What's New in Fireware v12.3

WatchGuard Training

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

WatchGuard Training

SD-WAN Actions

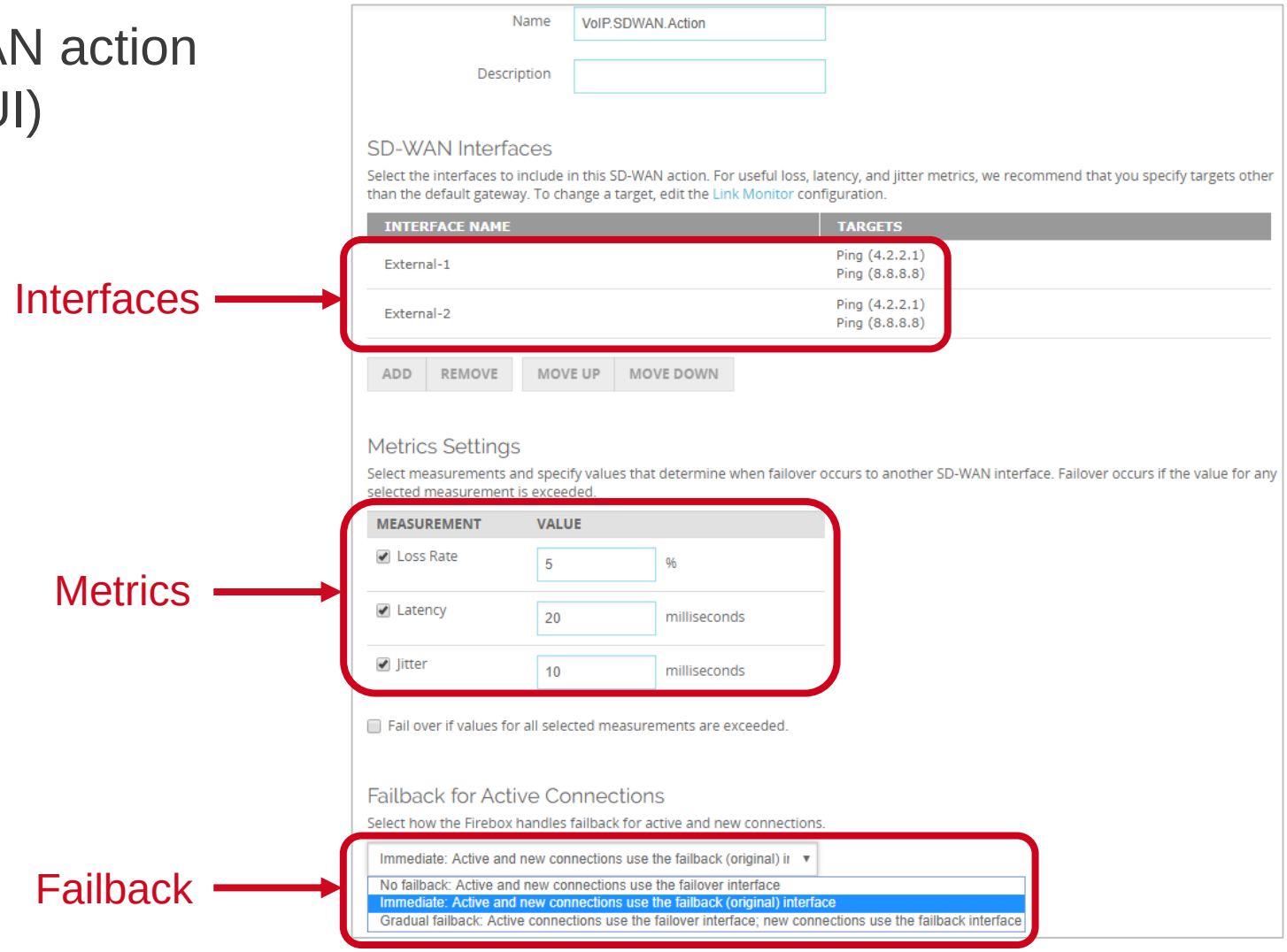
- The method used to route outbound traffic that matches a policy has changed: *SD-WAN actions* replace policy-based routing
- SD-WAN actions offer more granular control of external interface failover and failback for traffic that matches a policy
  - In an SD-WAN action, you can select to use network 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

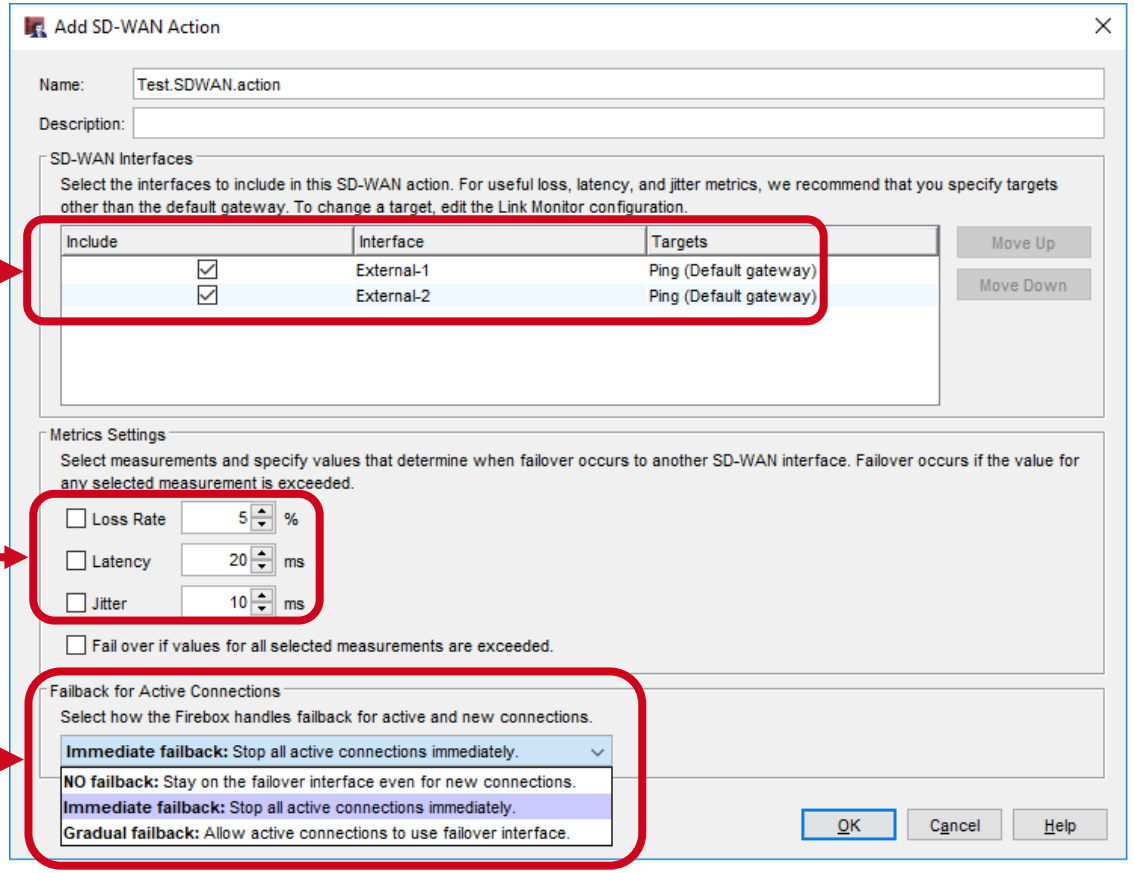
SD-WAN Actions

- SD-WAN action (Web UI)



SD-WAN Actions

- SD-WAN action (Policy Manager)

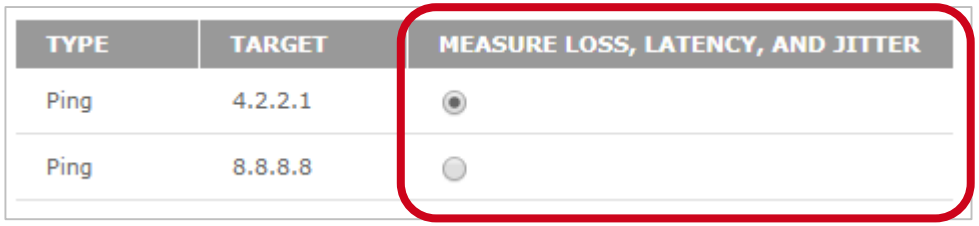


SD-WAN Actions

- **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



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

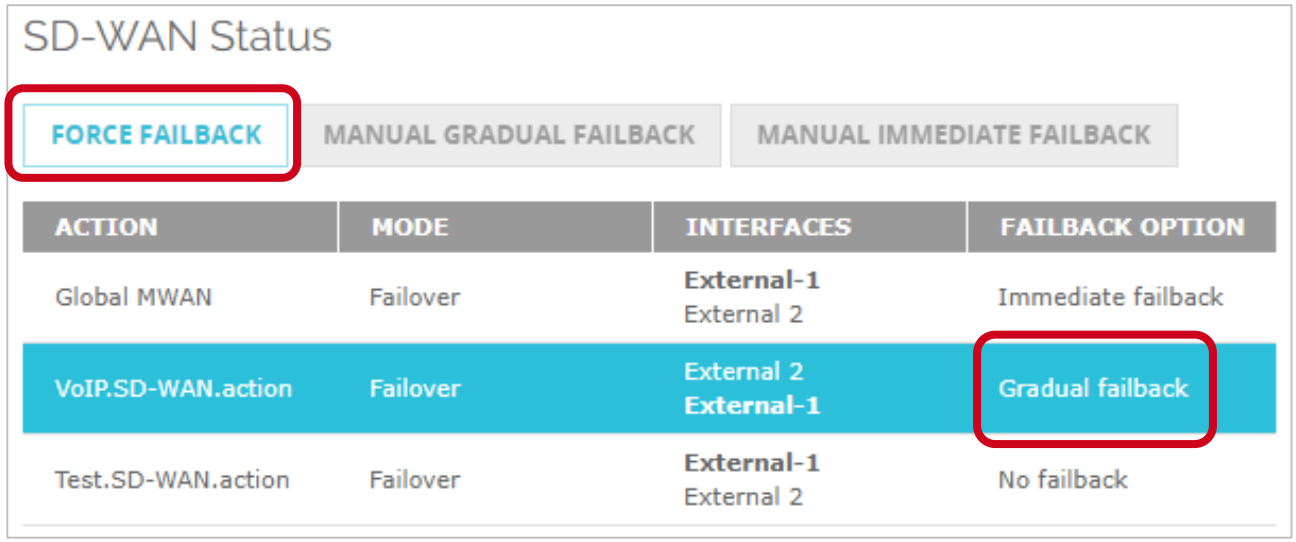
- **Failback —**
- If you select **No failback** or **Gradual failback** in the SD-WAN action, you can select to manually fail back connections at a later time
- To initiate manual failback:
  - In Fireware Web UI, select **System Status > SD-WAN Status**
  - In FSM, select the **SD-WAN** tab

