



What's New in Fireware v12.3

What's New in Fireware v12.3

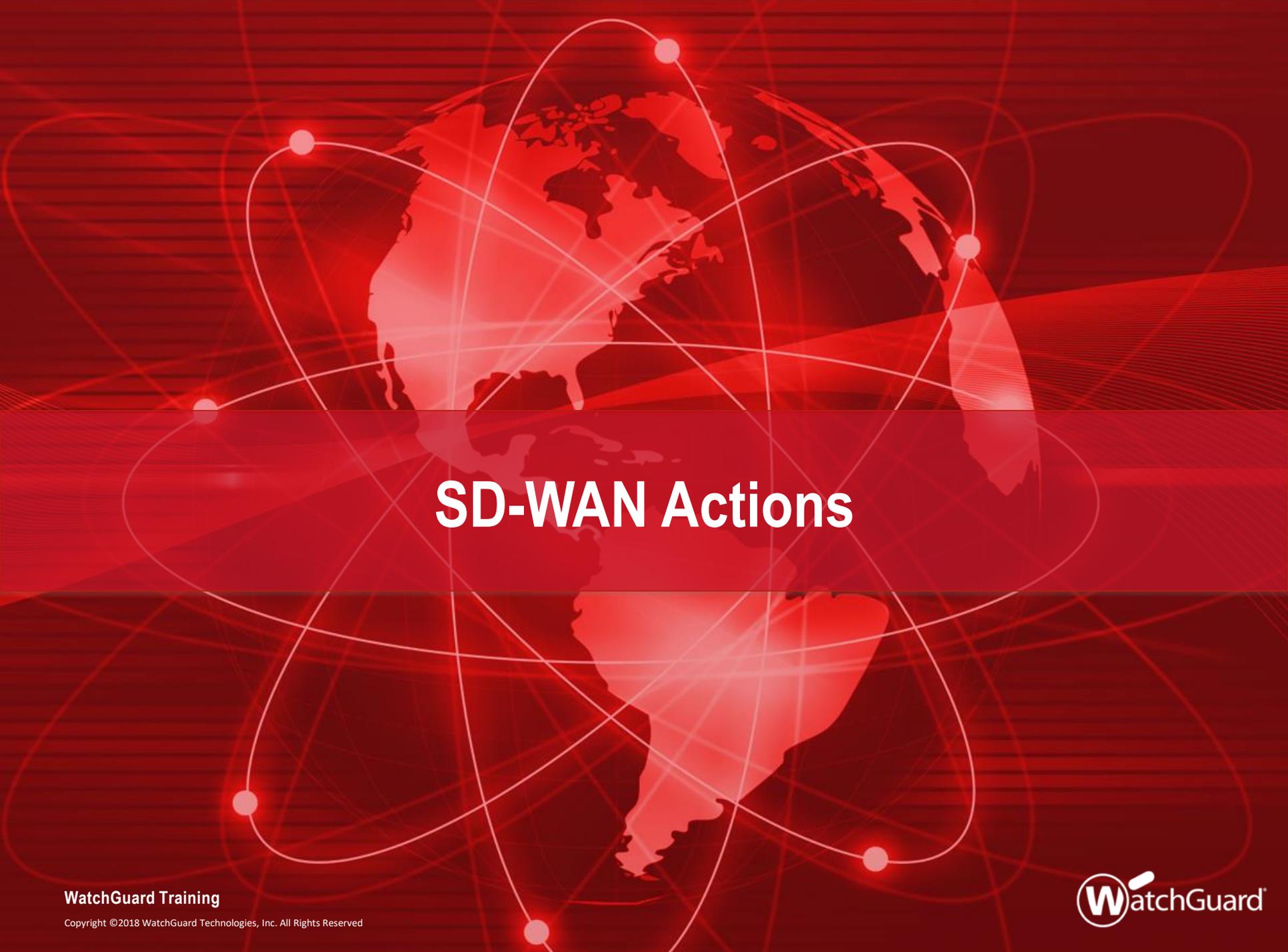
- Updates to Networking functionality:
 - SD-WAN actions
 - SD-WAN reporting enhancements
 - Link monitor enhancements
 - NetFlow support
 - Centralized FireCluster diagnostics
- Updates to Mobile VPN functionality
 - Mobile VPN Selection Assistance
 - Mobile VPN with SSL wizard
 - 2FA support for SSL OpenVPN clients

What's New in Fireware v12.3

- Updates for Policies, Proxies, and Services:
 - Geolocation actions
 - WebBlocker enhancements
 - Services usability enhancements
 - STARTTLS in the IMAP proxy
 - TCP-UDP proxy action enhancements
 - Policy highlighting enhancements
- Tigerpaw Integration

What's New in Fireware v12.3

- USB backup enhancements
- Active Directory wizard
- IPv6 support for Active Directory single sign-on
- SSO Agent debug information
- Gateway Wireless Controller enhancements
- WatchGuard IPSec Mobile VPN Client updates



SD-WAN Actions

SD-WAN Actions

- The method used to route outbound traffic that matches a policy has changed: *SD-WAN actions* replace policy-based routing
- SD-WAN actions offer more granular control of external interface failover and failback for traffic that matches a policy
 - In an SD-WAN action, you can select to use network performance metrics (loss, latency, and jitter) to determine whether an interface fails over or fails back
 - If you select no metrics, the up/down status of the interface is used to determine whether an interface fails over or fails back
- Policies that include SD-WAN actions are especially effective for applications that are latency-sensitive, such as VoIP and video conferencing

SD-WAN Actions

- Policies that include SD-WAN actions take precedence over multi-WAN settings
- To configure SD-WAN actions:
 - Web UI — Select **Network > SD-WAN**
 - Policy Manager — Select **Network > Configuration > SD-WAN**
- You can also edit or create an SD-WAN action from within a policy
- In an SD-WAN action, you specify:
 - One or more external interfaces
 - (Optional) Loss rate, latency, and jitter values
 - Failback options

SD-WAN Actions

- SD-WAN action (Web UI)

Interfaces

Name

Description

SD-WAN Interfaces

Select the interfaces to include in this SD-WAN action. For useful loss, latency, and jitter metrics, we recommend that you specify targets other than the default gateway. To change a target, edit the [Link Monitor](#) configuration.

INTERFACE NAME	TARGETS
External-1	Ping (4.2.2.1) Ping (8.8.8.8)
External-2	Ping (4.2.2.1) Ping (8.8.8.8)

ADD REMOVE MOVE UP MOVE DOWN

Metrics Settings

Select measurements and specify values that determine when failover occurs to another SD-WAN interface. Failover occurs if the value for any selected measurement is exceeded.

MEASUREMENT	VALUE	
<input checked="" type="checkbox"/> Loss Rate	<input type="text" value="5"/>	%
<input checked="" type="checkbox"/> Latency	<input type="text" value="20"/>	milliseconds
<input checked="" type="checkbox"/> Jitter	<input type="text" value="10"/>	milliseconds

Fail over if values for all selected measurements are exceeded.

Failback for Active Connections

Select how the Firebox handles failback for active and new connections.

Immediate: Active and new connections use the failback (original) interface

No failback: Active and new connections use the failover interface

Immediate: Active and new connections use the failback (original) interface

Gradual failback: Active connections use the failover interface; new connections use the failback interface

Metrics

Failback

SD-WAN Actions

- SD-WAN action (Policy Manager)

Interfaces

Metrics

Failback

Add SD-WAN Action

Name: Test.SDWAN.action

Description:

SD-WAN Interfaces
Select the interfaces to include in this SD-WAN action. For useful loss, latency, and jitter metrics, we recommend that you specify targets other than the default gateway. To change a target, edit the Link Monitor configuration.

Include	Interface	Targets	
<input checked="" type="checkbox"/>	External-1	Ping (Default gateway)	Move Up
<input checked="" type="checkbox"/>	External-2	Ping (Default gateway)	Move Down

Metrics Settings
Select measurements and specify values that determine when failover occurs to another SD-WAN interface. Failover occurs if the value for any selected measurement is exceeded.

Loss Rate 5 %

Latency 20 ms

Jitter 10 ms

Fail over if values for all selected measurements are exceeded.

Failback for Active Connections
Select how the Firebox handles failback for active and new connections.

Immediate failback: Stop all active connections immediately. (selected)

NO failback: Stay on the failover interface even for new connections.

Immediate failback: Stop all active connections immediately.

Gradual failback: Allow active connections to use failover interface.

OK Cancel Help

SD-WAN Actions

■ SD-WAN interfaces —

- You must add at least one external interface or BOVPN virtual interface
- To configure loss, latency, and jitter values for failover and failback:
 - You must add two or more external interfaces
 - External interfaces must have a link monitor target
- The first interface in the list is the primary interface
- The primary interface is preferred if it is up and has metrics that do not exceed the values you specified
- You can move interfaces up or down in the list to change the primary interface

SD-WAN Actions

■ SD-WAN interfaces —

- For useful interface performance data, we recommend that you specify link monitor targets other than the default gateway
- The link monitor settings moved in Fireware v12.3. To change a link monitor **target**:
 - From the Web UI, select **Network > Link Monitor**
 - From PM, select **Network > Configuration > Link Monitor**
- In the Link Monitor configuration, you can select to measure loss, latency, and jitter for only one target

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	4.2.2.1	<input checked="" type="radio"/>
Ping	8.8.8.8	<input type="radio"/>

SD-WAN Actions

■ SD-WAN interfaces —

- Loss, latency, and jitter metrics apply only to external interfaces
 - These metrics do not apply to BOVPN virtual interfaces
- You can specify a BOVPN virtual interface in the SD-WAN action to route matching traffic to the virtual interface. However, if you do so:
 - You cannot add other interfaces to the SD-WAN action, which means failover to other interfaces is not available
 - SD-WAN actions with both BOVPN virtual interfaces and external interfaces are not supported
 - You cannot specify link monitor targets for the virtual interfaces
 - You cannot specify loss, latency, or jitter values

SD-WAN Actions

- **Loss rate, latency, and jitter —**
 - Select one or more of these measures to use as the basis for failover and failback
 - For example, if you specify a jitter value of 10 ms, and jitter on the interface exceeds 10 ms, connections fail over to another interface
 - Because each network is different, and some applications are more sensitive to performance issues, you must select loss, latency, and jitter values based on your knowledge of your network
 - To establish baseline values for interface performance, you can use the historical data for SD-WAN loss, latency, and jitter available in the Web UI at **Dashboard > Interfaces > SD-WAN**

SD-WAN Actions

▪ Failover —

- Only failover mode is supported (round robin, interface overflow, and routing table modes are not supported)
- If you selected to measure loss, latency, or jitter:
 - By default, failover occurs if the primary interface has metrics that exceed **any** the values you specified
 - To initiate failover only if **all** of the values are exceeded, you must select the **Fail over if values for all selected measurements are exceeded** option
- If you did not select to measure loss, latency or jitter, failover occurs if the interface is down
 - An interface is considered down if the link monitor target fails
 - Active and new connections use the failover interface

SD-WAN Actions

- **Failback —**
 - You can select one of three failback options:
 - **No failback** — Active and new connections remain on the failover interface and never fail back to the original interface
 - **Immediate** — Active and new connections immediately fail back to the original interface
 - **Gradual** — Active connections remain on the failover interface. New connections use the original interface.
 - The default setting is **Immediate failback**

SD-WAN Actions

- **Failback —**
- If you select **No failback** or **Gradual failback** in the SD-WAN action, you can select to manually fail back connections at a later time
- To initiate manual failback:
 - In Fireware Web UI, select **System Status > SD-WAN Status**
 - In FSM, select the **SD-WAN** tab

SD-WAN Actions

- **Failback —**
 - If you select **Gradual failback** in the SD-WAN action:
 - You can select the **Force Failback** option on the SD-WAN status page
 - This option terminates active connections and forces new connections to use the failback (original) interface
 - If you select **No failback** in the SD-WAN action, you can select these options on the SD-WAN status page:
 - **Manual Gradual** — Keeps active connections on the failover interface and forces new connections to use the failback (original) interface
 - **Manual Immediate Failback** — Terminates active connections and forces new connections to use the failback interface

SD-WAN Actions

- **Failback (Web UI) —**
 - If the failback option is **Gradual Failback**, you can click the action and click **Force Failback**

SD-WAN Status

[FORCE FAILBACK](#)
[MANUAL GRADUAL FAILBACK](#)
[MANUAL IMMEDIATE FAILBACK](#)

ACTION	MODE	INTERFACES	FAILBACK OPTION
Global MWAN	Failover	External-1 External 2	Immediate failback
VoIP.SD-WAN.action	Failover	External 2 External-1	Gradual failback
Test.SD-WAN.action	Failover	External-1 External 2	No failback

SD-WAN Actions

- **Failback (Web UI) —**
 - If the failback option is **No failback**, you can click the action and click **Manual Gradual Failback** or **Manual Immediate Failback**

SD-WAN Status

FORCE FAILBACK **MANUAL GRADUAL FAILBACK** **MANUAL IMMEDIATE FAILBACK**

ACTION	MODE	INTERFACES	FAILBACK OPTION
Global MWAN	Failover	External-1 External 2	Immediate failback
VoIP.SD-WAN.action	Failover	External 2 External-1	Gradual failback
Test.SD-WAN.action	Failover	External-1 External 2	No failback

SD-WAN Actions

Failback (FSM) —

- If the failback option is **Gradual Failback**, you can right-click the action and select **Force Failback**

The screenshot shows the Firebox System Manager interface. The main content area displays a table of SD-WAN actions. The table has four columns: Action, Mode, Interfaces, and Failback option. The 'VoIP.SD-WAN.action' row is highlighted, and a red box around the 'Force Failback' button is visible. The 'Failback option' for this row is 'Gradual failback', also highlighted with a red box.

Action	Mode	Interfaces	Failback option
Global MWAN	Failover	External-1 External 2	Immediate failback
VoIP.SD-WAN.action	Failover	External 2 External-1	Gradual failback
Test.SD-WAN.action	Failover	External-1 External 2	No failback

Refresh Interval: 5 seconds

SD-WAN Actions

- **Failback (FSM) —**
 - If the failback option is **No Failback**, you can right-click the action and select **Gradual Failback** or **Immediate Failback**

The screenshot shows the Firebox System Manager interface. At the top, there's a navigation bar with tabs: Front Panel, Traffic Monitor, Bandwidth Meter, Service Watch, Status Report, Authentication List, Blocked Sites, Subscription Services, Gateway Wireless Controller, SD-WAN, Traffic Management, and User Quotas. Below this is a graph area showing latency with the text "[Latency] 0.01 ms [Auto-Scale]". The main part of the interface is a table with columns: Action, Mode, Interfaces, and Failback option. The table contains three rows: Global MWAN, VoIP.SD-WAN.action, and Test.SD-WAN.action. The Test.SD-WAN.action row is highlighted in blue. A context menu is open over this row, showing "Gradual Failback" and "Immediate Failback" options. The "No failback" option in the table is also circled in red.

Action	Mode	Interfaces	Failback option
Global MWAN	Failover	External-1 External 2	Immediate failback
VoIP.SD-WAN.action	Failover	External 2 External-1	Gradual failback
Test.SD-WAN.action	Failover	External-1 External 2	No failback

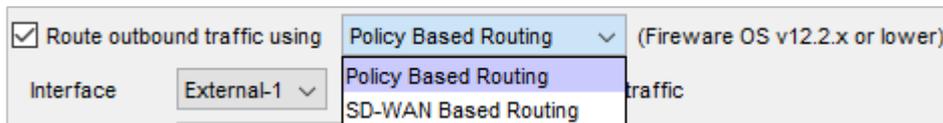
SD-WAN Actions

- After you configure an SD-WAN action, you can enable SD-WAN routing in a policy
- In the policy, select the **SD-WAN** tab and select the SD-WAN action from the list

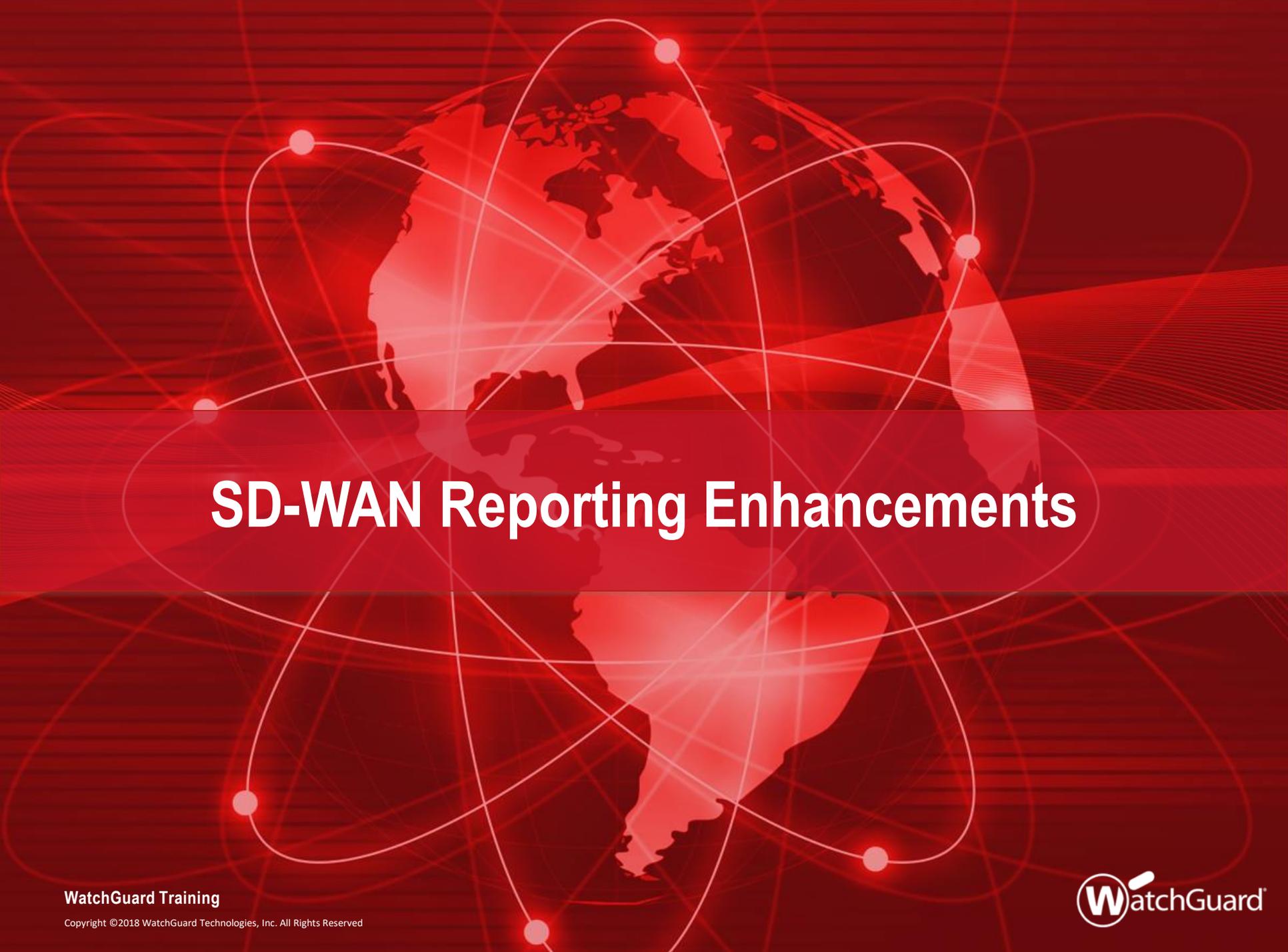
The screenshot shows the 'Firewall Policies / Edit' configuration page. The 'Name' field is set to 'SIP-ALG' and the 'Enable' checkbox is checked. The 'SD-WAN' tab is selected, and the 'SD-WAN Action' dropdown menu is open, showing options: 'None', 'VoIP.SDWAN.action', and 'Create new'. The 'VoIP.SDWAN.action' option is highlighted. Below the dropdown are 'SAVE' and 'CANCEL' buttons.

