreak X-Header: X- [] : [] (Optional)
- Query Timeout Settings:**
 - SMTP: forward with tag (dropdown)
 - POP3: forward with tag (dropdown)
 - Timeout Value: 5 (1-10 Seconds)
 - Timeout Tag: [Timeout] (Optional)
 - Timeout X-Header: X- [] : [] (Optional)

At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 171 Configuration > UTM Profile > Anti-Spam > Mail Scan

LABEL	DESCRIPTION
Sender Reputation	
Enable Sender Reputation Checking (SMTP only)	Select this to have the USG scan for spam e-mail by IP Reputation. Spam or Unwanted Bulk Email is determined by the sender's IP address.
Mail Content Analysis	
Enable Mail Content Analysis	Select this to identify Spam Email by content, such as malicious content.
Mail Content Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of e-mails that are determined to spam based on the mail content analysis. This tag is only added if the anti-spam policy is configured to forward spam mail with a spam tag.
Mail Content X-Header	Specify the name and value for the X-Header to be added when an email is determined to be spam by mail content.
Virus Outbreak Detection	

Table 171 Configuration > UTM Profile > Anti-Spam > Mail Scan

LABEL	DESCRIPTION
Enable Virus Outbreak Detection	This scans emails for attached viruses.
Virus Outbreak Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of e-mails that are determined have an attached viruses. This tag is only added if the anti-spam policy is configured to forward spam mail with a spam tag.
Virus Outbreak X-Header	Specify the name and value for the X-Header to be added when an email is determined to have an attached virus.
Query Timeout Settings	
SMTP	Select how the USG is to handle SMTP mail query timeout. Select drop to discard SMTP mail. Select forward to allow SMTP mail to go through. Select forward with tag to add a tag to an SMTP query timeout mail's mail subject and send it on to the destination.
POP3	Select how the USG is to handle POP3 mail query timeout. Select forward to allow POP3 mail to go through. Select forward with tag to add a tag to an POP3 query timeout mail's mail subject and send it on to the destination.
Timeout Value	Set how long the USG waits for a reply from the mail scan server. If there is no reply before this time period expires, the USG takes the action defined in the relevant Actions when Query Timeout field.
Timeout Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that the USG forwards if queries to the mail scan servers time out.
Timeout X-Header	Specify the name and value for the X-Header to be added when queries to the mail scan servers time out.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.5 The Anti-Spam Black List Screen

Click **Configuration > UTM Profile > Anti-Spam > Black /White List** to display the **Anti-Spam Black List** screen.

Configure the black list to identify spam e-mail. You can create black list entries based on the sender's or relay server's IP address or e-mail address. You can also create entries that check for particular e-mail header fields with specific values or specific subject text. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 297 Configuration > UTM Profile > Anti-Spam > Black/White List > Black List

The following table describes the labels in this screen.

Table 172 Configuration > UTM Profile > Anti-Spam > Black/White List > Black List

LABEL	DESCRIPTION
General Settings	
Enable Black List Checking	Select this check box to have the USG treat e-mail that matches (an active) black list entry as spam.
Black List Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that match the USG's spam black list.
Black List X-Header	Specify the name and value for the X-Header to be added to e-mails that match the USG's spam black list.
Rule Summary	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
Type	This field displays whether the entry is based on the e-mail's subject, source or relay IP address, source e-mail address, or header.
Content	This field displays the subject content, source or relay IP address, source e-mail address, or header value for which the entry checks.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.5.1 The Anti-Spam Black or White List Add/Edit Screen

In the anti-spam **Black List** or **White List** screen, click the **Add** icon or an **Edit** icon to display the following screen.

Use this screen to configure an anti-spam black list entry to identify spam e-mail. You can create entries based on specific subject text, or the sender's or relay's IP address or e-mail address. You can also create entries that check for particular header fields and values.

Figure 298 Configuration > UTM Profile > Anti-Spam > Black/White List > Black List (or White List) > Add

The following table describes the labels in this screen.

Table 173 Configuration > UTM Profile > Anti-Spam > Black/White List > Black/White List > Add

LABEL	DESCRIPTION
Enable Rule	Select this to have the USG use this entry as part of the black or white list. To actually use the entry, you must also turn on the use of the list in the corresponding list screen, enable the anti-spam feature in the anti-spam general screen, and configure an anti-spam policy to use the list.
Type	Use this field to base the entry on the e-mail's subject, source or relay IP address, source e-mail address, or header. Select Subject to have the USG check e-mail for specific content in the subject line. Select IP Address to have the USG check e-mail for a specific source or relay IP address. Select IPv6 Address to have the USG check e-mail for a specific source or relay IPv6 address. Select E-Mail Address to have the USG check e-mail for a specific source e-mail address or domain name. Select Mail Header to have the USG check e-mail for specific header fields and values. Configure black list header entries to check for e-mail from bulk mail programs or with content commonly used in spam. Configure white list header entries to allow certain header values that identify the e-mail as being from a trusted source.
Mail Subject Keyword	This field displays when you select the Subject type. Enter up to 63 ASCII characters of text to check for in e-mail headers. Spaces are not allowed, although you could substitute a question mark (?). See Section 28.5.2 on page 444 for more details.
Sender or Mail Relay IP Address	This field displays when you select the IP Address type. Enter an IP address in dotted decimal notation.
Sender or Mail Relay IPv6 Address	This field displays when you select the IPv6 Address type. Enter an IPv6 address with prefix.
Netmask	This field displays when you select the IP type. Enter the subnet mask here, if applicable.
Sender E-Mail Address	This field displays when you select the E-Mail type. Enter a keyword (up to 63 ASCII characters). See Section 28.5.2 on page 444 for more details.

Table 173 Configuration > UTM Profile > Anti-Spam > Black/White List > Black/White List > Add

LABEL	DESCRIPTION
Mail Header Field Name	This field displays when you select the Mail Header type. Type the name part of an e-mail header (the part that comes before the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the "Received:" header for a specific mail server's domain, enter "Received" here.
Field Value Keyword	This field displays when you select the Mail Header type. Type the value part of an e-mail header (the part that comes after the colon). Use up to 63 ASCII characters. For example, if you want the entry to check the "Received:" header for a specific mail server's domain, enter the mail server's domain here. See Section 28.5.2 on page 444 for more details.
OK	Click OK to save your changes.
Cancel	Click Cancel to exit this screen without saving your changes.

28.5.2 Regular Expressions in Black or White List Entries

The following applies for a black or white list entry based on an e-mail subject, e-mail address, or e-mail header value.

- Use a question mark (?) to let a single character vary. For example, use "a?c" (without the quotation marks) to specify abc, acc and so on.
- You can also use a wildcard (*). For example, if you configure *def.com, any e-mail address that ends in def.com matches. So "mail.def.com" matches.
- The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.
- The USG checks the first header with the name you specified in the entry. So if the e-mail has more than one "Received" header, the USG checks the first one.

28.6 The Anti-Spam White List Screen

Click **Configuration > UTM Profile > Anti-Spam > Black/White List** and then the **White List** tab to display the **Anti-Spam White List** screen.

Configure the white list to identify legitimate e-mail. You can create white list entries based on the sender's or relay's IP address or e-mail address. You can also create entries that check for particular header fields and values or specific subject text.

Figure 299 Configuration > UTM Profile > Anti-Spam > Black/White List > White List

The following table describes the labels in this screen.

Table 174 Configuration > UTM Profile > Anti-Spam > Black/White List > White List

LABEL	DESCRIPTION
General Settings	
Enable White List Checking	Select this check box to have the USG forward e-mail that matches (an active) white list entry without doing any more anti-spam checking on that individual e-mail.
White List X-Header	Specify the name and value for the X-Header to be added to e-mails that match the USG's spam white list.
Rule Summary	
Add	Click this to create a new entry. See Section 28.5.1 on page 443 for details.
Edit	Select an entry and click this to be able to modify it. See Section 28.5.1 on page 443 for details.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
Type	This field displays whether the entry is based on the e-mail's subject, source or relay IP address, source e-mail address, or a header.
Content	This field displays the subject content, source or relay IP address, source e-mail address, or header value for which the entry checks.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.7 The DNSBL Screen

Click **Configuration > UTM Profile > Anti-Spam > DNSBL** to display the anti-spam **DNSBL** screen. Use this screen to configure the USG to check the sender and relay IP addresses in e-mail headers against DNS (Domain Name Service)-based spam Black Lists (DNSBLs).

Figure 300 Configuration > UTM Profile > Anti-Spam > DNSBL

The screenshot shows the DNSBL configuration interface. At the top, there are tabs for Profile, Mail Scan, Black/White List, and DNSBL. Below the tabs is a 'Hide Advanced Settings' button. The main content is organized into three sections:

- General Settings:**
 - Enable DNS Black List (DNSBL) Checking
 - DNSBL Spam Tag: [Spam] (Optional)
 - DNSBL X-Header: X- [] : [] (Optional)
 - Max. IPs Checking Per Mail: 3 (1-5) ⓘ
 - IP Selection Per Mail: last N IPs
- Query Timeout Settings:**
 - SMTP: forward with tag
 - POP3: forward with tag
 - Timeout Value: 5 (1-10 Seconds)
 - Timeout Tag: [Timeout] (Optional)
 - Timeout X-Header: X- [] : [] (Optional)
- DNSBL Domain List:**
 - Buttons: Add, Edit, Remove, Activate, Inactivate
 - Table with columns: Status, #, DNSBL Domain
 - Page 1 of 1, Show 50 items, No data to display

Note: Each mail relay and sender IP in mail header (under max. number) will be checked against the DNSBL domain servers listed and enabled above.

At the bottom of the screen are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

Table 175 Configuration > UTM Profile > Anti-Spam > DNSBL

LABEL	DESCRIPTION
Show Advanced Settings / Hide Advanced Settings	Click this button to display a greater or lesser number of configuration fields.
Enable DNS Black List (DNSBL) Checking	Select this to have the USG check the sender and relay IP addresses in e-mail headers against the DNSBL servers maintained by the DNSBL domains listed in the USG.
DNSBL Spam Tag	Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of e-mails that have a sender or relay IP address in the header that matches a black list maintained by one of the DNSBL domains listed in the USG. This tag is only added if the anti-spam policy is configured to forward spam mail with a spam tag.
DSBNL X-Header	Specify the name and value for the X-Header to be added to e-mails that have a sender or relay IP address in the header that matches a black list maintained by one of the DNSBL domains listed in the USG.
Max. IPs Checking Per Mail	Set the maximum number of sender and relay server IP addresses in the mail header to check against the DNSBL domain servers.
IP Selection Per Mail	Select first N IPs to have the USG start checking from the first IP address in the mail header. This is the IP of the sender or the first server that forwarded the mail. Select last N IPs to have the USG start checking from the last IP address in the mail header. This is the IP of the last server that forwarded the mail.
Query Timeout Setting	
SMTP	Select how the USG is to handle SMTP mail (mail going to an e-mail server) if the queries to the DNSBL domains time out. Select drop to discard SMTP mail. Select forward to allow SMTP mail to go through. Select forward with tag to add a DNSBL timeout tag to the mail subject of an SMTP mail and send it.
POP3	Select how the USG is to handle POP3 mail (mail coming to an e-mail client) if the queries to the DNSBL domains time out. Select forward to allow POP3 mail to go through. Select forward with tag to add a DNSBL timeout tag to the mail subject of an POP3 mail and send it.
Timeout Value	Set how long the USG waits for a reply from the DNSBL domains listed below. If there is no reply before this time period expires, the USG takes the action defined in the relevant Actions when Query Timeout field.
Timeout Tag	Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that the USG forwards if queries to the DNSBL domains time out.
Timeout X-Header	Specify the name and value for the X-Header to be added to e-mails that the USG forwards if queries to the DNSBL domains time out.
DNSBL Domain List	
Add	Click this to create a new entry.
Edit	Select an entry and click this to be able to modify it.
Remove	Select an entry and click this to delete it.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .

Table 175 Configuration > UTM Profile > Anti-Spam > DNSBL (continued)

LABEL	DESCRIPTION
Status	The activate (light bulb) icon is lit when the entry is active and dimmed when the entry is inactive.
#	This is the entry's index number in the list.
DNSBL Domain	This is the name of a domain that maintains DNSBL servers. Enter the domain that is maintaining a DNSBL.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

28.8 Anti-Spam Technical Reference

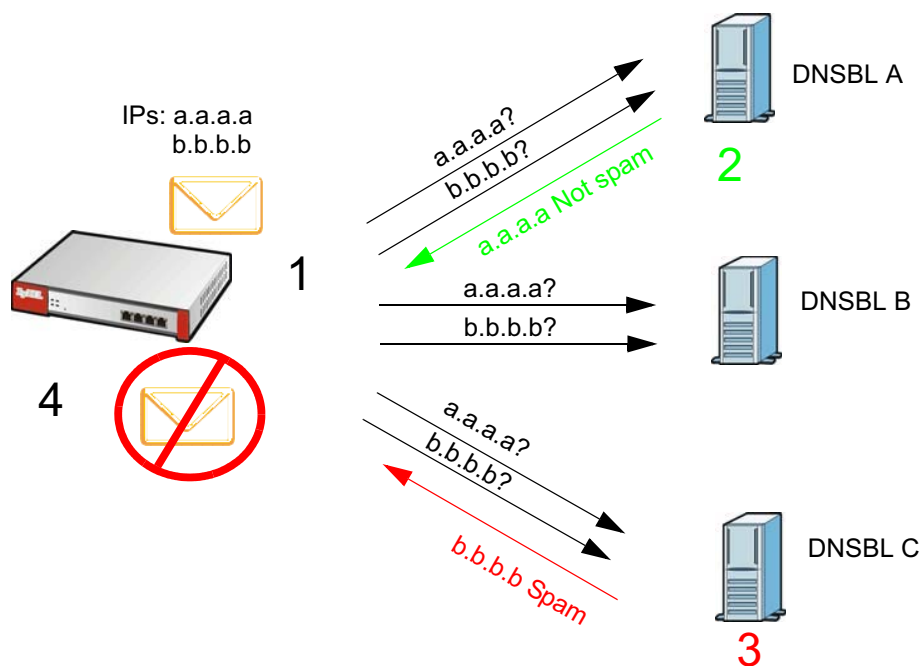
Here is more detailed anti-spam information.

DNSBL

- The USG checks only public sender and relay IP addresses, it does not check private IP addresses.
- The USG sends a separate query (DNS lookup) for each sender or relay IP address in the e-mail's header to each of the USG's DNSBL domains at the same time.
- The DNSBL servers send replies as to whether or not each IP address matches an entry in their list. Each IP address has a separate reply.
- As long as the replies are indicating the IP addresses do not match entries on the DNSBL lists, the USG waits until it receives at least one reply for each IP address.
- If the USG receives a DNSBL reply that one of the IP addresses is in the DNSBL list, the USG immediately classifies the e-mail as spam and takes the anti-spam policy's configured action for spam. The USG does not wait for any more DNSBL replies.
- If the USG receives at least one non-spam reply for each of an e-mail's routing IP addresses, the USG immediately classifies the e-mail as legitimate and forwards it.
- Any further DNSBL replies that come after the USG classifies an e-mail as spam or legitimate have no effect.
- The USG records DNSBL responses for IP addresses in a cache for up to 72 hours. The USG checks an e-mail's sender and relay IP addresses against the cache first and only sends DNSBL queries for IP addresses that are not in the cache.

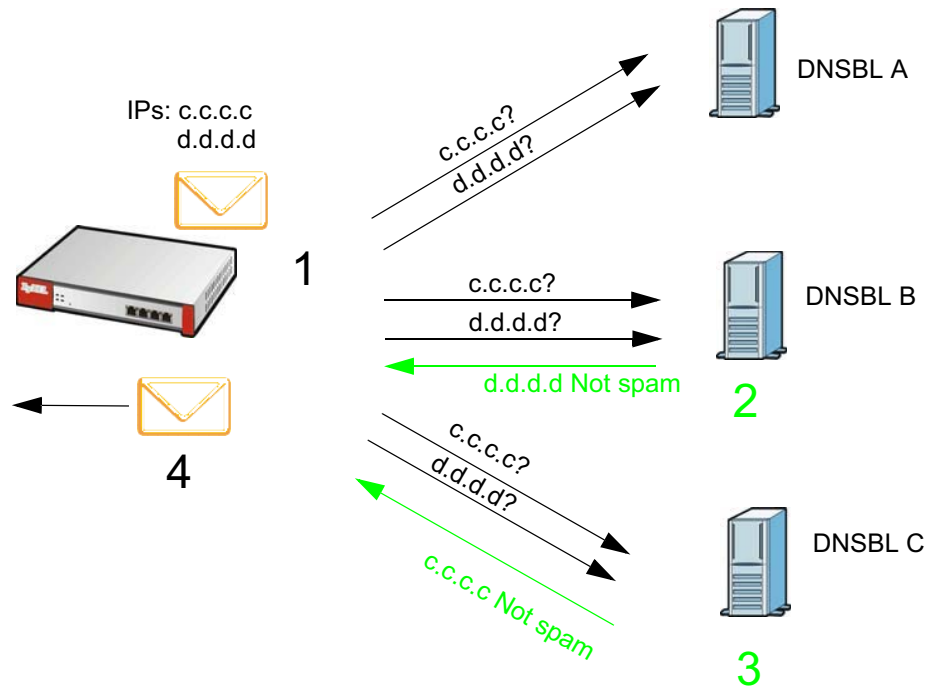
Here is an example of an e-mail classified as spam based on DNSBL replies.

Figure 301 DNSBL Spam Detection Example



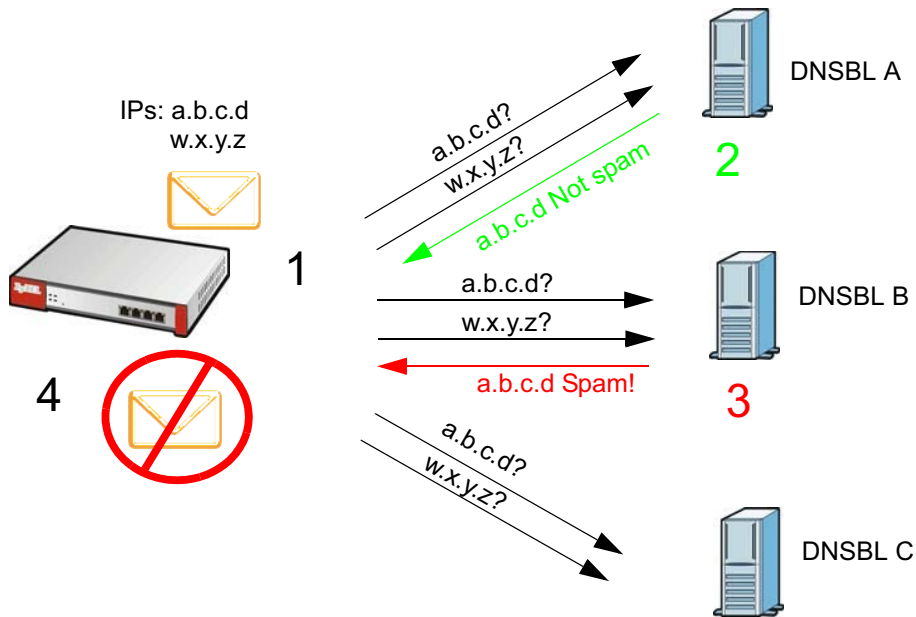
- 1 The USG receives an e-mail that was sent from IP address a.a.a.a and relayed by an e-mail server at IP address b.b.b.b. The USG sends a separate query to each of its DNSBL domains for IP address a.a.a.a. The USG sends another separate query to each of its DNSBL domains for IP address b.b.b.b.
- 2 DNSBL A replies that IP address a.a.a.a does not match any entries in its list (not spam).
- 3 DNSBL C replies that IP address b.b.b.b matches an entry in its list.
- 4 The USG immediately classifies the e-mail as spam and takes the action for spam that you defined in the anti-spam policy. In this example it was an SMTP mail and the defined action was to drop the mail. The USG does not wait for any more DNSBL replies.