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

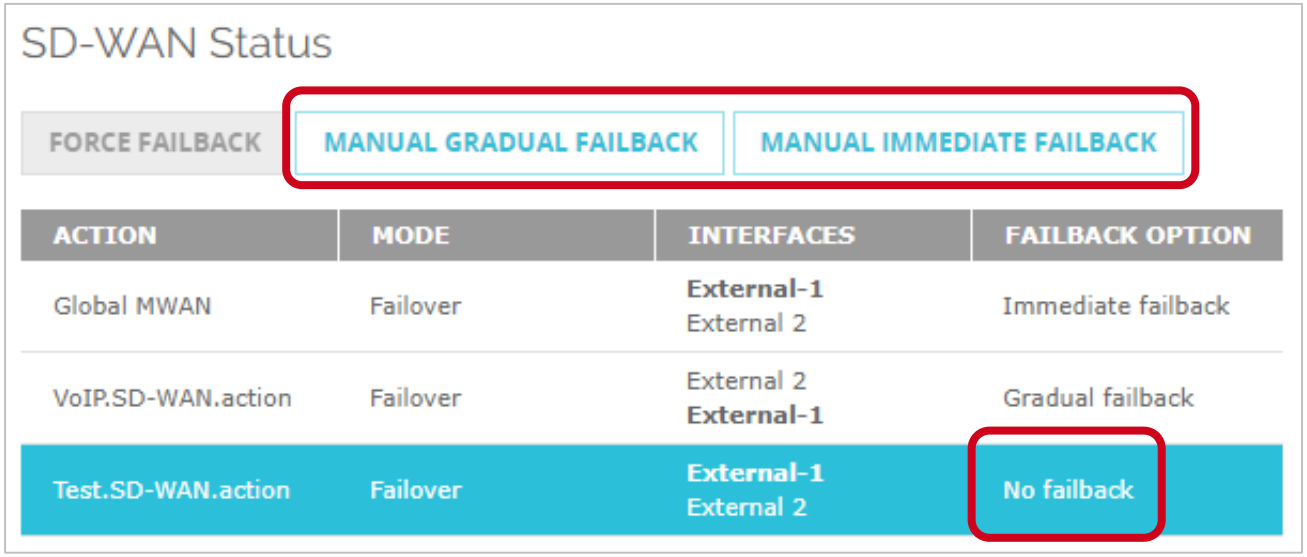
SD-WAN Actions

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



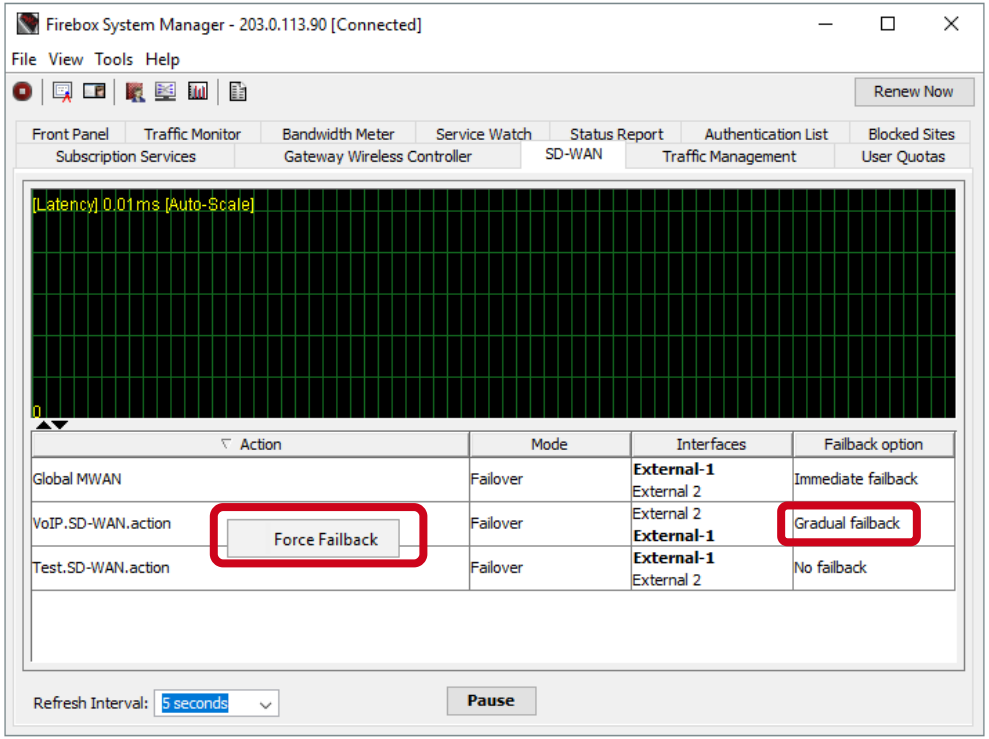
SD-WAN Actions

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



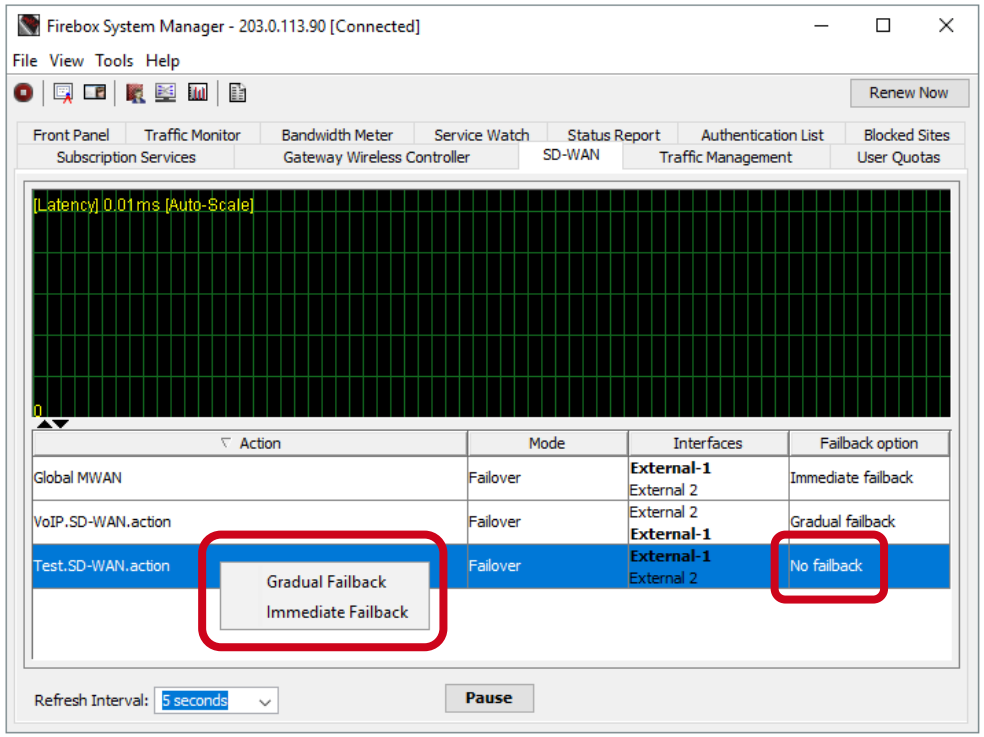
SD-WAN Actions

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



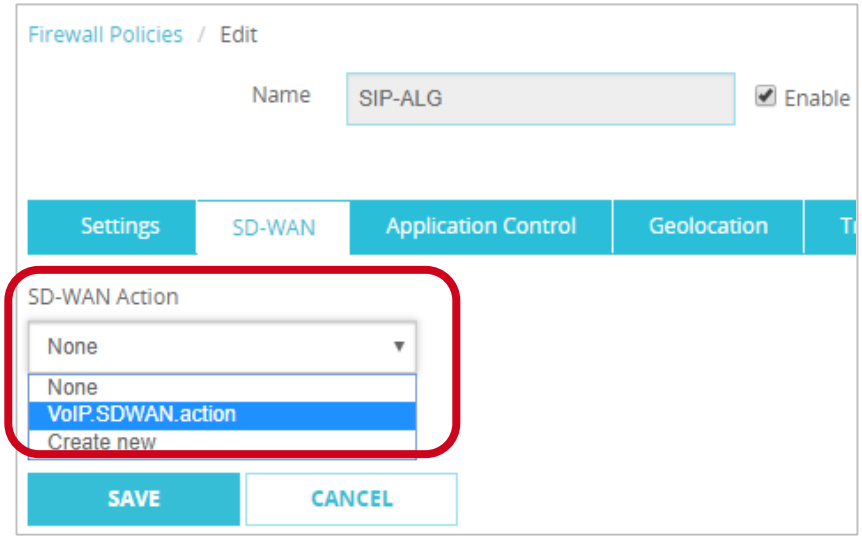
SD-WAN Actions

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



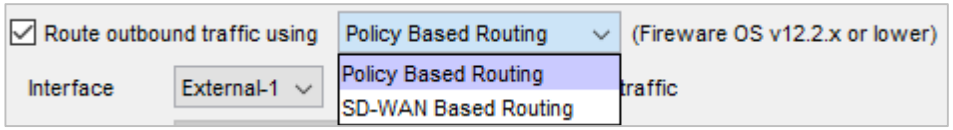
SD-WAN Actions

- 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



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



SD-WAN Reporting Enhancements

WatchGuard Training

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

WatchGuard Training

Link Monitor Enhancements

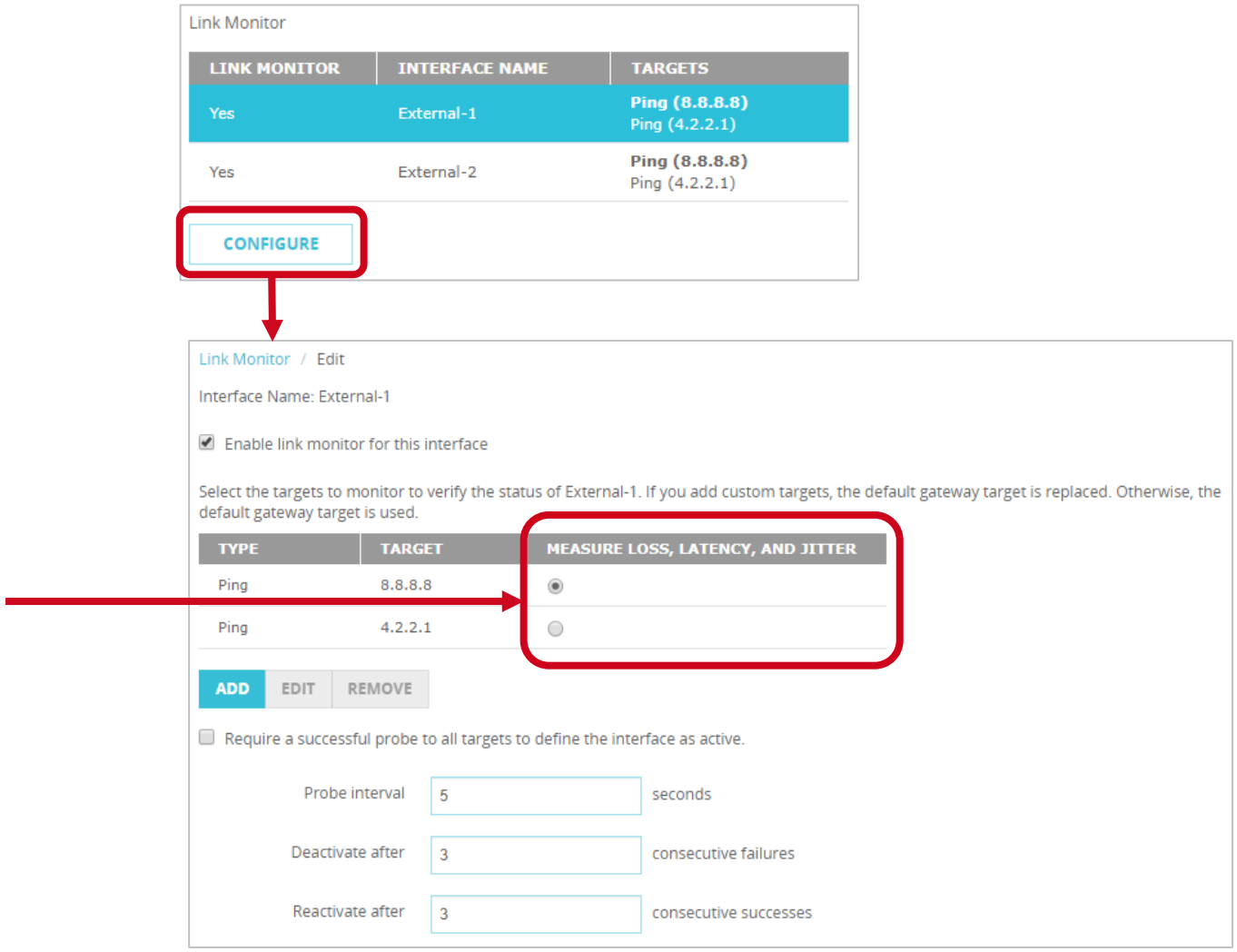
- Link monitor settings have moved from the Multi-WAN configuration
  - Web UI — Select **Network > Link Monitor**
  - Policy Manager — Select **Network > Configuration > Link Monitor**
- In the Web UI, you can now configure link monitor targets for an external interface regardless of whether multi-WAN 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