SD-WAN Actions

- Configuration conversion
 - For policies you created in Fireware v12.2.1 or lower:
 - Policy-based routing without failover is converted to an SD-WAN action with a single interface
 - Policy-based routing with failover is converted to an SD-WAN action with multiple interfaces
 - In Policy Manager, the policy-based routing setting is still available for backwards compatibility with older Fireware OS versions



The screenshot shows a configuration panel with a checked checkbox labeled "Route outbound traffic using". To its right is a dropdown menu currently set to "Policy Based Routing", with a note "(Fireware OS v12.2.x or lower)". Below this, there is an "Interface" label and a dropdown menu set to "External-1". A second dropdown menu is open, showing three options: "Policy Based Routing" (highlighted in blue), "SD-WAN Based Routing", and "SD-WAN Based Routing". The word "traffic" is partially visible to the right of the second dropdown menu.



SD-WAN Reporting Enhancements

SD-WAN Reporting Enhancements

- The accuracy of SD-WAN reporting is improved
- To calculate loss, latency, and jitter, the Firebox now uses the 100 most recent probe results from link monitor targets
 - Probe results are stored in groups of 10
 - When 10 groups are each filled with 10 probe results, probe results in the oldest group are cleared, and 10 new results are stored
- Jitter calculation
 - The standard deviation is now used instead of the corrected standard deviation



Link Monitor Enhancements

Link Monitor Enhancements

- Link monitor settings have moved from the Multi-WAN configuration
 - Web UI — Select **Network > Link Monitor**
 - Policy Manager — Select **Network > Configuration > Link Monitor**
- In the Web UI, you can now configure link monitor targets for an external interface regardless of whether multi-WAN is enabled
 - For example, if your configuration includes only one external interface, you can configure link monitor targets for that interface in the Web UI
 - In Policy Manager, you cannot configure link monitor targets if multi-WAN is disabled

Link Monitor Enhancements

- If multi-WAN is enabled, you can configure link monitor targets for an external interface that is not a multi-WAN member
- If you configure only one link monitor target for an interface, loss, latency, and jitter are measured for that target by default
- If you configure two or more link monitor targets for an interface, you must select one target for which loss, latency, and jitter are measured
 - You cannot select to measure loss, latency, and jitter for more than one target for an interface

Link Monitor Enhancements

- Web UI

Link Monitor

LINK MONITOR	INTERFACE NAME	TARGETS
Yes	External-1	Ping (8.8.8.8) Ping (4.2.2.1)
Yes	External-2	Ping (8.8.8.8) Ping (4.2.2.1)

CONFIGURE

Link Monitor / Edit

Interface Name: External-1

Enable link monitor for this interface

Select the targets to monitor to verify the status of External-1. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	8.8.8.8	<input checked="" type="radio"/>
Ping	4.2.2.1	<input type="radio"/>

ADD EDIT REMOVE

Require a successful probe to all targets to define the interface as active.

Probe interval seconds

Deactivate after consecutive failures

Reactivate after consecutive successes

Select to measure loss, latency, and jitter for one target

Link Monitor Enhancements

- Policy Manager

Select to measure loss, latency, and jitter for one target

Network Configuration

Interfaces | Link Aggregation | Bridge | VLAN | Loopback | Bridge Protocols | WINS/DNS | Dynamic DNS | Multi-WAN | **Link Monitor** | SD-WAN | PPPoE

Link Monitor Configuration

External Interfaces:

- External
- External-2

Settings:

Enable Link Monitor for this interface

Select the targets to verify the status of **External**. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Type	Target	Measure Loss, Latency, and Jitter
Ping	8.8.8.8	<input type="checkbox"/>
Ping	4.2.2.1	<input checked="" type="checkbox"/>

Require a successful probe to all targets to define the interface as active.

Use these settings for **External**:

Probe Interval: 5 Seconds

Deactivate After: 3 Consecutive Failures

Reactivate After: 3 Consecutive Successes

OK Cancel Help

Link Monitor Enhancements

- When you enable link monitor for an interface, the default gateway is the target
 - For meaningful data, we recommend that you specify a target other than the default gateway
 - If you add a custom target, the default gateway target is replaced
 - If you remove all custom targets that you added, the default gateway target is automatically added back

Link Monitor Enhancements

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	Default gateway	<input checked="" type="radio"/>

ADD EDIT REMOVE

Add Link Monitor Target ×

Type

Target

OK CANCEL

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	4.2.2.1	<input checked="" type="radio"/>

ADD EDIT REMOVE

Link Monitor Enhancements

- You can now specify DNS targets

Add Link Monitor Target ×

Type

Target

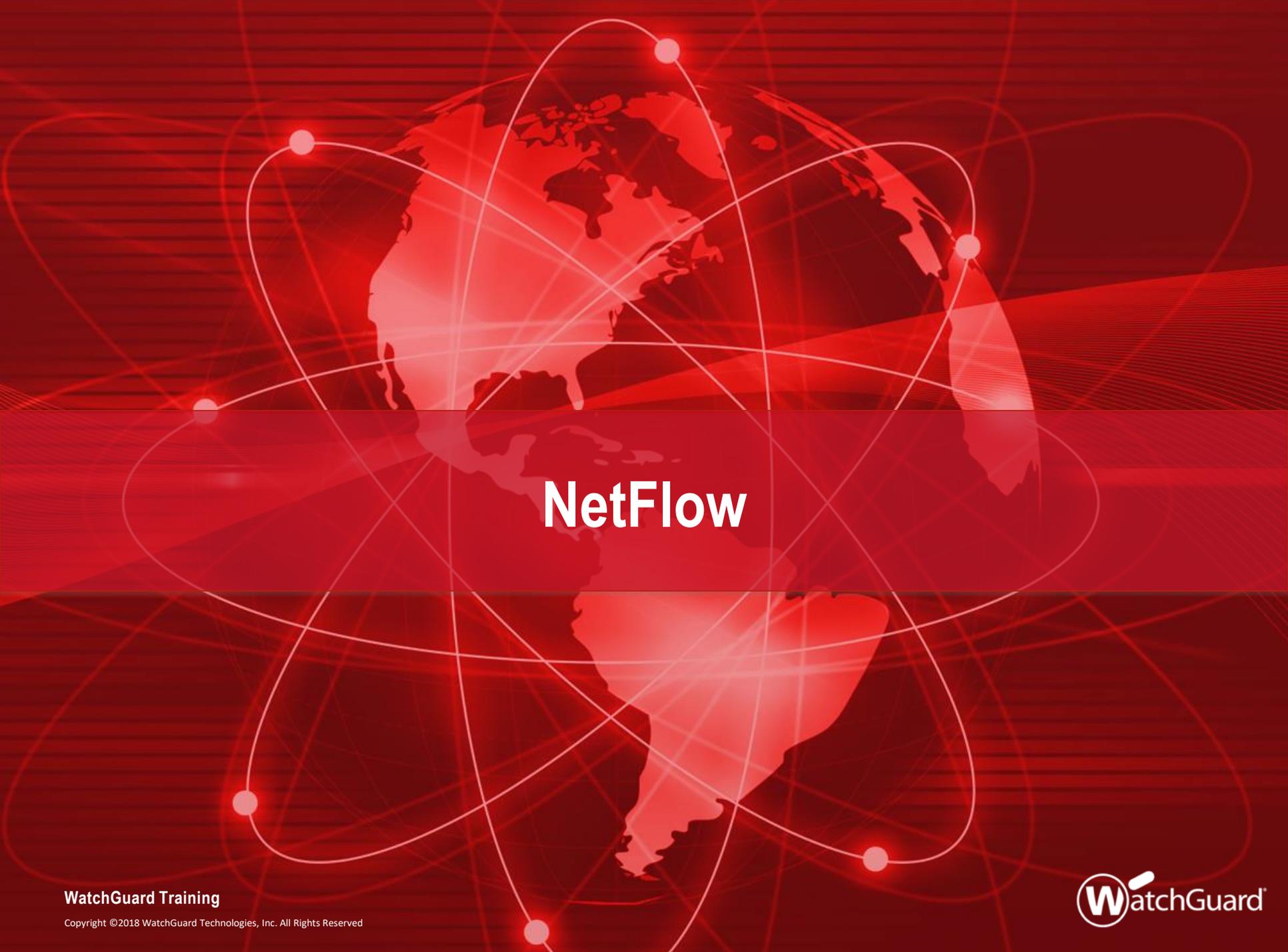
Query domain

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	8.8.8.8	<input checked="" type="radio"/>
Ping	4.2.2.1	<input type="radio"/>
DNS	host.example.com@192.0.2.2	<input type="radio"/>

Link Monitor Enhancements

- You can now specify up to three link monitor targets for an interface

TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	8.8.8.8	<input checked="" type="radio"/>
TCP	198.51.100.2:80	<input type="radio"/>
DNS	host.example.com@192.0.2.2	<input type="radio"/>



NetFlow

NetFlow

- Configure NetFlow to gain more insight into Firebox traffic
- For example, you can troubleshoot network congestion by viewing the source and destination of traffic for an interface, and the class of service

NetFlow

- NetFlow is a protocol created by Cisco that is used to collect and analyze IP network traffic
- When you configure NetFlow on your Firebox, you specify the IP address of a third-party server known as a *collector*
- The collector runs software that uses the NetFlow protocol to analyze network traffic
 - Many third-party software solutions support NetFlow
- The Firebox sends streams of data known as *net flows* to the collector for analysis
- The collector can receive data from multiple sources

NetFlow

- Web UI — Select **System** > **NetFlow**

NetFlow

Enable NetFlow

Protocol Version V5 V9

Collector Address :

Active Flow Timeout minutes

Sampling Mode Sample every 1 out of packets

Select interfaces to monitor traffic received on those interfaces

<input type="checkbox"/>	INTERFACE NAME	TYPE	ZONE
<input type="checkbox"/>		All	All
<input type="checkbox"/>	Firebox		
<input checked="" type="checkbox"/>	External-1	Physical	External
<input type="checkbox"/>	External-2	Physical	External
<input checked="" type="checkbox"/>	Trusted	Physical	Trusted

NetFlow

- Policy Manager — Select **Setup > NetFlow**

The screenshot shows the 'Netflow Settings' dialog box. At the top, there is a checkbox labeled 'Enable NetFlow (Fireware OS v12.3 and higher)' which is checked. Below this is a 'Settings' section containing: 'Protocol Version' with radio buttons for 'V5' (selected) and 'V9'; 'Collector Address' with a text box containing '203.0.113.2' and a port spinner box set to '9995'; 'Active Flow Timeout' with a spinner box set to '3' and the unit 'minutes'; 'Enable Sampling' with an unchecked checkbox; and 'Sample Frequency' with a spinner box set to '2' and the unit 'packets'. The 'Monitored Interfaces' section has the instruction 'Select interfaces to monitor traffic received on those interfaces.' and a list of checkboxes: 'Interfaces' (unchecked), 'Firebox' (unchecked), 'External-1' (checked), 'External-2' (unchecked), and 'Trusted' (checked). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

NetFlow

- Protocol Version —
 - Fireware supports NetFlow versions 5 and 9
 - V9 can monitor IPv6 traffic
- Collector Address —
 - You must specify an IPv4 or IPv6 address for the collector
 - FQDNs are not supported
- Active Flow Timeout —
 - Specify a value that is lower than the **Active Flow Timeout** value on the collector
 - This helps to avoid data loss. If the Active Flow Timeout value is lower on the collector, the collector might stop listening while the Firebox is still sending data

NetFlow

- Sampling mode —
 - In this mode, the Firebox randomly selects 1 out of every n packets to sample
 - For example, if you specify a Sampling mode of 100, the Firebox samples 1 out of every 100 packets
 - Sampling mode can help reduce performance impacts to the Firebox
 - We recommend Sampling mode for large-scale environments only

NetFlow

- Interfaces —
 - Only traffic received on selected interfaces is monitored unless you select the **Firebox** option
 - If you select **Firebox**, traffic sent out from the Firebox, also known as self-generated or Firebox-generated traffic, is monitored
 - Physical, VLAN, bridge, wireless, and link aggregation interfaces are supported in all zones (Trusted, External, Optional, and Custom)
 - BOVPN virtual interfaces are not supported

NetFlow

- Interfaces —
 - If you have a long list of interfaces, you can use the **Interface Name** search box to find an interface
 - For example, type `ext` to find all interface names that contain those letters
 - You can also filter by type and zone

INTERFACE NAME	
<input type="checkbox"/>	External-1
<input type="checkbox"/>	External-2

INTERFACE NAME	TYPE	ZONE
<input type="checkbox"/>	Physical	Trusted

NetFlow

■ Interfaces —

- (Web UI) To enable NetFlow on all interfaces, select the check box adjacent to **Interface Name**
- (Policy Manager) To enable NetFlow on all interfaces, the select **Interfaces** check box

<input checked="" type="checkbox"/>	INTERFACE NAME	TYPE	ZONE
<input checked="" type="checkbox"/>	Firebox	All	All
<input checked="" type="checkbox"/>	External-1	Physical	External
<input checked="" type="checkbox"/>	External-2	Physical	External
<input checked="" type="checkbox"/>	Trusted	Physical	Trusted

Select interfaces to monitor traffic received on those interfaces.

- Interfaces
- Firebox
- External-1
- External-2
- Trusted

NetFlow

- Flows —
 - The Firebox sends a flow to the collector when the flow terminates either normally or abnormally
 - For a long-lasting flow, the flow terminates after the number of minutes elapse that you specified for the **Active Flow Timeout** value
- Data security —
 - Flows are sent as UDP packets in clear text, which means you must make sure the path between the Firebox and collector is secure

NetFlow

- Performance impact —
 - NetFlow can impact the performance of the Firebox in some cases
 - To mitigate performance impacts, limit the number of interfaces that you monitor. For large-scale enterprise networks, consider enabling Sampling mode.
- NetFlow is not available in device configuration templates



FireCluster Diagnostics

FireCluster Diagnostics

- A new FireCluster diagnostics page centralizes cluster data, gives you more insight into cluster health, and reduces troubleshooting time

FireCluster Diagnostics

- The **FireCluster Diagnostics** page shows detailed real-time and historical information about your FireCluster
 - You can see uptime information, performance and health statistics, and historical data for events
 - If an event occurs, you can view or download a detailed Event Status Report
 - For example, if a primary cluster member fails over to a backup cluster member, the **FireCluster Diagnostics** page shows the failover event and reason for the failover, and you can view or download a report for this event to see more details
- In Fireware v12.3, the **FireCluster Diagnostics** page is available only in Fireware Web UI and applies only to Active/Passive clusters

FireCluster Diagnostics

■ Web UI

30 SECONDS ▾
⏸

FireCluster Diagnostics

✓ Synchronized

Cluster enabled for 1581 hr(s): 47 mins(s): 53 sec(s)

Connections: 40

Connections per second: unknown

[More Details](#)

MEMBER ROLE	SERIAL NUMBER	STATUS	UPTIME	CPU	MEMORY
Master	80DA02BD37DA6	Online	0:09:44	0%	28%
Backup	80DA0336CDED2	Online	0:06:24	0%	26%

Cluster Member History LAST 7 DAYS ▾

Failovers: 4

Faults: 0

Cluster Downtime: 0d 0h 0m

CLUSTER STATUS	PERCENTAGE	TIME
Both Members Up	99.884%	6d 23h 48m
Single Member Up	0.116%	0d 0h 11m
Both Members Down	0.000%	0d 0h 0m

History from 2018-10-25 12:00:00 AM to 2018-11-01 09:43:21 AM

DATE ↑	EVENT	REASON	DURATION
2018-10-29 11:25:24 AM	Failover	Unknown	5 second(s)
2018-10-29 11:28:40 AM	Failover	Interface eth0 link is down	5 second(s)
2018-10-29 11:31:33 AM	Upgrade	Cluster upgrade completed successfully	5 second(s)
2018-11-01 09:31:38 AM	Failover	Unknown	5 second(s)
2018-11-01 09:35:00 AM	Failover	Unknown	5 second(s)
2018-11-01 09:37:44 AM	Upgrade	Cluster upgrade completed successfully	5 second(s)

FireCluster Diagnostics

- This data appears on the FireCluster Diagnostics page:
 - Uptime information —
 - How long the cluster members have been synchronized
 - How long each member has been online
 - Performance statistics —
 - CPU and memory usage
 - Network connections
 - Connection rate

FireCluster Diagnostics

- Historical data —
 - Total amount of time both members have been up
 - Total amount of time only a single member has been up
 - Total amount of time both members have been down
 - Color-coded graph that shows the cluster status for the last 24 hours
 - A list of cluster events that includes date, reason, and duration of each event
 - A link to a log file that reveals detailed information about cluster events

FireCluster Diagnostics

- When an event occurs, you can click the event to see an Event Status Report that includes:
 - Event description (event type, reason, and time)
 - Runtime status (how long members have been paired and up)
 - Cluster health information (four health indexes)
 - Interfaces status (up or down)
 - Cluster synchronization status (for the configuration, password, certificate, license, and DHCP)
 - VPN synchronization
 - Cluster OP events (list of cluster events with time stamps)
- You can download this report as a .TGZ file



Mobile VPN Selection Assistance

Mobile VPN Selection Assistance

- A new **Get Started** page helps you select the best mobile VPN product for your network
- From the **Get Started** page, you can:
 - See some benefits of each mobile VPN type, along with security information, client compatibility information, and our recommendations
 - Select to configure any mobile VPN type
 - See which mobile VPN types are configured on the Firebox

Mobile VPN with SSL Wizard

■ Web UI

Mobile VPN

The Firebox supports several types of Mobile VPN tunnels. For most networks, we recommend Mobile VPN with IKEv2 or Mobile VPN with SSL. The Firebox supports simultaneous connections to more than one mobile VPN type.