Here is an example of an e-mail classified as legitimate based on DNSBL replies.

Figure 302 DNSBL Legitimate E-mail Detection Example

- 1 The USG receives an e-mail that was sent from IP address c.c.c.c and relayed by an e-mail server at IP address d.d.d.d. The USG sends a separate query to each of its DNSBL domains for IP address c.c.c.c. The USG sends another separate query to each of its DNSBL domains for IP address d.d.d.d.
- 2 DNSBL B replies that IP address d.d.d.d does not match any entries in its list (not spam).
- 3 DNSBL C replies that IP address c.c.c.c does not match any entries in its list (not spam).
- 4 Now that the USG has received at least one non-spam reply for each of the e-mail's routing IP addresses, the USG immediately classifies the e-mail as legitimate and forwards it. The USG does not wait for any more DNSBL replies.

If the USG receives conflicting DNSBL replies for an e-mail routing IP address, the USG classifies the e-mail as spam. Here is an example.

Figure 303 Conflicting DNSBL Replies Example

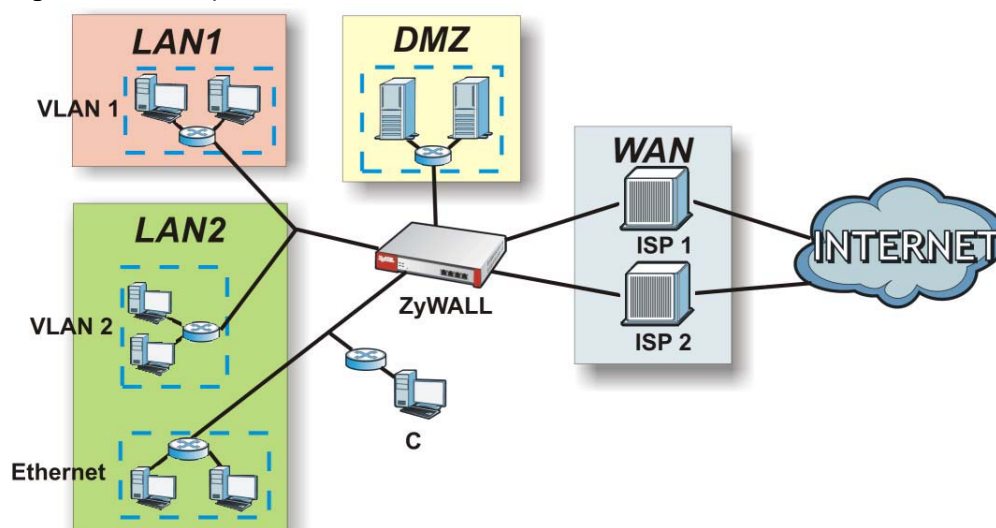
- 1 The USG receives an e-mail that was sent from IP address a.b.c.d and relayed by an e-mail server at IP address w.x.y.z. The USG sends a separate query to each of its DNSBL domains for IP address a.b.c.d. The USG sends another separate query to each of its DNSBL domains for IP address w.x.y.z.
- 2 DNSBL A replies that IP address a.b.c.d does not match any entries in its list (not spam).
- 3 While waiting for a DNSBL reply about IP address w.x.y.z, the USG receives a reply from DNSBL B saying IP address a.b.c.d is in its list.
- 4 The USG immediately classifies the e-mail as spam and takes the action for spam that you defined in the anti-spam policy. In this example it was an SMTP mail and the defined action was to drop the mail. The USG does not wait for any more DNSBL replies.

29.1 Zones Overview

Set up zones to configure network security and network policies in the USG. A zone is a group of interfaces and/or VPN tunnels. The USG uses zones instead of interfaces in many security and policy settings, such as Secure Policies rules, UTM Profile, and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

Figure 304 Example: Zones



Use the **Zone** screens (see [Section 29.7.2 on page 497](#)) to manage the USG's zones.

29.1.1 What You Need to Know

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic.

Intra-zone Traffic

- Intra-zone traffic is traffic between interfaces or VPN tunnels in the same zone. For example, in [Figure 304 on page 452](#), traffic between VLAN 2 and the Ethernet is intra-zone traffic.

Inter-zone Traffic

Inter-zone traffic is traffic between interfaces or VPN tunnels in different zones. For example, in [Figure 304 on page 452](#), traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in [Figure 304 on page 452](#), traffic to or from computer **C** is extra-zone traffic.
- Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to **Any** or **All**. See the specific feature for more information.

29.1.2 The Zone Screen

The **Zone** screen provides a summary of all zones. In addition, this screen allows you to add, edit, and remove zones. To access this screen, click **Configuration > Object > Zone**.

Figure 305 Configuration > Object > Zone

The following table describes the labels in this screen.

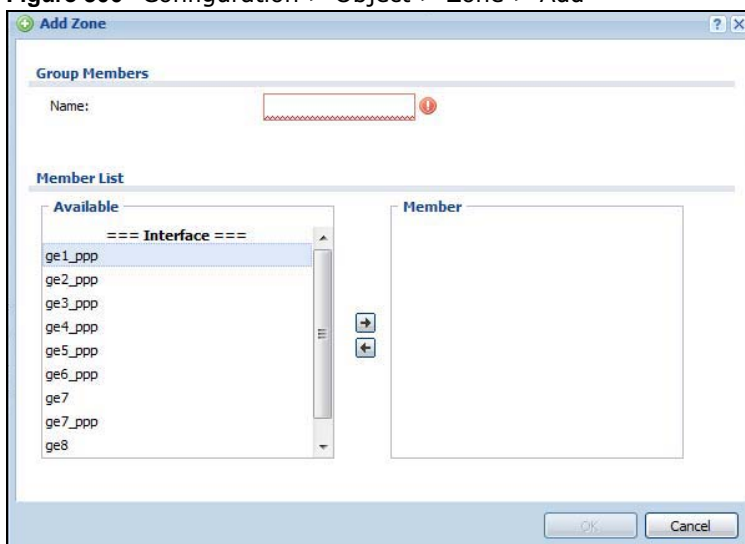
Table 176 Configuration > Object > Zone

LABEL	DESCRIPTION
User Configuration / System Default	The USG comes with pre-configured System Default zones that you cannot delete. You can create your own User Configuration zones
Add	Click this to create a new, user-configured zone.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove a user-configured trunk, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry. Click Refresh to update information in this screen.
#	This field is a sequential value, and it is not associated with any interface.
Name	This field displays the name of the zone.
Member	This field displays the names of the interfaces that belong to each zone.
Reference	This field displays the number of times an Object Reference is used in a policy.

29.1.2.1 Zone Edit

The **Zone Edit** screen allows you to add or edit a zone. To access this screen, go to the **Zone** screen (see [Section 29.7.2 on page 497](#)), and click the **Add** icon or an **Edit** icon.

Figure 306 Configuration > Object > Zone > Add



The following table describes the labels in this screen.

Table 177 Configuration > Object > Zone > Add/Edit

LABEL	DESCRIPTION
Name	For a system default zone, the name is read only. For a user-configured zone, type the name used to refer to the zone. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Member List	Available lists the interfaces and VPN tunnels that do not belong to any zone. Select the interfaces and VPN tunnels that you want to add to the zone you are editing, and click the right arrow button to add them. Member lists the interfaces and VPN tunnels that belong to the zone. Select any interfaces that you want to remove from the zone, and click the left arrow button to remove them.
OK	Click OK to save your customized settings and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

29.2 User/Group Overview

This section describes how to set up user accounts, user groups, and user settings for the USG. You can also set up rules that control when users have to log in to the USG before the USG routes traffic for them.

- The **User** screen (see [Section 29.2.2 on page 457](#)) provides a summary of all user accounts.

- The **Group** screen (see [Section 29.2.3 on page 460](#)) provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. User groups may consist of access users and other user groups. You cannot put admin users in user groups
- The **Setting** screen (see [Section 29.2.4 on page 461](#)) controls default settings, login settings, lockout settings, and other user settings for the USG. You can also use this screen to specify when users must log in to the USG before it routes traffic for them.
- The **MAC Address** screen (see [Section 29.2.5 on page 466](#)) allows you to configure the MAC addresses or OUI (Organizationally Unique Identifier) of wireless clients for MAC authentication using the local user database. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.

29.2.1 What You Need To Know

User Account

A user account defines the privileges of a user logged into the USG. User accounts are used in security policies, in addition to controlling access to configuration and services in the USG.

User Types

These are the types of user accounts the USG uses.

Table 178 Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
Admin Users		
admin	Change USG configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console
limited-admin	Look at USG configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH, Console
Access Users		
user	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
guest	Access network services	WWW
ext-user	External user account	WWW
ext-group-user	External group user account	WWW

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See [Chapter 29 on page 510](#) for more information about authentication methods.)

Ext-User Accounts

Set up an **ext-user** account if the user is authenticated by an external server and you want to set up specific policies for this user in the USG. If you do not want to set up policies for this user, you do not have to set up an **ext-user** account.

All **ext-user** users should be authenticated by an external server, such as AD, LDAP or RADIUS. If the USG tries to use the local database to authenticate an **ext-user**, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in those chapters in this guide.)

Note: If the USG tries to authenticate an **ext-user** using the local database, the attempt always fails.

Once an **ext-user** user has been authenticated, the USG tries to get the user type (see [Table 178 on page 455](#)) from the external server. If the external server does not have the information, the USG sets the user type for this session to **User**.

For the rest of the user attributes, such as reauthentication time, the USG checks the following places, in order.

- 1 User account in the remote server.
- 2 User account (Ext-User) in the USG.
- 3 Default user account for AD users (**ad-users**), LDAP users (**ldap-users**) or RADIUS users (**radius-users**) in the USG.

See [Setting up User Attributes in an External Server on page 468](#) for a list of attributes and how to set up the attributes in an external server.

Ext-Group-User Accounts

Ext-Group-User accounts work are similar to ext-user accounts but allow you to group users by the value of the group membership attribute configured for the AD or LDAP server. See [Section 29.8.5.1 on page 505](#) for more on the group membership attribute.

User Groups

User groups may consist of user accounts or other user groups. Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one.

Note: You cannot put access users and admin users in the same user group.

Note: You cannot put the default **admin** account into any user group.

The sequence of members in a user group is not important.

User Awareness

By default, users do not have to log into the USG to use the network services it provides. The USG automatically routes packets for everyone. If you want to restrict network services that certain users can use via the USG, you can require them to log in to the USG first. The USG is then 'aware' of the user who is logged in and you can create 'user-aware policies' that define what services they can use. See [Section 29.2.6 on page 467](#) for a user-aware login example.

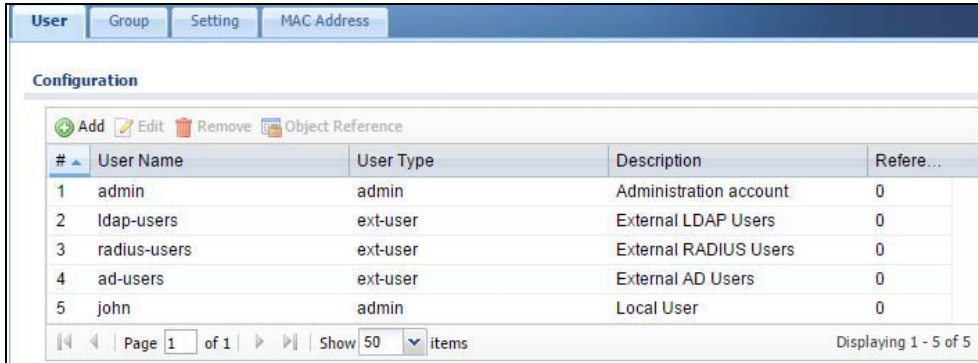
Finding Out More

- See [Section 29.2.6 on page 467](#) for some information on users who use an external authentication server in order to log in.
- The USG supports TTLS using PAP so you can use the USG's local user database to authenticate users with WPA or WPA2 instead of needing an external RADIUS server.

29.2.2 User/Group User Summary Screen

The **User** screen provides a summary of all user accounts. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group**.

Figure 307 Configuration > Object > User/Group > User



#	User Name	User Type	Description	Refere...
1	admin	admin	Administration account	0
2	ldap-users	ext-user	External LDAP Users	0
3	radius-users	ext-user	External RADIUS Users	0
4	ad-users	ext-user	External AD Users	0
5	john	admin	Local User	0

The following table describes the labels in this screen.

Table 179 Configuration > Object > User/Group > User

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific user.
User Name	This field displays the user name of each user.
User Type	This field displays the types of user accounts the USG uses: <ul style="list-style-type: none"> • admin - this user can look at and change the configuration of the USG • limited-admin - this user can look at the configuration of the USG but not to change it • user - this user has access to the USG's services and can also browse user-mode commands (CLI). • guest - this user has access to the USG's services but cannot look at the configuration • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 455 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 456 for more information about this type.
Description	This field displays the description for each user.
Reference	This displays the number of times an object reference is used in a profile.

29.2.2.1 User Add/Edit Screen

The **User Add/Edit** screen allows you to create a new user account or edit an existing one.

29.2.2.2 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]
- - [dashes]

The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not 'bob'.
- User names have to be different than user group names.
- Here are the reserved user names:
 - adm
 - admin
 - any
 - bin
 - daemon
 - debug
 - devicehaecived
 - ftp
 - games
 - halt
 - ldap-users
 - lp
 - mail
 - news
 - nobody
 - operator
 - radius-users
 - root
 - shutdown
 - sshd
 - sync
 - uucp
 - zyxel

To access this screen, go to the **User** screen (see [Section 29.2.2 on page 457](#)), and click either the **Add** icon or an **Edit** icon.

Figure 308 Configuration > Object > User/Group > User > Add

The following table describes the labels in this screen.

Table 180 Configuration > Object > User/Group > User > Add

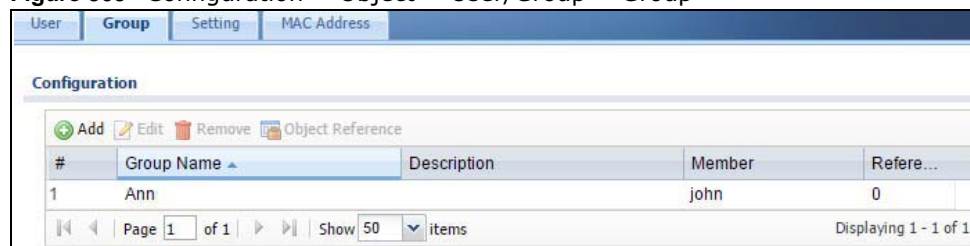
LABEL	DESCRIPTION
User Name	Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 29.2.2.2 on page 457 .
User Type	This field displays the types of user accounts the USG uses: <ul style="list-style-type: none"> • admin - this user can look at and change the configuration of the USG • limited-admin - this user can look at the configuration of the USG but not to change it • user - this user has access to the USG's services and can also browse user-mode commands (CLI). • guest - this user has access to the USG's services but cannot look at the configuration. • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 455 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 456 for more information about this type.
Password	This field is not available if you select the ext-user or ext-group-user type. Enter the password of this user account. It can consist of 4 - 31 alphanumeric characters.
Retype	This field is not available if you select the ext-user or ext-group-user type.
Group Identifier	This field is available for a ext-group-user type user account. Specify the value of the AD or LDAP server's Group Membership Attribute that identifies the group to which this user belongs.
Associated AAA Server Object	This field is available for a ext-group-user type user account. Select the AAA server to use to authenticate this account's users.
Description	Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided.
Authentication Timeout Settings	If you want the system to use default settings, select Use Default Settings . If you want to set authentication timeout to a value other than the default settings, select Use Manual Settings then fill your preferred values in the fields that follow.
Lease Time	If you select Use Default Settings in the Authentication Timeout Settings field, the default lease time is shown. If you select Use Manual Settings , you need to enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 29.2.4 on page 461), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	If you select Use Default Settings in the Authentication Timeout Settings field, the default lease time is shown. If you select Use Manual Settings , you need to type the number of minutes this user can be logged into the USG in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time , the user has no opportunity to renew the session without logging out.
Configuration Validation	Use a user account from the group specified above to test if the configuration is correct. Enter the account's user name in the User Name field and click Test .

Table 180 Configuration > Object > User/Group > User > Add (continued)

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.2.3 User/Group Group Summary Screen

User groups consist of access users and other user groups. You cannot put admin users in user groups. The **Group** screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group > Group**.

Figure 309 Configuration > Object > User/Group > Group

The following table describes the labels in this screen. See [Section 29.2.3.1 on page 460](#) for more information as well.

Table 181 Configuration > Object > User/Group > Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so. Removing a group does not remove the user accounts in the group.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific user group.
Group Name	This field displays the name of each user group.
Description	This field displays the description for each user group.
Member	This field lists the members in the user group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

29.2.3.1 Group Add/Edit Screen

The **Group Add/Edit** screen allows you to create a new user group or edit an existing one. To access this screen, go to the **Group** screen (see [Section 29.2.3 on page 460](#)), and click either the **Add** icon or an **Edit** icon.

Figure 310 Configuration > Object > User/Group > Group > Add

The following table describes the labels in this screen.

Table 182 Configuration > Object > User/Group > Group > Add

LABEL	DESCRIPTION
Name	Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names.
Description	Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	The Member list displays the names of the users and user groups that have been added to the user group. The order of members is not important. Select users and groups from the Available list that you want to be members of this group and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.2.4 User/Group Setting Screen

The **Setting** screen controls default settings, login settings, lockout settings, and other user settings for the USG. You can also use this screen to specify when users must log in to the USG before it routes traffic for them.

To access this screen, login to the Web Configurator, and click **Configuration > Object > User/Group > Setting**.