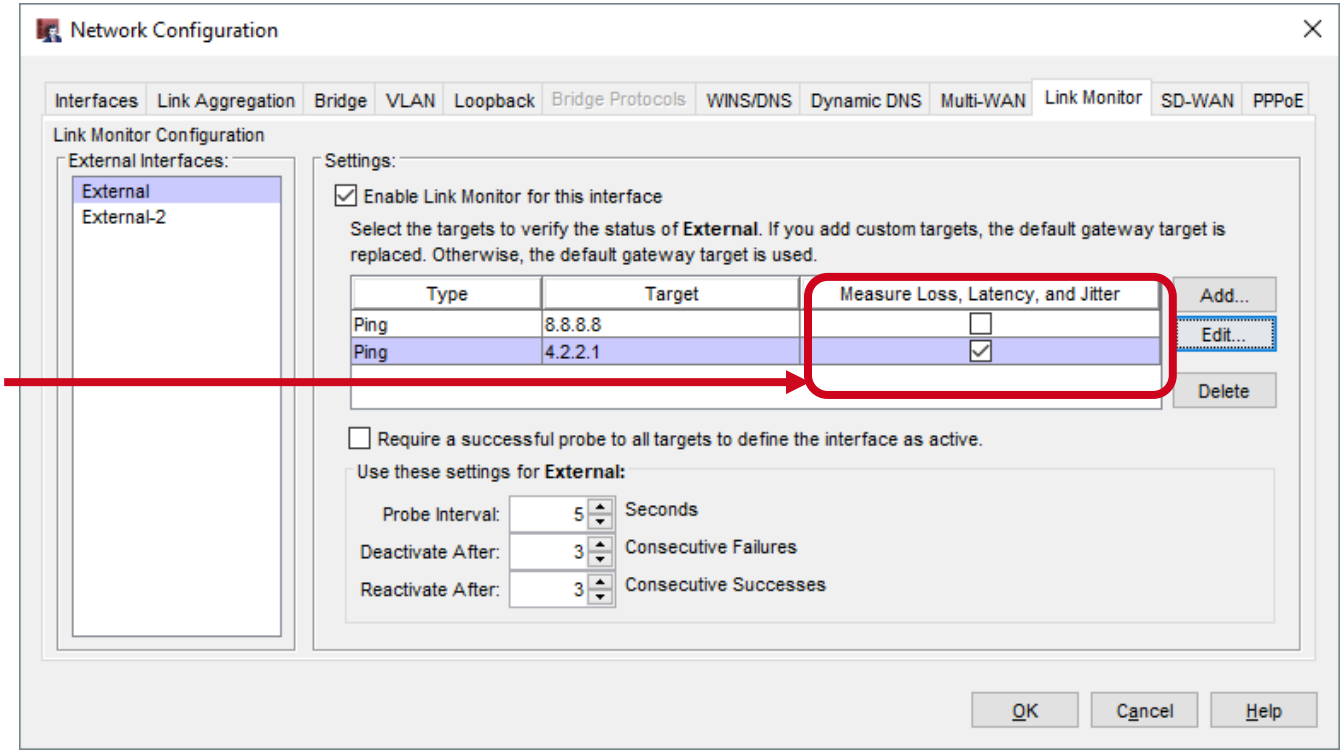


Select to measure loss, latency, and jitter for one target

Link Monitor Enhancements

- Policy Manager

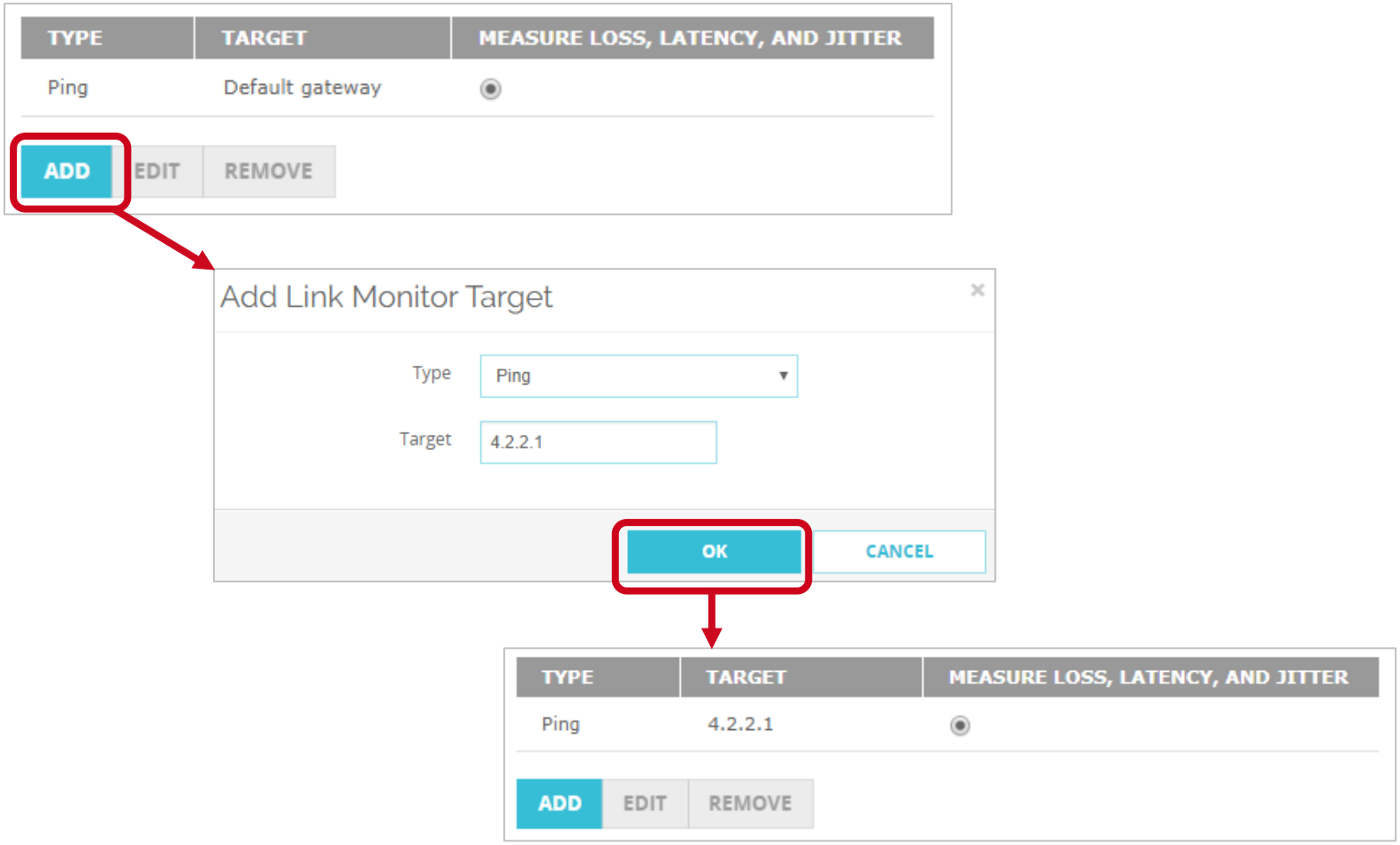
Select to measure loss, latency, and jitter for one target



Link Monitor Enhancements

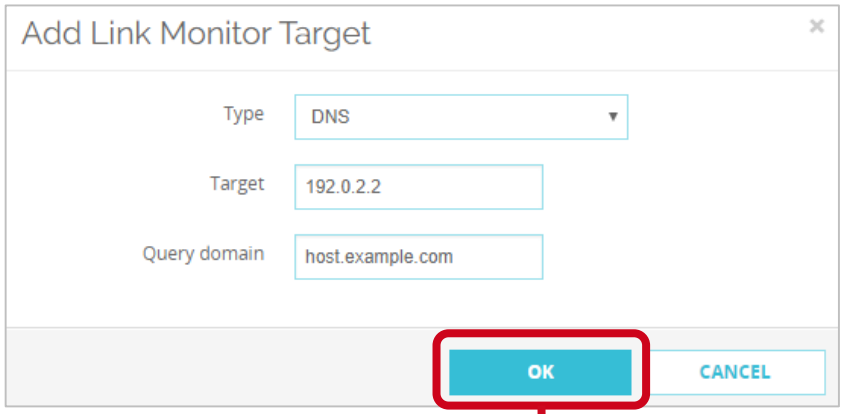
- When you enable link monitor for an interface, the default gateway is the target
  - For meaningful data, we recommend that you specify a target other than the default gateway
  - If you add a custom target, the default gateway target is replaced
  - If you remove all custom targets that you added,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

Link Monitor Enhancements



Link Monitor Enhancements

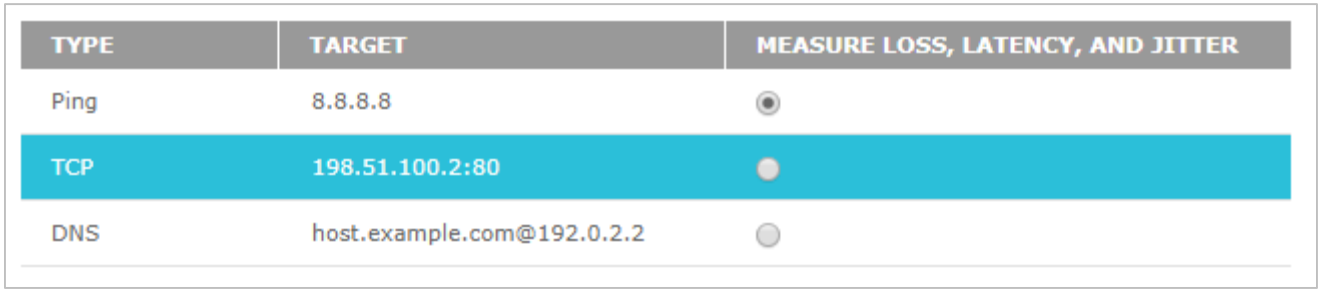
- You can now specify DNS targets



TYPE	TARGET	MEASURE LOSS, LATENCY, AND JITTER
Ping	8.8.8.8	
Ping	4.2.2.1	
DNS	host.example.com@192.0.2.2	

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	◉
TCP	198.51.100.2:80	○
DNS	host.example.com@192.0.2.2	○

NetFlow

WatchGuard Training

NetFlow

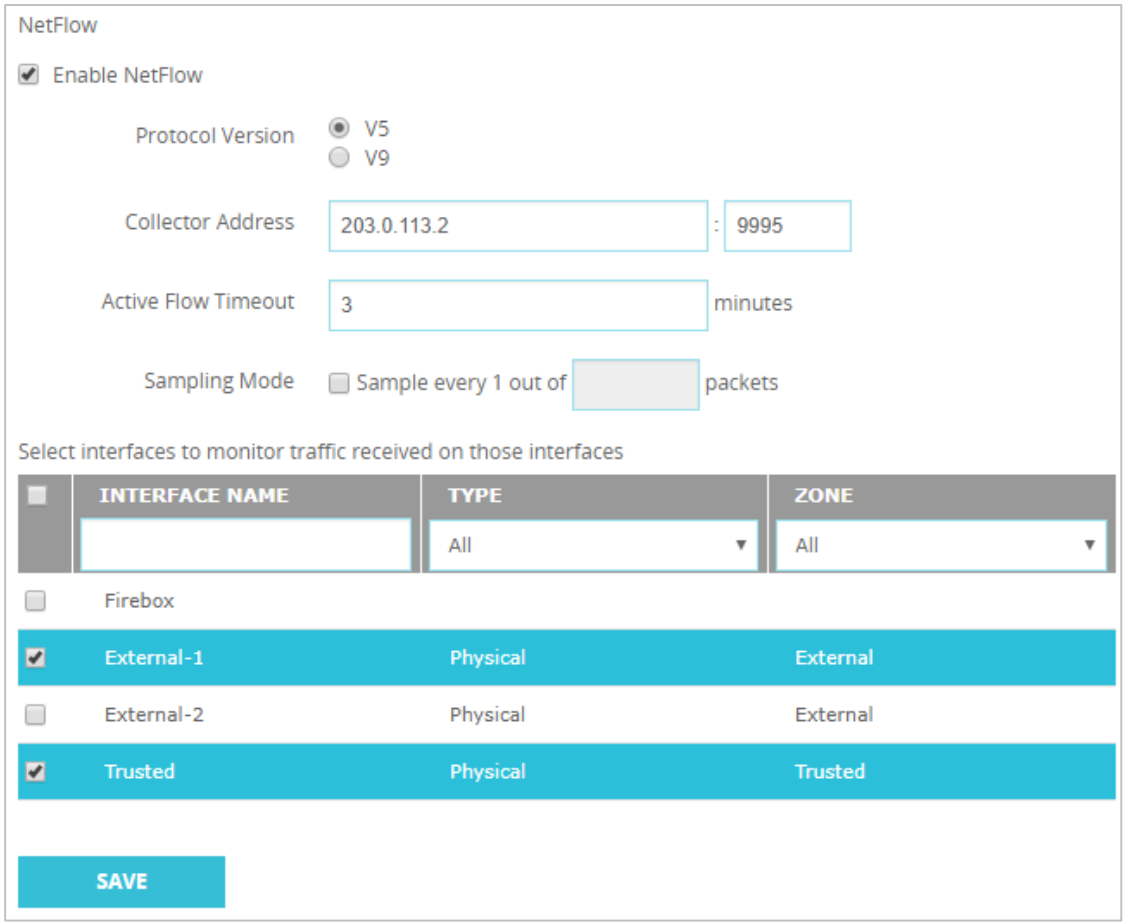
- Configure NetFlow to gain more insight into Firebox traffic
- For example, you can troubleshoot network congestion by viewing the source and destination of traffic for an interface, and the class of service