✓ IKEv2

Mobile VPN with IKEv2 is the most secure option and provides high-performance VPN connections. Users can connect with native Windows, macOS, or iOS clients, or with the strongSwan app for Android.

We recommend Mobile VPN with IKEv2 in most cases.

[LAUNCH WIZARD](#) [Manually Configure](#)

✓ SSL

Mobile VPN with SSL/TLS is a secure option, but it is slower than other mobile VPN types. Windows and macOS users download a client from a Firebox portal. Android and iOS users download a profile from the Firebox portal for use with an OpenVPN client.

We recommend Mobile VPN with SSL when IKEv2 IPsec traffic is not allowed on the remote network or when split-tunneling is required.

[CONFIGURE](#) [DOWNLOAD CLIENT](#)

✓ L2TP

Mobile VPN with L2TP is a less secure option unless you configure a certificate instead of a pre-shared key. L2TP is not secure when IPsec is disabled. Users can connect with native clients on most operating systems, but manual configuration is required.

We recommend Mobile VPN with L2TP only for users with legacy operating systems that do not support IKEv2.

[CONFIGURE](#)

✓ IPsec

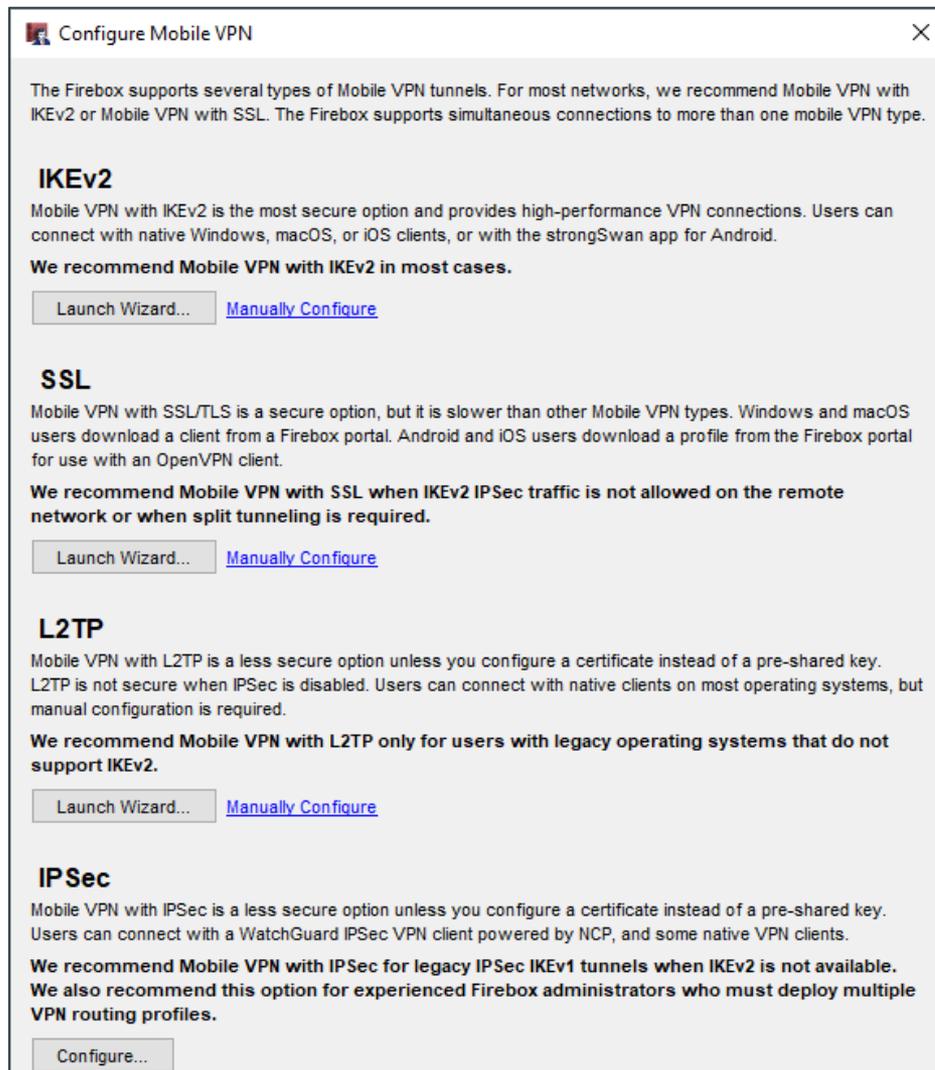
Mobile VPN with IPsec is a less secure option unless you configure a certificate instead of a pre-shared key. Users can connect with a WatchGuard IPsec VPN client powered by NCP, and some native VPN clients.

We recommend Mobile VPN with IPsec for legacy IPsec IKEv1 tunnels when IKEv2 is not available. We also recommend this option for experienced Firebox administrators who must deploy multiple VPN routing profiles.

[CONFIGURE](#)

Mobile VPN Selection Assistance

- Policy Manager



Configure Mobile VPN

The Firebox supports several types of Mobile VPN tunnels. For most networks, we recommend Mobile VPN with IKEv2 or Mobile VPN with SSL. The Firebox supports simultaneous connections to more than one mobile VPN type.

IKEv2

Mobile VPN with IKEv2 is the most secure option and provides high-performance VPN connections. Users can connect with native Windows, macOS, or iOS clients, or with the strongSwan app for Android.

We recommend Mobile VPN with IKEv2 in most cases.

Launch Wizard... [Manually Configure](#)

SSL

Mobile VPN with SSL/TLS is a secure option, but it is slower than other Mobile VPN types. Windows and macOS users download a client from a Firebox portal. Android and iOS users download a profile from the Firebox portal for use with an OpenVPN client.

We recommend Mobile VPN with SSL when IKEv2 IPsec traffic is not allowed on the remote network or when split tunneling is required.

Launch Wizard... [Manually Configure](#)

L2TP

Mobile VPN with L2TP is a less secure option unless you configure a certificate instead of a pre-shared key. L2TP is not secure when IPsec is disabled. Users can connect with native clients on most operating systems, but manual configuration is required.

We recommend Mobile VPN with L2TP only for users with legacy operating systems that do not support IKEv2.

Launch Wizard... [Manually Configure](#)

IPSec

Mobile VPN with IPSec is a less secure option unless you configure a certificate instead of a pre-shared key. Users can connect with a WatchGuard IPSec VPN client powered by NCP, and some native VPN clients.

We recommend Mobile VPN with IPSec for legacy IPSec IKEv1 tunnels when IKEv2 is not available. We also recommend this option for experienced Firebox administrators who must deploy multiple VPN routing profiles.

Configure...



Mobile VPN with SSL Wizard

Mobile VPN with SSL Wizard

- Mobile VPN with SSL configuration is simplified with a new wizard

Mobile VPN with SSL Wizard

- You can now use a wizard to configure Mobile VPN with SSL
- The wizard prompts you for these settings and automatically creates a Mobile VPN with SSL configuration:
 - Primary domain name or IP address for client connections
 - (Optional) Backup domain name or IP address for client connections
 - Authentication servers
 - Users and groups
 - Virtual IP address pool for mobile users
- After you complete the wizard, you can manually edit the configuration and specify additional settings

Mobile VPN with SSL Wizard

- You can select to use the wizard or manually configure Mobile VPN with SSL
 - On the new Mobile VPN selection page in the Web UI and Policy Manager, the **Launch Wizard** option appears if Mobile VPN with SSL is not already configured
 - Click **Configure Manually** to skip the wizard

Mobile VPN with SSL Wizard

- Web UI

Mobile VPN

The Firebox supports several types of Mobile VPN tunnels. For most networks, we recommend Mobile VPN with IKEv2 or Mobile VPN with SSL. The Firebox supports simultaneous connections to more than one mobile VPN type.

✓ IKEv2

Mobile VPN with IKEv2 is the most secure option and provides high-performance VPN connections. Users can connect with native Windows, macOS, or iOS clients, or with the strongSwan app for Android.

We recommend Mobile VPN with IKEv2 in most cases.

[LAUNCH WIZARD](#) [Manually Configure](#)

✓ SSL

Mobile VPN with SSL/TLS is a secure option, but it is slower than other mobile VPN types. Windows and macOS users download a client from a Firebox portal. Android and iOS users download a profile from the Firebox portal for use with an OpenVPN client.

We recommend Mobile VPN with SSL when IKEv2 IPsec traffic is not allowed on the remote network or when split-tunneling is required.

[CONFIGURE](#) [DOWNLOAD CLIENT](#)

✓ L2TP

Mobile VPN with L2TP is a less secure option unless you configure a certificate instead of a pre-shared key. L2TP is not secure when IPsec is disabled. Users can connect with native clients on most operating systems, but manual configuration is required.

We recommend Mobile VPN with L2TP only for users with legacy operating systems that do not support IKEv2.

[CONFIGURE](#)

✓ IPsec

Mobile VPN with IPsec is a less secure option unless you configure a certificate instead of a pre-shared key. Users can connect with a WatchGuard IPsec VPN client powered by NCP, and some native VPN clients.

We recommend Mobile VPN with IPsec for legacy IPsec IKEv1 tunnels when IKEv2 is not available. We also recommend this option for experienced Firebox administrators who must deploy multiple VPN routing profiles.

[CONFIGURE](#)

Mobile VPN with SSL Wizard

Mobile VPN / Mobile VPN with SSL / Setup Wizard

Welcome to the WatchGuard Mobile VPN with SSL Setup Wizard



Complete this wizard to configure the Mobile VPN with SSL settings on your Firebox.

NEXT CANCEL

Mobile VPN / Mobile VPN with SSL / Setup Wizard

Specify the server addresses for client connections.

Specify the Firebox domain names or IP addresses for clients to connect to.

Primary

Backup

BACK **NEXT** CANCEL

Mobile VPN with SSL Wizard

Mobile VPN / Mobile VPN with SSL / Setup Wizard

Select the user authentication servers.

Specify the authentication servers to use for connections to Mobile SSL with VPN. The first authentication server in the list is the default server.

AUTHENTICATION SERVER

Firebox-DB (default)

Firebox-DB

Firebox-DB
example.com
RADIUS
SecurID
LDAP

Mobile VPN / Mobile VPN with SSL / Setup Wizard

Add users and groups.

Specify the users and groups for Mobile VPN with SSL. The users and groups you added to the SSLVPN-Users group.

SELECT	NAME	TYPE	SERVER
<input checked="" type="checkbox"/>	SSLVPN-Users	Group	Any
<input type="checkbox"/>	test	Group	Firebox-DB
<input type="checkbox"/>	ipsec-users	Group	Firebox-DB

Create new: Firebox-DB User

Mobile VPN with SSL Wizard

Mobile VPN / Mobile VPN with SSL / Setup Wizard

Define the virtual IP address pool.

Enter a subnet to be used as virtual address pool. Your Firebox allows 500 Mobile VPN with SSL users.

/

Mobile VPN / Mobile VPN with SSL / Setup Wizard

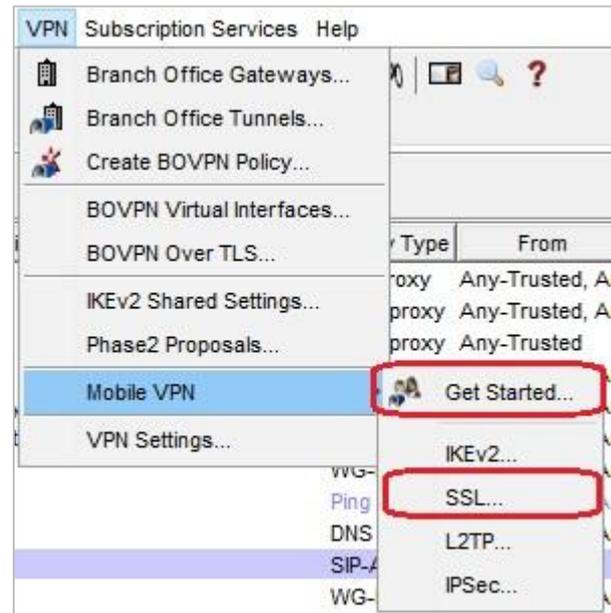
The changes were saved successfully ×

The Mobile VPN with SSL Setup Wizard is complete.

Mobile VPN with SSL is now configured on your Firebox.

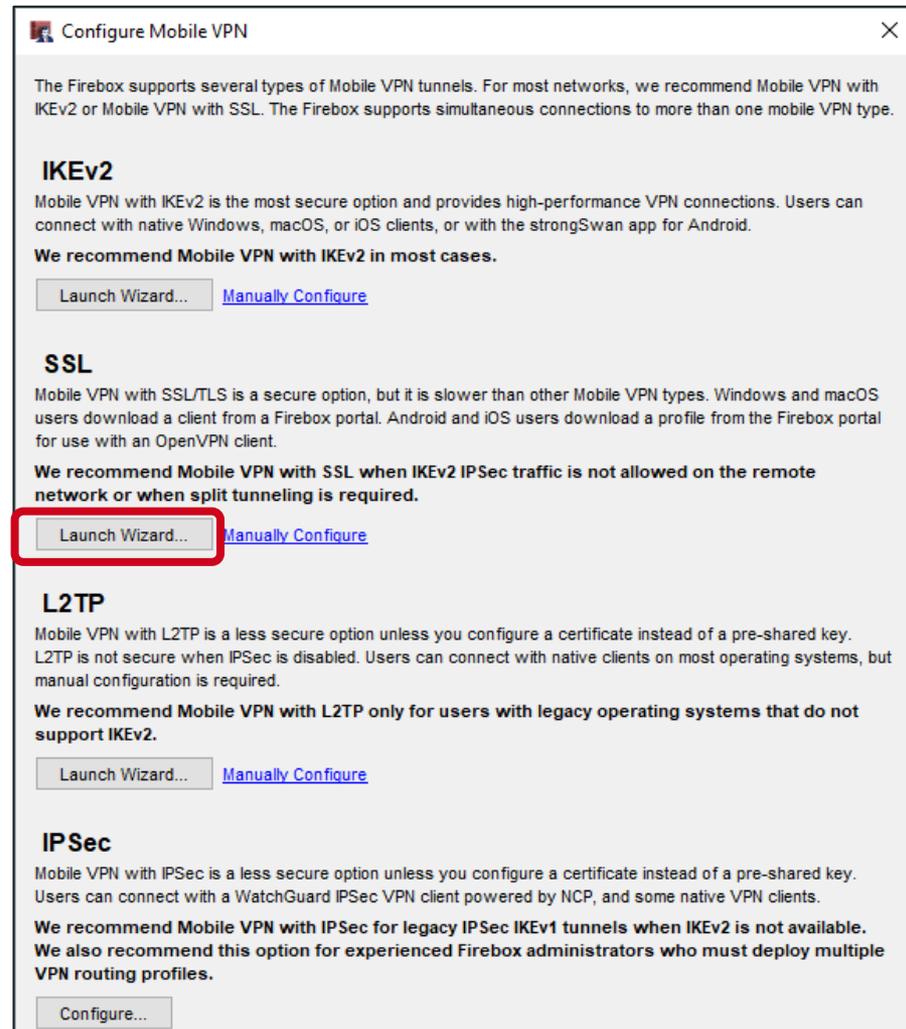
Mobile VPN with SSL Wizard

- In Policy Manager, to launch the wizard, select either of these options:
 - **VPN > Get Started**
 - **VPN > SSL**



Mobile VPN with SSL Wizard

- If you selected **Get Started**, the new VPN selection page appears
- Click **Launch Wizard**



Configure Mobile VPN

The Firebox supports several types of Mobile VPN tunnels. For most networks, we recommend Mobile VPN with IKEv2 or Mobile VPN with SSL. The Firebox supports simultaneous connections to more than one mobile VPN type.

IKEv2

Mobile VPN with IKEv2 is the most secure option and provides high-performance VPN connections. Users can connect with native Windows, macOS, or iOS clients, or with the strongSwan app for Android.

We recommend Mobile VPN with IKEv2 in most cases.

[Manually Configure](#)

SSL

Mobile VPN with SSL/TLS is a secure option, but it is slower than other Mobile VPN types. Windows and macOS users download a client from a Firebox portal. Android and iOS users download a profile from the Firebox portal for use with an OpenVPN client.

We recommend Mobile VPN with SSL when IKEv2 IPsec traffic is not allowed on the remote network or when split tunneling is required.

[Manually Configure](#)

L2TP

Mobile VPN with L2TP is a less secure option unless you configure a certificate instead of a pre-shared key. L2TP is not secure when IPsec is disabled. Users can connect with native clients on most operating systems, but manual configuration is required.

We recommend Mobile VPN with L2TP only for users with legacy operating systems that do not support IKEv2.

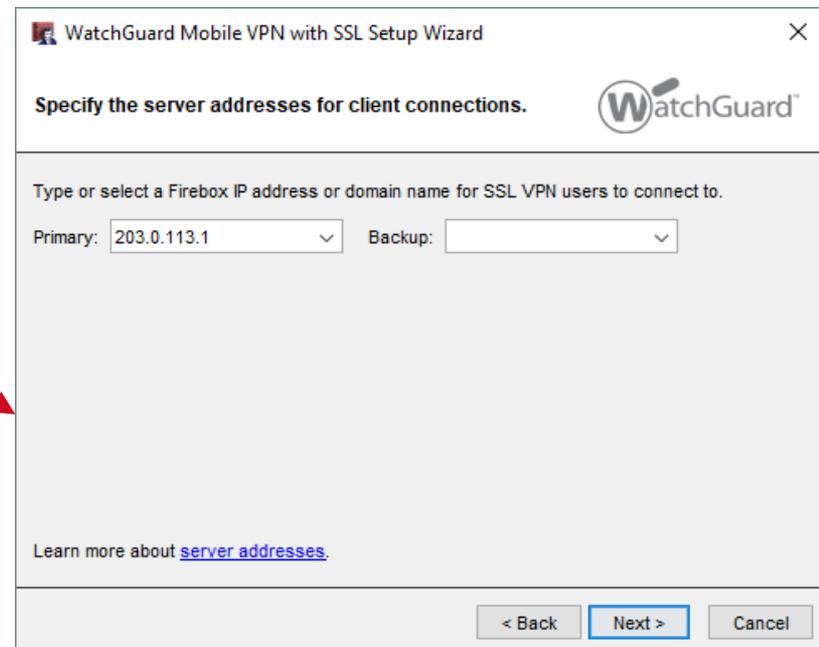
[Manually Configure](#)

IPsec

Mobile VPN with IPsec is a less secure option unless you configure a certificate instead of a pre-shared key. Users can connect with a WatchGuard IPsec VPN client powered by NCP, and some native VPN clients.