Figure 311 Configuration > Object > User/Group > Setting

User Default Setting

Default Authentication Timeout Settings

[Edit](#)

#	User Type	Lease Time	Reauthentication Time
1	admin	1440	1440
2	limited-admin	1440	1440
3	user	1440	1440
4	guest	1440	1440
5	ext-user	1440	1440
6	ext-group-user	1440	1440

Page 1 of 1 | Show 50 items | Displaying 1 - 6 of 6

Miscellaneous Settings

Allow renewing lease time automatically

Enable user idle detection

User idle timeout: (1-60 minutes)

User Logon Settings

Limit the number of simultaneous logons for administration account

Maximum number per administration account: (1-200)

Limit the number of simultaneous logons for access account

Maximum number per access account: (1-200)

User Lockout Settings

Enable logon retry limit

Maximum retry count: (1-99)

Lockout period: (1-65535 minutes)

The following table describes the labels in this screen.

Table 183 Configuration > Object > User/Group > Setting

LABEL	DESCRIPTION
User Authentication Timeout Settings	
Default Authentication Timeout Settings	These authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
#	This field is a sequential value, and it is not associated with a specific entry.

Table 183 Configuration > Object > User/Group > Setting (continued)

LABEL	DESCRIPTION
User Type	<p>These are the kinds of user account the USG supports.</p> <ul style="list-style-type: none"> • admin - this user can look at and change the configuration of the USG • limited-admin - this user can look at the configuration of the USG but not to change it • user - this user has access to the USG's services but cannot look at the configuration • guest - this user has access to the USG's services but cannot look at the configuration • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 455 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 456 for more information about this type.
Lease Time	<p>This is the default lease time in minutes for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out.</p> <p>Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 29.2.4 on page 461), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.</p>
Reauthentication Time	<p>This is the default reauthentication time in minutes for each type of user account. It defines the number of minutes the user can be logged into the USG in one session before having to log in again. Unlike Lease Time, the user has no opportunity to renew the session without logging out.</p>
Miscellaneous Settings	
Allow renewing lease time automatically	<p>Select this check box if access users can renew lease time automatically, as well as manually, simply by selecting the Updating lease time automatically check box on their screen.</p>
Enable user idle detection	<p>This is applicable for access users.</p> <p>Select this check box if you want the USG to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The USG automatically logs out the access user once the User idle timeout has been reached.</p>
User idle timeout	<p>This is applicable for access users.</p> <p>This field is effective when Enable user idle detection is checked. Type the number of minutes each access user can be logged in and idle before the USG automatically logs out the access user.</p>
User Logon Settings	
Limit the number of simultaneous logons for administration account	<p>Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses.</p>
Maximum number per administration account	<p>This field is effective when Limit ... for administration account is checked. Type the maximum number of simultaneous logins by each admin user.</p>
Limit the number of simultaneous logons for access account	<p>Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses.</p>
Maximum number per access account	<p>This field is effective when Limit ... for access account is checked. Type the maximum number of simultaneous logins by each access user.</p>

Table 183 Configuration > Object > User/Group > Setting (continued)

LABEL	DESCRIPTION
User Lockout Settings	
Enable logon retry limit	Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time.
Maximum retry count	This field is effective when Enable logon retry limit is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified lockout period . The number must be between 1 and 99.
Lockout period	This field is effective when Enable logon retry limit is checked. Type the number of minutes the user must wait to try to login again, if logon retry limit is enabled and the maximum retry count is reached. This number must be between 1 and 65,535 (about 45.5 days).
Apply	Click Apply to save the changes.
Reset	Click Reset to return the screen to its last-saved settings.

29.2.4.1 Default User Authentication Timeout Settings Edit Screens

The **Default Authentication Timeout Settings Edit** screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the **Configuration > Object > User/Group > Setting** screen (see [Section 29.2.4 on page 461](#)), and click one of the **Default Authentication Timeout Settings** section's **Edit** icons.

Figure 312 Configuration > Object > User/Group > Setting > Edit

The screenshot shows a dialog box titled "Edit User Auth Settings". It contains the following fields and values:

- User Type: admin
- Lease Time: 1440 (0-1440 minutes, 0 is unlimited)
- Reauthentication Time: 1440 (0-1440 minutes, 0 is unlimited)

At the bottom of the dialog, there are "OK" and "Cancel" buttons.

The following table describes the labels in this screen.

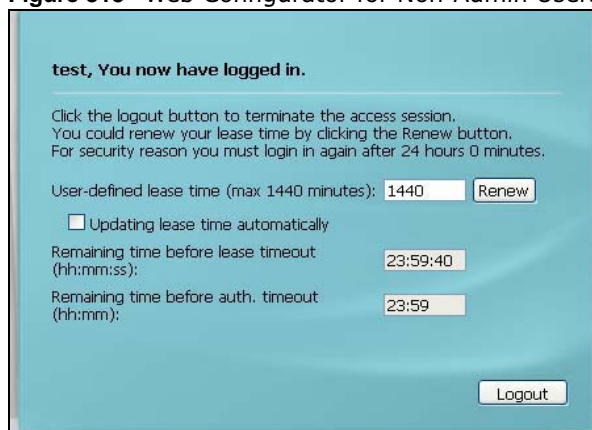
Table 184 Configuration > Object > User/Group > Setting > Edit

LABEL	DESCRIPTION
User Type	This read-only field identifies the type of user account for which you are configuring the default settings. <ul style="list-style-type: none"> • admin - this user can look at and change the configuration of the USG • limited-admin - this user can look at the configuration of the USG but not to change it. • user - this user has access to the USG's services but cannot look at the configuration. • guest - this user has access to the USG's services but cannot look at the configuration. • ext-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 455 for more information about this type. • ext-group-user - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-Group-User Accounts on page 456 for more information about this type.
Lease Time	Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the Renew button on their screen. If you allow access users to renew time automatically (see Section 29.2.4 on page 461), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires.
Reauthentication Time	Type the number of minutes this type of user account can be logged into the USG in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike Lease Time , the user has no opportunity to renew the session without logging out.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.2.4.2 User Aware Login Example

Access users cannot use the Web Configurator to browse the configuration of the USG. Instead, after access users log into the USG, the following screen appears.

Figure 313 Web Configurator for Non-Admin Users



The following table describes the labels in this screen.

Table 185 Web Configurator for Non-Admin Users

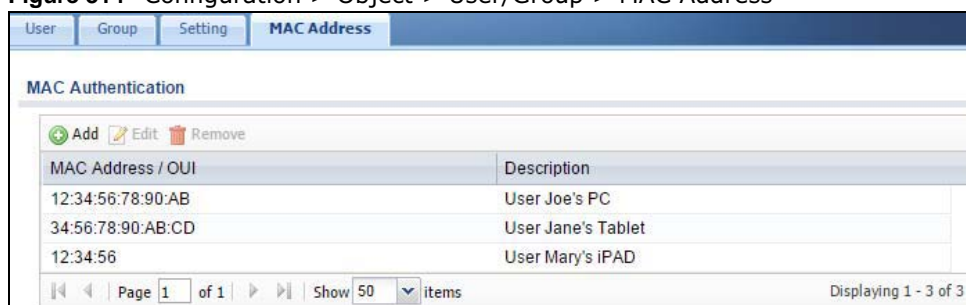
LABEL	DESCRIPTION
User-defined lease time (max ... minutes)	Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified.
Renew	Access users can click this button to reset the lease time, the amount of time remaining before the USG automatically logs them out. The USG sets this amount of time according to the <ul style="list-style-type: none"> • User-defined lease time field in this screen • Lease time field in the User Add/Edit screen (see Section 29.2.5.1 on page 467) • Lease time field in the Setting screen (see Section 29.2.4 on page 461)
Updating lease time automatically	This box appears if you checked the Allow renewing lease time automatically box in the Setting screen. (See Section 29.2.4 on page 461 .) Access users can select this check box to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the Renew button to reset the lease time.
Remaining time before lease timeout	This field displays the amount of lease time that remains, though the user might be able to reset it.
Remaining time before auth. timeout	This field displays the amount of time that remains before the USG automatically logs the access user out, regardless of the lease time.

29.2.5 User/Group MAC Address Summary Screen

This screen shows the MAC addresses of wireless clients, which can be authenticated by their MAC addresses using the local user database. Click **Configuration > Object > User/Group > MAC Address** to open this screen.

Note: You need to configure an SSID security profile's MAC authentication settings to have the AP use the USG's local database to authenticate wireless clients by their MAC addresses.

Figure 314 Configuration > Object > User/Group > MAC Address



The following table describes the labels in this screen.

Table 186 Configuration > Object > User/Group > MAC Address

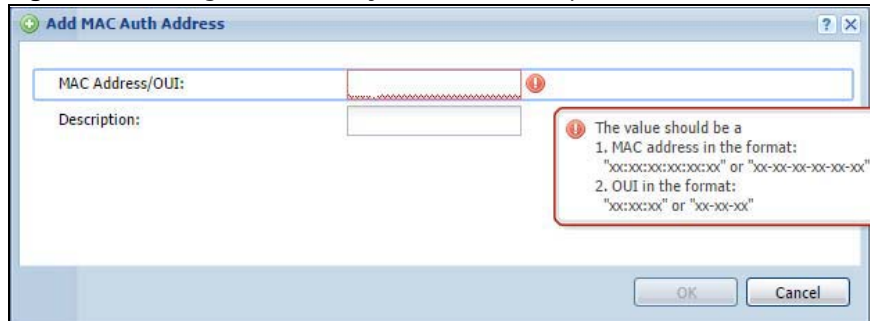
LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.

Table 186 Configuration > Object > User/Group > MAC Address (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
MAC Address/OUI	This field displays the MAC address or OUI (Organizationally Unique Identifier of computer hardware manufacturers) of wireless clients using MAC authentication with the USG local user database.
Description	This field displays a description of the device identified by the MAC address or OUI.

29.2.5.1 MAC Address Add/Edit Screen

This screen allows you to create a new allowed device or edit an existing one. To access this screen, go to the **MAC Address** screen (see [Section 29.2.5 on page 466](#)), and click either the **Add** icon or an **Edit** icon.

Figure 315 Configuration > Object > User/Group > MAC Address > Add

The following table describes the labels in this screen.

Table 187 Configuration > Object > User/Group > MAC Address > Add

LABEL	DESCRIPTION
MAC Address/OUI	Type the MAC address (six hexadecimal number pairs separated by colons or hyphens) or OUI (three hexadecimal number pairs separated by colons or hyphens) to identify specific wireless clients for MAC authentication using the USG local user database. The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.
Description	Enter an optional description of the wireless device(s) identified by the MAC or OUI. You can use up to 60 characters, punctuation marks, and spaces.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.2.6 User /Group Technical Reference

This section provides some information on users who use an external authentication server in order to log in.

Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in LDAP or RADIUS servers, use the following keywords in the user configuration file.

Table 188 LDAP/RADIUS: Keywords for User Attributes

KEYWORD	CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR
type	User Type. Possible Values: admin, limited-admin, user, guest.
leaseTime	Lease Time. Possible Values: 1-1440 (minutes).
reauthTime	Reauthentication Time. Possible Values: 1-1440 (minutes).

The following examples show you how you might set up user attributes in LDAP and RADIUS servers.

Figure 316 LDAP Example: Keywords for User Attributes

```
type: admin
leaseTime: 99
reauthTime: 199
```

Figure 317 RADIUS Example: Keywords for User Attributes

```
type=user;leaseTime=222;reauthTime=222
```

Creating a Large Number of Ext-User Accounts

If you plan to create a large number of **Ext-User** accounts, you might use CLI commands, instead of the Web Configurator, to create the accounts. Extract the user names from the LDAP or RADIUS server, and create a shell script that creates the user accounts.

29.3 AP Profile Overview

This section shows you how to configure preset profiles for the Access Points (APs) connected to your USG's wireless network.

- The **Radio** screen ([Section 29.3.1 on page 469](#)) creates radio configurations that can be used by the APs.
- The **SSID** screen ([Section 29.3.2 on page 475](#)) configures three different types of profiles for your networked APs.

29.3.0.1 What You Need To Know

The following terms and concepts may help as you read this section.

Wireless Profiles

At the heart of all wireless AP configurations on the USG are profiles. A profile represents a group of saved settings that you can use across any number of connected APs. You can set up the following wireless profile types:

- **Radio** - This profile type defines the properties of an AP's radio transmitter. You can have a maximum of 32 radio profiles on the USG.
- **SSID** - This profile type defines the properties of a single wireless network signal broadcast by an AP. Each radio on a single AP can broadcast up to 8 SSIDs. You can have a maximum of 32 SSID profiles on the USG.
- **Security** - This profile type defines the security settings used by a single SSID. It controls the encryption method required for a wireless client to associate itself with the SSID. You can have a maximum of 32 security profiles on the USG.
- **MAC Filtering** - This profile provides an additional layer of security for an SSID, allowing you to block access or allow access to that SSID based on wireless client MAC addresses. If a client's MAC address is on the list, then it is either allowed or denied, depending on how you set up the MAC Filter profile. You can have a maximum of 32 MAC filtering profiles on the USG.

SSID

The SSID (Service Set Identifier) is the name that identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. In other words, it is the name of the wireless network that clients use to connect to it.

WEP

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the AP and the wireless stations associated with it in order to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. Key differences between WPA(2) and WEP are improved data encryption and user authentication.

IEEE 802.1x

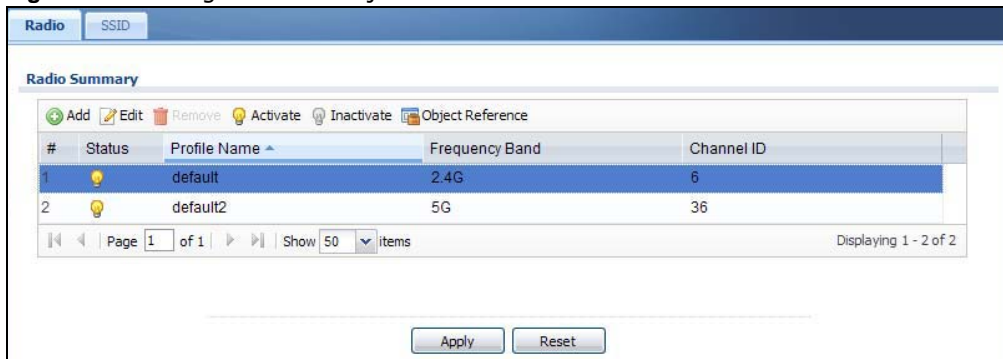
The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication is done using an external RADIUS server.

29.3.1 Radio Screen

This screen allows you to create radio profiles for the APs on your network. A radio profile is a list of settings that the built-in AP can use to configure its radio transmitters. To access this screen click **Configuration > Object > AP Profile**.

Note: You can have a maximum of 32 radio profiles on the USG.

Figure 318 Configuration > Object > AP Profile > Radio



The following table describes the labels in this screen.

Table 189 Configuration > Object > AP Profile > Radio

LABEL	DESCRIPTION
Add	Click this to add a new radio profile.
Edit	Click this to edit the selected radio profile.
Remove	Click this to remove the selected radio profile.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Object Reference	Click this to view which other objects are linked to the selected radio profile.
#	This field is a sequential value, and it is not associated with a specific profile.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the radio profile.
Frequency Band	This field indicates the frequency band which this radio profile is configured to use.
Channel ID	This field indicates the broadcast channel which this radio profile is configured to use.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

29.3.1.1 Add/Edit Radio Profile

This screen allows you to create a new radio profile or edit an existing one. To access this screen, click the **Add** button or select a radio profile from the list and click the **Edit** button.

Figure 319 Configuration > Object > AP Profile > Add/Edit Radio Profile

The following table describes the labels in this screen.

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile

LABEL	DESCRIPTION
Hide / Show Advanced Settings	Click this to hide or show the Advanced Settings in this window.
Create New Object	Select an item from this menu to create a new object of that type. Any objects created in this way are automatically linked to this radio profile.
General Settings	

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
Activate	Select this option to make this profile active.
Profile Name	Enter up to 31 alphanumeric characters to be used as this profile's name. Spaces and underscores are allowed.
802.11 Band	<p>Select the wireless band which this radio profile should use.</p> <p>2.4 GHz is the frequency used by IEEE 802.11b/g/n wireless clients.</p> <p>5 GHz is the frequency used by IEEE 802.11ac/a/n wireless clients.</p>
Channel Width	<p>Select the wireless channel bandwidth you want the AP to use.</p> <p>A standard 20 MHz channel offers transfer speeds of up to 217Mbps (2.4GHz) or 217Mbps (5GHZ) whereas a 40MHz channel uses two standard channels and offers speeds of up to 450Mbps (2.4GHz) or 450Mbps (5GHZ). An IEEE 802.11ac-specific 80MHz channel offers speeds of up to 1.3Gbps.</p> <p>40 MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A 80 MHz channel consists of two adjacent 40 MHz channels. The wireless clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Because not all devices support 40 MHz and/or 80 MHz channels, select 20/40MHz or 20/40/80MHz to allow the AP to adjust the channel bandwidth automatically.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p>
Channel Selection	<p>Select the wireless channel which this radio profile should use.</p> <p>Select DCS to have the AP automatically select the radio channel upon which it broadcasts by scanning the area around it and determining what channels are currently being used by other devices.</p> <p>Select Manual and specify the channels the AP uses.</p> <p>It is recommended that you choose the channel least in use by other APs in the region where this profile will be implemented. This will reduce the amount of interference between wireless clients and the AP to which this profile is assigned.</p> <p>Some 5 GHz channels include the label indoor use only. These are for use with an indoor AP only. Do not use them with an outdoor AP.</p> <p>Note: If you change the country code later, Channel Selection is set to Manual automatically.</p>
DCS Time Interval	<p>This field is available when you set Channel Selection to DCS.</p> <p>Enter a number of minutes. This regulates how often the USG surveys the other APs within its broadcast radius. If the channel on which it is currently broadcasting suddenly comes into use by another AP, the USG will then dynamically select the next available clean channel or a channel with lower interference.</p>
Enable DCS Client Aware	<p>This field is available when you set Channel Selection to DCS.</p> <p>Select this to have the AP wait until all connected clients have disconnected before switching channels.</p> <p>If you disable this then the AP switches channels immediately regardless of any client connections. In this instance, clients that are connected to the AP when it switches channels are dropped.</p>

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
2.4 GHz Channel Selection Method	<p>This field is available when you set Channel Selection to DCS.</p> <p>Select auto to have the AP search for available channels automatically in the 2.4 GHz band. The available channels vary depending on what you select in the 2.4 GHz Channel Deployment field.</p> <p>Select manual and specify the channels the AP uses in the 2.4 GHz band.</p>
Channel ID	<p>This field is available only when you set Channel Selection to DCS and set 2.4 GHz Channel Selection Method to manual.</p> <p>Select the check boxes of the channels that you want the AP to use.</p>
2.4 GHz Channel Deployment	<p>This field is available only when you set Channel Selection to DCS and set 2.4 GHz Channel Selection Method to auto.</p> <p>Select Three-Channel Deployment to limit channel switching to channels 1,6, and 11, the three channels that are sufficiently attenuated to have almost no impact on one another. In other words, this allows you to minimize channel interference by limiting channel-hopping to these three "safe" channels.</p> <p>Select Four-Channel Deployment to limit channel switching to four channels. Depending on the country domain, if the only allowable channels are 1-11 then the USG uses channels 1, 4, 7, 11 in this configuration; otherwise, the USG uses channels 1, 5, 9, 13 in this configuration. Four channel deployment expands your pool of possible channels while keeping the channel interference to a minimum.</p>
Enable 5 GHz DFS Aware	<p>This field is available only when you select 11a, 11a/n or 11ac in the 802.11 Band field.</p> <p>Select this if your APs are operating in an area known to have RADAR devices. This allows the device to downgrade its frequency to below 5 GHz in the event a RADAR signal is detected, thus preventing it from interfering with that signal.</p> <p>Enabling this forces the AP to select a non-DFS channel.</p>
5 GHz Channel Selection Method	This shows auto and allows the AP to search for available channels automatically in the 5 GHz band.
Advanced Settings	
Country Code	<p>Select the country where the USG is located/installed.</p> <p>The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems.</p>
Guard Interval	<p>This field is available only when the channel width is 20/40MHz or 20/40/80MHz.</p> <p>Set the guard interval for this radio profile to either short or long.</p> <p>The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the interval increases data transfer rates but also increases interference. Increasing the interval reduces data transfer rates but also reduces interference.</p>
Enable A-MPDU Aggregation	<p>Select this to enable A-MPDU aggregation.</p> <p>Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.</p>
A-MPDU Limit	Enter the maximum frame size to be aggregated.
A-MPDU Subframe	Enter the maximum number of frames to be aggregated each time.