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

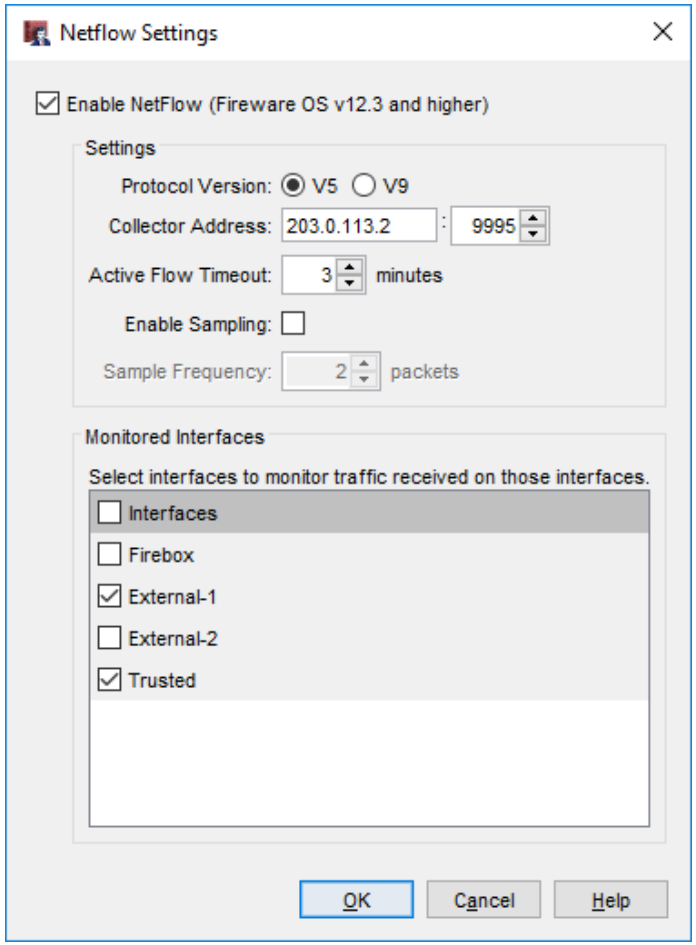
NetFlow

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



NetFlow

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



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

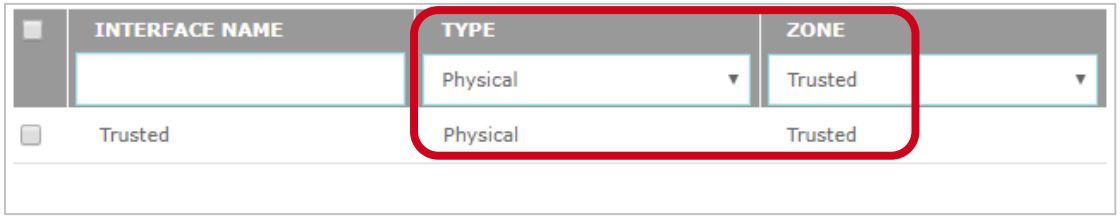
- Sampling mode —
  - In this mode, the Firebox randomly selects 1 out of every *n* packets to sample
  - For example, if you specify a Sampling mode of 100, the Firebox samples 1 out of every 100 packets
  - Sampling mode can help reduce performance impacts to the Firebox
  - We recommend Sampling mode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

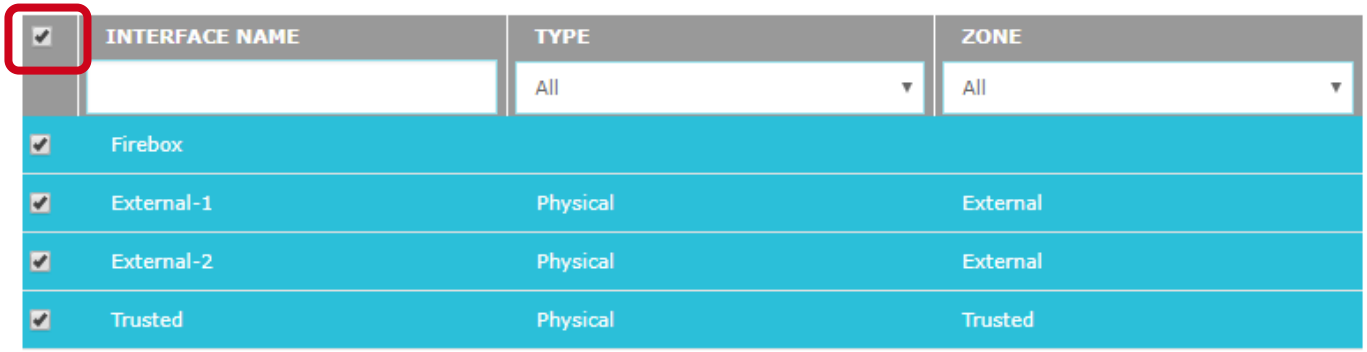
NetFlow

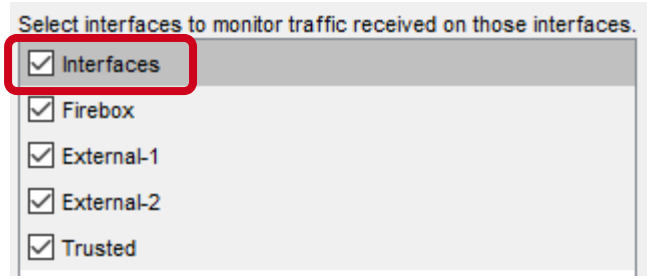
- Interfaces —
  - If you have a long list of interfaces, you can use the **Interface Name** search box to find an interface
  - For example, type `ext` to find all interface names that contain those letters
  - You can also filter by type and zone



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





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

WatchGuard Training

FireCluster Diagnostics

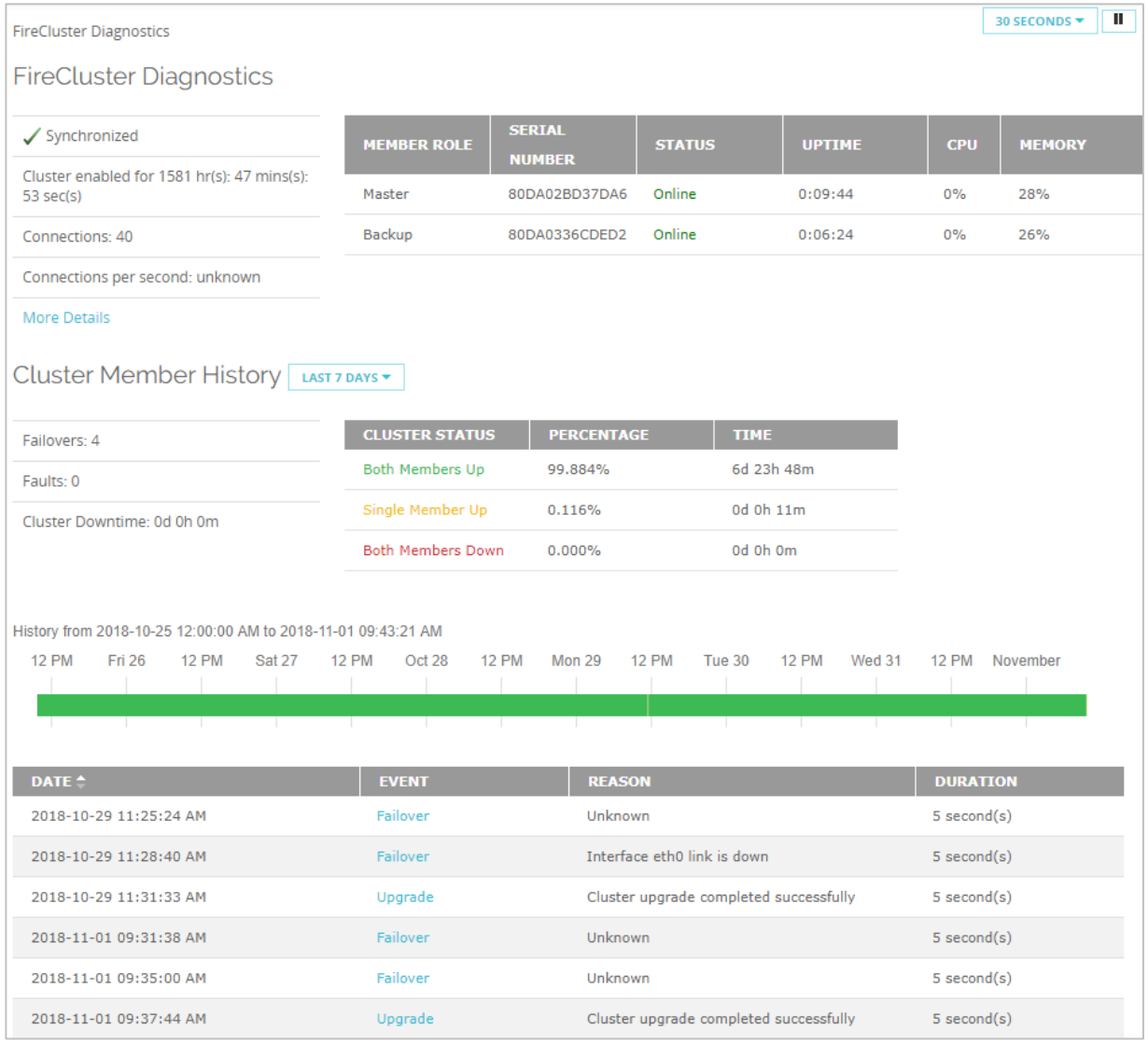
- A new FireCluster diagnostics page centralizes cluster data, gives you more insight into cluster health, and reduces troubleshooting time