We recommend Mobile VPN with IPsec for legacy IPsec IKEv1 tunnels when IKEv2 is not available. We also recommend this option for experienced Firebox administrators who must deploy multiple VPN routing profiles.

Mobile VPN with SSL Wizard



Mobile VPN with SSL Wizard

WatchGuard Mobile VPN with SSL Setup Wizard

Specify the server addresses for client connections.

Type or select a Firebox IP address or domain name for SSL VPN users to connect to.

Primary: Backup:

[Learn more about server addresses.](#)

< Back **Next >** Cancel

WatchGuard Mobile VPN with SSL Setup Wizard

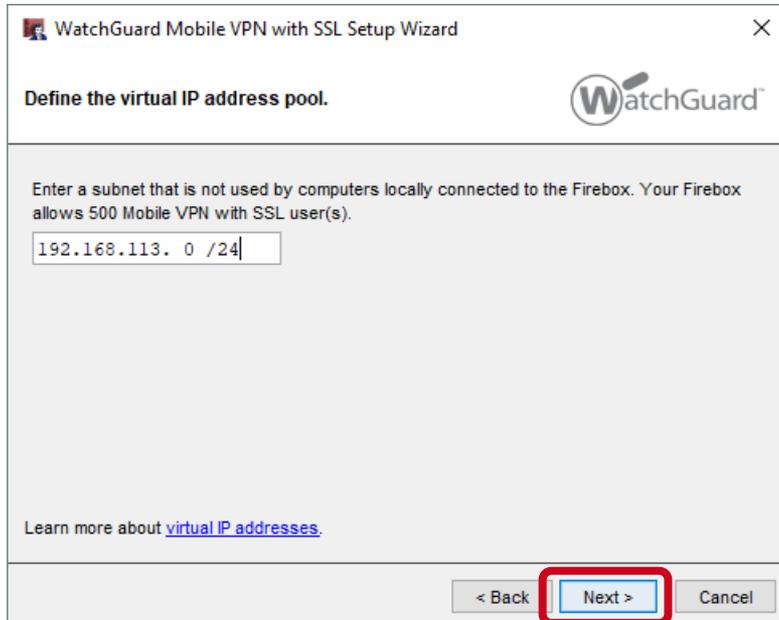
Add users and groups.

Specify the users and groups for Mobile VPN with SSL. The users and groups you specify are automatically added to the SSLVPN-Users group.

<input type="checkbox"/>	Name	Type	Authentication Server	New...
<input checked="" type="checkbox"/>	SSLVPN-Users	Group	Any	
<input type="checkbox"/>	ipsec-users	Group	Firebox-DB	
<input type="checkbox"/>	test	Group	Firebox-DB	

< Back **Next >** Cancel

Mobile VPN with SSL Wizard



WatchGuard Mobile VPN with SSL Setup Wizard

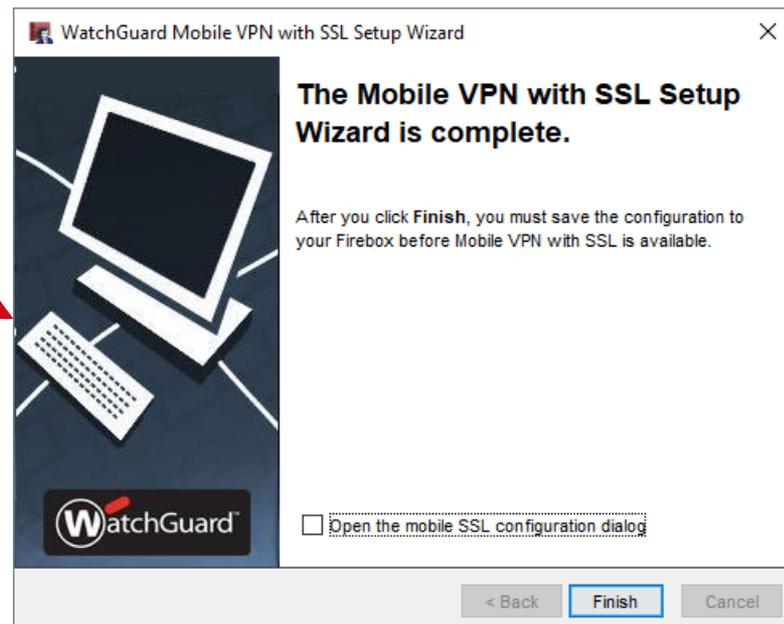
Define the virtual IP address pool.

Enter a subnet that is not used by computers locally connected to the Firebox. Your Firebox allows 500 Mobile VPN with SSL user(s).

192.168.113. 0 /24

Learn more about [virtual IP addresses](#).

< Back Next > Cancel



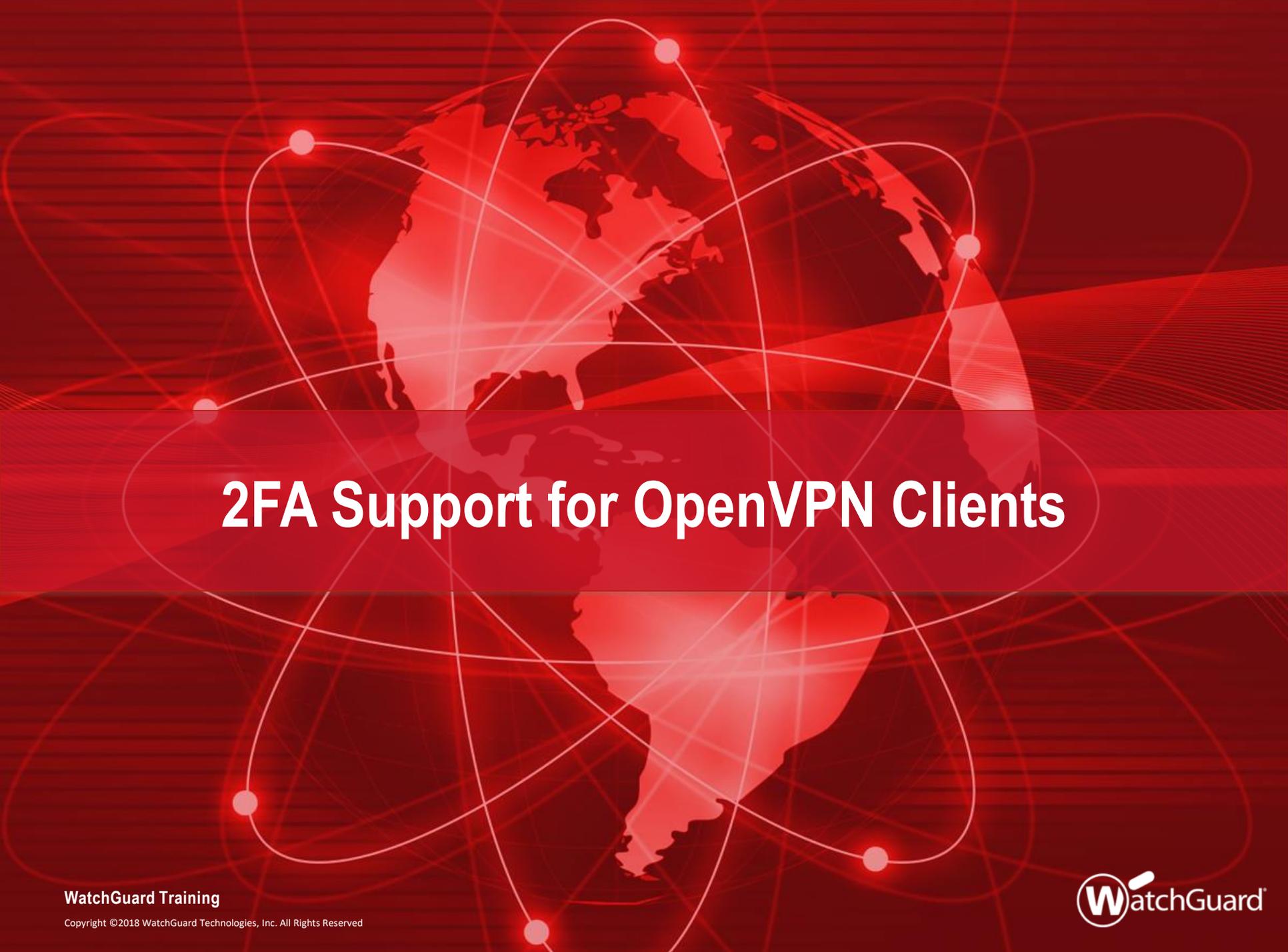
WatchGuard Mobile VPN with SSL Setup Wizard

The Mobile VPN with SSL Setup Wizard is complete.

After you click **Finish**, you must save the configuration to your Firebox before Mobile VPN with SSL is available.

Open the mobile SSL configuration dialog

< Back Finish Cancel



2FA Support for OpenVPN Clients

MFA Support for OpenVPN Clients

- Mobile VPN with SSL now supports two-factor, challenge-response authentication for native OpenVPN clients



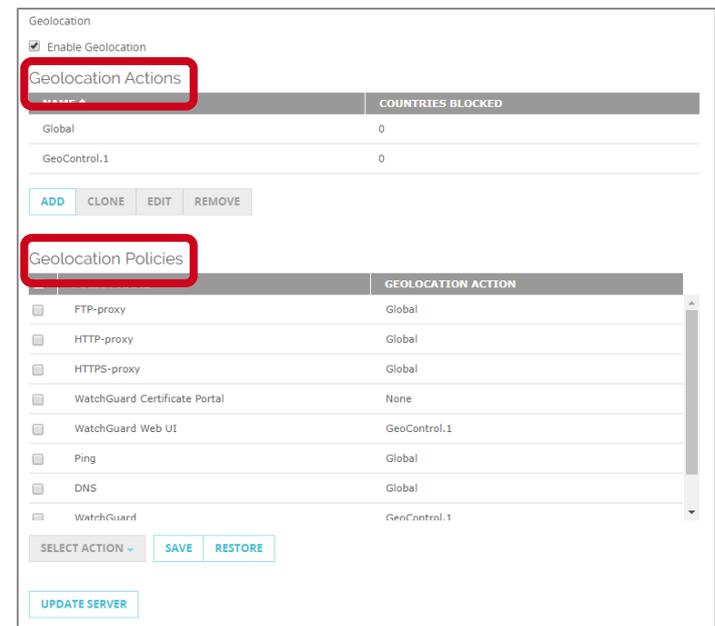
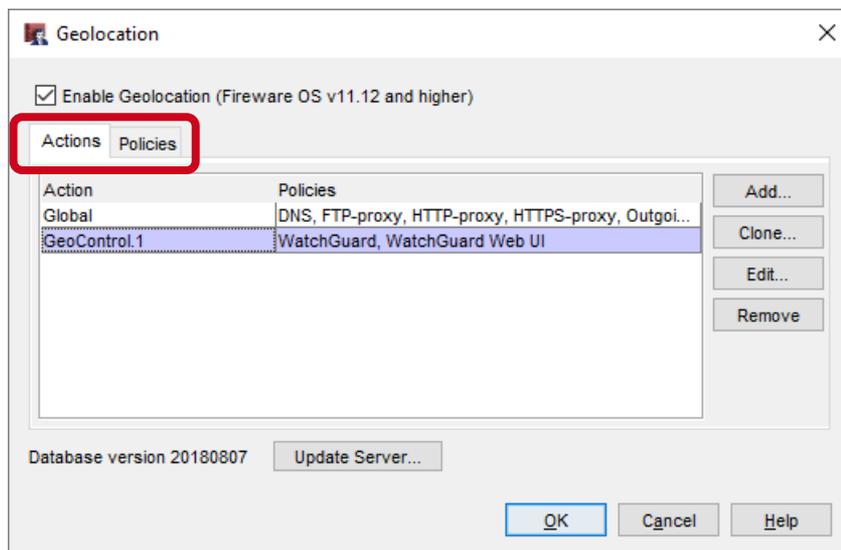
Mobile VPN with SSL users who have OpenVPN clients can type a one-time password to connect to the Firebox



Geolocation Actions

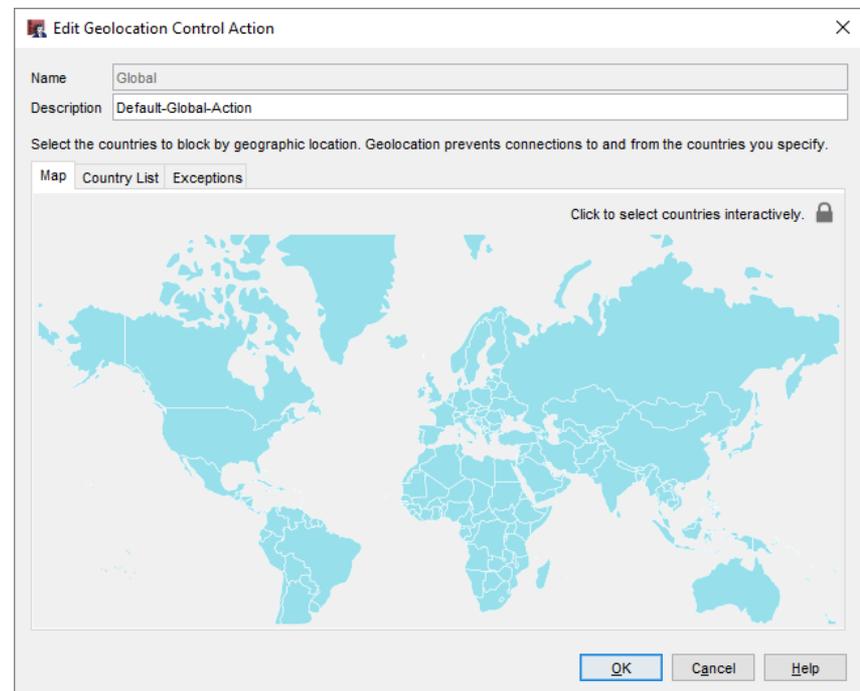
Geolocation Actions

- The Geolocation service now supports multiple actions so that you can specify different geographical restrictions by policy
- Geolocation settings now include **Actions** and **Policies**
 - **Actions:** Add and edit actions
 - **Policies:** Assign actions to policies



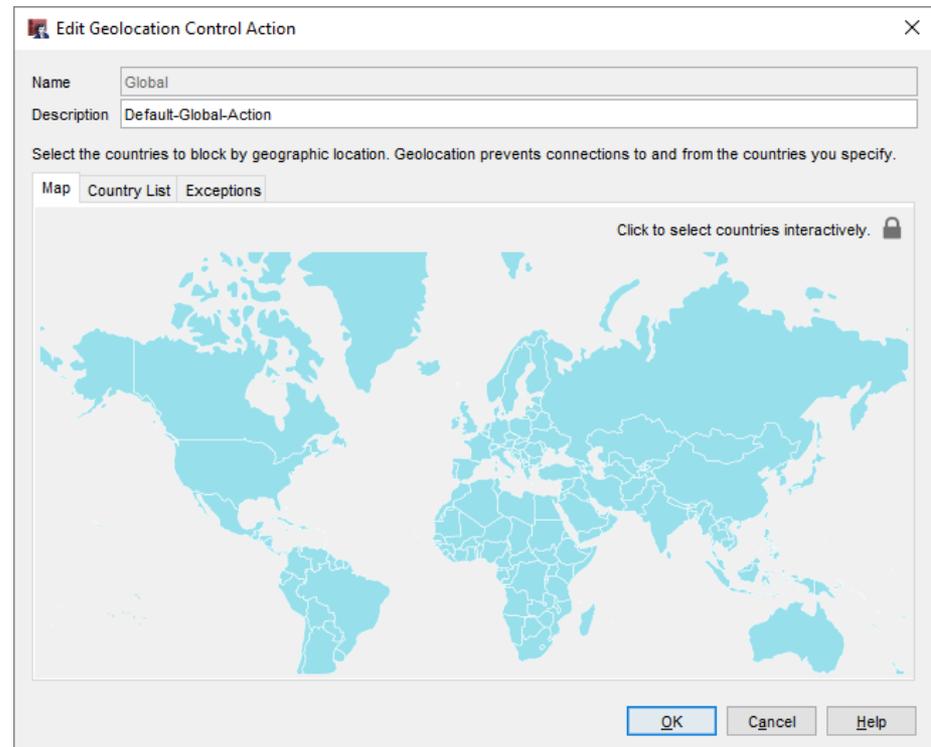
Geolocation Actions

- Geolocation actions contain the same settings that were previously configured as global Geolocation settings:
 - Countries to block
 - Exceptions (shared by all Geolocation actions)
- The **Global** action is added by default
 - You cannot remove it