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
Enable A-MSDU Aggregation	Select this to enable A-MSDU aggregation. Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.
A-MSDU Limit	Enter the maximum frame size to be aggregated.
RTS/CTS Threshold	Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. A high value helps save current consumption of the access point.
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.
Enable Signal Threshold	Select the check box to use the signal threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP. Clear the check box to not require wireless clients to have a minimum signal strength to connect to the AP.
Station Signal Threshold	Set a minimum client signal strength. A wireless client is allowed to connect to the AP only when its signal strength is stronger than the specified threshold. -20 dBm is the strongest signal you can require and -76 is the weakest.
Disassociate Station Threshold	Set a minimum kick-off signal strength. When a wireless client's signal strength is lower than the specified threshold, the USG disconnects the wireless client from the AP. -20 dBm is the strongest signal you can require and -90 is the weakest.
Allow Station Connection after Multiple Retries	Select this option to allow a wireless client to try to associate with the AP again after it is disconnected due to weak signal strength.
Station Retry Count	Set the maximum number of times a wireless client can attempt to re-connect to the AP.
Multicast Settings	Use this section to set a transmission mode and maximum rate for multicast traffic.
Transmission Mode	Set how the AP handles multicast traffic. Select Multicast to Unicast to broadcast wireless multicast traffic to all of the wireless clients as unicast traffic. Unicast traffic dynamically changes the data rate based on the application's bandwidth requirements. The retransmit mechanism of unicast traffic provides more reliable transmission of the multicast traffic, although it also produces duplicate packets. Select Fixed Multicast Rate to send wireless multicast traffic at a single data rate. You must know the multicast application's bandwidth requirements and set it in the following field.
Multicast Rate (Mbps)	If you set the multicast transmission mode to fixed multicast rate, set the data rate for multicast traffic here. For example, to deploy 4 Mbps video, select a fixed multicast rate higher than 4 Mbps.

Table 190 Configuration > Object > AP Profile > Add/Edit Radio Profile (continued)

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.3.2 SSID Screen

The SSID screens allow you to configure three different types of profiles for your networked APs: an SSID list, which can assign specific SSID configurations to your APs; a security list, which can assign specific encryption methods to the APs when allowing wireless clients to connect to them; and a MAC filter list, which can limit connections to an AP based on wireless clients MAC addresses.

29.3.2.1 SSID List

This screen allows you to create and manage SSID configurations that can be used by the APs. An SSID, or Service Set IDentifier, is basically the name of the wireless network to which a wireless client can connect. The SSID appears as readable text to any device capable of scanning for wireless frequencies (such as the WiFi adapter in a laptop), and is displayed as the wireless network name when a person makes a connection to it.

To access this screen click **Configuration > Object > AP Profile > SSID**.

Note: You can have a maximum of 32 SSID profiles on the USG.

Figure 320 Configuration > Object > AP Profile > SSID > SSID List

The following table describes the labels in this screen.

Table 191 Configuration > Object > AP Profile > SSID > SSID List

LABEL	DESCRIPTION
Add	Click this to add a new SSID profile.
Edit	Click this to edit the selected SSID profile.
Remove	Click this to remove the selected SSID profile.
Object Reference	Click this to view which other objects are linked to the selected SSID profile (for example, radio profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the SSID profile.
SSID	This field indicates the SSID name as it appears to wireless clients.
Security Profile	This field indicates which (if any) security profile is associated with the SSID profile.
QoS	This field indicates the QoS type associated with the SSID profile.

Table 191 Configuration > Object > AP Profile > SSID > SSID List (continued)

LABEL	DESCRIPTION
MAC Filtering Profile	This field indicates which (if any) MAC Filter Profile is associated with the SSID profile.
VLAN ID	This field indicates the VLAN ID associated with the SSID profile.

29.3.2.2 Add/Edit SSID Profile

This screen allows you to create a new SSID profile or edit an existing one. To access this screen, click the **Add** button or select an SSID profile from the list and click the **Edit** button.

Figure 321 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile

The following table describes the labels in this screen.

Table 192 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile

LABEL	DESCRIPTION
Create new Object	Select an object type from the list to create a new one associated with this SSID profile.
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
SSID	Enter the SSID name for this profile. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.
Security Profile	Select a security profile from this list to associate with this SSID. If none exist, you can use the Create new Object menu to create one. Note: It is highly recommended that you create security profiles for all of your SSIDs to enhance your network security.

Table 192 Configuration > Object > AP Profile > SSID > Add/Edit SSID Profile (continued)

LABEL	DESCRIPTION
MAC Filtering Profile	<p>Select a MAC filtering profile from the list to associate with this SSID. If none exist, you can use the Create new Object menu to create one.</p> <p>MAC filtering allows you to limit the wireless clients connecting to your network through a particular SSID by wireless client MAC addresses. Any clients that have MAC addresses not in the MAC filtering profile of allowed addresses are denied connections.</p> <p>The disable setting means no MAC filtering is used.</p>
QoS	<p>Select a Quality of Service (QoS) access category to associate with this SSID. Access categories minimize the delay of data packets across a wireless network. Certain categories, such as video or voice, are given a higher priority due to the time sensitive nature of their data packets.</p> <p>QoS access categories are as follows:</p> <p>disable: Turns off QoS for this SSID. All data packets are treated equally and not tagged with access categories.</p> <p>WMM: Enables automatic tagging of data packets. The USG assigns access categories to the SSID by examining data as it passes through it and making a best guess effort. If something looks like video traffic, for instance, it is tagged as such.</p> <p>WMM_VOICE: All wireless traffic to the SSID is tagged as voice data. This is recommended if an SSID is used for activities like placing and receiving VoIP phone calls.</p> <p>WMM_VIDEO: All wireless traffic to the SSID is tagged as video data. This is recommended for activities like video conferencing.</p> <p>WMM_BEST_EFFORT: All wireless traffic to the SSID is tagged as "best effort," meaning the data travels the best route it can without displacing higher priority traffic. This is good for activities that do not require the best bandwidth throughput, such as surfing the Internet.</p> <p>WMM_BACKGROUND: All wireless traffic to the SSID is tagged as low priority or "background traffic", meaning all other access categories take precedence over this one. If traffic from an SSID does not have strict throughput requirements, then this access category is recommended. For example, an SSID that only has network printers connected to it.</p>
VLAN ID	Enter the VLAN ID that will be used to tag all traffic originating from this SSID if the VLAN is different from the native VLAN.
Hidden SSID	<p>Select this if you want to "hide" your SSID from wireless clients. This tells any wireless clients in the vicinity of the AP using this SSID profile not to display its SSID name as a potential connection. Not all wireless clients respect this flag and display it anyway.</p> <p>When an SSID is "hidden" and a wireless client cannot see it, the only way you can connect to the SSID is by manually entering the SSID name in your wireless connection setup screen(s) (these vary by client, client connectivity software, and operating system).</p>
Enable Intra-BSS Traffic Blocking	Select this option to prevent crossover traffic from within the same SSID.
Local VAP Setting	This part of the screen only applies to USG models that have built-in wireless functionality (AP) - see Table 1 on page 18 .
VLAN Support	<p>Select On to have the USG assign the VLAN ID listed in the top part of the screen to the built-in AP.</p> <p>Select Off to have the USG ignore the VLAN ID listed in the top part of the screen. Select an Outgoing Interface to have the USG assign an IP address in the same subnet as the selected interface to the built-in AP.</p>
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

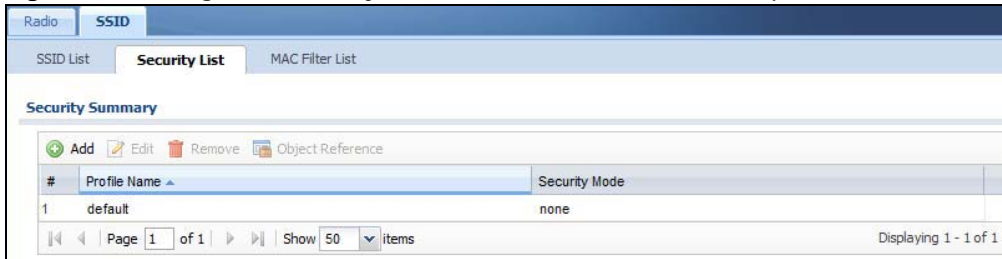
29.3.2.3 Security List

This screen allows you to manage wireless security configurations that can be used by your SSIDs. Wireless security is implemented strictly between the AP broadcasting the SSID and the stations that are connected to it.

To access this screen click **Configuration > Object > AP Profile > SSID > Security List**.

Note: You can have a maximum of 32 security profiles on the USG.

Figure 322 Configuration > Object > AP Profile > SSID > Security List



The following table describes the labels in this screen.

Table 193 Configuration > Object > AP Profile > SSID > Security List

LABEL	DESCRIPTION
Add	Click this to add a new security profile.
Edit	Click this to edit the selected security profile.
Remove	Click this to remove the selected security profile.
Object Reference	Click this to view which other objects are linked to the selected security profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the security profile.
Security Mode	This field indicates this profile's security mode (if any).

29.3.2.3.1 Add/Edit Security Profile

This screen allows you to create a new security profile or edit an existing one. To access this screen, click the **Add** button or select a security profile from the list and click the **Edit** button.

Note: This screen's options change based on the **Security Mode** selected. Only the default screen is displayed here.

Figure 323 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

The following table describes the labels in this screen.

Table 194 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Security Mode	Select a security mode from the list: none , wep , wpa2 , or wpa2-mix .
Radius Server Type	Select Internal to use the USG's internal authentication database, or External to use an external RADIUS server for authentication.

Table 194 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

LABEL	DESCRIPTION
Primary / Secondary Radius Server Activate	Select this to have the USG use the specified RADIUS server.
Radius Server IP Address	Enter the IP address of the RADIUS server to be used for authentication.
Radius Server Port	Enter the port number of the RADIUS server to be used for authentication.
Radius Server Secret	Enter the shared secret password of the RADIUS server to be used for authentication.
MAC Authentication	Select this to use an external server or the USG's local database to authenticate wireless clients by their MAC addresses. Users cannot get an IP address if the MAC authentication fails. An external server can use the wireless client's account (username/password) or Calling Station ID for MAC authentication. Configure the ones the external server uses.
Delimiter (Account)	Select the separator the external server uses for the two-character pairs within account MAC addresses.
Case (Account)	Select the case (upper or lower) the external server requires for letters in the account MAC addresses.
Delimiter (Calling Station ID)	RADIUS servers can require the MAC address in the Calling Station ID RADIUS attribute. Select the separator the external server uses for the pairs in calling station MAC addresses.
Case (Calling Station ID)	Select the case (upper or lower) the external server requires for letters in the calling station MAC addresses.
802.1X	Select this to enable 802.1x secure authentication.
Auth. Method	This field is available only when you set the RADIUS server type to Internal . Select an authentication method if you have created any in the Configuration > Object > Auth. Method screen.
ReAuthentication Timer	Enter the interval (in seconds) between authentication requests. Enter a 0 for unlimited requests.
The following fields are available if you set Security Mode to wep .	
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Authentication Type	Select a WEP authentication method. Choices are Open or Share key.
Key Length	Select the bit-length of the encryption key to be used in WEP connections. If you select WEP-64 : <ul style="list-style-type: none"> Enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each Key used. or <ul style="list-style-type: none"> Enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each Key used. If you select WEP-128 : <ul style="list-style-type: none"> Enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each Key used. or <ul style="list-style-type: none"> Enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each Key used.
Key 1~4	Based on your Key Length selection, enter the appropriate length hexadecimal or ASCII key.

Table 194 Configuration > Object > AP Profile > SSID > Security Profile > Add/Edit Security Profile

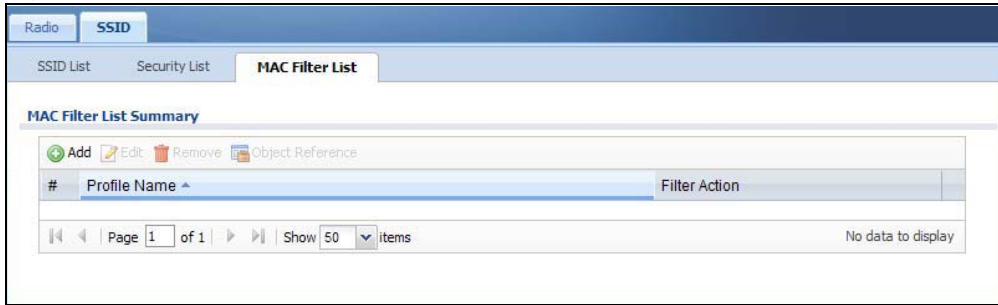
LABEL	DESCRIPTION
The following fields are available if you set Security Mode to wpa2 or wpa2-mix .	
PSK	Select this option to use a Pre-Shared Key with WPA encryption.
Pre-Shared Key	Enter a pre-shared key of between 8 and 63 case-sensitive ASCII characters (including spaces and symbols) or 64 hexadecimal characters.
Cipher Type	Select an encryption cipher type from the list. <ul style="list-style-type: none"> • auto - This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection. • tkip - This is the Temporal Key Integrity Protocol encryption method added later to the WEP encryption protocol to further secure. Not all wireless clients may support this. • aes - This is the Advanced Encryption Standard encryption method. It is a more recent development over TKIP and considerably more robust. Not all wireless clients may support this.
Idle Timeout	Enter the idle interval (in seconds) that a client can be idle before authentication is discontinued.
Group Key Update Timer	Enter the interval (in seconds) at which the AP updates the group WPA encryption key.
Pre-Authentication	This field is available only when you set Security Mode to wpa2 or wpa2-mix and enable 802.1x authentication. Enable or Disable pre-authentication to allow the AP to send authentication information to other APs on the network, allowing connected wireless clients to switch APs without having to re-authenticate their network connection.
Management Frame Protection	This field is available only when you select wpa2 or wpa2-mix in the Security Mode field and set Cipher Type to aes . Data frames in 802.11 WLANs can be encrypted and authenticated with WEP, WPA or WPA2. But 802.11 management frames, such as beacon/probe response, association request, association response, de-authentication and disassociation are always unauthenticated and unencrypted. IEEE 802.11w Protected Management Frames allows APs to use the existing security mechanisms (encryption and authentication methods defined in IEEE 802.11i WPA/WPA2) to protect management frames. This helps prevent wireless DoS attacks. Select the check box to enable management frame protection (MFP) to add security to 802.11 management frames. Select Optional if you do not require the wireless clients to support MFP. Management frames will be encrypted if the clients support MFP. Select Required and wireless clients must support MFP in order to join the AP's wireless network.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.3.2.4 MAC Filter List

This screen allows you to create and manage security configurations that can be used by your SSIDs. To access this screen click **Configuration > Object > AP Profile > SSID > MAC Filter List**.

Note: You can have a maximum of 32 MAC filtering profiles on the USG.

Figure 324 Configuration > Object > AP Profile > SSID > MAC Filter List



The following table describes the labels in this screen.

Table 195 Configuration > Object > AP Profile > SSID > MAC Filter List

LABEL	DESCRIPTION
Add	Click this to add a new MAC filtering profile.
Edit	Click this to edit the selected MAC filtering profile.
Remove	Click this to remove the selected MAC filtering profile.
Object Reference	Click this to view which other objects are linked to the selected MAC filtering profile (for example, SSID profile).
#	This field is a sequential value, and it is not associated with a specific profile.
Profile Name	This field indicates the name assigned to the MAC filtering profile.
Filter Action	This field indicates this profile's filter action (if any).

29.3.2.4.1 Add/Edit MAC Filter Profile

This screen allows you to create a new MAC filtering profile or edit an existing one. To access this screen, click the **Add** button or select a MAC filter profile from the list and click the **Edit** button.

Figure 325 SSID > MAC Filter List > Add/Edit MAC Filter Profile

The following table describes the labels in this screen.

Table 196 SSID > MAC Filter List > Add/Edit MAC Filter Profile

LABEL	DESCRIPTION
Profile Name	Enter up to 31 alphanumeric characters for the profile name. This name is only visible in the Web Configurator and is only for management purposes. Spaces and underscores are allowed.
Filter Action	Select allow to permit the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select deny to block the wireless clients with the specified MAC addresses.
Add	Click this to add a MAC address to the profile's list.
Edit	Click this to edit the selected MAC address in the profile's list.
Remove	Click this to remove the selected MAC address from the profile's list.
#	This field is a sequential value, and it is not associated with a specific profile.
MAC Address	This field specifies a MAC address associated with this profile.
Description	This field displays a description for the MAC address associated with this profile. You can click the description to make it editable. Enter up to 60 characters, spaces and underscores allowed.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.4 MON Profile

29.4.1 Overview

This screen allows you to set up monitor mode configurations that allow your connected APs to scan for other wireless devices in the vicinity.

29.4.1.1 What You Can Do in this Chapter

The **MON Profile** screen ([Section 29.4.2 on page 484](#)) creates preset monitor mode configurations that can be used by the APs.

29.4.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Active Scan

An active scan is performed when an 802.11-compatible wireless monitoring device is explicitly triggered to scan a specified channel or number of channels for other wireless devices broadcasting on the 802.11 frequencies by sending probe request frames.