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



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

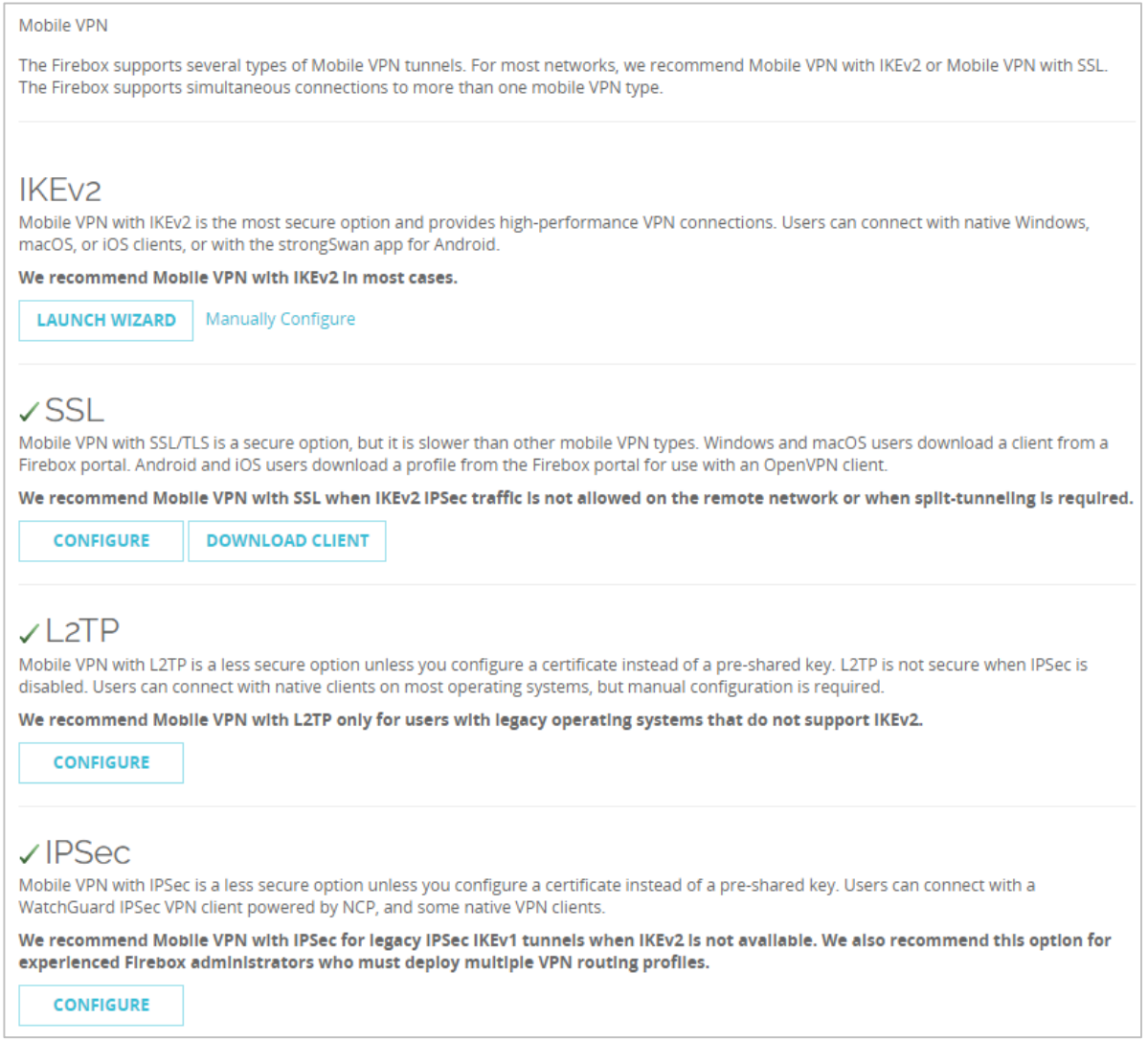
WatchGuard Training

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

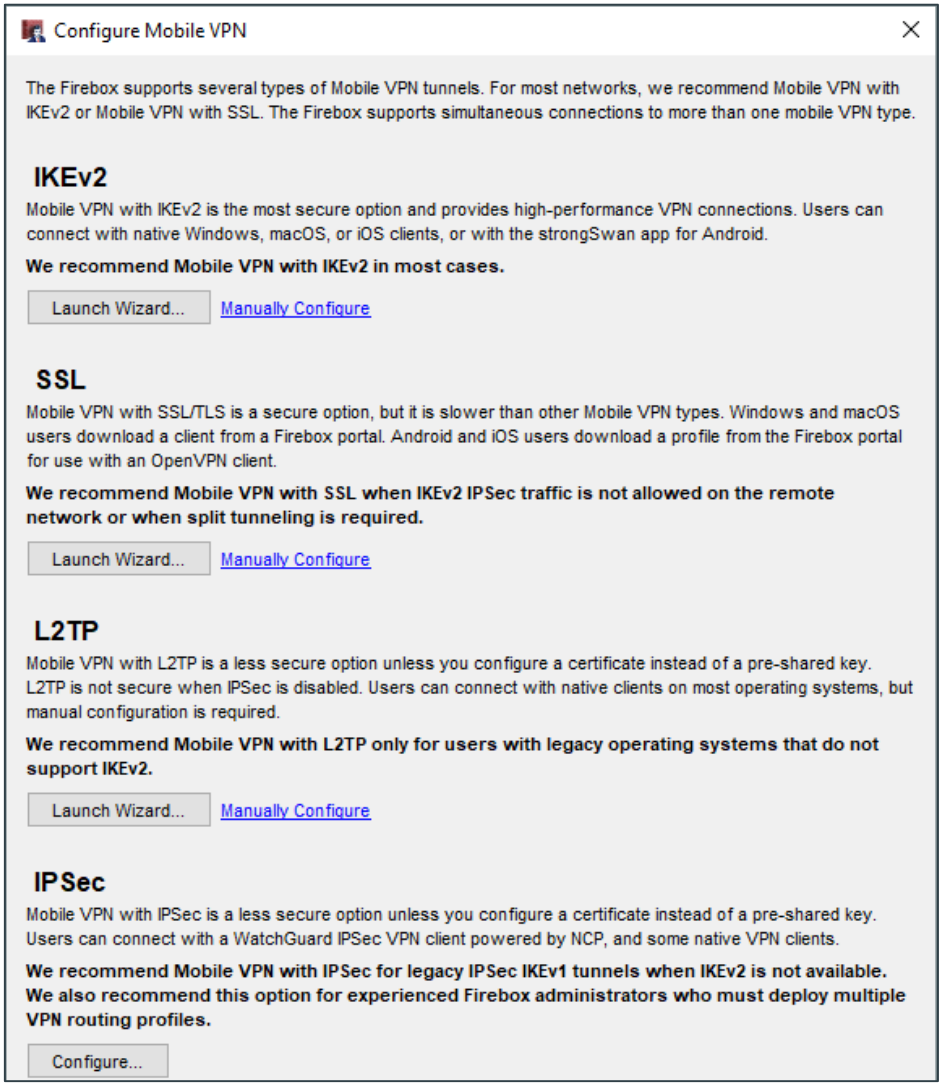
Mobile VPN with SSL Wizard

- Web UI



Mobile VPN Selection Assistance

- Policy Manager



Mobile VPN with SSL Wizard

WatchGuard Training

Mobile VPN with SSL Wizard

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

Mobile VPN with SSL Wizard

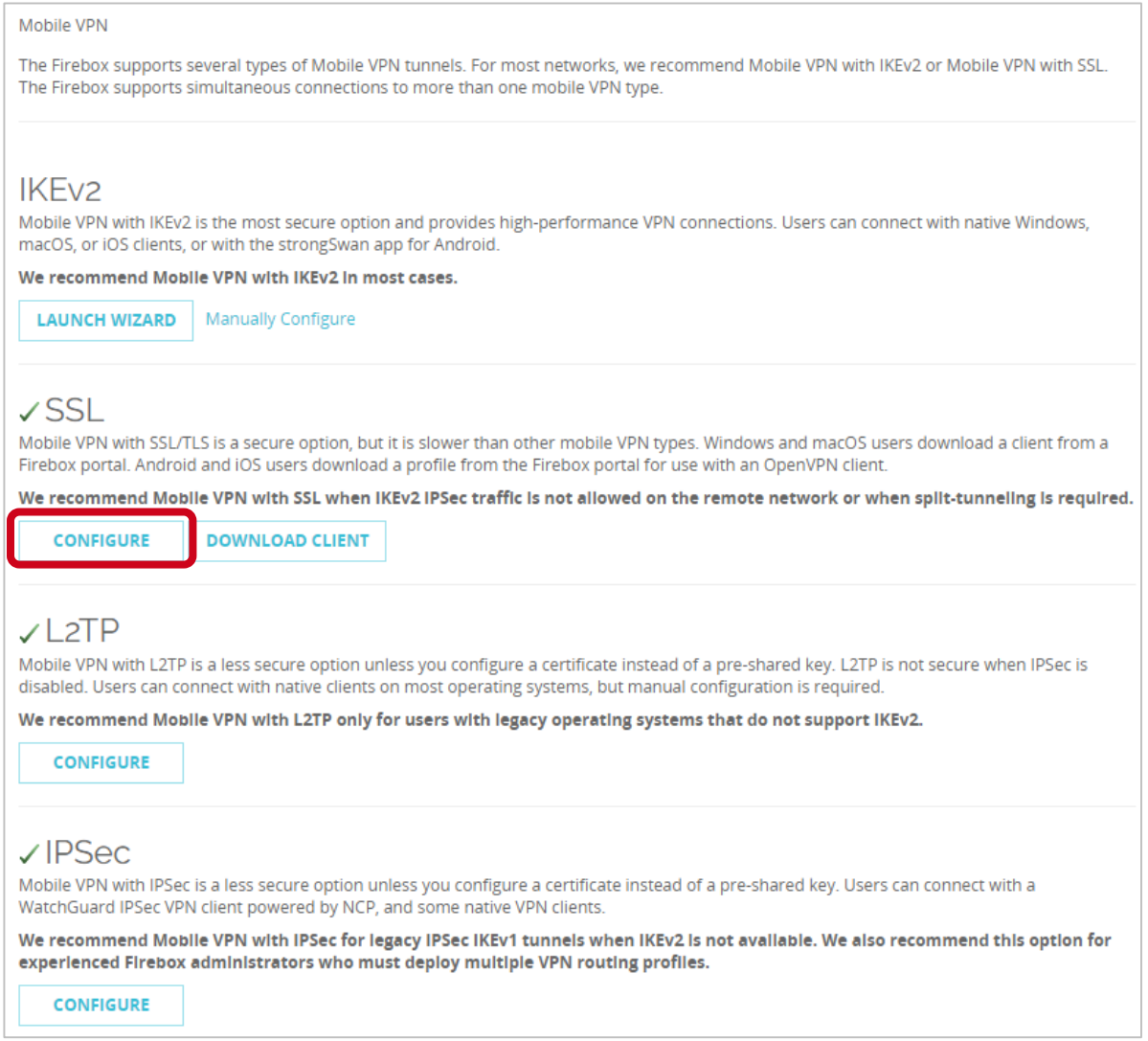
- You can now use a wizard to configure Mobile VPN with SSL
- The wizard prompts you for these settings and automatically creates a Mobile VPN with SSL configuration:
  - Primary domain name or IP address for client connections
  - (Optional) Backup domain name or IP address for client connections
  - 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

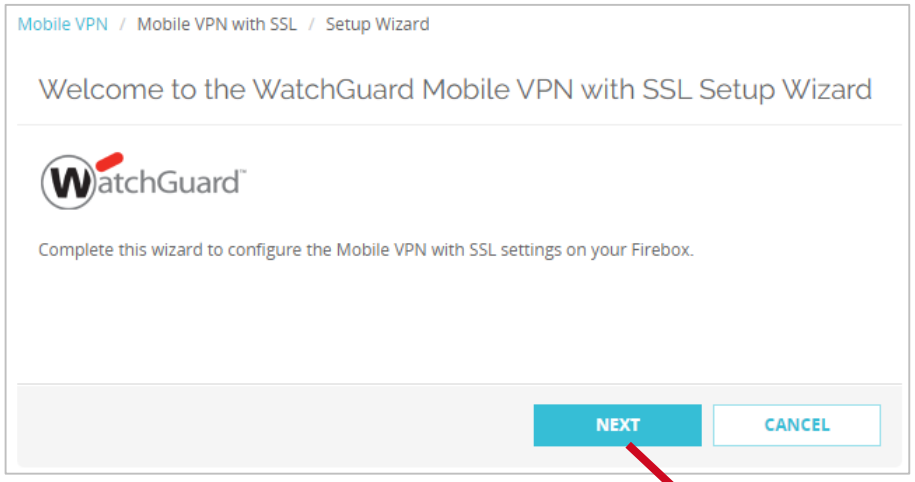
- You can select to use the wizard or manually configure Mobile VPN with SSL
  - On the new Mobile VPN selection page in the Web UI and Policy Manager, the **Launch Wizard** option appears if Mobile VPN with SSL is not already configured
  - Click **Configure Manually** to skip the wizard