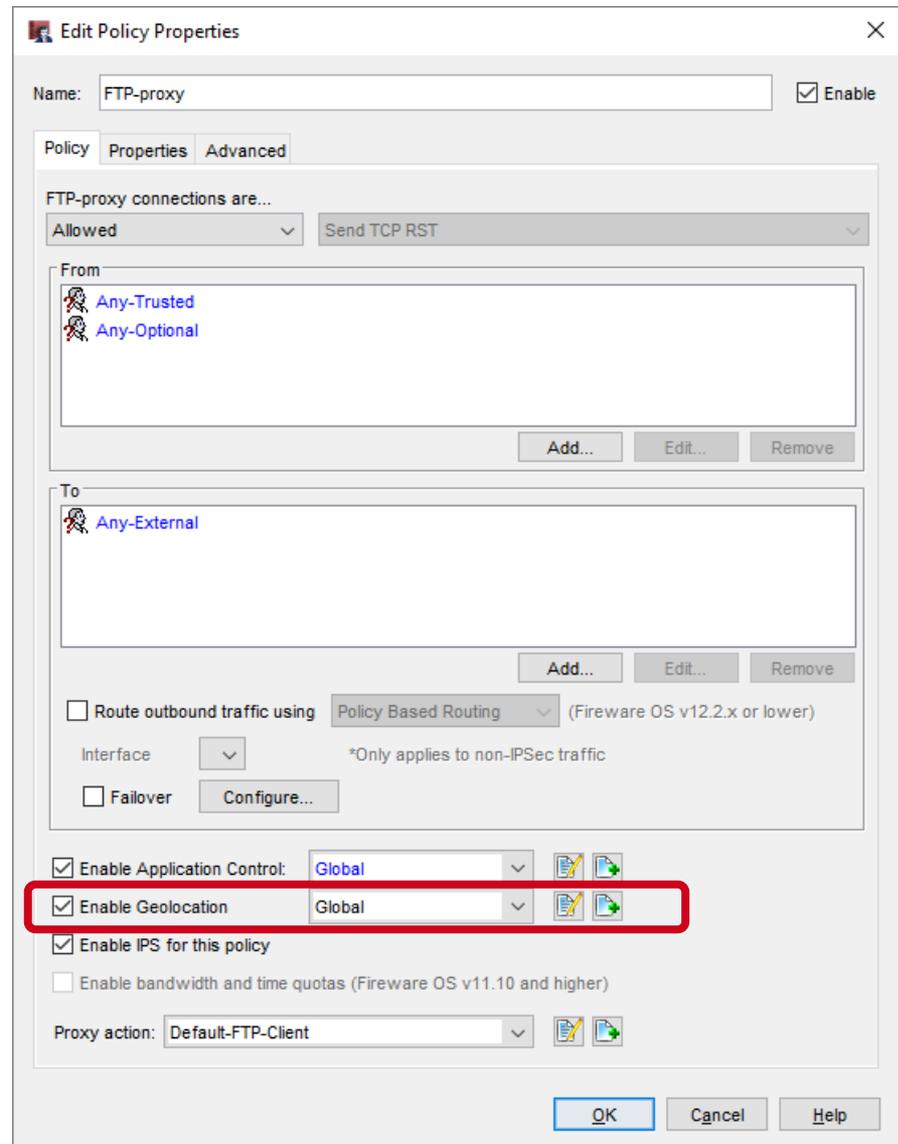
Geolocation Actions

- When you upgrade to Fireware v12.3:
 - Previous Geolocation settings are moved to the Global action
 - The Global action is assigned to all policies that have Geolocation enabled



Geolocation Actions

- You can also configure Geolocation in a policy
 - Enable Geolocation
 - Select the Geolocation action to use
 - Click the adjacent icons to to:
 - Edit the selected action
 - Add a new action



Geolocation Actions

- The Policies list has a new Geolocation column
- This column shows the configured Geolocation action for each policy

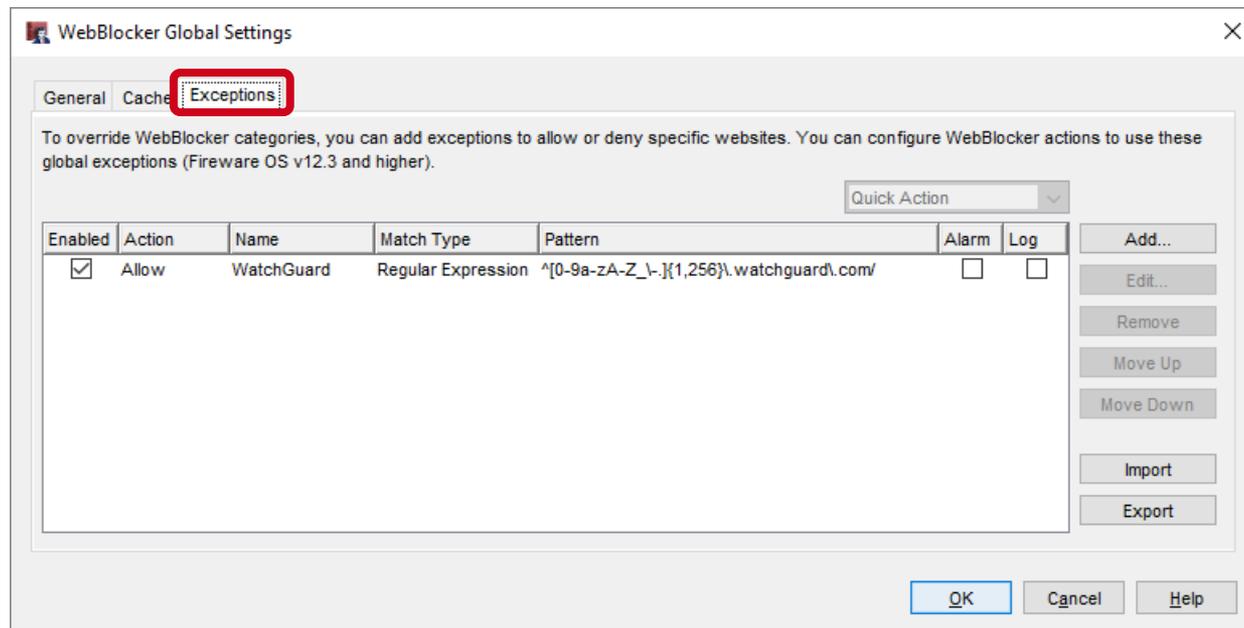
The screenshot shows the WatchGuard FireWall configuration interface. The 'Policies' list is displayed, and a new 'Geolocation' column has been added to the table. The 'Geolocation' column is highlighted with a red box, and all entries in this column are set to 'Global'.

Order	Action	Policy Name	Policy Type	From	To	Port	PBR	SD-WAN	App Control	Geolocation
	FTP-proxy	FTP-proxy	FTP-proxy	Any-Trusted, ,Any-External		tcp:21			Global	Global
	HTTP-proxy	HTTP-proxy	HTTP-proxy	Any-Trusted, ,Any-External		tcp:80			Global	Global
	HTTPS-proxy	HTTPS-proxy	HTTPS-proxy	Any-Trusted, ,Any-External		tcp:443			Global	Global
	WatchGuard Certificate Portal	WG-Cert-Portal	WG-Cert-Portal	Any-Trusted, ,Firebox		tcp:4126			None	Global
	WatchGuard Web UI	WG-Fireware-XTM-WebUI	WG-Fireware-XTM-WebUI	Any-Trusted, ,Firebox		tcp:8080			None	Global
	Ping	Ping	Ping	Any-Trusted, ,Any		icmp (type: 8, ...			Global	Global
	DNS	DNS	DNS	Any-Trusted, ,Any-External		tcp:53 udp:53			Global	Global
	WatchGuard	WG-Firebox-Mgmt	WG-Firebox-Mgmt	Any-Trusted, ,Firebox		tcp:4105 tcp:4...			None	Global
	Outgoing	TCP-UDP	TCP-UDP	Any-Trusted, ,Any-External		tcp:0 (Any) u...			Global	Global

WebBlocker Enhancements

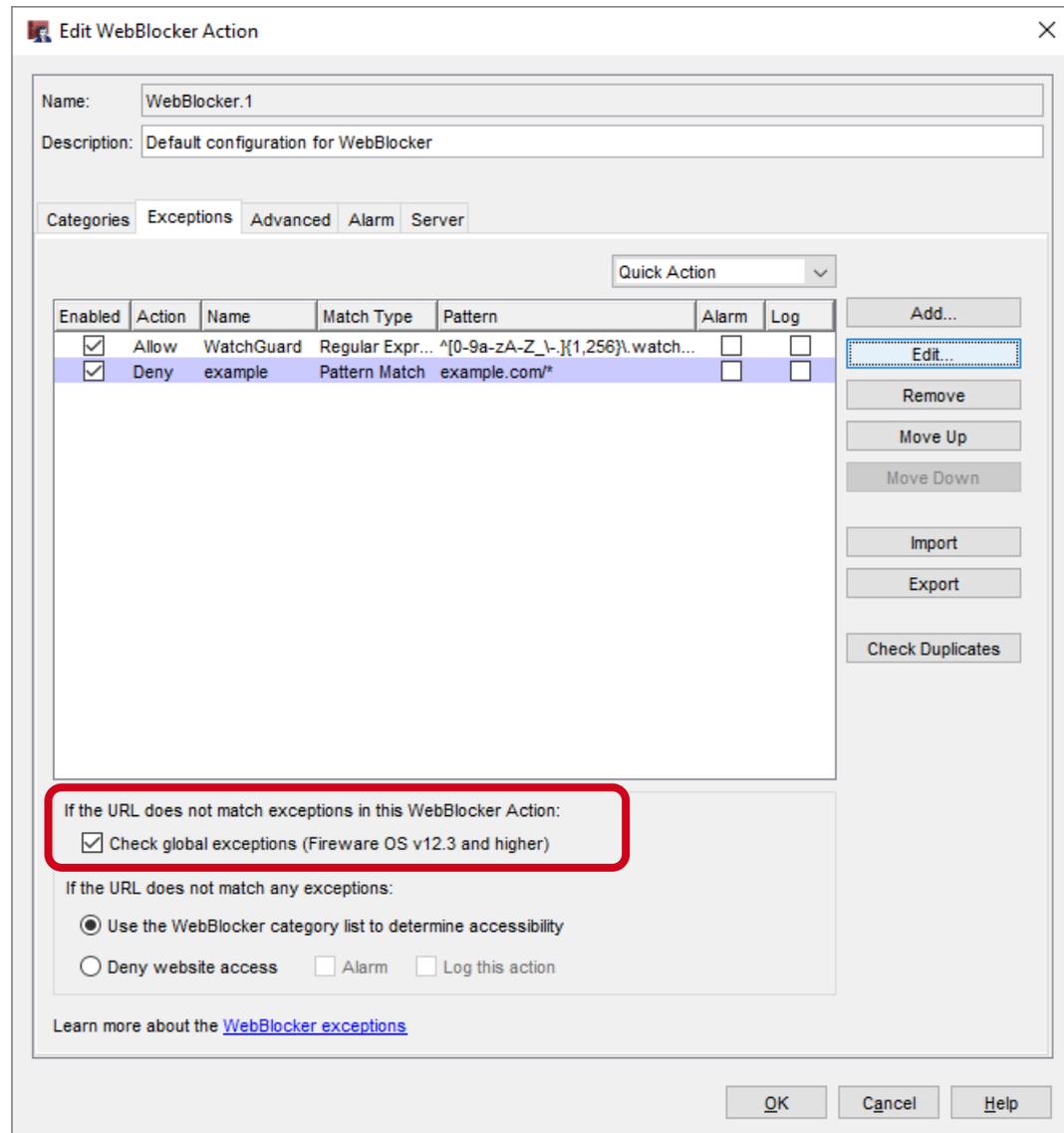
WebBlocker Enhancements

- WebBlocker has a new global exceptions list
 - This eliminates the need to add the same exceptions to multiple WebBlocker actions
 - The global exceptions list includes a predefined exception to allow connections to WatchGuard servers



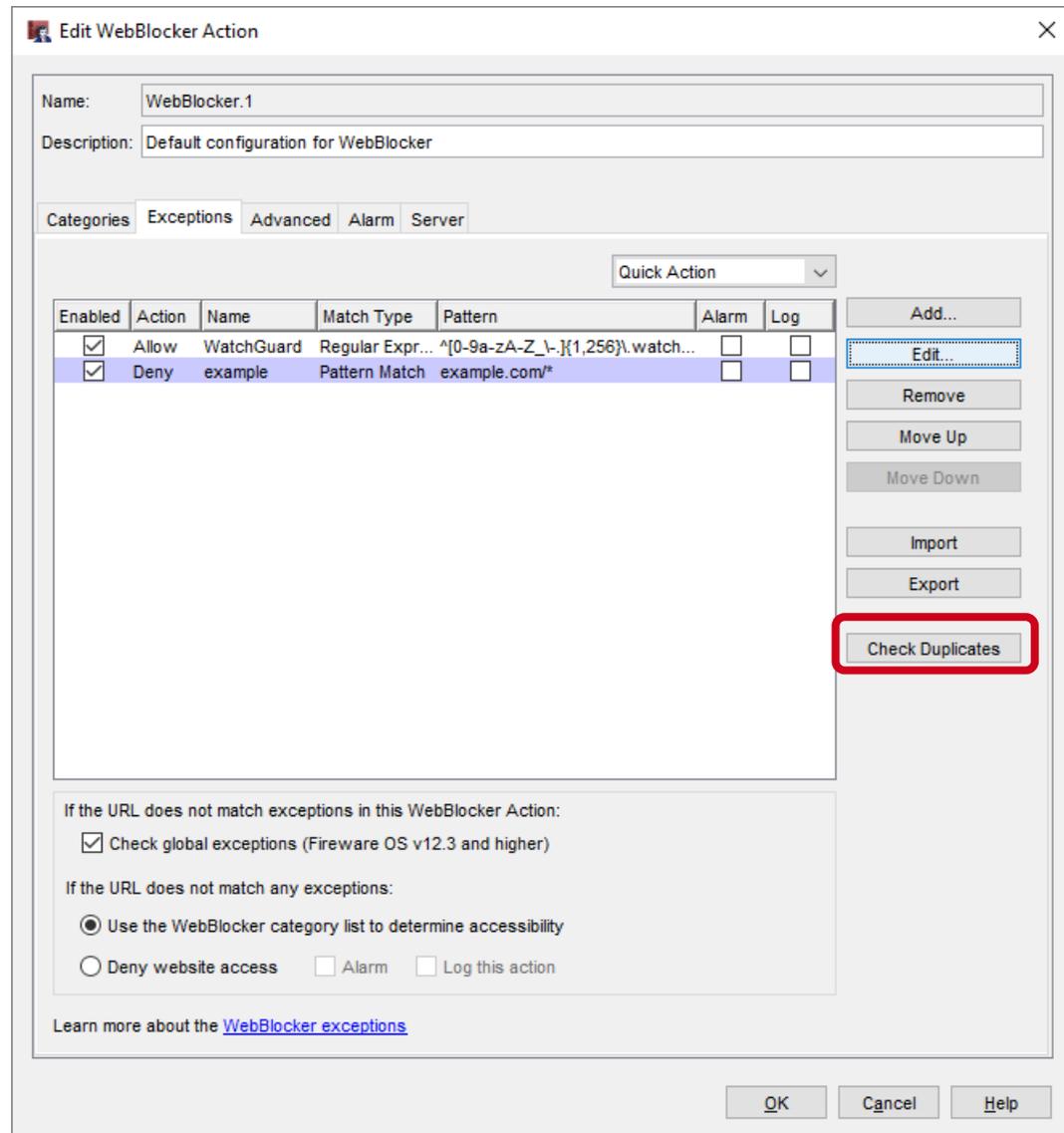
WebBlocker Enhancements

- In each WebBlocker action, you control whether the action uses the global exception list for URLs that do not match exceptions in the WebBlocker action
- Local exceptions take precedence over global exceptions



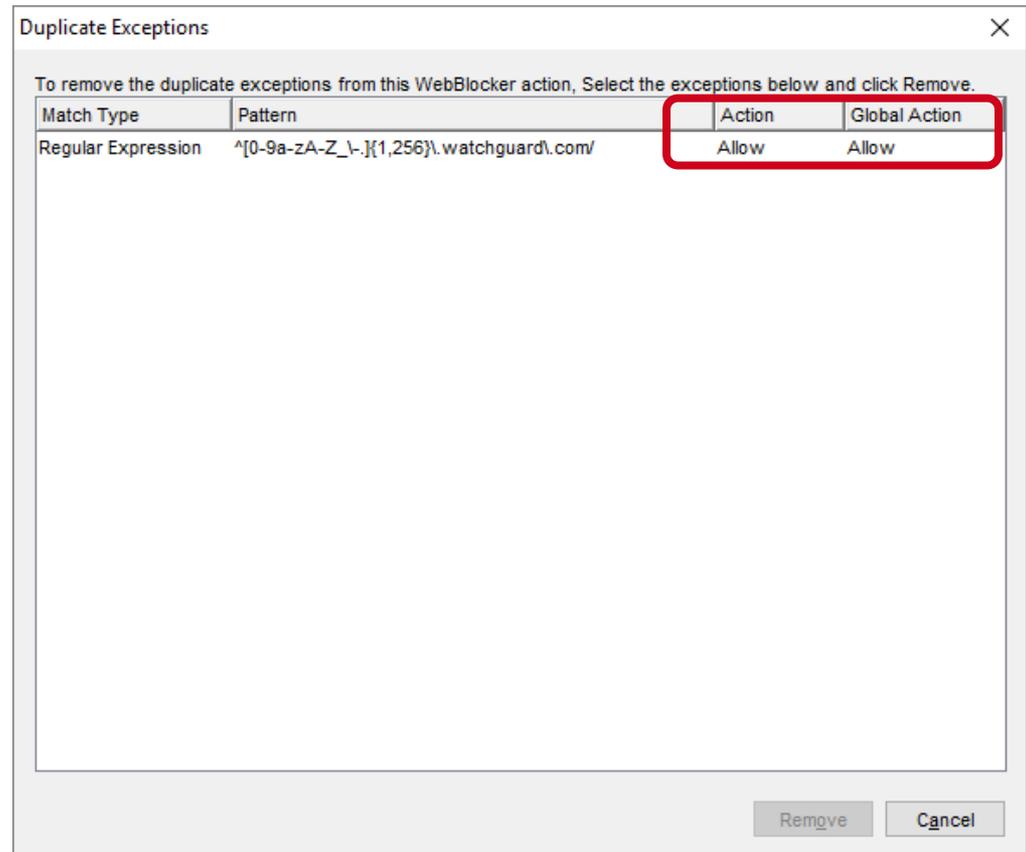
WebBlocker Enhancements

- To identify any duplication between the global exceptions and local exceptions in the WebBlocker action, click **Check Duplicates**
- This check compares all enabled exceptions that have the same Match Type and Pattern