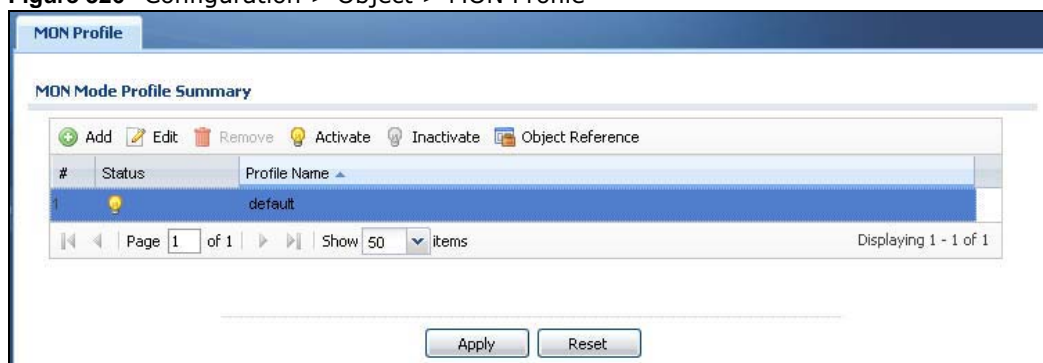
Passive Scan

A passive scan is performed when an 802.11-compatible monitoring device is set to periodically listen to a specified channel or number of channels for other wireless devices broadcasting on the 802.11 frequencies.

29.4.2 MON Profile

This screen allows you to create monitor mode configurations that can be used by the APs. To access this screen, login to the Web Configurator, and click **Configuration > Object > MON Profile**.

Figure 326 Configuration > Object > MON Profile



The following table describes the labels in this screen.

Table 197 Configuration > Object > MON Profile

LABEL	DESCRIPTION
Add	Click this to add a new monitor mode profile.
Edit	Click this to edit the selected monitor mode profile.
Remove	Click this to remove the selected monitor mode profile.
Activate	To turn on an entry, select it and click Activate .
Inactivate	To turn off an entry, select it and click Inactivate .
Object Reference	Click this to view which other objects are linked to the selected monitor mode profile (for example, an AP management profile).
#	This field is a sequential value, and it is not associated with a specific user.
Status	This icon is lit when the entry is active and dimmed when the entry is inactive.
Profile Name	This field indicates the name assigned to the monitor profile.
Apply	Click Apply to save your changes back to the USG.
Reset	Click Reset to return the screen to its last-saved settings.

29.4.2.1 Add/Edit MON Profile

This screen allows you to create a new monitor mode profile or edit an existing one. To access this screen, click the **Add** button or select an existing monitor mode profile and click the **Edit** button.

Figure 327 Configuration > Object > MON Profile > Add/Edit MON Profile

Add MON Profile

General Settings

Activate

Profile Name:

Channel dwell time: (100ms~1000ms)

Scan Channel Mode: ▼

Country Code: ▼

Set Scan Channel List (2.4 GHz)

Channel ID
<input type="checkbox"/> 1
<input type="checkbox"/> 2
<input type="checkbox"/> 3
<input type="checkbox"/> 4
<input type="checkbox"/> 5
<input type="checkbox"/> 6
<input type="checkbox"/> 7
<input type="checkbox"/> 8
<input type="checkbox"/> 9

Set Scan Channel List (5 GHz)

Channel ID
<input type="checkbox"/> 36

OK Cancel

The following table describes the labels in this screen.

Table 198 Configuration > Object > MON Profile > Add/Edit MON Profile

LABEL	DESCRIPTION
Activate	Select this to activate this monitor mode profile.
Profile Name	This field indicates the name assigned to the monitor mode profile.
Channel dwell time	Enter the interval (in milliseconds) before the AP switches to another channel for monitoring.
Scan Channel Mode	Select auto to have the AP switch to the next sequential channel once the Channel dwell time expires. Select manual to set specific channels through which to cycle sequentially when the Channel dwell time expires. Selecting this options makes the Scan Channel List options available.
Country Code	Select the country where the USG is located/installed. The available channels vary depending on the country you selected. Be sure to select the correct/same country for both radios on an AP and all connected APs, in order to prevent roaming failure and interference to other systems.

Table 198 Configuration > Object > MON Profile > Add/Edit MON Profile (continued)

LABEL	DESCRIPTION
Set Scan Channel List (2.4 GHz)	Move a channel from the Available channels column to the Channels selected column to have the APs using this profile scan that channel when Scan Channel Mode is set to manual . These channels are limited to the 2 GHz range (802.11 b/g/n).
Set Scan Channel List (5 GHz)	Move a channel from the Available channels column to the Channels selected column to have the APs using this profile scan that channel when Scan Channel Mode is set to manual . These channels are limited to the 5 GHz range (802.11 a/n).
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.5 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

- The **Address** screen ([Section 29.5.2 on page 487](#)) provides a summary of all addresses in the USG. Use the **Address Add/Edit** screen to create a new address or edit an existing one.
- Use the **Address Group** summary screen ([Section 29.5.2.2 on page 489](#)) and the **Address Group Add/Edit** screen, to maintain address groups in the USG.

29.5.1 What You Need To Know

Address objects and address groups are used in dynamic routes, security policies, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

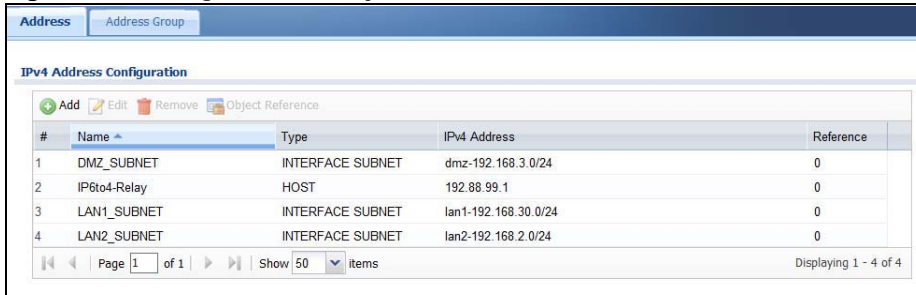
29.5.2 Address Summary Screen

The address screens are used to create, maintain, and remove addresses. There are the types of address objects.

- **HOST** - a host address is defined by an **IP Address**.
- **RANGE** - a range address is defined by a **Starting IP Address** and an **Ending IP Address**.
- **SUBNET** - a network address is defined by a **Network IP address** and **Netmask** subnet mask.

The **Address** screen provides a summary of all addresses in the USG. To access this screen, click **Configuration > Object > Address > Address**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 328 Configuration > Object > Address > Address



The following table describes the labels in this screen. See [Section 29.5.2.1 on page 488](#) for more information as well.

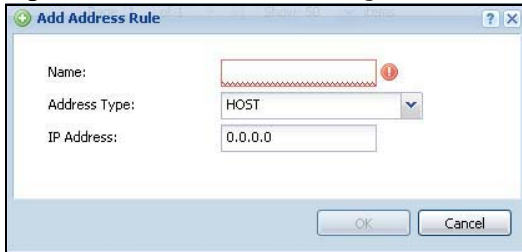
Table 199 Configuration > Object > Address > Address

LABEL	DESCRIPTION
IPv4 Address Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address.
Name	This field displays the configured name of each address object.
Type	This field displays the type of each address object. " INTERFACE " means the object uses the settings of one of the USG's interfaces.
IPv4 Address	This field displays the IPv4 addresses represented by each address object. If the object's settings are based on one of the USG's interfaces, the name of the interface displays first followed by the object's current address settings.
Reference	This displays the number of times an object reference is used in a profile.

29.5.2.1 IPv4 Address Add/Edit Screen

The **Configuration > IPv4 Address Add/Edit** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see [Section 29.5.2 on page 487](#)), and click either the **Add** icon or an **Edit** icon in the **IPv4 Address Configuration** section.

Figure 329 IPv4 Address Configuration > Add/Edit



The following table describes the labels in this screen.

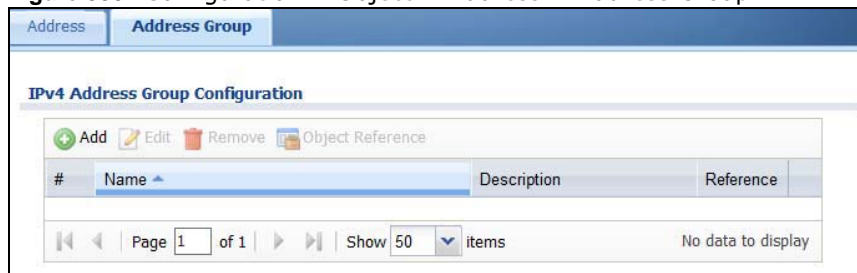
Table 200 IPv4 Address Configuration > Add/Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Address Type	Select the type of address you want to create. Choices are: HOST , RANGE , SUBNET , INTERFACE IP , INTERFACE SUBNET , and INTERFACE GATEWAY . Note: The USG automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change 1's IP address, the USG automatically updates the corresponding interface-based, LAN subnet address object.
IP Address	This field is only available if the Address Type is HOST . This field cannot be blank. Enter the IP address that this address object represents.
Starting IP Address	This field is only available if the Address Type is RANGE . This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents.
Ending IP Address	This field is only available if the Address Type is RANGE . This field cannot be blank. Enter the end of the range of IP address that this address object represents.
Network	This field is only available if the Address Type is SUBNET , in which case this field cannot be blank. Enter the IP address of the network that this address object represents.
Netmask	This field is only available if the Address Type is SUBNET , in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format.
Interface	If you selected INTERFACE IP , INTERFACE SUBNET , or INTERFACE GATEWAY as the Address Type , use this field to select the interface of the network that this address object represents.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.5.2.2 Address Group Summary Screen

The **Address Group** screen provides a summary of all address groups. To access this screen, click **Configuration > Object > Address > Address Group**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 330 Configuration > Object > Address > Address Group



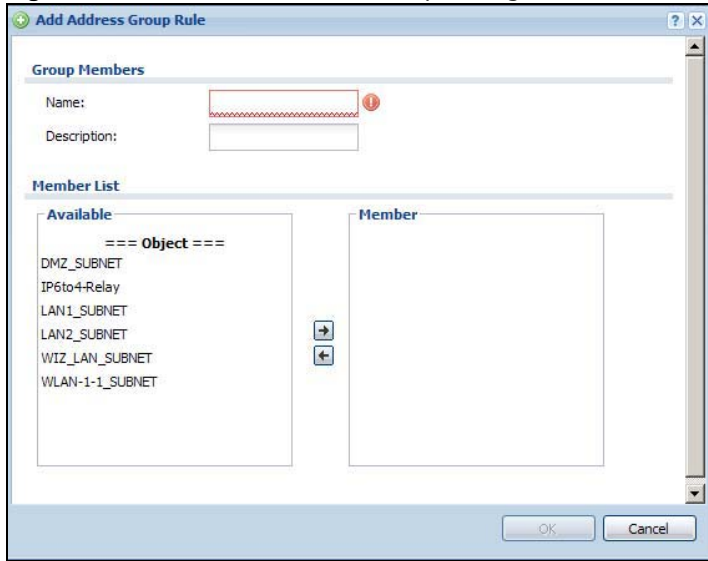
The following table describes the labels in this screen. See [Section 29.5.2.3 on page 490](#) for more information as well.

Table 201 Configuration > Object > Address > Address Group

LABEL	DESCRIPTION
IPv4 Address Group Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.
Reference	This displays the number of times an object reference is used in a profile.
IPv6 Address Group Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific address group.
Name	This field displays the name of each address group.
Description	This field displays the description of each address group, if any.

29.5.2.3 Address Group Add/Edit Screen

The **Address Group Add/Edit** screen allows you to create a new address group or edit an existing one. To access this screen, go to the **Address Group** screen (see [Section 29.5.2.2 on page 489](#)), and click either the **Add** icon or an **Edit** icon in the **IPv4 Address Group Configuration** or **IPv6 Address Group Configuration** section.

Figure 331 IPv4/IPv6 Address Group Configuration > Add

The following table describes the labels in this screen.

Table 202 IPv4/IPv6 Address Group Configuration > Add

LABEL	DESCRIPTION
Name	Enter a name for the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces.
Member List	<p>The Member list displays the names of the address and address group objects that have been added to the address group. The order of members is not important.</p> <p>Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them.</p> <p>Move any members you do not want included to the Available list.</p>
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.6 Service Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

- Use the **Service** screens ([Section 29.6.2 on page 492](#)) to view and configure the USG's list of services and their definitions.
- Use the **Service Group** screens ([Section 29.6.2 on page 492](#)) to view and configure the USG's list of service groups.

29.6.1 What You Need to Know

IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications
- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes, and security policies.

Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

29.6.2 The Service Summary Screen

The **Service** summary screen provides a summary of all services and their definitions. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the Web Configurator, and click **Configuration > Object > Service > Service**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Figure 332 Configuration > Object > Service > Service

#	Name	Content	Reference
1	AH	Protocol=51	2
2	AIM	TCP=5190	0
3	AUTH	TCP=113	0
4	Any_TCP	TCP/1-65535	0
5	Any_UDP	UDP/1-65535	0
6	BGP	TCP=179	0
7	BONJOUR	UDP=5353	0
8	BOOTP_CLIENT	UDP=68	0

The following table describes the labels in this screen.

Table 203 Configuration > Object > Service > Service

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific service.
Name	This field displays the name of each service.
Content	This field displays a description of each service.
Reference	This displays the number of times an object reference is used in a profile.

29.6.2.1 The Service Add/Edit Screen

The **Service Add/Edit** screen allows you to create a new service or edit an existing one. To access this screen, go to the **Service** screen (see [Section 29.6.2 on page 492](#)), and click either the **Add** icon or an **Edit** icon.

Figure 333 Configuration > Object > Service > Service > Edit

Add Service Rule (UDP=1538)

Name:

IP Protocol:

Starting Port: (1..65535)

Ending Port: (1..65535)

15 SNMP_TRAPS_TCP

16 SMTPS

OK Cancel

The following table describes the labels in this screen.

Table 204 Configuration > Object > Service > Service > Edit

LABEL	DESCRIPTION
Name	Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
IP Protocol	Select the protocol the service uses. Choices are: TCP , UDP , ICMP , ICMPv6 , and User Defined .
Starting Port Ending Port	This field appears if the IP Protocol is TCP or UDP . Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports.
ICMP Type	This field appears if the IP Protocol is ICMP or ICMPv6 . Select the ICMP message used by this service. This field displays the message text, not the message number.
IP Protocol Number	This field appears if the IP Protocol is User Defined . Enter the number of the next-level protocol (IP protocol). Allowed values are 1 - 255.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.6.3 The Service Group Summary Screen

The **Service Group** summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.




To access this screen, log in to the Web Configurator, and click **Configuration > Object > Service > Service Group**.

Figure 334 Configuration > Object > Service > Service Group

#	Family	Name	Description	Reference
1		CU-SEEME		0
2		DHCPv6		0
3		DNS		3
4		Default-Allow_DMZ_To_ZyWALL	System Default Allow From DMZ To ZyWALL	1
5	IPv6	Default-Allow_ICMPv6_Group	Default Allow icmpv6 to ZyWALL	1
6		Default-Allow_WAN_To_ZyWALL	System Default Allow From WAN To ZyWALL	1
7		Default-Allow_v6_DMZ_To_ZyWALL	System Default Allow IPv6 From DMZ to ZyWALL	1
8		Default-Allow_v6_WAN_To_ZyWALL	System Default Allow IPv6 Form WAN To ZyWALL	1
9	IPv6	Default-Allow_v6_any_to_ZyWALL	System Default Allow IPv6 From any To ZyWALL	1
10		IRC		0

The following table describes the labels in this screen. See [Section 29.6.3.1 on page 495](#) for more information as well.

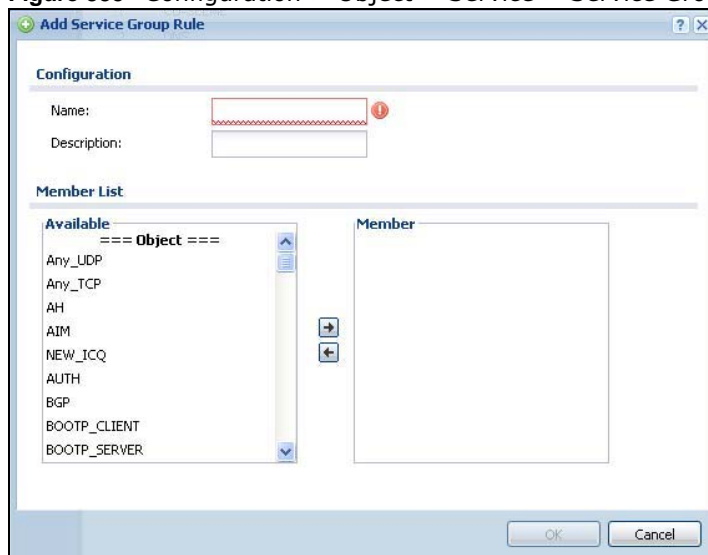
Table 205 Configuration > Object > Service > Service Group

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific service group.
Family	This field displays the Server Group supported type, which is according to your configurations in the Service Group Add/Edit screen. There are 3 types of families: <ul style="list-style-type: none">  : Supports IPv4 only  : Supports IPv6 only  : Supports both IPv4 and IPv6
Name	This field displays the name of each service group. By default, the USG uses services starting with "Default_Allow_" in the security policies to allow certain services to connect to the USG.
Description	This field displays the description of each service group, if any.
Reference	This displays the number of times an object reference is used in a profile.

29.6.3.1 The Service Group Add/Edit Screen

The **Service Group Add/Edit** screen allows you to create a new service group or edit an existing one. To access this screen, go to the **Service Group** screen (see [Section 29.6.3 on page 494](#)), and click either the **Add** icon or an **Edit** icon.

Figure 335 Configuration > Object > Service > Service Group > Edit



The following table describes the labels in this screen.

Table 206 Configuration > Object > Service > Service Group > Edit

LABEL	DESCRIPTION
Name	Enter the name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.
Member List	The Member list displays the names of the service and service group objects that have been added to the service group. The order of members is not important. Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them. Move any members you do not want included to the Available list.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.7 Schedule Overview

Use schedules to set up one-time and recurring schedules for policy routes, security policies, and content filtering. The USG supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the USG.

Note: Schedules are based on the USG's current date and time.

- Use the **Schedule** summary screen ([Section 29.7.2 on page 497](#)) to see a list of all schedules in the USG.
- Use the **One-Time Schedule Add/Edit** screen ([Section 29.7.2.1 on page 498](#)) to create or edit a one-time schedule.
- Use the **Recurring Schedule Add/Edit** screen ([Section 29.7.2.2 on page 499](#)) to create or edit a recurring schedule.
- Use the Schedule Group screen ([Section 29.7.3 on page 500](#)) to merge individual schedule objects as one object.