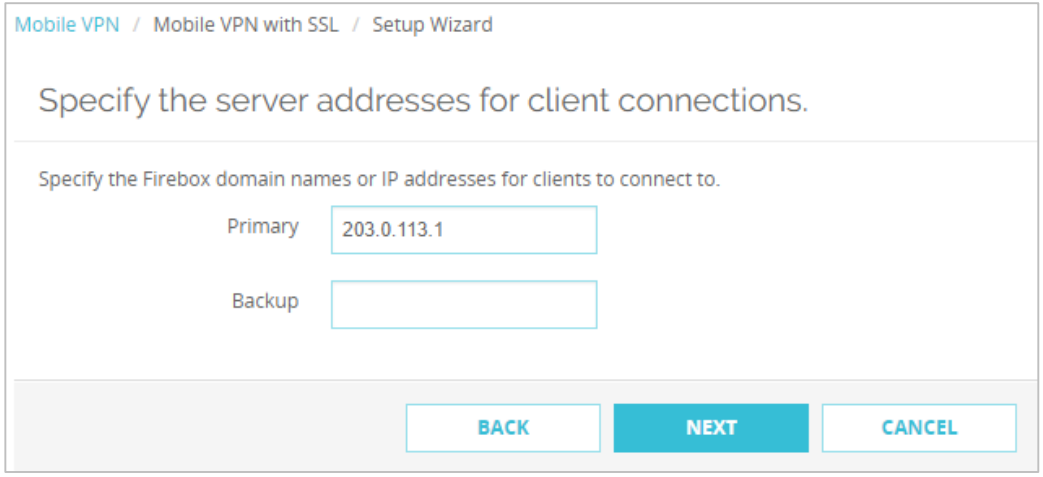
Mobile VPN with SSL Wizard

- Web UI

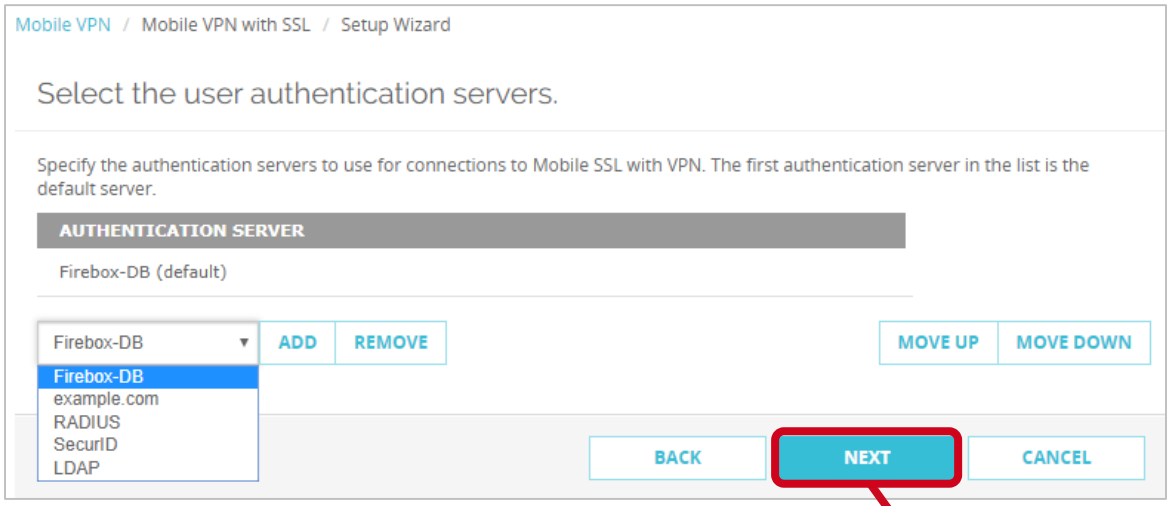


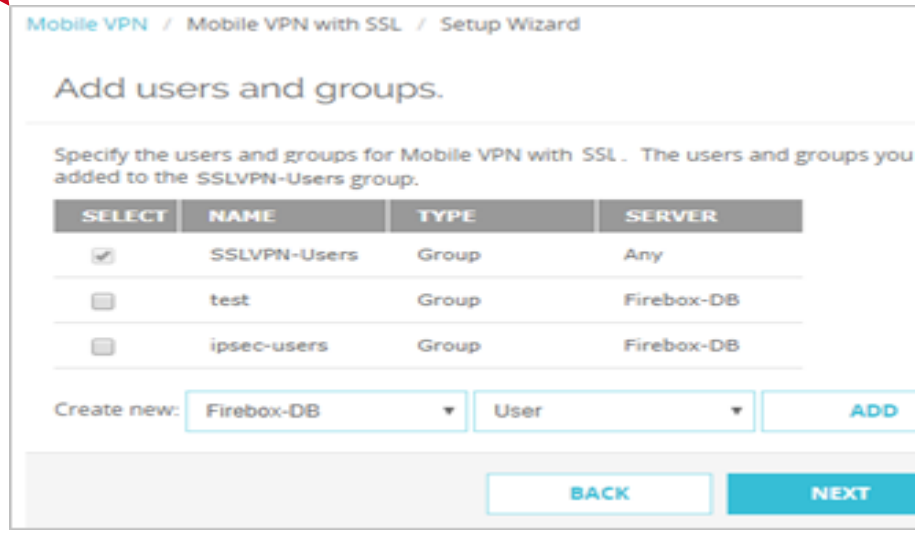
Mobile VPN with SSL Wizard



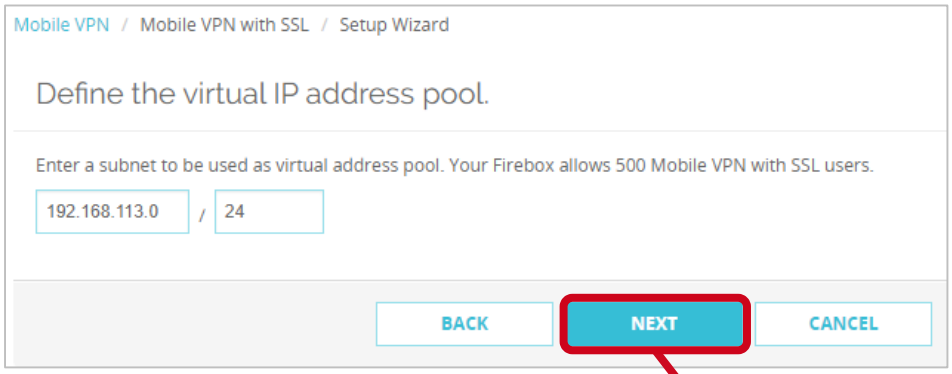


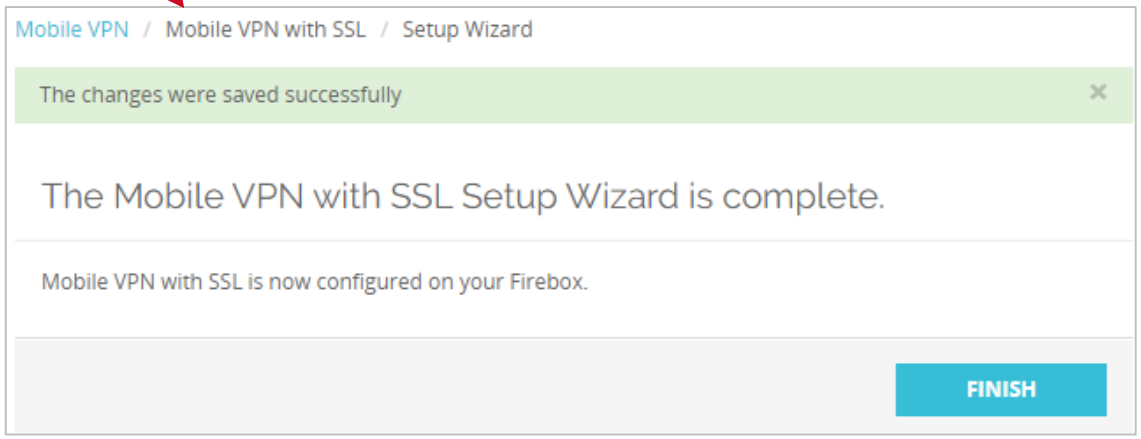
Mobile VPN with SSL Wizard





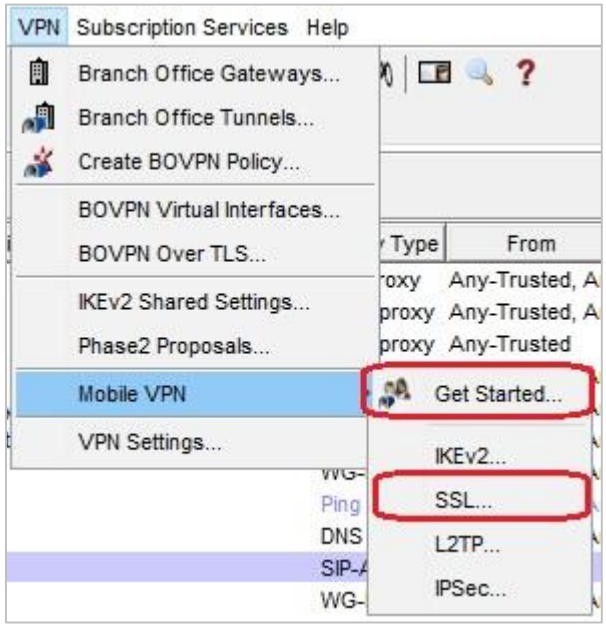
Mobile VPN with SSL Wizard





Mobile VPN with SSL Wizard

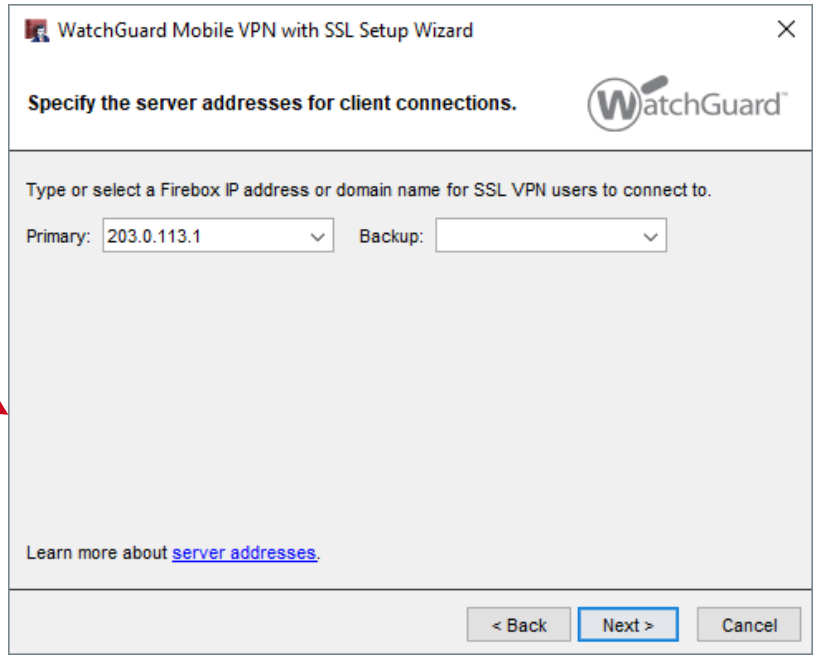
- In Policy Manager, to launch the wizard, select either of these options:
  - **VPN > Get Started**
  - **VPN > SSL**



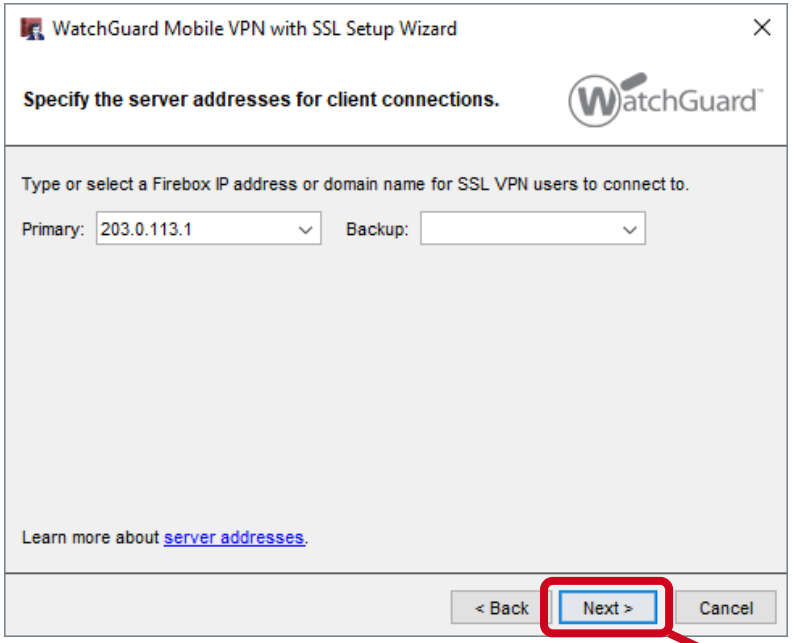
Mobile VPN with SSL Wizard

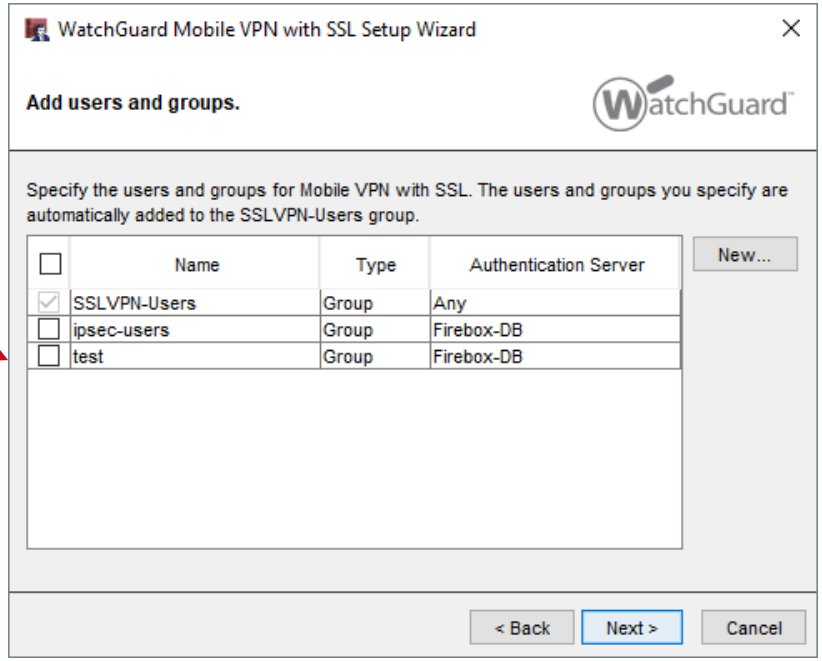
- If you selected **Get Started**, the new VPN selection page appears
- Click **Launch Wizard**