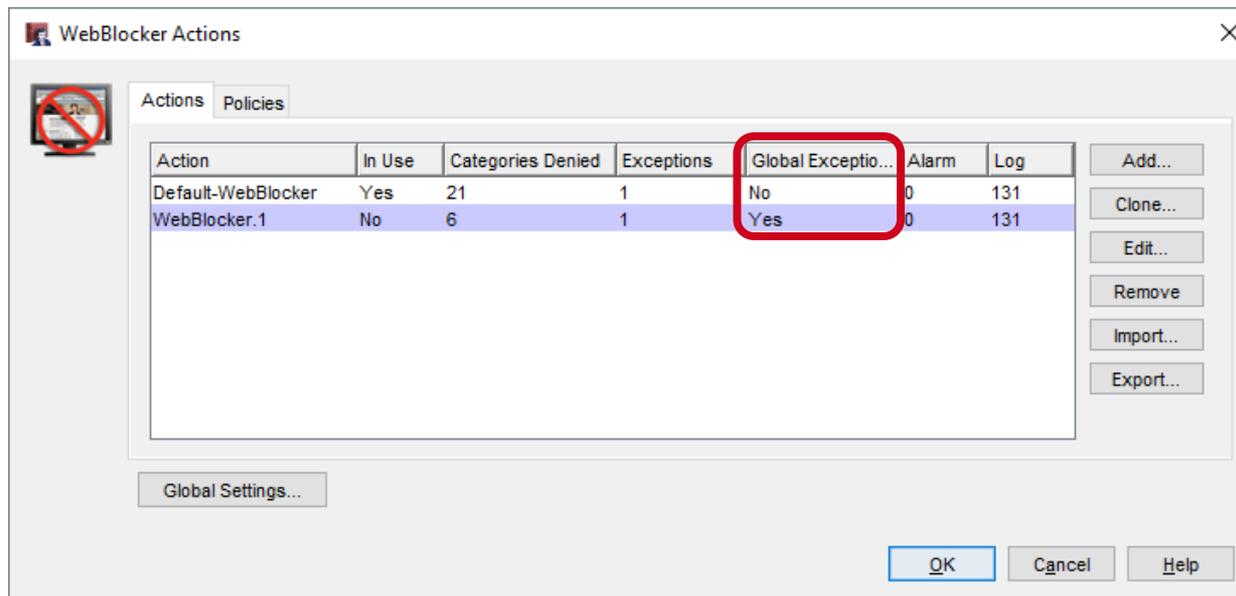
WebBlocker Enhancements

- The **Duplicate Exceptions** list shows both the global action and the local action for a duplicate exception
- To remove a duplicate exception from the local exceptions list, select the exception and click **Remove**



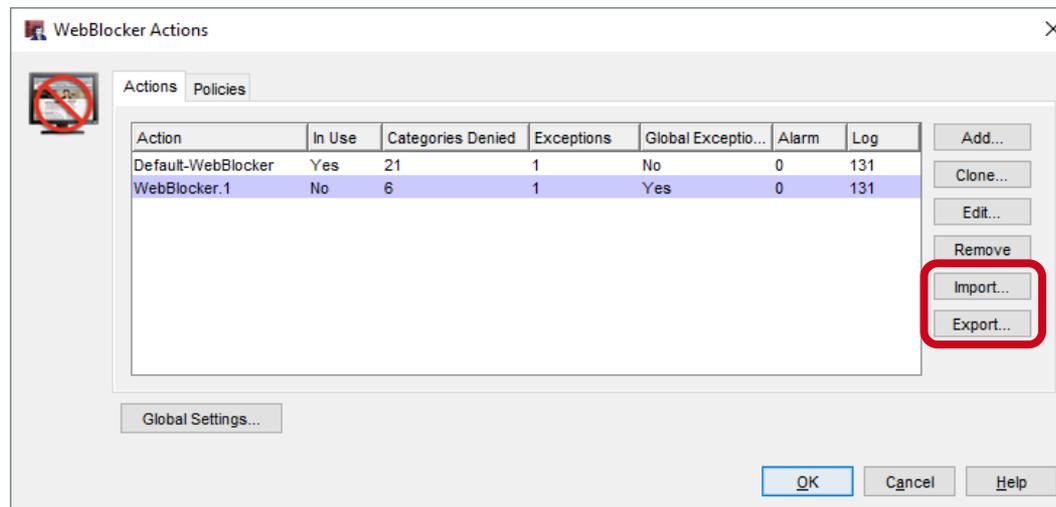
WebBlocker Enhancements

- In the WebBlocker Actions list, the **Global Exceptions** column shows whether each action uses the global exceptions list



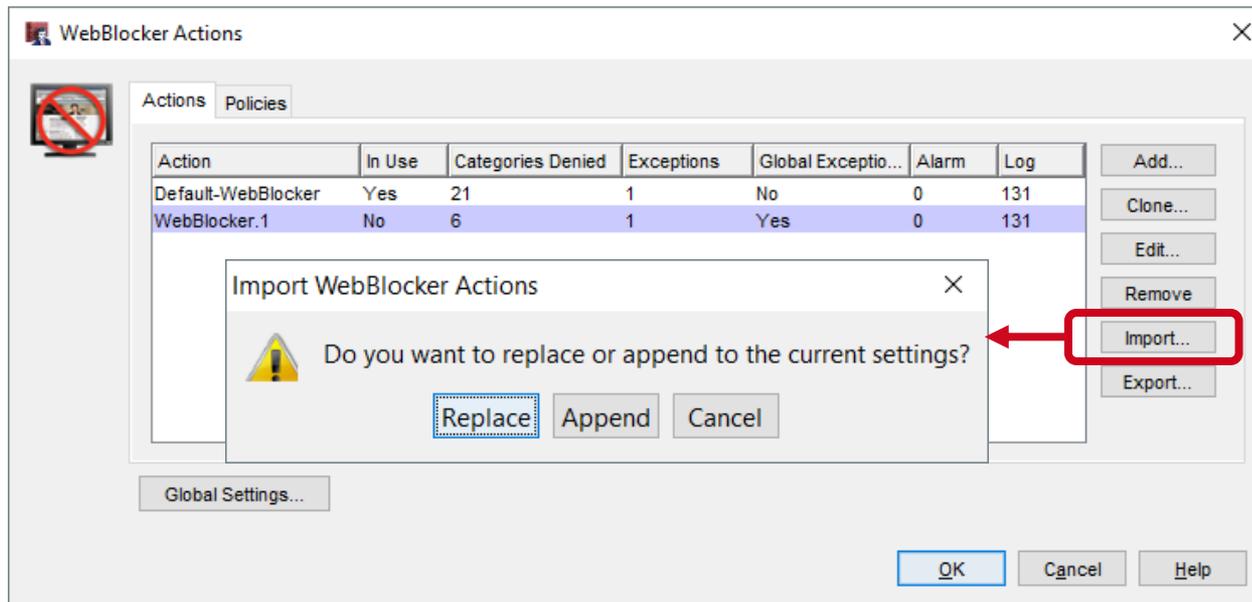
WebBlocker Enhancements

- To make it easier to use the same WebBlocker settings on different Fireboxes, you can now export and import WebBlocker actions
 - Import and export is supported only in Policy Manager
 - Exported WebBlocker actions are stored as XML in a text file
 - Default path: \users\\Documents\My WatchGuard



WebBlocker Enhancements

- When you import WebBlocker actions to your Firebox, specify whether to replace existing actions:
 - Replace — Add new actions and replace any existing actions with imported actions that have the same name
 - Append — Add new actions but do not replace existing actions



WebBlocker Enhancements

- In the WebBlocker action Advanced tab, you can now enable logs and alarms for WebBlocker local overrides:
 - Alarm — Select to send an alarm when a user enters the local override password
 - Log this action — Select to send a message to the log file when a user enters the local override password

The message appears in the log with "Allowed by overriding category action" in the details field

The screenshot shows the 'Advanced' tab of the WebBlocker configuration interface. Under the 'Local Override' section, there is a checkbox for 'Enable WebBlocker local override' which is checked. Below this, there are fields for 'Passphrase' and 'Confirm' (both masked with dots), and an 'Inactivity Timeout' set to 5 minutes. At the bottom of the section, two checkboxes are checked and highlighted with a red box: 'Alarm (Fireware OS v12.3 and higher)' and 'Log this action (Fireware OS v12.3 and higher)'.

WebBlocker Enhancements

- When your WebBlocker license expires, a new **License Bypass Action** column in the WebBlocker Actions page shows whether an action allows or denies access to all sites
- You can now change the license bypass action for WebBlocker actions after your WebBlocker license expires
- In the WebBlocker action, select the **Advanced** tab, then select **Allowed** or **Denied** from the **License Bypass** drop-down list

The screenshot displays the 'WebBlocker Actions' window. A red box highlights the 'License Bypass Action' column in the table, which shows 'Deny' for the 'Default-WebBlocker' action. Below the table, a detailed view of the 'License Bypass' configuration is shown, with a red box highlighting the dropdown menu that lists 'denied', 'allowed', and 'denied'.

Action	Categories Denied	Exceptions	Global Exceptions	Alarm	Log	License Bypass Action
Default-WebBlocker	21	2	Yes	0	131	Deny

License Bypass

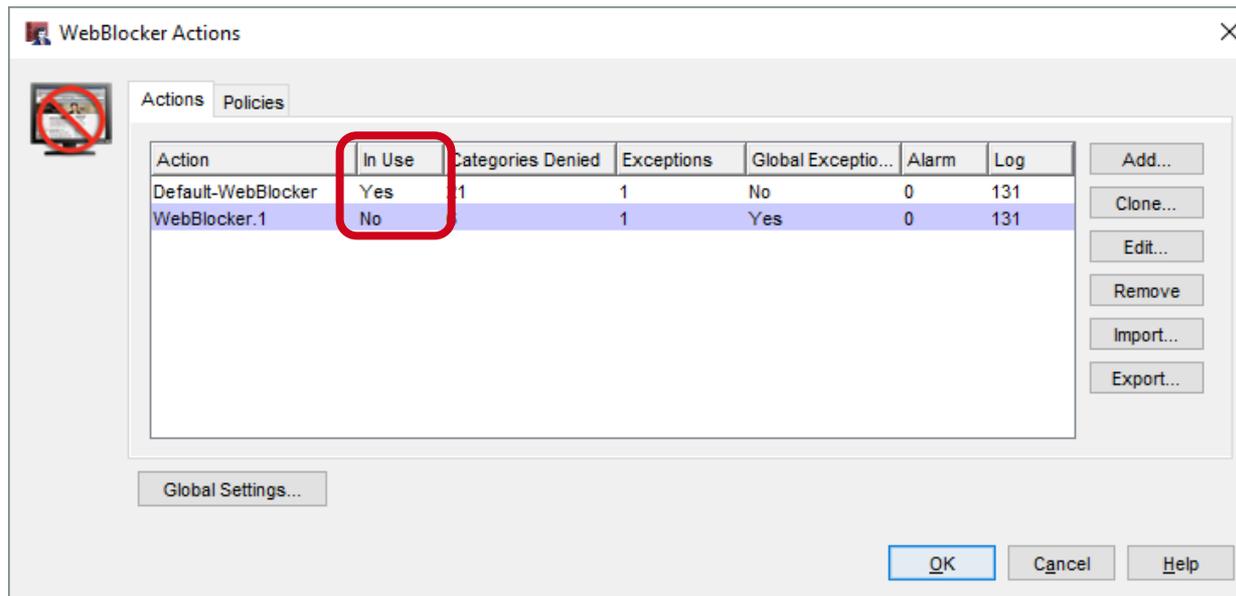
When the WebBlocker license expires, access to all sites is **denied** ▼

Override the diagnostic log level for proxy policies that use this WebBlocker action

Diagnostic log level for this WebBlocker action: Error ▼

WebBlocker Enhancements

- In Policy Manager, in the WebBlocker Actions list, a new **In Use** column shows whether each WebBlocker action is used by a proxy action
- You can use this column to identify WebBlocker actions that are no longer used and can be removed



Services Usability Enhancements

IntelligentAV

- IntelligentAV is now a separate menu item in the Subscription Services menu in Policy Manager and Firewall Web UI
- Previously, IntelligentAV was available from within the Gateway AV settings

The screenshot shows the Fireware Policy Manager window with the Subscription Services menu open. The menu items include: Access Portal, Application Control..., APT Blocker..., Botnet Detection..., Data Loss Prevention..., DNSWatch..., Gateway AntiVirus, Geolocation..., **IntelligentAV...**, Intrusion Prevention..., Mobile Security..., Quarantine Server..., Reputation Enabled Defense..., spamBlocker, Threat Detection..., and WebBlocker.

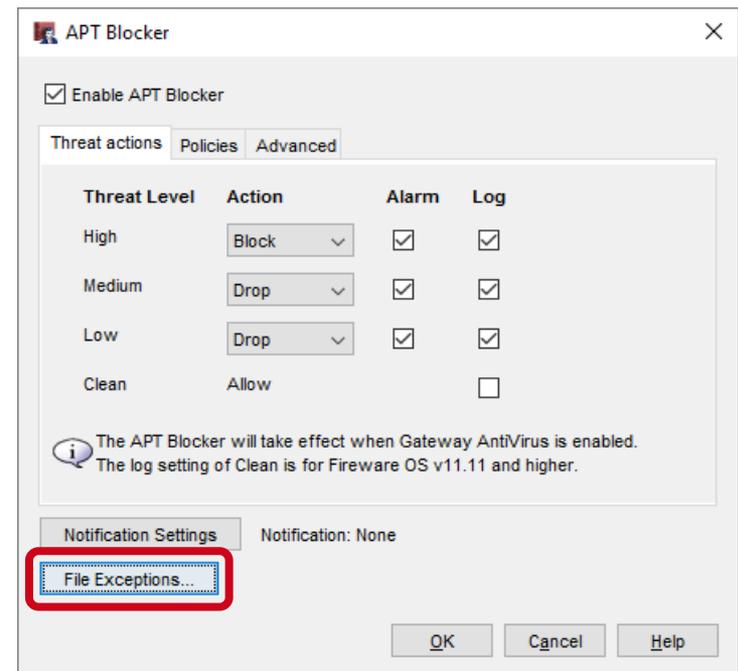
The main window displays a table of policies with the following columns: Order, Action, and Policy Name. The policies listed are:

Order	Action	Policy Name
1	[Icons]	FTP-proxy
2	[Icons]	HTTP-proxy
3	[Icons]	HTTPS-proxy
4	[Icons]	WatchGuard Certif
5	[Icons]	WatchGuard Web
6	[Icons]	Ping
7	[Icons]	DNS
8	[Icons]	WatchGuard
9	[Icons]	Outgoing

At the bottom right of the window, the text "Fireware OS v12.3.0" is visible.

File Exceptions

- The File Exceptions option has moved from the Subscription Services menu to a button within each of these services:
 - APT Blocker
 - Gateway AV
 - IntelligentAV
 - Data Loss Prevention
- This makes it easier to edit exceptions while you configure services
- The same file exceptions are still shared between these services



Intrusion Prevention Service

- In Fireware Web UI, the IPS menu item in the Subscription Services menu is now renamed to Intrusion Prevention Service

The screenshot displays the WatchGuard Fireware Web UI. On the left is a dark sidebar menu with the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, Access Portal, Application Control, APT Blocker, Botnet Detection, Data Loss Prevention, DNSWatch, Gateway AV, Geolocation, IntelligentAV, **Intrusion Prevention Service** (highlighted with a red box), Mobile Security, Network Discovery, Quarantine Server, and Reputation Enabled Defense. The main content area is titled 'Fireware Web UI' and shows a 'Front Panel' with three sections: 'Top Clients', 'Top Destinations', and 'Top Policies'. Each section contains a table with columns for NAME, RATE, BYTES, and HI.

NAME	RATE	BYTES	HI
10.158.4.36	4 Mbps	681 KB	6
203.0.113.70	184 bps	1 MB	1

NAME	RATE	BYTES	HI
203.0.113.90	4 Mbps	2 MB	7

NAME	RATE	BYTES	HI
WatchGuard Web UI	4 Mbps	681 KB	6
Allow-IKE-to-Firebox	184 bps	1 MB	1

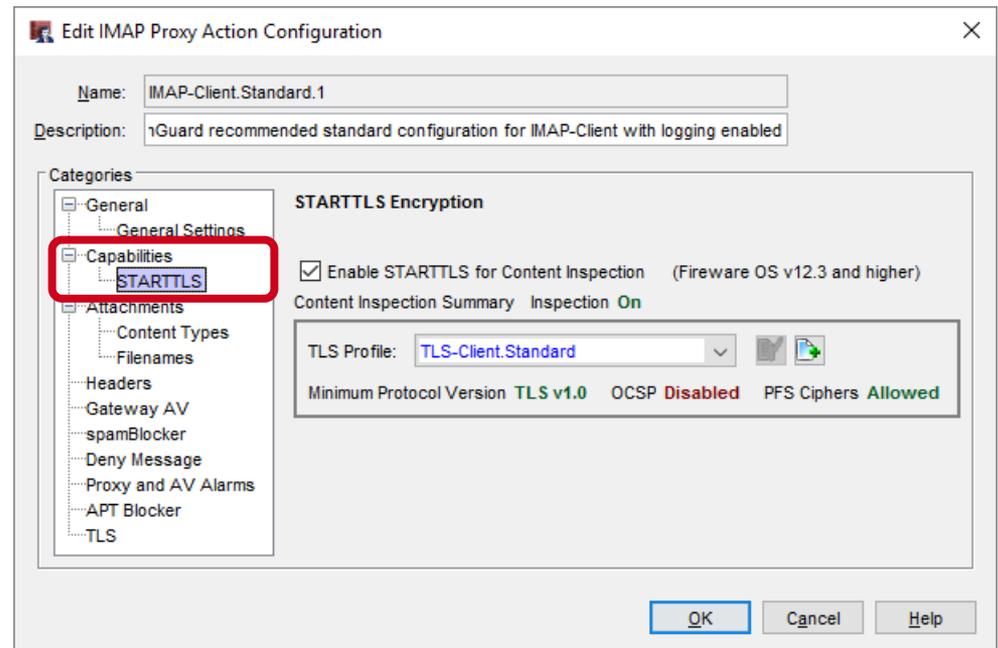
STARTTLS in the IMAP Proxy

STARTTLS in the IMAP Proxy

- The IMAP proxy now supports STARTTLS
 - This feature enables IMAP clients to use the STARTTLS command to upgrade an IMAP connection to a secure channel and perform content inspection on the encrypted data
- STARTTLS functionality for IMAP is simpler than for SMTP
 - In the IMAP proxy action there are no separate rules for sender and recipient encryption
 - The encryption is end-to-end