29.7.1 What You Need to Know

One-time Schedules

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring Schedules

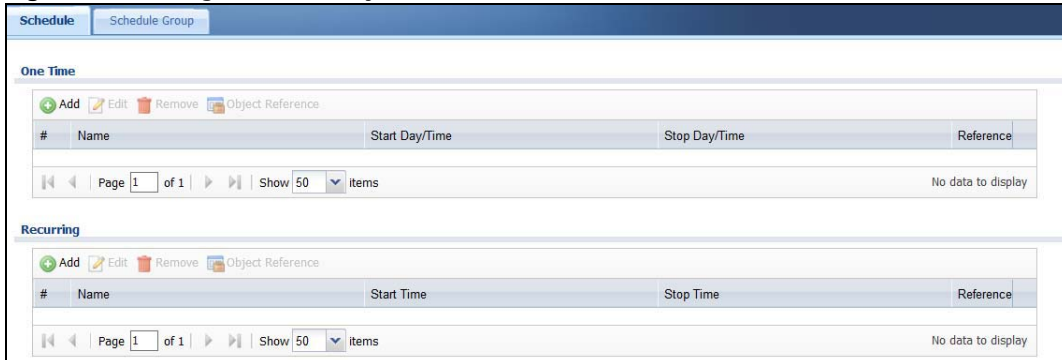
Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring

schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

29.7.2 The Schedule Summary Screen

The **Schedule** summary screen provides a summary of all schedules in the USG. To access this screen, click **Configuration > Object > Schedule**.

Figure 336 Configuration > Object > Schedule



The following table describes the labels in this screen. See [Section 29.7.2.1 on page 498](#) and [Section 29.7.2.2 on page 499](#) for more information as well.

Table 207 Configuration > Object > Schedule

LABEL	DESCRIPTION
One Time	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.
Start Day / Time	This field displays the date and time at which the schedule begins.
Stop Day / Time	This field displays the date and time at which the schedule ends.
Reference	This displays the number of times an object reference is used in a profile.
Recurring	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule, which is used to refer to the schedule.

Table 207 Configuration > Object > Schedule (continued)

LABEL	DESCRIPTION
Start Time	This field displays the time at which the schedule begins.
Stop Time	This field displays the time at which the schedule ends.
Reference	This displays the number of times an object reference is used in a profile.

29.7.2.1 The One-Time Schedule Add/Edit Screen

The **One-Time Schedule Add/Edit** screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see [Section 29.7.2 on page 497](#)), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

Figure 337 Configuration > Object > Schedule > Edit (One Time)

The following table describes the labels in this screen.

Table 208 Configuration > Object > Schedule > Edit (One Time)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartDate	Specify the year, month, and day when the schedule begins. <ul style="list-style-type: none"> • Year - 1900 - 2999 • Month - 1 - 12 • Day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StartTime	Specify the hour and minute when the schedule begins. <ul style="list-style-type: none"> • Hour - 0 - 23 • Minute - 0 - 59
StopDate	Specify the year, month, and day when the schedule ends. <ul style="list-style-type: none"> • Year - 1900 - 2999 • Month - 1 - 12 • Day - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)
StopTime	Specify the hour and minute when the schedule ends. <ul style="list-style-type: none"> • Hour - 0 - 23 • Minute - 0 - 59

Table 208 Configuration > Object > Schedule > Edit (One Time) (continued)

LABEL	DESCRIPTION
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.7.2.2 The Recurring Schedule Add/Edit Screen

The **Recurring Schedule Add/Edit** screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see [Section 29.7.2 on page 497](#)), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

Figure 338 Configuration > Object > Schedule > Edit (Recurring)

The **Year**, **Month**, and **Day** columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

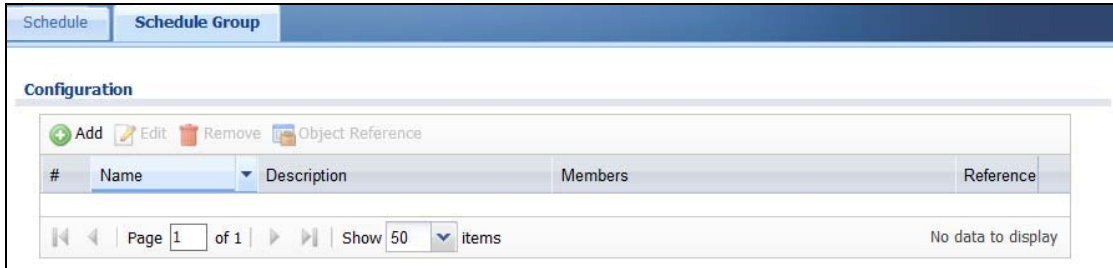
Table 209 Configuration > Object > Schedule > Edit (Recurring)

LABEL	DESCRIPTION
Configuration	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Date Time	
StartTime	Specify the hour and minute when the schedule begins each day. <ul style="list-style-type: none"> • Hour - 0 - 23 • Minute - 0 - 59
StopTime	Specify the hour and minute when the schedule ends each day. <ul style="list-style-type: none"> • Hour - 0 - 23 • Minute - 0 - 59
Weekly	
Week Days	Select each day of the week the recurring schedule is effective.
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.7.3 The Schedule Group Screen

The **Schedule Group** summary screen provides a summary of all groups of schedules in the USG. To access this screen, click **Configuration > Object > Schedule > Group**.

Figure 339 Configuration > Object > Schedule > Schedule Group



The following table describes the fields in the above screen.

Table 210 Configuration > Object > Schedule > Schedule Group

LABEL	DESCRIPTION
Configuration	
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object Reference	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific schedule.
Name	This field displays the name of the schedule group, which is used to refer to the schedule.
Description	This field displays the decription of the schedule group.
Members	This field lists the members in the schedule group. Each member is separated by a comma.
Reference	This displays the number of times an object reference is used in a profile.

29.7.3.1 The Schedule Group Add/Edit Screen

The **Schedule Group Add/Edit** screen allows you to define a schedule group or edit an existing one. To access this screen, go to the **Schedule** screen (see), and click either the **Add** icon or an **Edit** icon in the **Schedule Group** section.

Figure 340 Configuration > Schedule > Schedule Group > Add

The following table describes the fields in the above screen.

Table 211 Configuration > Schedule > Schedule Group > Add

LABEL	DESCRIPTION
Group Members	
Name	Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Description	Enter a description of the service group, if any. You can use up to 60 printable ASCII characters.
Member List	<p>The Member list displays the names of the service and service group objects that have been added to the service group. The order of members is not important.</p> <p>Select items from the Available list that you want to be members and move them to the Member list. You can double-click a single entry to move it or use the [Shift] or [Ctrl] key to select multiple entries and use the arrow button to move them.</p> <p>Move any members you do not want included to the Available list.</p>
OK	Click OK to save your changes back to the USG.
Cancel	Click Cancel to exit this screen without saving your changes.

29.8 AAA Server Overview

You can use a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a Active Directory, LDAP, or RADIUS server. Use the **AAA Server** screens to create and manage objects that contain settings for using AAA servers. You use

AAA server objects in configuring ext-group-user user objects and authentication method objects (see [Chapter 29 on page 510](#)).

29.8.1 Directory Service (AD/LDAP)

LDAP/AD allows a client (the USG) to connect to a server to retrieve information from a directory. A network example is shown next.

Figure 341 Example: Directory Service Client and Server



The following describes the user authentication procedure via an LDAP/AD server.

- 1 A user logs in with a user name and password pair.
- 2 The USG tries to bind (or log in) to the LDAP/AD server.
- 3 When the binding process is successful, the USG checks the user information in the directory against the user name and password pair.
- 4 If it matches, the user is allowed access. Otherwise, access is blocked.

29.8.2 RADIUS Server

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

Figure 342 RADIUS Server Network Example



29.8.3 ASAS

ASAS (Authenex Strong Authentication System) is a RADIUS server that works with the One-Time Password (OTP) feature. Purchase a USG OTP package in order to use this feature. The package

contains server software and physical OTP tokens (PIN generators). Do the following to use OTP. See the documentation included on the ASAS' CD for details.

- 1 Install the ASAS server software on a computer.
- 2 Create user accounts on the USG and in the ASAS server.
- 3 Import each token's database file (located on the included CD) into the server.
- 4 Assign users to OTP tokens (on the ASAS server).
- 5 Configure the ASAS as a RADIUS server in the USG's **Configuration > Object > AAA Server** screens.
- 6 Give the OTP tokens to (local or remote) users.
 - Use the **Configuration > Object > AAA Server > Active Directory** (or **LDAP**) screens ([Section 29.8.5 on page 504](#)) to configure Active Directory or LDAP server objects.
 - Use the **Configuration > Object > AAA Server > RADIUS** screen ([Section 29.8.2 on page 502](#)) to configure the default external RADIUS server to use for user authentication.

29.8.4 What You Need To Know

AAA Servers Supported by the USG

The following lists the types of authentication server the USG supports.

- Local user database

The USG uses the built-in local user database to authenticate administrative users logging into the USG's Web Configurator or network access users logging into the network through the USG. You can also use the local user database to authenticate VPN users.
- Directory Service (LDAP/AD)

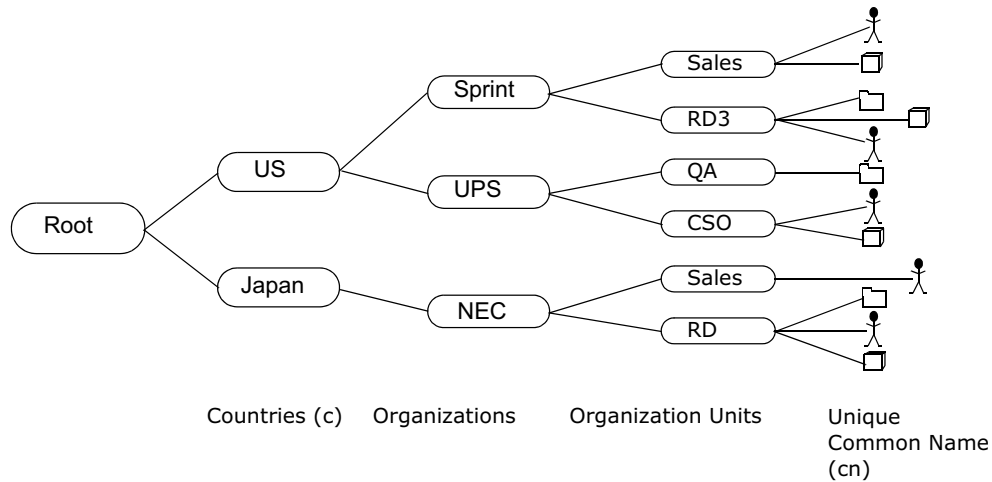
LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.
- RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

Directory Structure

The directory entries are arranged in a hierarchical order much like a tree structure. Normally, the directory structure reflects the geographical or organizational boundaries. The following figure shows a basic directory structure branching from countries to organizations to organizational units to individuals.

Figure 343 Basic Directory Structure



Distinguished Name (DN)

A DN uniquely identifies an entry in a directory. A DN consists of attribute-value pairs separated by commas. The leftmost attribute is the Relative Distinguished Name (RDN). This provides a unique name for entries that have the same "parent DN" ("cn=domain1.com, ou=Sales, o=MyCompany" in the following examples).

```
cn=domain1.com, ou = Sales, o=MyCompany, c=US
cn=domain1.com, ou = Sales, o=MyCompany, c=JP
```

Base DN

A base DN specifies a directory. A base DN usually contains information such as the name of an organization, a domain name and/or country. For example, o=MyCompany, c=UK where o means organization and c means country.

Bind DN

A bind DN is used to authenticate with an LDAP/AD server. For example a bind DN of cn=zywallAdmin allows the USG to log into the LDAP/AD server using the user name of zywallAdmin. The bind DN is used in conjunction with a bind password. When a bind DN is not specified, the USG will try to log in as an anonymous user. If the bind password is incorrect, the login will fail.

29.8.5 Active Directory or LDAP Server Summary

Use the **Active Directory** or **LDAP** screen to manage the list of AD or LDAP servers the USG can use in authenticating users.

Click **Configuration > Object > AAA Server > Active Directory** (or **LDAP**) to display the **Active Directory** (or **LDAP**) screen.

Figure 344 Configuration > Object > AAA Server > Active Directory (or LDAP)

The following table describes the labels in this screen.

Table 212 Configuration > Object > AAA Server > Active Directory (or LDAP)

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific AD or LDAP server.
Name	This field displays the name of the Active Directory.
Server Address	This is the address of the AD or LDAP server.
Base DN	This specifies a directory. For example, <code>o=ZYXEL, c=US</code> .

29.8.5.1 Adding an Active Directory or LDAP Server

Click **Object > AAA Server > Active Directory (or LDAP)** to display the **Active Directory (or LDAP)** screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 345 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add

Add Active Directory

General Settings

Name:

Description: (Optional)

Server Settings

Server Address: (IP or FQDN)

Backup Server Address: (IP or FQDN)(Optional)

Port: (1-65535)

Base DN: (1-65535)

Use SSL

Search time limit: (1-300 seconds)

Case-sensitive User Names i

Server Authentication

Bind DN:

Password:

Retype to Confirm:

User Login Settings

Login Name Attribute:

Alternative Login Name Attribute: (Optional)

Group Membership Attribute:

Domain Authentication for MSChap

Enable

User Name: Must be a user who has rights to add a machine to the domain.

User Password:

Retype to Confirm:

Realm:

NetBIOS Name: (Optional)

Configuration Validation

Please enter an existing user account in this server to validate the above settings.

Username:

The following table describes the labels in this screen.

Table 213 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumeric characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the AD or LDAP server.
Backup Server Address	If the AD or LDAP server has a backup server, enter its address here.
Port	Specify the port number on the AD or LDAP server to which the USG sends authentication requests. Enter a number between 1 and 65535. This port number should be the same on all AD or LDAP server(s) in this group.
Base DN	Specify the directory (up to 127 alphanumeric characters). For example, o=ZyXEL, c=US. This is only for LDAP .
Use SSL	Select Use SSL to establish a secure connection to the AD or LDAP server(s).
Search time limit	Specify the timeout period (between 1 and 300 seconds) before the USG disconnects from the AD or LDAP server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the AD or LDAP server(s) or the AD or LDAP server(s) is down.
Case-sensitive User Names	Select this if the server checks the case of the usernames.
Bind DN	Specify the bind DN for logging into the AD or LDAP server. Enter up to 127 alphanumeric characters. For example, cn=zywallAdmin specifies zywallAdmin as the user name.
Password	If required, enter the password (up to 15 alphanumeric characters) for the USG to bind (or log in) to the AD or LDAP server.
Retype to Confirm	Retype your new password for confirmation.
Login Name Attribute	Enter the type of identifier the users are to use to log in. For example "name" or "e-mail address".
Alternative Login Name Attribute	If there is a second type of identifier that the users can use to log in, enter it here. For example "name" or "e-mail address".
Group Membership Attribute	An AD or LDAP server defines attributes for its accounts. Enter the name of the attribute that the USG is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
Domain Authentication for MSChap	Select the Enable checkbox to enable domain authentication for MSChap. This is only for Active Directory .
User Name	Enter the user name for the user who has rights to add a machine to the domain. This is only for Active Directory .
User Password	Enter the password for the associated user name. This is only for Active Directory .

Table 213 Configuration > Object > AAA Server > Active Directory (or LDAP) > Add (continued)

LABEL	DESCRIPTION
Retype to Confirm	Retype your new password for confirmation. This is only for Active Directory .
Realm	Enter the realm FQDN. This is only for Active Directory .
NetBIOS Name	Type the NetBIOS name. This field is optional. NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN which allows local computers to find computers on the remote network and vice versa.
Configuration Validation	Use a user account from the server specified above to test if the configuration is correct. Enter the account's user name in the Username field and click Test .
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

29.8.6 RADIUS Server Summary

Use the **RADIUS** screen to manage the list of RADIUS servers the USG can use in authenticating users.

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen.

Figure 346 Configuration > Object > AAA Server > RADIUS

The following table describes the labels in this screen.

Table 214 Configuration > Object > AAA Server > RADIUS

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the index number.
Name	This is the name of the RADIUS server entry.
Server Address	This is the address of the AD or LDAP server.

29.8.6.1 Adding a RADIUS Server

Click **Configuration > Object > AAA Server > RADIUS** to display the **RADIUS** screen. Click the **Add** icon or an **Edit** icon to display the following screen. Use this screen to create a new AD or LDAP entry or edit an existing one.

Figure 347 Configuration > Object > AAA Server > RADIUS > Add

The following table describes the labels in this screen.

Table 215 Configuration > Object > AAA Server > RADIUS > Add

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 63 alphanumeric characters) for identification purposes.
Description	Enter the description of each server, if any. You can use up to 60 printable ASCII characters.
Server Address	Enter the address of the RADIUS server.
Authentication Port	Specify the port number on the RADIUS server to which the USG sends authentication requests. Enter a number between 1 and 65535.
Backup Server Address	If the RADIUS server has a backup server, enter its address here.
Backup Authentication Port	Specify the port number on the RADIUS server to which the USG sends authentication requests. Enter a number between 1 and 65535.

Table 215 Configuration > Object > AAA Server > RADIUS > Add (continued)

LABEL	DESCRIPTION
Timeout	Specify the timeout period (between 1 and 300 seconds) before the USG disconnects from the RADIUS server. In this case, user authentication fails. Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down.
NAS IP Address	Type the IP address of the NAS (Network Access Server).
Case-sensitive User Names	Select this if you want configure your username as case-sensitive.
Key	Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the USG. The key is not sent over the network. This key must be the same on the external authentication server and the USG.
Group Membership Attribute	A RADIUS server defines attributes for its accounts. Select the name and number of the attribute that the USG is to check to determine to which group a user belongs. If it does not display, select user-defined and specify the attribute's number. This attribute's value is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values. For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create a ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management".
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

29.9 Auth. Method Overview

Authentication method objects set how the USG authenticates wireless, HTTP/HTTPS clients, and peer IPsec routers (extended authentication) clients. Configure authentication method objects to have the USG use the local user database, and/or the authentication servers and authentication server groups specified by AAA server objects. By default, user accounts created and stored on the USG are authenticated locally.

- Use the **Configuration > Object > Auth. Method** screens ([Section 29.9.3 on page 511](#)) to create and manage authentication method objects.

29.9.1 Before You Begin

Configure AAA server objects before you configure authentication method objects.