Mobile VPN with SSL Wizard

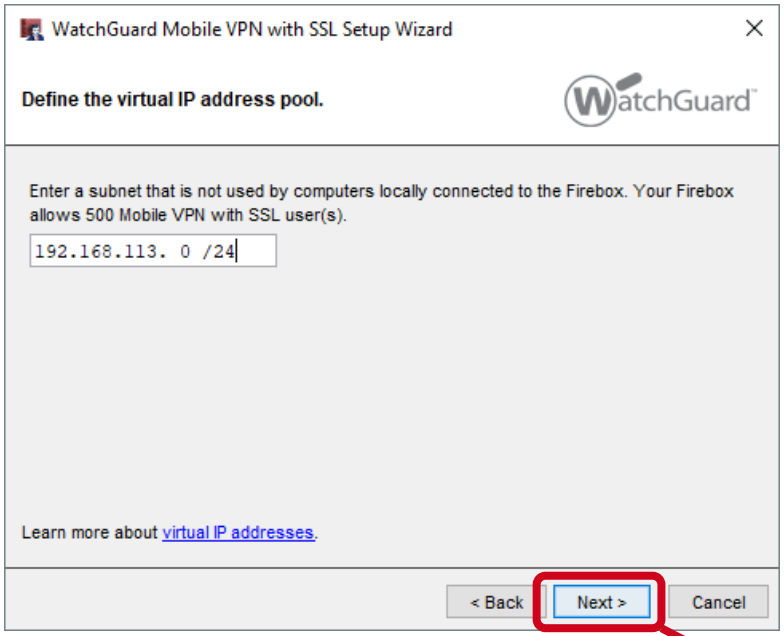


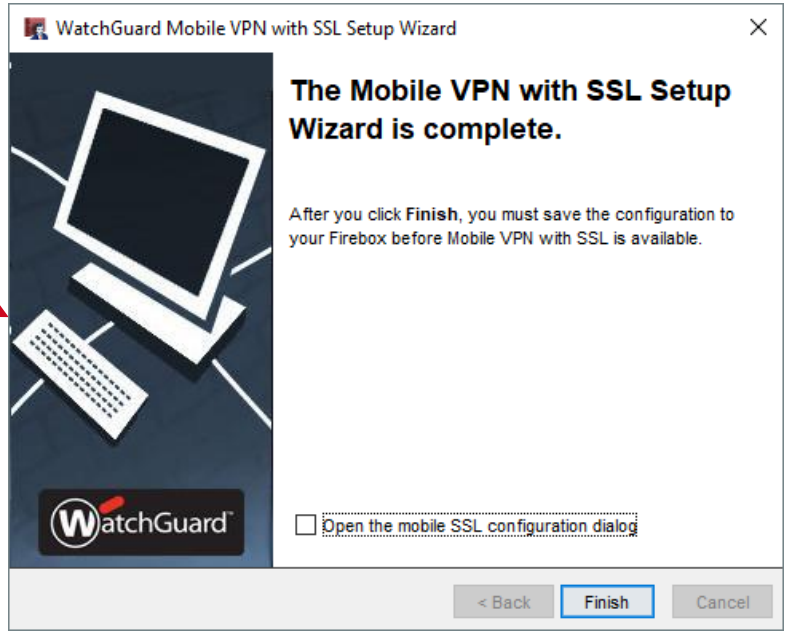
Mobile VPN with SSL Wizard

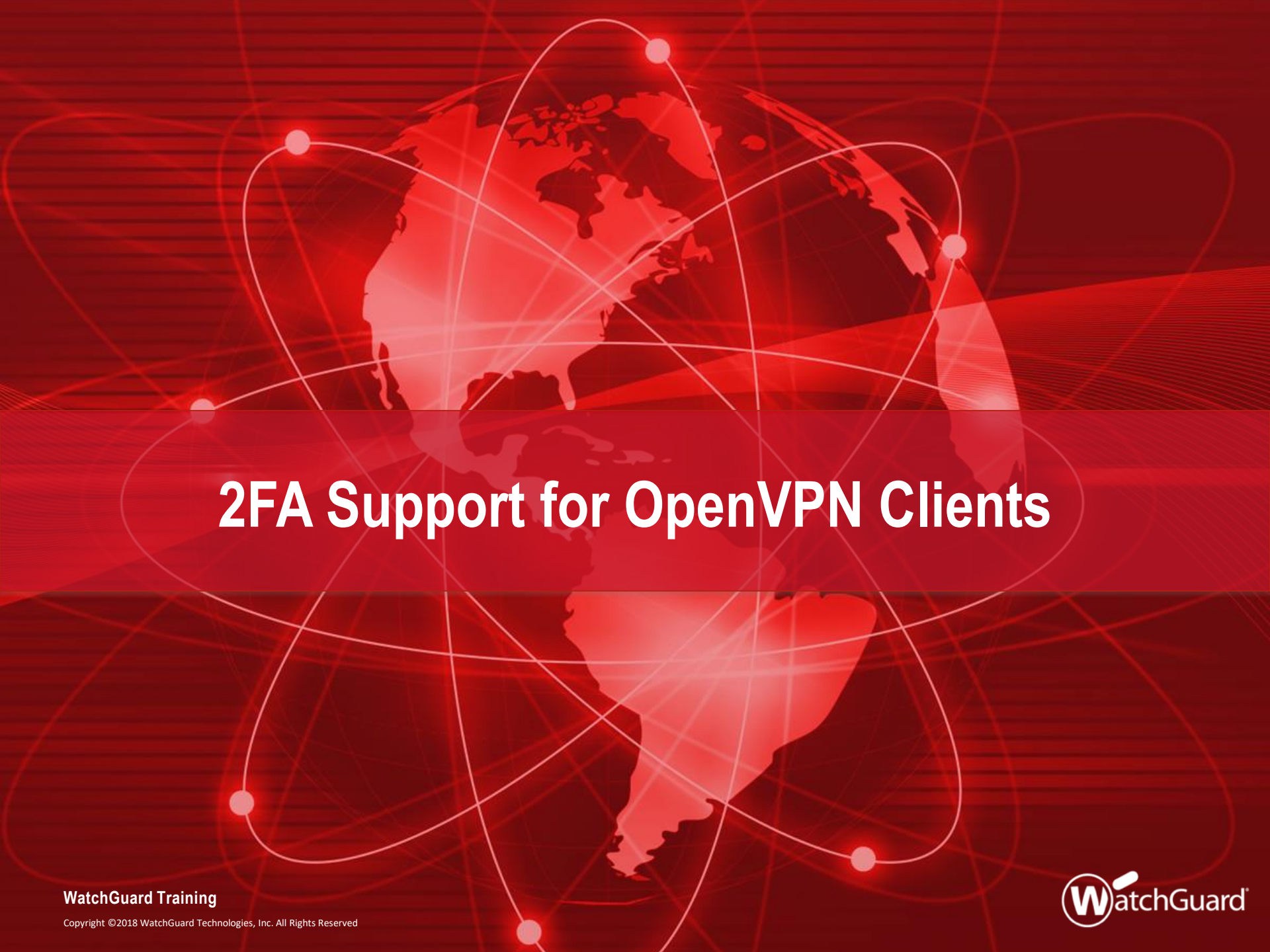




Mobile VPN with SSL Wizard







WatchGuard Training

MFA Support for OpenVPN Clients

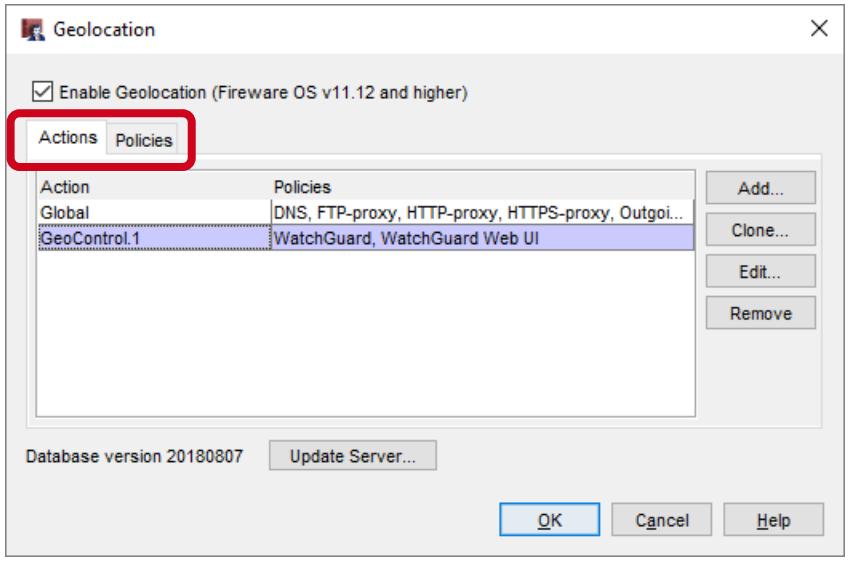
- Mobile VPN with SSL now supports two-factor, challenge-response authentication for native OpenVPN clients

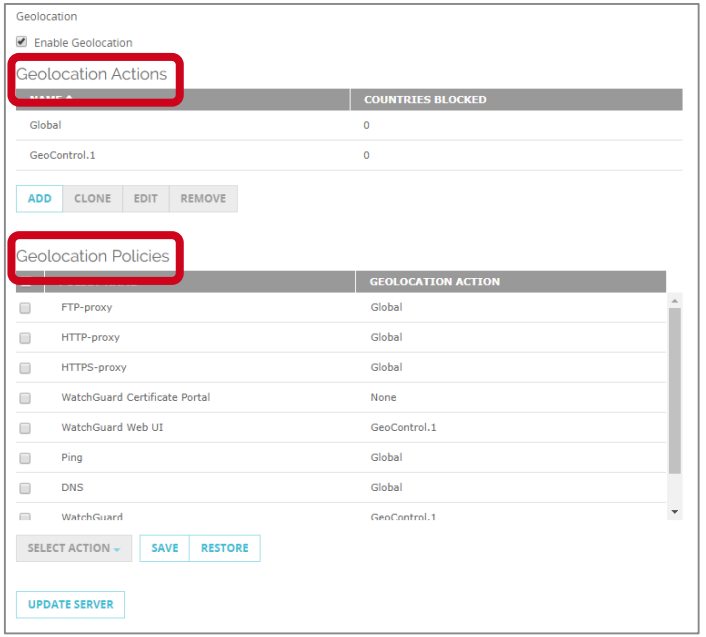
Mobile VPN with SSL users who have OpenVPN clients can type a one-time password to connect to the Firebox

Geolocation Actions

Geolocation Actions

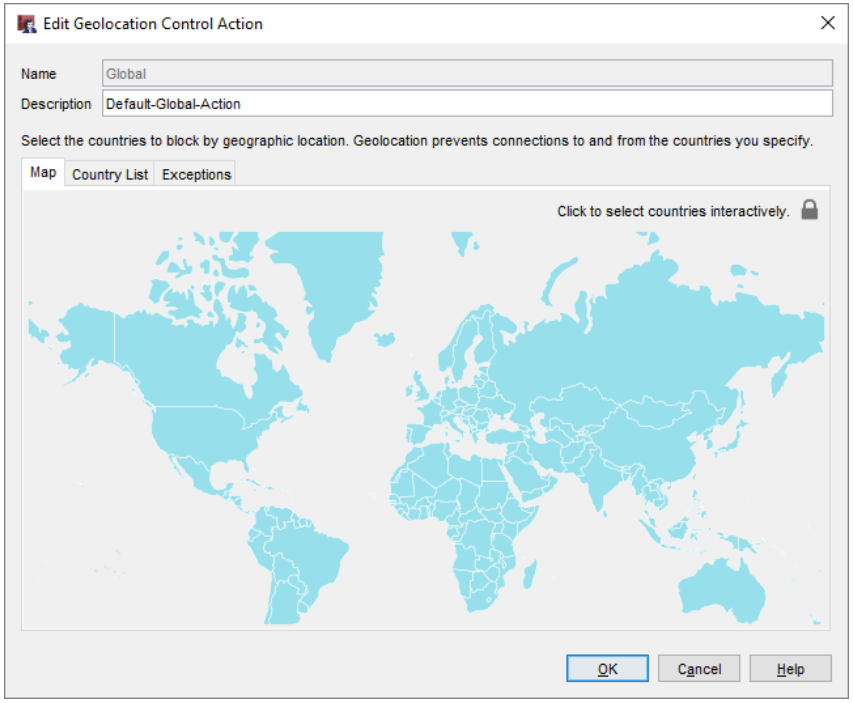
- The Geolocation service now supports multiple actions so that you can specify different geographical restrictions by policy
- Geolocation settings now include **Actions** and **Policies**
  - **Actions:** Add and edit actions
  - **Policies:** Assign actions to policies