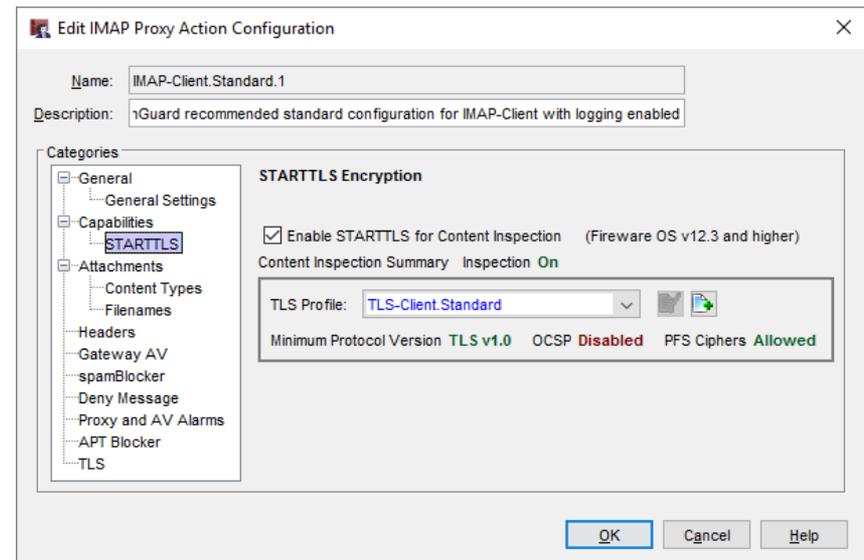
STARTTLS in the IMAP Proxy

- In the IMAP proxy action, STARTTLS settings are below **Capabilities**
 - To enable STARTTLS, select the **Enable STARTTLS for Content Inspection** check box
 - The **Content Inspection Summary** appears only when STARTTLS is enabled
 - When STARTTLS is enabled, Inspection is always On



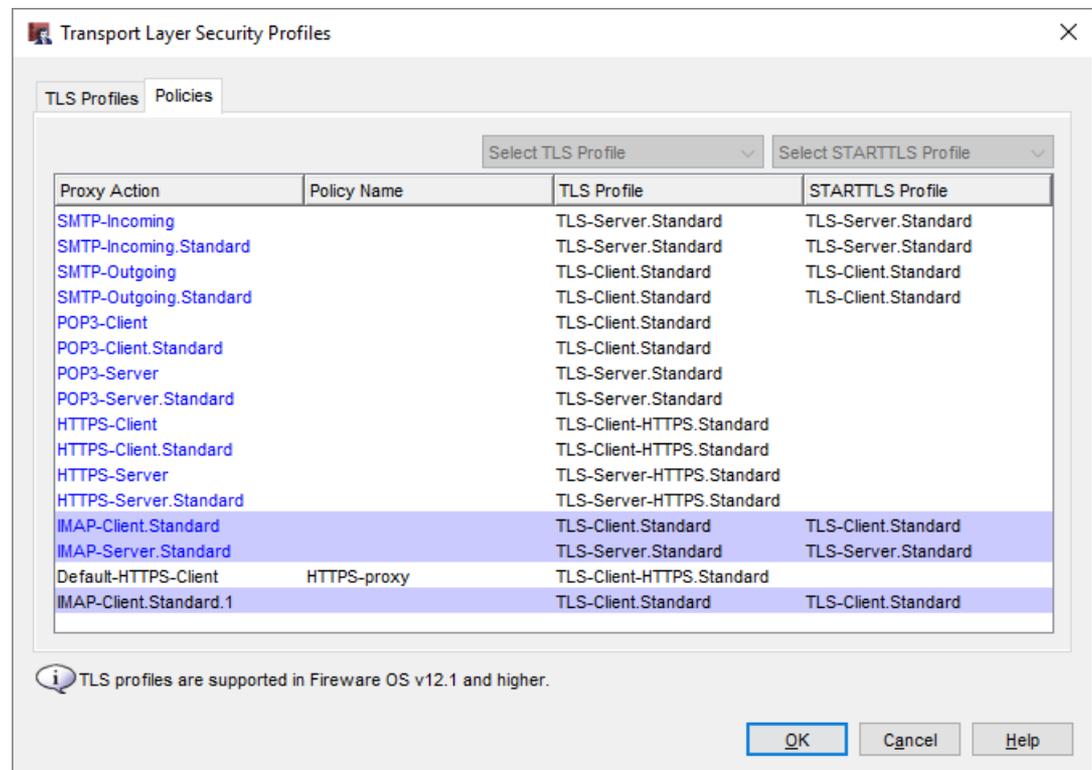
STARTTLS in the IMAP Proxy

- You can enable both STARTTLS and IMAPS (TLS) in the same proxy action
- When both STARTTLS and IMAPS (TLS) are enabled, each connection uses only one encryption method:
 - Connections on port 993 use IMAPS
 - Connections on port 143 use STARTTLS



STARTTLS in the IMAP Proxy

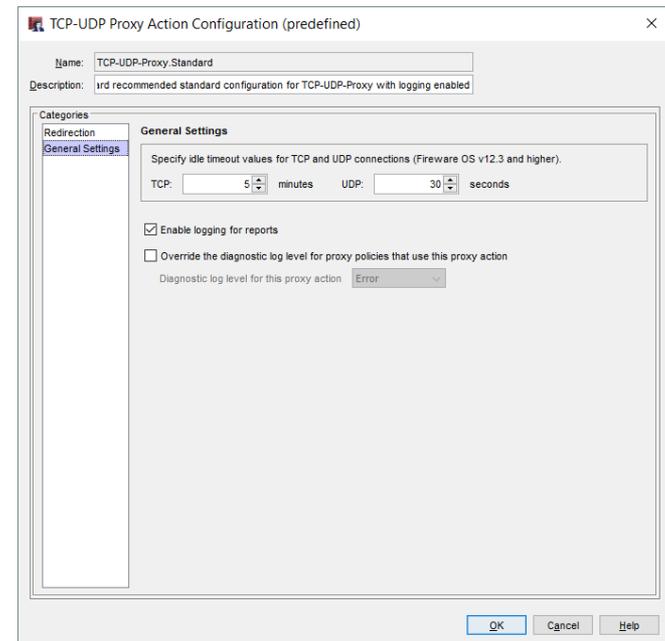
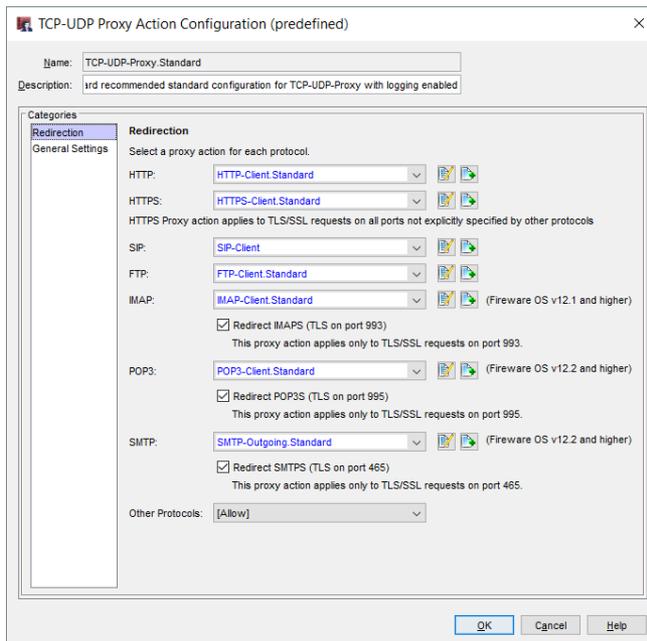
- The IMAP proxy action can now use two different TLS profiles, one for TLS and one for STARTTLS
- In the TLS Profiles configuration, the Policies list now shows both the TLS and STARTTLS profiles configured in each IMAP proxy action



TCP-UDP Proxy Action Enhancements

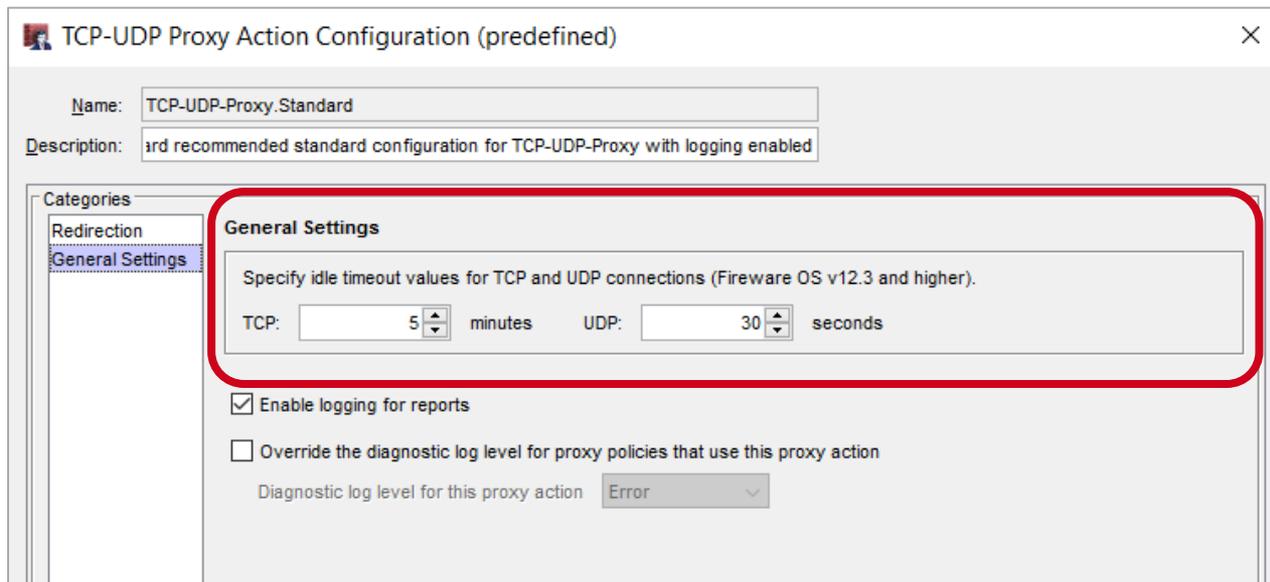
TCP-UDP Proxy Action Enhancements

- TCP-UDP Proxy Action settings are now reorganized into two categories:
 - **Redirection:** Configure proxy actions to redirect traffic
 - **General Settings:** Configure timeout values and logging settings



TCP-UDP Proxy Action Enhancements

- You can now specify when idle TCP and UDP connections will timeout:
 - **TCP:** Specify a number of minutes (default is 5 minutes)
 - **UDP:** Specify a number of seconds (default is 30 seconds)



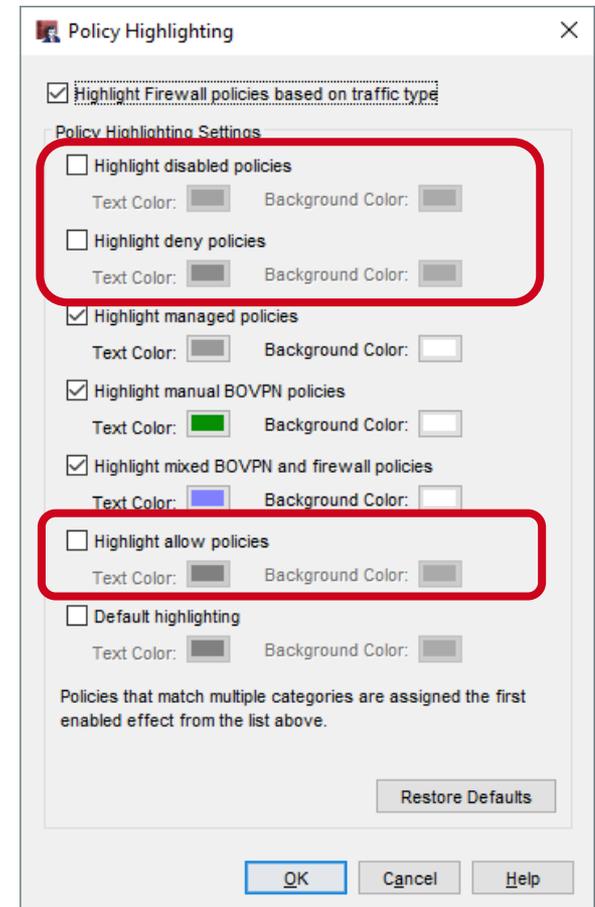
The screenshot shows the 'TCP-UDP Proxy Action Configuration (predefined)' window. The 'Name' field is 'TCP-UDP-Proxy.Standard' and the 'Description' is 'Ird recommended standard configuration for TCP-UDP-Proxy with logging enabled'. The 'Categories' list on the left includes 'Redirection' and 'General Settings'. The 'General Settings' section is highlighted with a red box and contains the following text: 'Specify idle timeout values for TCP and UDP connections (Fireware OS v12.3 and higher)'. Below this text, there are two input fields: 'TCP: 5 minutes' and 'UDP: 30 seconds'. The 'TCP' field has a spinner control with the number '5' and the unit 'minutes'. The 'UDP' field has a spinner control with the number '30' and the unit 'seconds'. Below the timeout settings, there are two checkboxes: 'Enable logging for reports' (checked) and 'Override the diagnostic log level for proxy policies that use this proxy action' (unchecked). At the bottom, there is a 'Diagnostic log level for this proxy action' dropdown menu set to 'Error'.



Policy Highlighting Enhancements

Policy Highlighting Enhancements

- In Policy Manager, the Policy Highlighting dialog box now includes three new settings:
 - Highlight disabled policies
 - Highlight deny policies
 - Highlight allow policies
- When you upgrade, the new settings are disabled by default
- Policy highlighting settings are now listed in order of precedence
- If a policy matches more than one setting, it uses colors from the highest ranked setting it matches





Tigerpaw Integration

Tigerpaw Integration

- You can now integrate a Firebox with Tigerpaw, a professional service automation tool
- Integration is similar to the existing ConnectWise and Autotask integrations
- Tigerpaw integration enables you to:
 - Automatically synchronize your Firebox asset and subscription information to Tigerpaw cloud or on-premise servers
 - Set event monitoring thresholds for a wide range of Firebox parameters to automatically create service order tickets in Tigerpaw

Tigerpaw Integration

- Available as a new tab on the **System > Technology Integrations** page
- Configure Tigerpaw server login credentials, external account ID, details for service orders and assets

Technology Integrations

Autotask | ConnectWise | **Tigerpaw**

Enable Tigerpaw

Login Credentials

Hostname

Username

Password

Account

You must provide the external account ID of a Tigerpaw account.

External Account ID

Service Orders

You must choose the service-order type, board, and priority that is used for new service orders.

Service Order Type [LOOKUP](#)

Service Order Board [LOOKUP](#)

Ticket Priority [LOOKUP](#)

Asset

You must provide the type and name of the Tigerpaw Asset that will be created for the Firebox.

Asset Type [LOOKUP](#)

Asset Name

Tigerpaw Integration

- Set thresholds for event monitoring
- Events that exceed the threshold automatically generate a service order in Tigerpaw

Event Monitoring

You may choose to configure event-monitoring thresholds which control event reporting.

Certificate Expiration	<input type="text" value="60 days prior"/>	PRESETS
Feature-Key Expiration	<input type="text" value="60 days prior"/>	PRESETS
CPU Usage	<input type="text" value="Disabled"/>	PRESETS
Memory Usage	<input type="text" value="> 90% over 10 minutes"/>	PRESETS
Total Connections	<input type="text" value="> 90% over 5 minutes"/>	PRESETS
Total SSLVPN Connections	<input type="text" value="Disabled"/>	PRESETS
Total IPSec Connections	<input type="text" value="Disabled"/>	PRESETS
Total L2TP Connections	<input type="text" value="Disabled"/>	PRESETS
Interface Status	<input type="text" value="Any down over 10 seconds"/>	PRESETS
Botnet Detection	<input type="text" value="Disabled"/>	PRESETS
Flood Detection	<input type="text" value="Disabled"/>	PRESETS
Virus Detection	<input type="text" value="> 10 over 30 minutes"/>	PRESETS
Intrusion Detection	<input type="text" value="> 10 over 30 minutes"/>	PRESETS
Spam Detection	<input type="text" value="> 100 over 30 minutes"/>	PRESETS

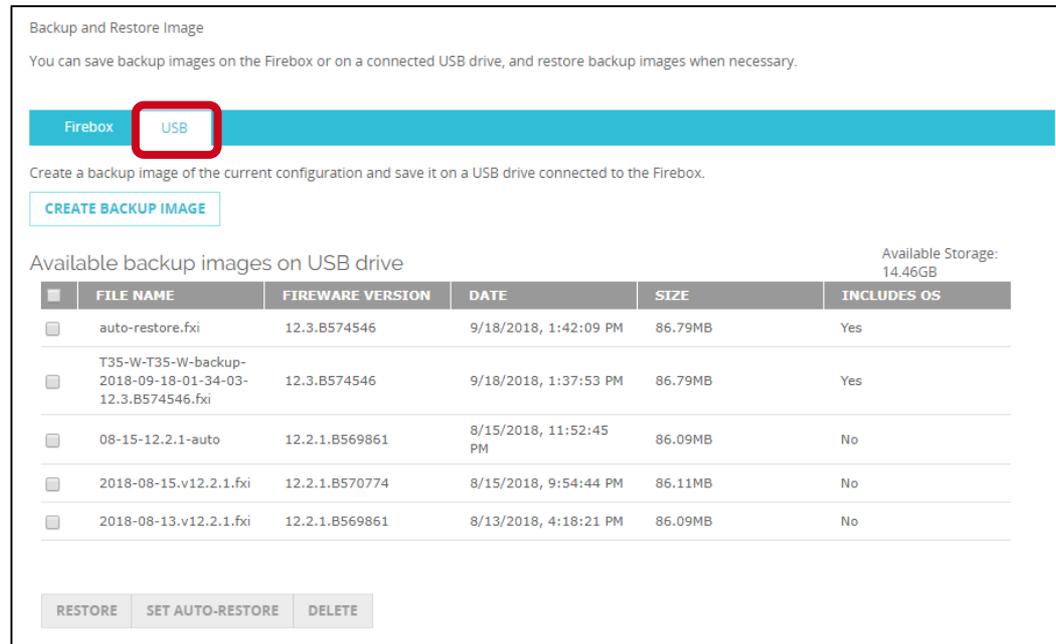
USB Backup Enhancements

USB Backup Enhancements

- This release adds enhancements to the back up process when you save backup images on a USB drive connected to the Firebox:
 - The Backup and Restore Image page in Web UI now enables you to back up and restore images from the connected USB drive
 - When you save a backup image to the USB drive, you can now choose whether to include Fireware OS
 - Auto-restore of a backup image from the USB drive now works
 - The auto-restore backup image is now stored on the USB drive in a folder path that includes the Firebox model
 - When you downgrade Fireware OS, you can now restore a compatible backup image from the USB drive

Manage Backup Images on a USB Drive

- You can now use the Backup and Restore Image page in Fireware Web UI to see and manage backup images saved on a USB drive connected to the Firebox
 - Select **System > Backup and Restore**
 - Select the **USB** tab



Backup and Restore Image

You can save backup images on the Firebox or on a connected USB drive, and restore backup images when necessary.