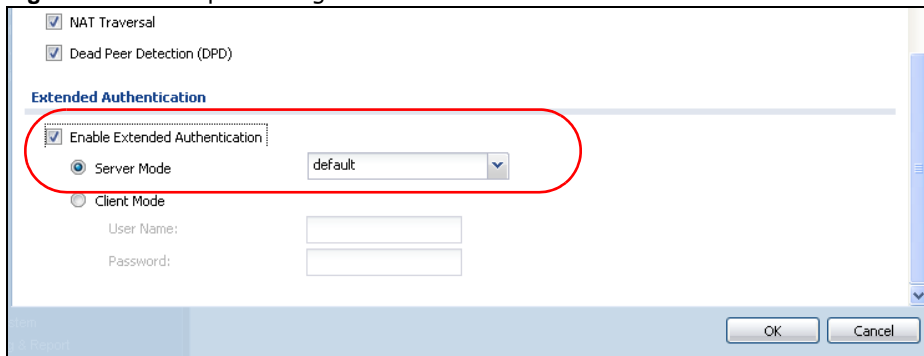
29.9.2 Example: Selecting a VPN Authentication Method

After you set up an authentication method object in the **Auth. Method** screens, you can use it in the **VPN Gateway** screen to authenticate VPN users for establishing a VPN connection. Refer to the chapter on VPN for more information.

Follow the steps below to specify the authentication method for a VPN connection.

- 1 Access the **Configuration > VPN > IPSec VPN > VPN Gateway > Edit** screen.
- 2 Click **Show Advance Setting** and select **Enable Extended Authentication**.
- 3 Select **Server Mode** and select an authentication method object from the drop-down list box.
- 4 Click **OK** to save the settings.

Figure 348 Example: Using Authentication Method in VPN

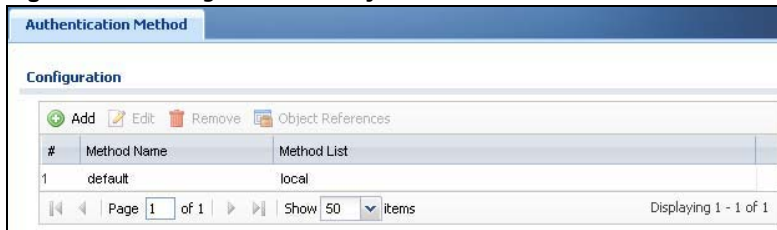


29.9.3 Authentication Method Objects

Click **Configuration > Object > Auth. Method** to display the screen as shown.

Note: You can create up to 16 authentication method objects.

Figure 349 Configuration > Object > Auth. Method



The following table describes the labels in this screen.

Table 216 Configuration > Object > Auth. Method

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the index number.
Method Name	This field displays a descriptive name for identification purposes.
Method List	This field displays the authentication method(s) for this entry.

29.9.3.1 Creating an Authentication Method Object

Follow the steps below to create an authentication method object.

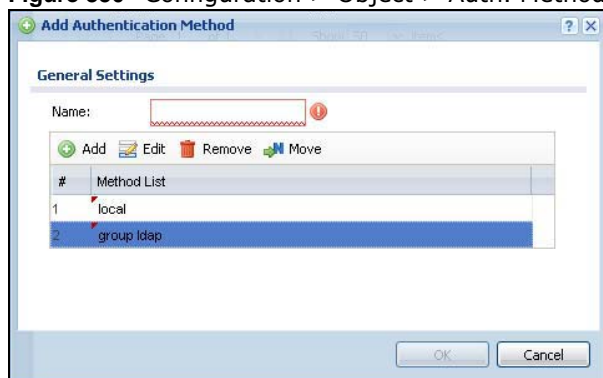
- 1 Click **Configuration > Object > Auth. Method**.
- 2 Click **Add**.
- 3 Specify a descriptive name for identification purposes in the **Name** field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".
- 4 Click **Add** to insert an authentication method in the table.
- 5 Select a server object from the **Method List** drop-down list box.
- 6 You can add up to four server objects to the table. The ordering of the **Method List** column is important. The USG authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

If two accounts with the same username exist on two authentication servers you specify, the USG does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.

Note: You can NOT select two server objects of the same type.

- 7 Click **OK** to save the settings or click **Cancel** to discard all changes and return to the previous screen.

Figure 350 Configuration > Object > Auth. Method > Add



The following table describes the labels in this screen.

Table 217 Configuration > Object > Auth. Method > Add

LABEL	DESCRIPTION
Name	Specify a descriptive name for identification purposes. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, "My_Device".
Add	Click this to create a new entry. Select an entry and click Add to create a new entry after the selected entry.
Edit	Double-click an entry or select it and click Edit to open a screen where you can modify the entry's settings.

Table 217 Configuration > Object > Auth. Method > Add (continued)

LABEL	DESCRIPTION
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Move	To change a method's position in the numbered list, select the method and click Move to display a field to type a number for where you want to put it and press [ENTER] to move the rule to the number that you typed. The ordering of your methods is important as USG authenticates the users using the authentication methods in the order they appear in this screen.
#	This field displays the index number.
Method List	Select a server object from the drop-down list box. You can create a server object in the AAA Server screen. The USG authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen. If two accounts with the same username exist on two authentication servers you specify, the USG does not continue the search on the second authentication server when you enter the username and password that doesn't match the one on the first authentication server.
OK	Click OK to save the changes.
Cancel	Click Cancel to discard the changes.

29.10 Certificate Overview

The USG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

- Use the **My Certificates** screens (see [Section 29.10.3 on page 516](#) to [Section 29.10.3.3 on page 522](#)) to generate and export self-signed certificates or certification requests and import the CA-signed certificates.
- Use the **Trusted Certificates** screens (see [Section 29.10.4 on page 523](#) to [Section 29.10.4.2 on page 527](#)) to save CA certificates and trusted remote host certificates to the USG. The USG trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

29.10.1 What You Need to Know

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

- 1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
- 2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
- 3 Tim uses his private key to sign the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).
- 5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The USG uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The USG does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The USG can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The USG only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Self-signed Certificates

You can have the USG act as a certification authority and sign its own certificates.

Factory Default Certificate

The USG generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The USG currently allows the importation of a PKCS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the USG.

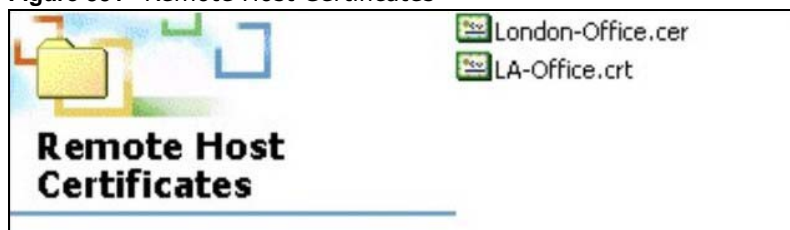
Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

29.10.2 Verifying a Certificate

Before you import a trusted certificate into the USG, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

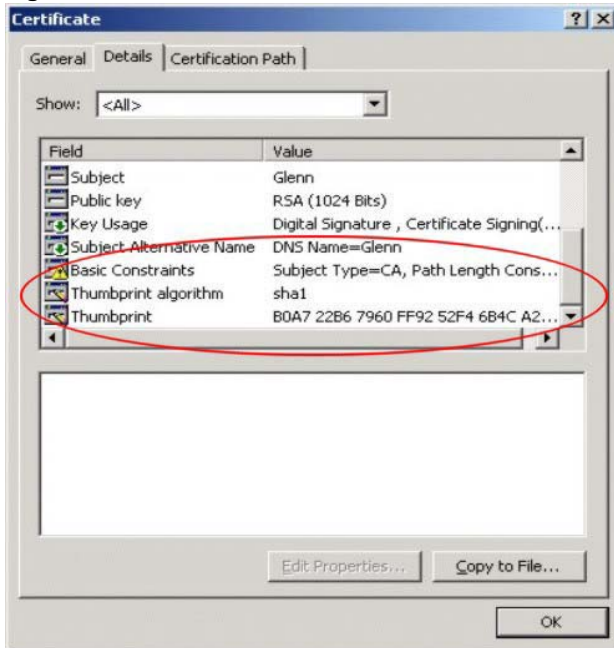
- 1 Browse to where you have the certificate saved on your computer.
- 2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 351 Remote Host Certificates



- 3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 352 Certificate Details

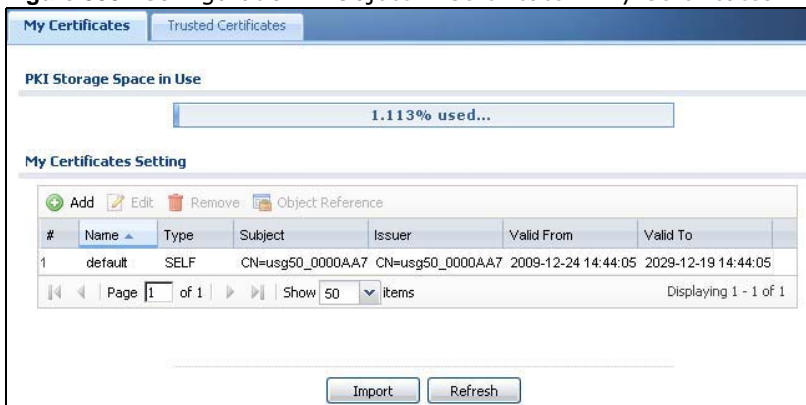


- 4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

29.10.3 The My Certificates Screen

Click **Configuration > Object > Certificate > My Certificates** to open the **My Certificates** screen. This is the USG's summary list of certificates and certification requests.

Figure 353 Configuration > Object > Certificate > My Certificates



The following table describes the labels in this screen.

Table 218 Configuration > Object > Certificate > My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the USG's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Add	Click this to go to the screen where you can have the USG generate a certificate or a certification request.
Edit	Double-click an entry or select it and click Edit to open a screen with an in-depth list of information about the certificate.
Remove	The USG keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object References	You cannot delete certificates that any of the USG's features are configured to use. Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request. SELF represents a self-signed certificate. CERT represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click Import to open a screen where you can save a certificate to the USG.
Refresh	Click Refresh to display the current validity status of the certificates.

29.10.3.1 The My Certificates Add Screen

Click **Configuration > Object > Certificate > My Certificates** and then the **Add** icon to open the **My Certificates Add** screen. Use this screen to have the USG create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

Figure 354 Configuration > Object > Certificate > My Certificates > Add

The following table describes the labels in this screen.

Table 219 Configuration > Object > Certificate > My Certificates > Add

LABEL	DESCRIPTION
Name	Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#\$%^&()_+[]{}',.- characters.
Subject Information	<p>Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although you must specify a Host IP Address, Host IPv6 Address, Host Domain Name, or E-Mail. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.</p> <p>Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string.</p> <p>A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.</p> <p>An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.</p>
Organizational Unit	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.

Table 219 Configuration > Object > Certificate > My Certificates > Add (continued)

LABEL	DESCRIPTION
Organization	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Town (City)	Identify the town or city where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
State, (Province)	Identify the state or province where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Country	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
Key Type	Select RSA to use the Rivest, Shamir and Adleman public-key algorithm. Select DSA to use the Digital Signature Algorithm public-key algorithm.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Extended Key Usage	
Server Authentication	Select this to have USG generate and store a request for server authentication certificate.
Client Authentication	Select this to have USG generate and store a request for client authentication certificate.
IKE Intermediate	Select this to have USG generate and store a request for IKE Intermediate authentication certificate.
Create a self-signed certificate	Select this to have the USG generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select this to have the USG generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the My Certificate Details screen (see Section 29.10.3.2 on page 520) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select this to have the USG generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the Trusted Certificates screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the Reference Number and Key if the certification authority requires them.
OK	Click OK to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return to the My Certificates screen.

If you configured the **My Certificate Create** screen to have the USG enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the USG to enroll a certificate online.

The following table describes the labels in this screen.

Table 220 Configuration > Object > Certificate > My Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#\$\$%^&()_+[]{}',.- characters.
Certification Path	This field displays for a certificate, not a certification request. Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The USG does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the USG.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), State (ST), and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same as the Subject Name field. "none" displays for a certification request.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The USG uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. "none" displays for a certification request.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the USG uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request.

Table 220 Configuration > Object > Certificate > My Certificates > Edit (continued)

LABEL	DESCRIPTION
MD5 Fingerprint	This is the certificate's message digest that the USG calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the USG calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate Only	Use this button to save a copy of the certificate without its private key. Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
Password	If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device.
Export Certificate with Private Key	Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
OK	Click OK to save your changes back to the USG. You can only change the name.
Cancel	Click Cancel to quit and return to the My Certificates screen.

29.10.3.3 The My Certificates Import Screen

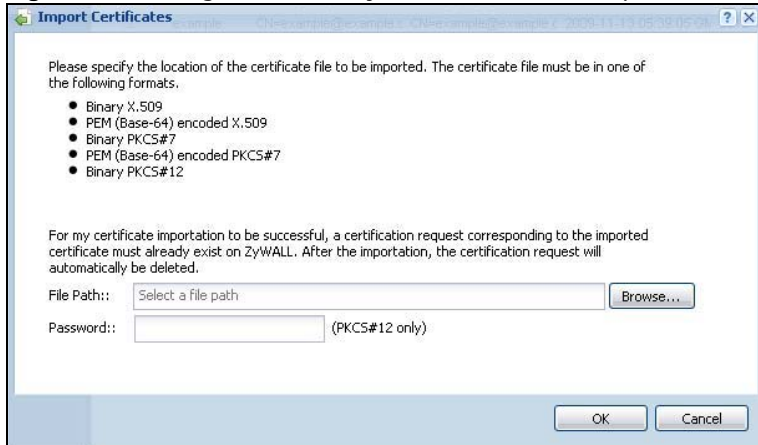
Click **Configuration > Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the USG.

Note: You can import a certificate that matches a corresponding certification request that was generated by the USG. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 356 Configuration > Object > Certificate > My Certificates > Import



The following table describes the labels in this screen.

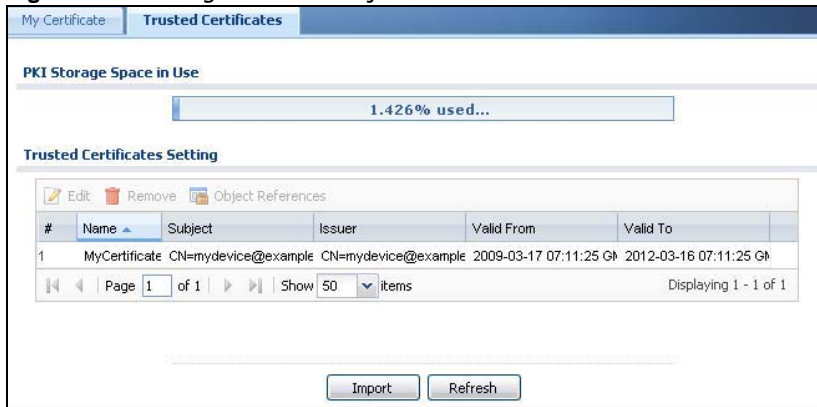
Table 221 Configuration > Object > Certificate > My Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the USG.
Browse	Click Browse to find the certificate file you want to upload.
Password	This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported.
OK	Click OK to save the certificate on the USG.
Cancel	Click Cancel to quit and return to the My Certificates screen.

29.10.4 The Trusted Certificates Screen

Click **Configuration > Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the USG to accept as trusted. The USG also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

Figure 357 Configuration > Object > Certificate > Trusted Certificates



The following table describes the labels in this screen.

Table 222 Configuration > Object > Certificate > Trusted Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the USG's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates.
Edit	Double-click an entry or select it and click Edit to open a screen with an in-depth list of information about the certificate.
Remove	The USG keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates. To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so. Subsequent certificates move up by one when you take this action.
Object References	You cannot delete certificates that any of the USG's features are configured to use. Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired.
Import	Click Import to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the USG.
Refresh	Click this button to display the current validity status of the certificates.

29.10.4.1 The Trusted Certificates Edit Screen

Click **Configuration > Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the USG to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 358 Configuration > Object > Certificate > Trusted Certificates > Edit

Edit Trusted Certificates

Configuration

Name:

Certification Path

Certificate Validation

Enable X.509v3 CRL Distribution Points and OCSP checking

OCSP Server

URL:

ID:

Password:

LDAP Server

Address: Port:

ID:

Password:

Certificate Information

Type: Self-signed X.509 Certificate

Version: V3

Serial Number: 1237273885

Subject: CN=mydevice@example.com

Issuer: CN=mydevice@example.com

Signature Algorithm: rsa-pkcs1-sha1

Valid From: 2009-03-17 07:11:25 GMT

Valid To: 2012-03-16 07:11:25 GMT

Key Algorithm: rsaEncryption (512 bits)

Subject Alternative Name: mydevice@example.com

Key Usage: DigitalSignature, KeyEncipherment, KeyCertSign

Basic Constraint: Subject Type=CA, Path Length Constraint=1

MD5 Fingerprint: 78:34:e2:25:e3:79:92:e2:b6:33:5f:a9:17:be:72:4f

SHA1 Fingerprint: ef:07:15:b5:e7:22:93:8b:1e:a7:e9:8f:cb:06:4c:04:f4:68:9c:e2

Certificate

-----BEGIN X509 CERTIFICATE-----
MIIBeTCCASOgAwIBAgIEsb9NHTANBgkqhkiG9w0BAQUFADAARMR0wGwYDVQQDDBRB
eWRldmJ2UbleGFicGxLmNvbTAeFw0wOTAzMjcwNzExMjYwMDAwMTYwNzEx
MjYwMDAwMDAwMFoGZmVzZGVzaW50ZGV4YVw1wG9uY290MFwwDQYJKoZIhvcN

The following table describes the labels in this screen.

Table 223 Configuration > Object > Certificate > Trusted Certificates > Edit

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#\$\$%^&()_+[]{}',.- characters.
Certification Path	Click the Refresh button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The USG does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Enable X.509v3 CRL Distribution Points and OCSP checking	Select this check box to turn on/off certificate revocation. When it is turned on, the USG validates a certificate by getting Certificate Revocation List (CRL) through HTTP or LDAP (can be configured after selecting the LDAP Server check box) and online responder (can be configured after selecting the OCSP Server check box).
OCSP Server	Select this check box if the directory server uses OCSP (Online Certificate Status Protocol).
URL	Type the protocol, IP address and path name of the OCSP server.
ID	The USG may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority).
LDAP Server	Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.
Address	Type the IP address (in dotted decimal notation) of the directory server.
Port	Use this field to specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
ID	The USG may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority).
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

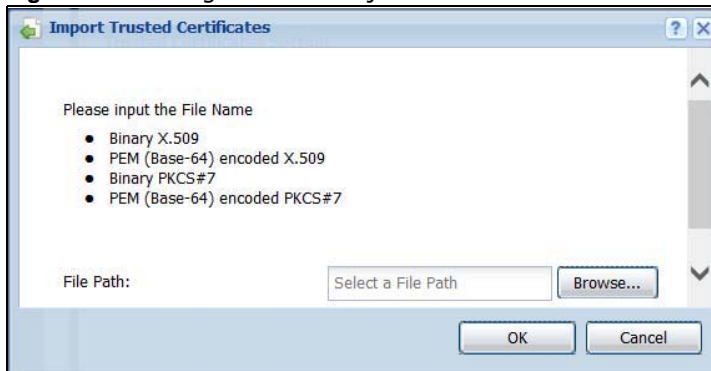
Table 223 Configuration > Object > Certificate > Trusted Certificates > Edit (continued)

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the USG uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the USG calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the USG calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export Certificate	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
OK	Click OK to save your changes back to the USG. You can only change the name.
Cancel	Click Cancel to quit and return to the Trusted Certificates screen.

29.10.4.2 The Trusted Certificates Import Screen

Click **Configuration > Object > Certificate > Trusted Certificates > Import** to open the **Trusted Certificates Import** screen. Follow the instructions in this screen to save a trusted certificate to the USG.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 359 Configuration > Object > Certificate > Trusted Certificates > Import

The following table describes the labels in this screen.

Table 224 Configuration > Object > Certificate > Trusted Certificates > Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse to find it. You cannot import a certificate with the same name as a certificate that is already in the USG.
Browse	Click Browse to find the certificate file you want to upload.
OK	Click OK to save the certificate on the USG.
Cancel	Click Cancel to quit and return to the previous screen.

29.10.5 Certificates Technical Reference

OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the USG checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the USG only gets information on the certificates that it needs to verify, not a huge list. When the USG requests certificate status information, the OCSP server returns a "expired", "current" or "unknown" response.

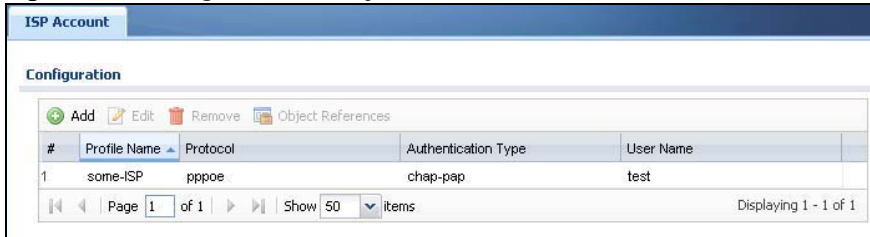
29.11 ISP Account Overview

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE/PPTP interfaces. An ISP account is a profile of settings for Internet access using PPPoE or PPTP.

Use the **Object > ISP Account** screens ([Section 29.11.1 on page 528](#)) to create and manage ISP accounts in the USG.

29.11.1 ISP Account Summary

This screen provides a summary of ISP accounts in the USG. To access this screen, click **Configuration > Object > ISP Account**.

Figure 360 Configuration > Object > ISP Account

The following table describes the labels in this screen. See [the ISP Account Edit section](#) below for more information as well.

Table 225 Configuration > Object > ISP Account

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field is a sequential value, and it is not associated with a specific entry.
Profile Name	This field displays the profile name of the ISP account. This name is used to identify the ISP account.
Protocol	This field displays the protocol used by the ISP account.
Authentication Type	This field displays the authentication type used by the ISP account.
User Name	This field displays the user name of the ISP account.

29.11.1.1 ISP Account Edit

The **ISP Account Edit** screen lets you add information about new accounts and edit information about existing accounts. To open this window, open the **ISP Account** screen. (See [Section 29.11.1 on page 528](#).) Then, click on an **Add** icon or **Edit** icon to open the **ISP Account Edit** screen below.

Figure 361 Configuration > Object > ISP Account > Edit

The following table describes the labels in this screen.

Table 226 Configuration > Object > ISP Account > Edit

LABEL	DESCRIPTION
Profile Name	This field is read-only if you are editing an existing account. Type in the profile name of the ISP account. The profile name is used to refer to the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
Protocol	This field is read-only if you are editing an existing account. Select the protocol used by the ISP account. Options are: pppoe - This ISP account uses the PPPoE protocol. pptp - This ISP account uses the PPTP protocol.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: CHAP/PAP - Your USG accepts either CHAP or PAP when requested by this remote node. Chap - Your USG accepts CHAP only. PAP - Your USG accepts PAP only. MSCHAP - Your USG accepts MSCHAP only. MSCHAP-V2 - Your USG accepts MSCHAP-V2 only.
Encryption Method	This field is available if this ISP account uses the PPTP protocol. Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: nomppe - This ISP account does not use MPPE. mppe-40 - This ISP account uses 40-bit MPPE. mppe-128 - This ISP account uses 128-bit MMPE.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above. The password can only consist of alphanumeric characters (A-Z, a-z, 0-9). This field can be blank.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
Server IP	If this ISP account uses the PPPoE protocol, this field is not displayed. If this ISP account uses the PPTP protocol, type the IP address of the PPTP server.
Connection ID	This field is available if this ISP account uses the PPTP protocol. Type your identification name for the PPTP server. This field can be blank.
Service Name	If this ISP account uses the PPPoE protocol, type the PPPoE service name to access. PPPoE uses the specified service name to identify and reach the PPPoE server. This field can be blank. If this ISP account uses the PPTP protocol, this field is not displayed.
Compression	Select On button to turn on stac compression, and select Off to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four.
Idle Timeout	This value specifies the number of seconds that must elapse without outbound traffic before the USG automatically disconnects from the PPPoE/PPTP server. This value must be an integer between 0 and 360. If this value is zero, this timeout is disabled.
OK	Click OK to save your changes back to the USG. If there are no errors, the program returns to the ISP Account screen. If there are errors, a message box explains the error, and the program stays in the ISP Account Edit screen.
Cancel	Click Cancel to return to the ISP Account screen without creating the profile (if it is new) or saving any changes to the profile (if it already exists).

29.12 SSL Application Overview

You use SSL application objects in SSL VPN. Configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access. You can apply one or more SSL application objects in the **VPN > SSL VPN** screen for a user account/user group.

- Use the **SSL Application** screen ([Section 29.12.2 on page 533](#)) to view the USG's configured SSL application objects.
- Use the **SSL Application Edit** screen to create or edit web-based application objects to allow remote users to access an application via standard web browsers ([Section 29.12.2.1 on page 533](#)).
- You can also use the **SSL Application Edit** screen to specify the name of a folder on a Linux or Windows file server which remote users can access using a standard web browser ([Section 29.12.2.1 on page 533](#)).

29.12.1 What You Need to Know

Application Types

You can configure the following SSL application on the USG.

- Web-based
A web-based application allows remote users to access an intranet site using standard web browsers.

Remote User Screen Links

Available SSL application names are displayed as links in remote user screens. Depending on the application type, remote users can simply click the links or follow the steps in the pop-up dialog box to access.

Remote Desktop Connections

Use SSL VPN to allow remote users to manage LAN computers. Depending on the functions supported by the remote desktop software, they can install or remove software, run programs, change settings, and open, copy, create, and delete files. This is useful for troubleshooting, support, administration, and remote access to files and programs.

The LAN computer to be managed must have VNC (Virtual Network Computing) or RDP (Remote Desktop Protocol) server software installed. The remote user's computer does not use VNC or RDP client software. The USG works with the following remote desktop connection software:

RDP

- Windows Remote Desktop (supported in Internet Explorer)

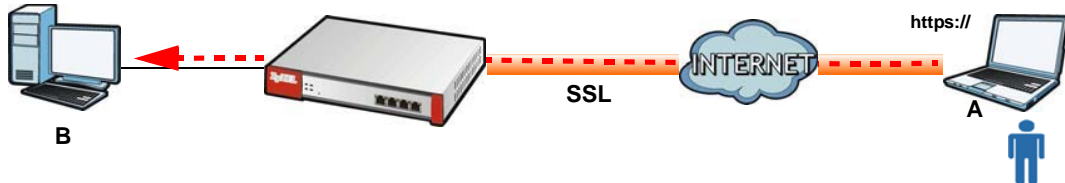
VNC

- RealVNC
- TightVNC

- UltraVNC

For example, user A uses an SSL VPN connection to log into the USG. Then he manages LAN computer B which has RealVNC server software installed.

Figure 362 SSL-protected Remote Management



Weblinks

You can configure weblink SSL applications to allow remote users to access web sites.

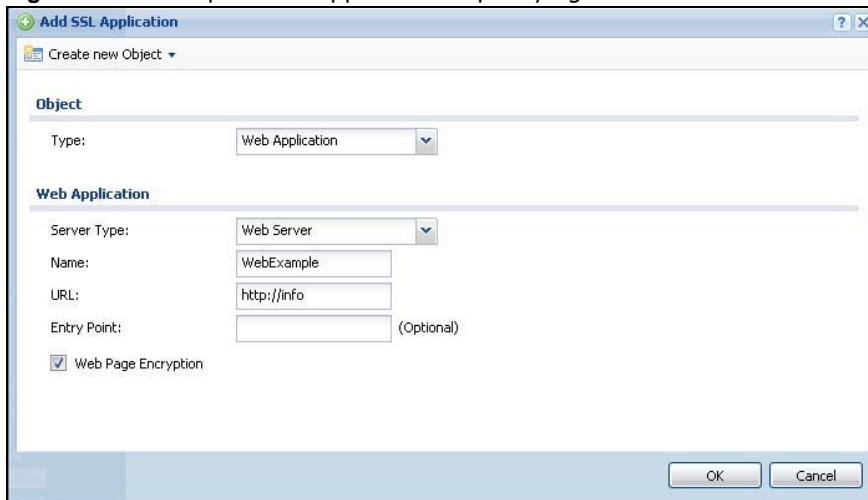
29.12.1.1 Example: Specifying a Web Site for Access

This example shows you how to create a web-based application for an internal web site. The address of the web site is `http://info` with web page encryption.

- 1 Click **Configuration > Object > SSL Application** in the navigation panel.
- 2 Click the **Add** button and select **Web Application** in the **Type** field.
In the **Server Type** field, select **Web Server**.
Enter a descriptive name in the **Display Name** field. For example, "CompanyIntranet".
In the **URLAddress** field, enter "`http://my-info`".
Select **Web Page Encryption** to prevent users from saving the web content.
Click **OK** to save the settings.

The configuration screen should look similar to the following figure.

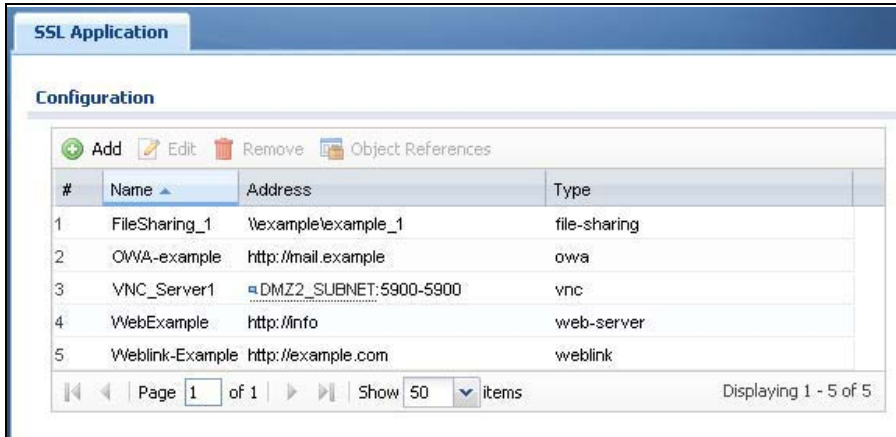
Figure 363 Example: SSL Application: Specifying a Web Site for Access



29.12.2 The SSL Application Screen

The main **SSL Application** screen displays a list of the configured SSL application objects. Click **Configuration > Object > SSL Application** in the navigation panel.

Figure 364 Configuration > Object > SSL Application



The following table describes the labels in this screen.

Table 227 Configuration > Object > SSL Application

LABEL	DESCRIPTION
Add	Click this to create a new entry.
Edit	Double-click an entry or select it and click Edit to be able to modify the entry's settings.
Remove	To remove an entry, select it and click Remove . The USG confirms you want to remove it before doing so.
Object References	Select an entry and click Object References to open a screen that shows which settings use the entry.
#	This field displays the index number.
Name	This field displays the name of the object.
Address	This field displays the IP address/URL of the application server or the location of a file share.
Type	This field shows whether the object is a file-sharing, web-server, Outlook Web Access, Virtual Network Computing, or Remote Desktop Protocol SSL application.

29.12.2.1 Creating/Editing an SSL Application Object

You can create a web-based application that allows remote users to access an application via standard web browsers. You can also create a file sharing application that specify the name of a folder on a file server (Linux or Windows) which remote users can access. Remote users can access files using a standard web browser and files are displayed as links on the screen.

To configure an SSL application, click the **Add** or **Edit** button in the **SSL Application** screen and select **Web Application** or **File Sharing** in the **Type** field. The screen differs depending on what object type you choose.

Note: If you are creating a file sharing SSL application, you must also configure the shared folder on the file server for remote access. Refer to the document that comes with your file server.

Figure 365 Configuration > Object > SSL Application > Add/Edit: Web Application

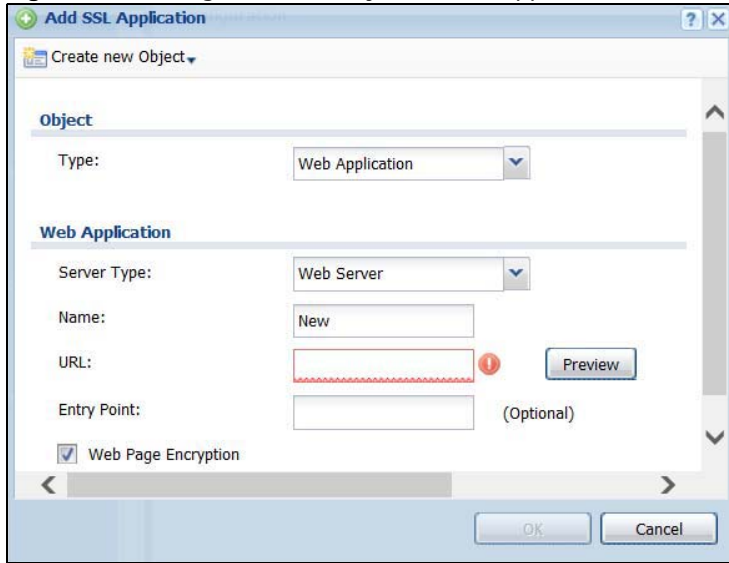
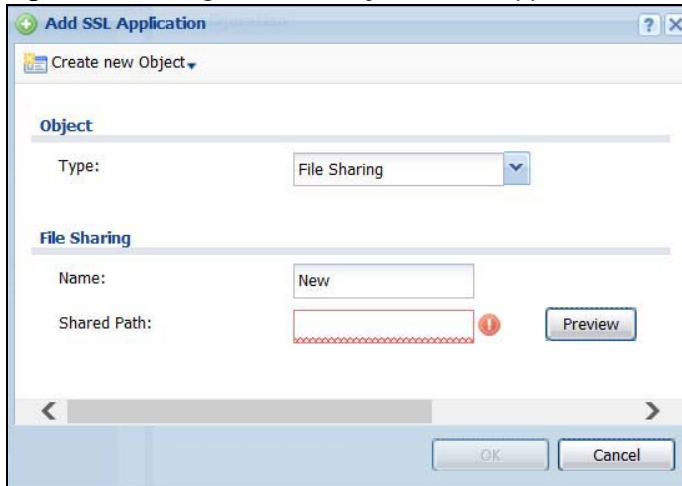


Figure 366 Configuration > Object > SSL Application > Add/Edit: File Sharing



The following table describes the labels in this screen.

Table 228 Configuration > Object > SSL Application > Add/Edit: Web Application/File Sharing

LABEL	DESCRIPTION
Create new Object	Use this to configure any new settings objects that you need to use in this screen.
Object	
Type	Select Web Application or File Sharing from the drop-down list box.
Web Application	

Table 228 Configuration > Object > SSL Application > Add/Edit: Web Application/File Sharing

LABEL	DESCRIPTION
Server Type	<p>This field only appears when you choose Web Application as the object type.</p> <p>Specify the type of service for this SSL application.</p> <p>Select Web Server to allow access to the specified web site hosted on the local network.</p> <p>Select OWA (Outlook Web Access) to allow users to access e-mails, contacts, calendars via Microsoft Outlook-like interface using supported web browsers. The USG supports one OWA object.</p> <p>Select VNC to allow users to manage LAN computers that have Virtual Network Computing remote desktop server software installed.</p> <p>Select RDP to allow users to manage LAN computers that have Remote Desktop Protocol remote desktop server software installed.</p> <p>Select Weblink to create a link to a web site that you expect the SSL VPN users to commonly use.</p>
Name	<p>Enter a descriptive name to identify this object. You can enter up to 31 characters ("0-9", "a-z", "A-Z", "-", and "_"). Spaces are not allowed.</p>
URL	<p>This field only appears when you choose Web Application as the object type.</p> <p>This field displays if the Server Type is set to Web Server, OWA, or Weblink.</p> <p>Enter the Fully-Qualified Domain Name (FQDN) or IP address of the application server.</p> <p>Note: You must enter the "http://" or "https://" prefix.</p> <p>Remote users are restricted to access only files in this directory. For example, if you enter "\remote\" in this field, remote users can only access files in the "remote" directory.</p> <p>If a link contains a file that is not within this domain, then remote users cannot access it.</p>
Preview	<p>This field only appears when you choose Web Application or File Sharing as the object type.</p> <p>This field displays if the Server Type is set to Web Server, OWA or Weblink.</p> <p>Note: If your Internet Explorer or other browser screen doesn't show a preview, it may be due to your web browser security settings. You need to add the USG's IP address in the trusted sites of your web browser. For example, in Internet Explorer, click Tools > Internet Options > Security > Trusted Sites > Sites and type the USG's IP address, then click Add. For other web browsers, please check the browser help.</p> <p>Click Preview to access the URL you specified in a new web browser screen.</p>
Entry Point	<p>This field only appears when you choose Web Application as the object type.</p> <p>This field displays if the Server Type is set to Web Server or OWA.</p> <p>This field is optional. You only need to configure this field if you need to specify the name of the directory or file on the local server as the home page or home directory on the user screen.</p>
Web Page Encryption	<p>This field only appears when you choose Web Application as the object type.</p> <p>Select this option to prevent users from saving the web content.</p>

Table 228 Configuration > Object > SSL Application > Add/Edit: Web Application/File Sharing

LABEL	DESCRIPTION
Shared Path	<p>This field only appears when you choose File Sharing as the object type.</p> <p>Specify the IP address, domain name or NetBIOS name (computer name) of the file server and the name of the share to which you want to allow user access. Enter the path in one of the following formats.</p> <p>"\\<IP address>\<share name>"</p> <p>"\\<domain name>\<share name>"</p> <p>"\\<computer name>\<share name>"</p> <p>For example, if you enter "\\my-server\Tmp", this allows remote users to access all files and/or folders in the "\Tmp" share on the "my-server" computer.</p>
OK	Click OK to save the changes and return to the main SSL Application Configuration screen.
Cancel	Click Cancel to discard the changes and return to the main SSL Application Configuration screen.