Firebox **USB**

Create a backup image of the current configuration and save it on a USB drive connected to the Firebox.

[CREATE BACKUP IMAGE](#)

Available backup images on USB drive Available Storage: 14.46GB

	FILE NAME	FIREWARE VERSION	DATE	SIZE	INCLUDES OS
<input type="checkbox"/>	auto-restore.fx	12.3.B574546	9/18/2018, 1:42:09 PM	86.79MB	Yes
<input type="checkbox"/>	T35-W-T35-W-backup-2018-09-18-01-34-03-12.3.B574546.fx	12.3.B574546	9/18/2018, 1:37:53 PM	86.79MB	Yes
<input type="checkbox"/>	08-15-12.2.1-auto	12.2.1.B569861	8/15/2018, 11:52:45 PM	86.09MB	No
<input type="checkbox"/>	2018-08-15.v12.2.1.fx	12.2.1.B570774	8/15/2018, 9:54:44 PM	86.11MB	No
<input type="checkbox"/>	2018-08-13.v12.2.1.fx	12.2.1.B569861	8/13/2018, 4:18:21 PM	86.09MB	No

[RESTORE](#) [SET AUTO-RESTORE](#) [DELETE](#)

Include Fireware OS in USB Backup Images

- You can now choose whether to include the Fireware OS in backup images saved to the USB drive
- To save backup images to the USB drive:
 - Fireware Web UI: Select **System > Backup and Restore Image**. Click **Create Backup Image**.
 - Firebox System Manager: Select **Tools > USB Drive**. Click **Create**.
- Select the **Include OS** check box to include the Fireware OS in the backup image (not included by default)

Add Backup Image Name X

Specify a password to use to encrypt the backup image file. This password will be required if you want to restore the backup image to the USB drive later.

Image Name .fxi

Password

Confirm

include OS

Select an Auto-Restore Backup Image

- A Firebox in recovery mode can now automatically restore a backup image created in Fireware 12.3 from the USB drive
- To use the auto-restore feature, you must upgrade SysB on your Firebox to version 12.3
- To select the backup image to auto-restore:
 1. In Fireware Web UI or FSM, select a backup image that includes the Fireware OS
 2. Click **Set Auto-Restore**
 3. Type the password that was used to encrypt the file

The screenshot shows the Fireware Web UI interface for selecting a backup image. At the top, there are tabs for 'Firebox' and 'USB'. Below the tabs, there is a section titled 'Available backup images on USB drive' with a sub-header 'Available Storage: 14.46GB'. A table lists several backup images with columns for 'FILE NAME', 'FIREWARE VERSION', 'DATE', 'SIZE', and 'INCLUDES OS'. The second row, representing a backup image with Fireware version 12.3, is highlighted in blue and has a red checkmark in the selection column. Below the table, there are three buttons: 'RESTORE', 'SET AUTO-RESTORE', and 'DELETE'. The 'SET AUTO-RESTORE' button is highlighted with a red rectangular box.

	FILE NAME	FIREWARE VERSION	DATE	SIZE	INCLUDES OS
<input type="checkbox"/>	auto-restore.fx	12.3.B574546	9/18/2018, 1:48:05 PM	86.79MB	Yes
<input checked="" type="checkbox"/>	T35-W-T35-W-backup-2018-09-18-01-34-03-12.3.B574546.fx	12.3.B574546	9/18/2018, 1:37:53 PM	86.79MB	Yes
<input type="checkbox"/>	08-15-12.2.1-auto	12.2.1.B569861	8/15/2018, 11:52:45 PM	86.09MB	No
<input type="checkbox"/>	2018-08-13.v12.2.1.fx	12.2.1.B569861	8/13/2018, 4:18:21 PM	86.09MB	No

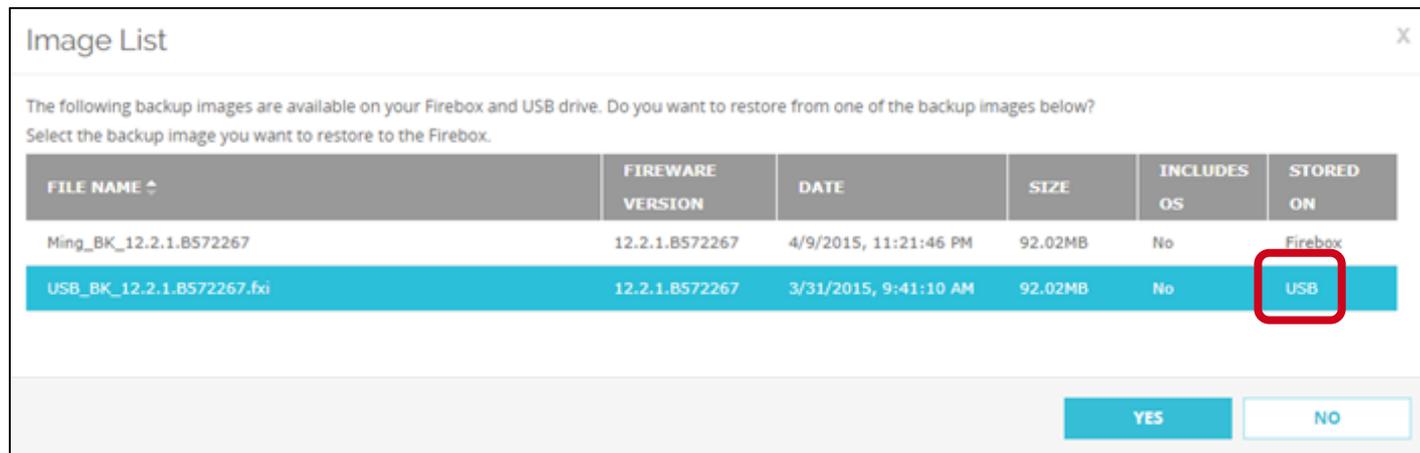
A duplicate of the selected image is saved on the USB drive at:
 /pending/usb/auto-restore/<Firebox Model>/auto-restore.fx

Auto-Restore Backup from the USB Drive

- To auto-restore the selected backup image from the connected USB drive, you must start your Firebox in [recovery mode](#)
- If the USB drive contains a valid auto-restore image for the Firebox, the Firebox automatically restores the backup image and reboots

Downgrade and Restore USB Backup Image

- If you use the Fireware Web UI Upgrade feature to downgrade the Fireware OS, you can now choose to restore a backup image that does not include the Fireware OS from a USB drive



- To use a backup image from the USB drive that includes the Fireware OS to downgrade, use the Restore feature



Active Directory Wizard

Active Directory Wizard

- You can now use a wizard to configure Active Directory server settings on your Firebox
- The wizard simplifies the configuration process because it automatically determines these settings based on the domain name you specify:
 - Search base settings
 - Active Directory server address
- After you complete the wizard, you can manually edit the Active Directory server settings
- If you prefer not to use the wizard, you can click **Skip** to manually configure an Active Directory server

Active Directory Wizard

- Policy Manager —
 - Select **Next** to use the wizard
 - Select **Skip** to manually configure settings



Active Directory Wizard

The image shows two overlapping windows from the WatchGuard Active Directory Wizard. The background window is the 'Domain Name' step, and the foreground window is the 'Active Directory Server' step. A red box highlights the 'Next >' button in the background window, with a red arrow pointing to the foreground window.

Active Directory Domain Wizard

Domain Name

What is the name of the Active Directory domain?

Domain Name

Learn more about [domain name](#).

< Back **Next >**

Active Directory Domain Wizard

Active Directory Server

What is the Domain Name or IP Address for the Active Directory server?

Server Address

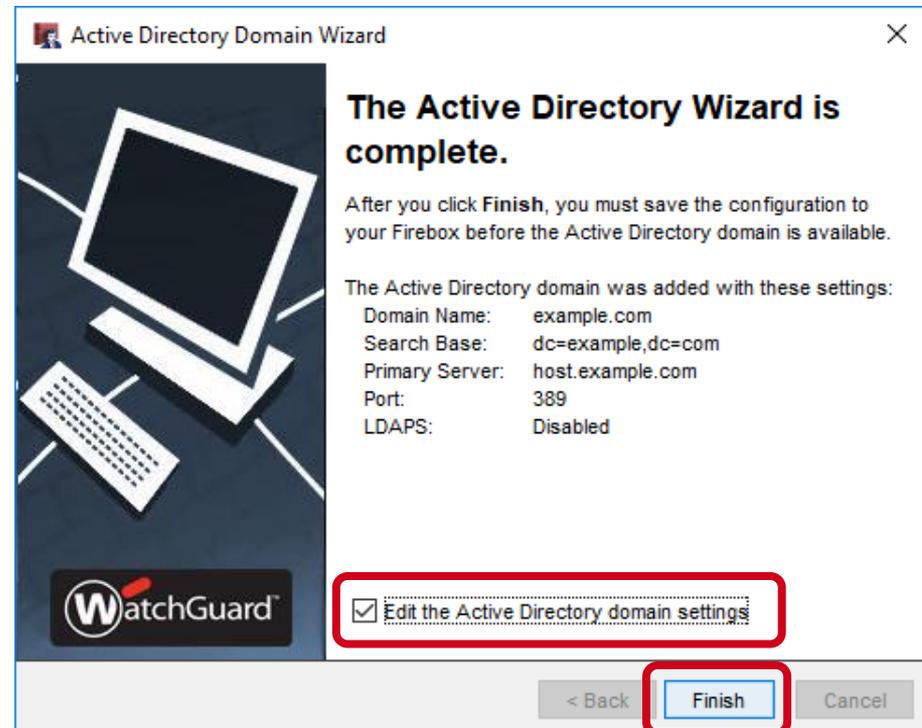
Enable secure SSL connections to your Active Directory server (LDAPS)

Learn more about [server addresses](#).

< Back **Next >** Cancel

Active Directory Wizard

- On the last page of the wizard, you can select to edit the Active Directory server settings after you click **Finish**



Active Directory Wizard

- If you select to edit the settings, or if you select **Skip** in the wizard, the manual configuration page appears

Edit Active Directory Domain

Make sure that your users can successfully authenticate to the Active Directory servers you specify.

Domain Name:

IP Address / DNS Name:

IP / DNS	Port
host.example.com	389

Timeout:

Dead Time:

Search Base:

Group String:

Login Attribute:

DN of Searching User:

Password of Searching User:

Enable LDAPS
 Validate server certificate



IPv6 Support for Active Directory SSO

IPv6 Support for Active Directory SSO

- Most Active Directory single sign-on (SSO) components now support IPv6
 - The Firebox, SSO Agent, SSO Client, and Event Log Monitor support IPv6
 - Exchange Monitor does not support IPv6 in Fireware v12.3
- On the Firebox, you can configure either an IPv4 or IPv6 address for the SSO agent if the Firebox can connect to either

SSO Agents

Specify the IP address of servers on which the SSO Agent is installed. The first SSO Agent in the list is active unless failover occurs to another SSO Agent. To initiate manual failover, [click here](#).

<input type="checkbox"/>	SSO AGENT IP ADDRESS	DESCRIPTION
<input type="checkbox"/>	1.1.1.1	
<input type="checkbox"/>	2018::1	

IPv6 Support for Active Directory SSO

- You can also specify an IPv6 address for a network, range, or host in the **SSO Exceptions** list
- To reduce unnecessary network traffic, make sure to add exceptions for IPv6 hosts you want to exclude from SSO queries

Add SSO Exception

Choose Type Host IPv6 ▾

Host IPv6

Description

Host IPv6
Host IPv4
Network IPv4
Host Range IPv4
Host IPv6
Network IPv6
Host Range IPv6

SSO Exceptions

Specify networks and hosts that do not require SSO authentication.

<input type="checkbox"/>	SSO EXCEPTION	DESCRIPTION
<input type="checkbox"/>	2.2.2.2	
<input type="checkbox"/>	2017::1	
<input type="checkbox"/>	2017::3-2017::88	
<input type="checkbox"/>	2010::0/64	

IPv6 Support for Active Directory SSO

- If user computers on your network have both IPv4 and IPv6 addresses, we recommend that you enable both IPv4 and IPv6 support on servers where Event Log Monitor or the SSO Agent are installed

IPv6 Support for Active Directory SSO

- IPv4 and IPv6 traffic is processed separately in environments that use both
 - For example, a user named *test3* has a computer with both IPv4 and IPv6 addresses. In the **Authenticated Users** list on the Firebox, two different sessions appear for the user *test3*:

Authenticated Users

LOG OFF USERS

	USER	TYPE	DOMAIN	CLIENT	ELAPSED TIME	IP ADDRESS
<input type="checkbox"/>	test3	Firewall User	qasso.net	Single Sign-On	0 days 03:35:11	fd9f:2836:f23:d351::20
<input type="checkbox"/>	Administrator	Firewall User	qasso.net	Single Sign-On	0 days 03:25:40	10.50.0.10
<input type="checkbox"/>	test3	Firewall User	qasso.net	Single Sign-On	0 days 03:25:38	10.50.0.19

IPv6 Support for Active Directory SSO

- To see the IPv6 address of an authenticated user:
 - Web UI – Select **System Status > Authentication List**
 - Firebox System Manager – Select **Authentication List**



SSO Agent Debug Information

SSO Agent Debug Info

- Real-time information about single sign-on components helps you troubleshoot SSO issues on your network

SSO Agent Debug Information

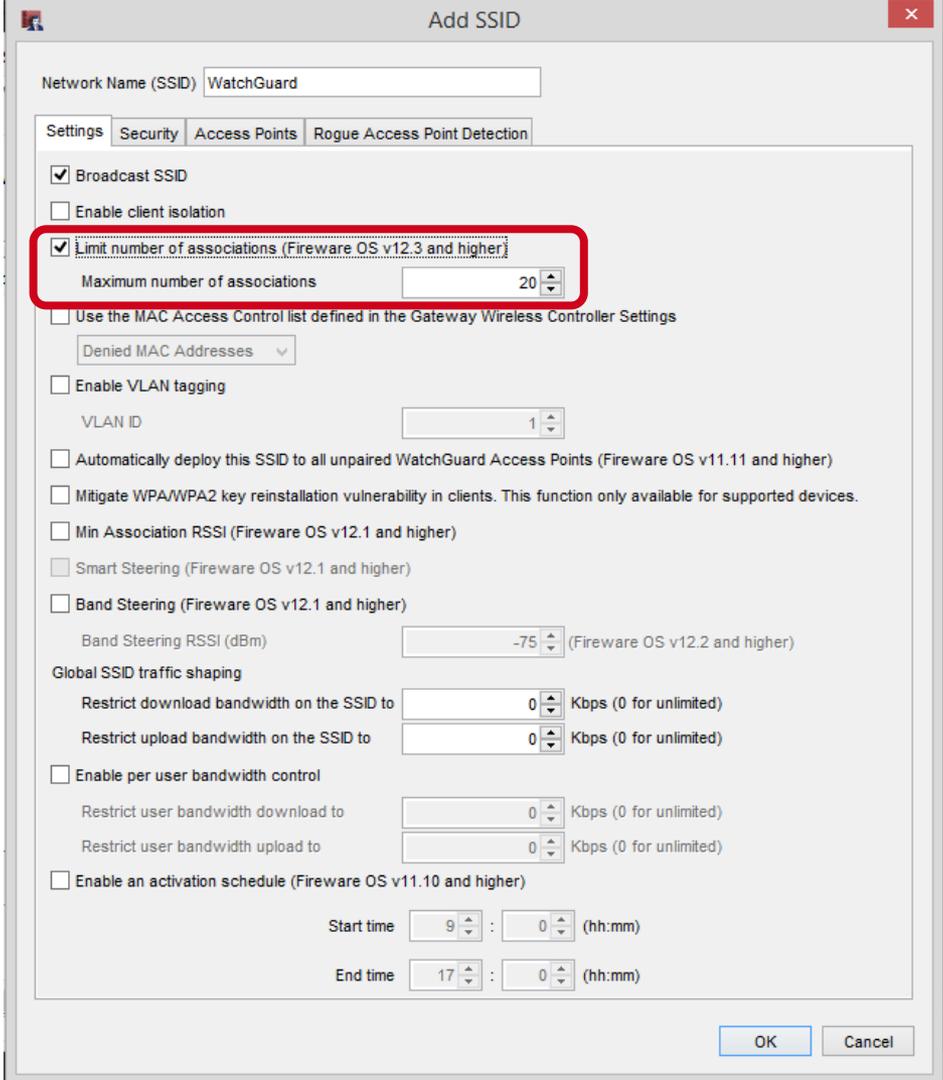
- In the SSO Agent on the **Status** page, you can now see this information:
 - SSO client connection information
 - Version and build numbers for the SSO Agent, Event Log Manager, Exchange Manager, and SSO clients
- This information refreshes every 3 seconds
- Click a column to sort the list



Gateway Wireless Controller Enhancements

Client Limits Per SSID

- You can now apply a limit to the number of clients that can associate to an SSID
- Supported by AP120, AP320, AP322, AP325, and AP420
- The option is located in the SSID configuration



The screenshot shows the 'Add SSID' configuration window. The 'Network Name (SSID)' is 'WatchGuard'. The 'Settings' tab is selected. The 'Limit number of associations (Fireware OS v12.3 and higher)' checkbox is checked and highlighted with a red box. The 'Maximum number of associations' is set to 20. Other options include 'Broadcast SSID', 'Enable client isolation', 'Use the MAC Access Control list', 'Enable VLAN tagging', 'Automatically deploy this SSID', 'Mitigate WPA/WPA2 key reinstallation vulnerability', 'Min Association RSSI', 'Smart Steering', 'Band Steering', and 'Global SSID traffic shaping'.

AP Actions Performed in Background

- When you take actions on multiple APs, such as reboot, reset, and firmware update actions, these actions are now performed asynchronously as a background process
- This greatly improves the UI response times and returns you to the UI to perform other tasks while the AP operations complete

Deprecated Features

- Automatic AP activation no longer occurs when an AP pairs to a Gateway Wireless Controller
 - You must go to www.watchguard.com/activate to activate your AP before you pair the AP to the Gateway Wireless Controller
- You can no longer configure client limits per radio for the legacy AP300



WatchGuard IPSec Mobile VPN Client

WatchGuard IPSec Mobile VPN Client

- The WatchGuard IPSec mobile VPN client has these enhancements:
 - Supports Microsoft Windows 10 version 1809
 - Appears only in the Windows taskbar when the client is open
- Silent installation is improved in this release:
 - Additional parameters previously required for compatibility with InstallShield are now built in



Thank You!