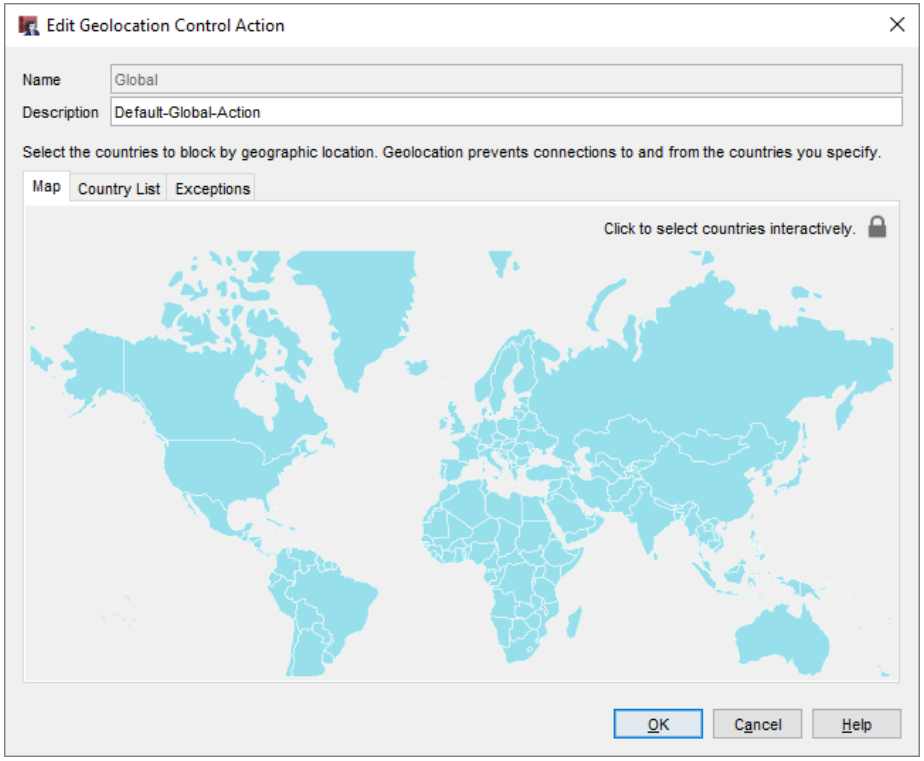
Geolocation Actions

- 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



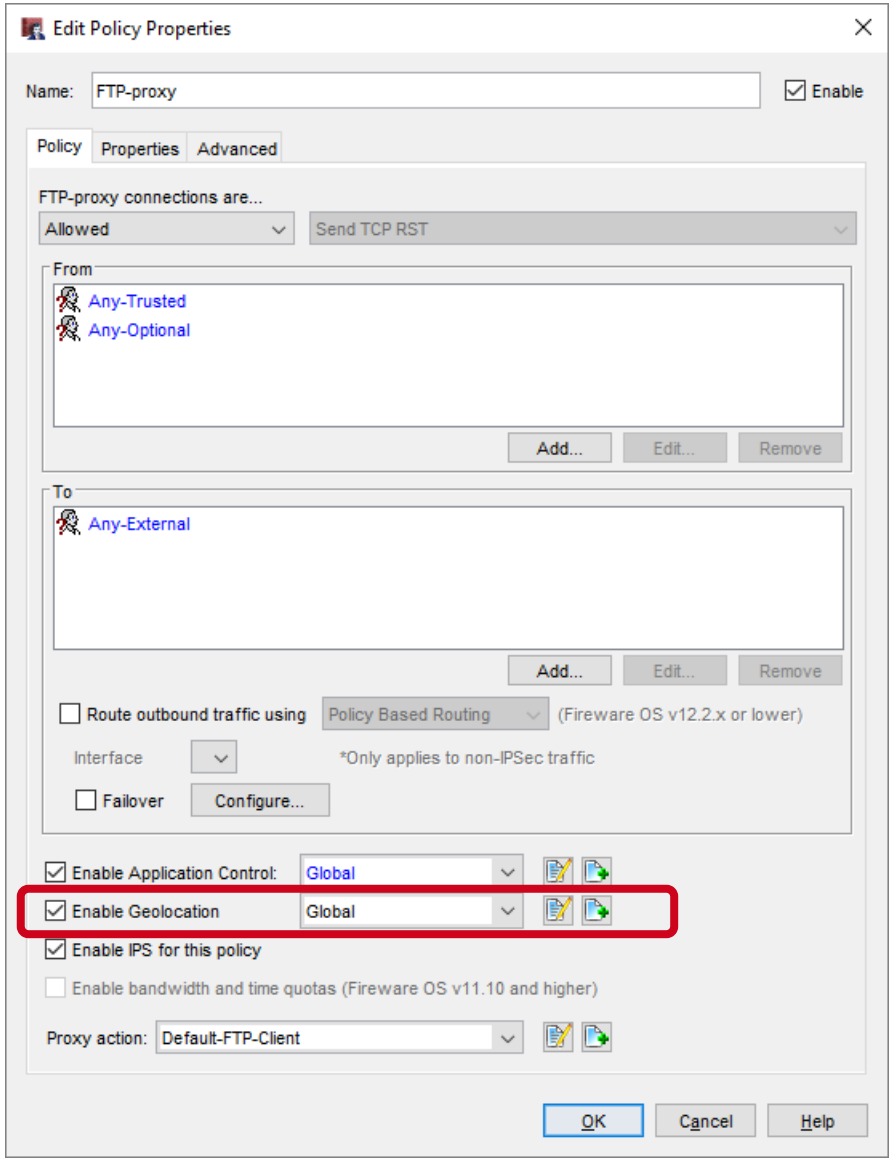
Geolocation Actions

- 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



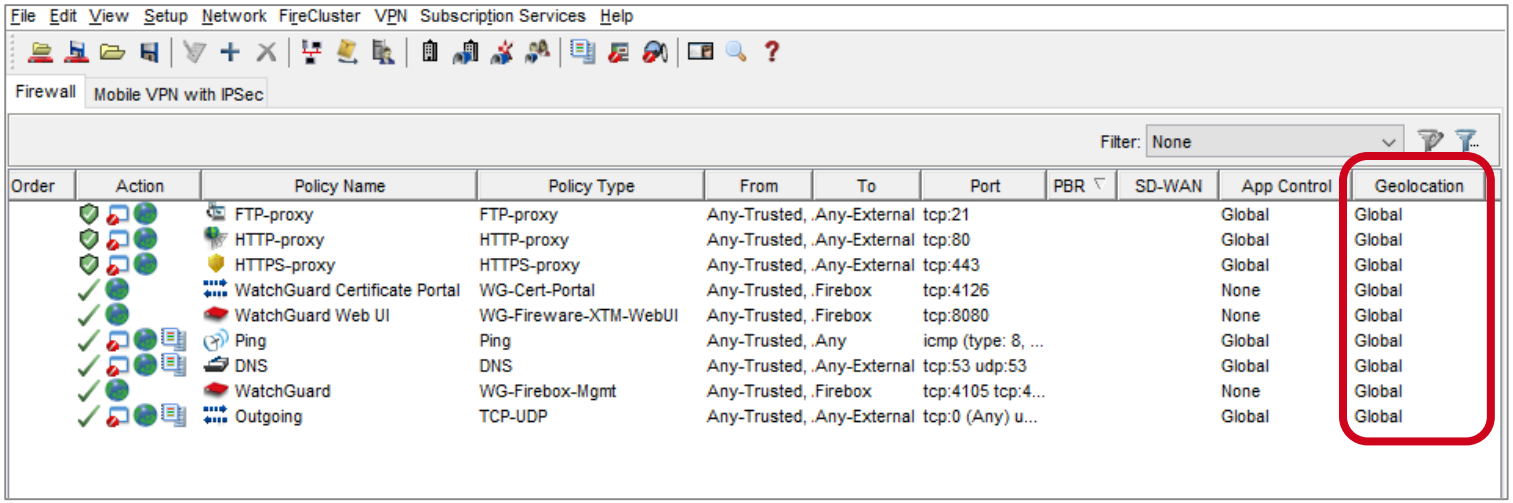
Geolocation Actions

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



Geolocation Actions

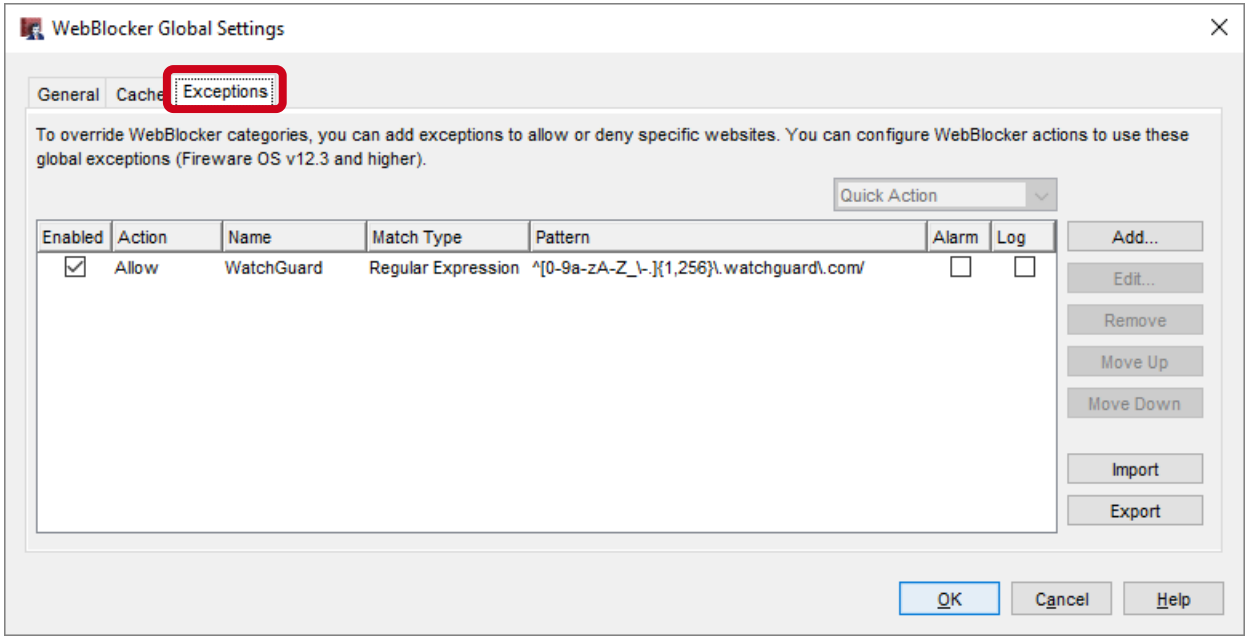
- The Policies list has a new Geolocation column
- This column shows the configured Geolocation action for each policy



WebBlocker Enhancements

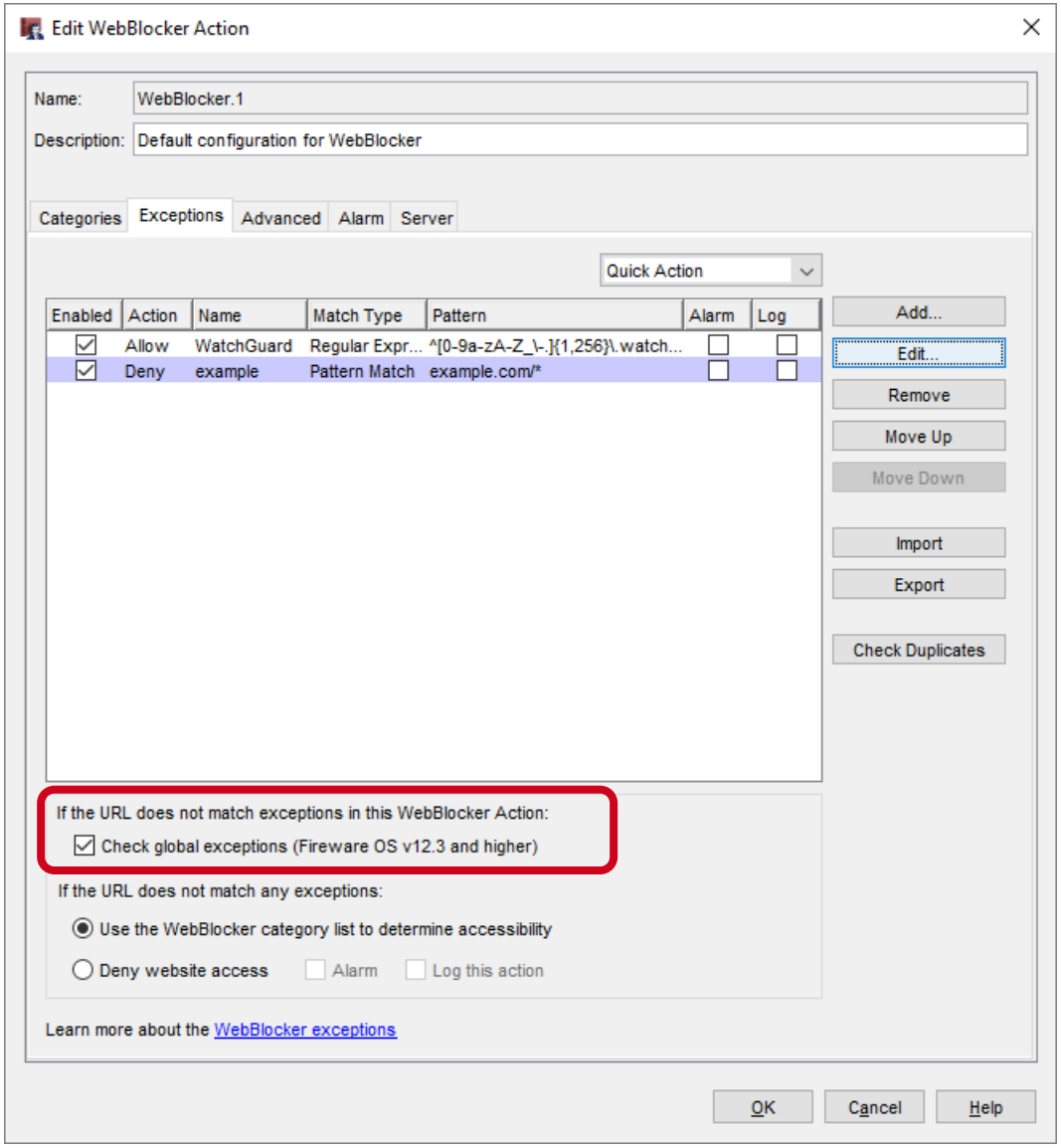
WebBlocker Enhancements

- 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



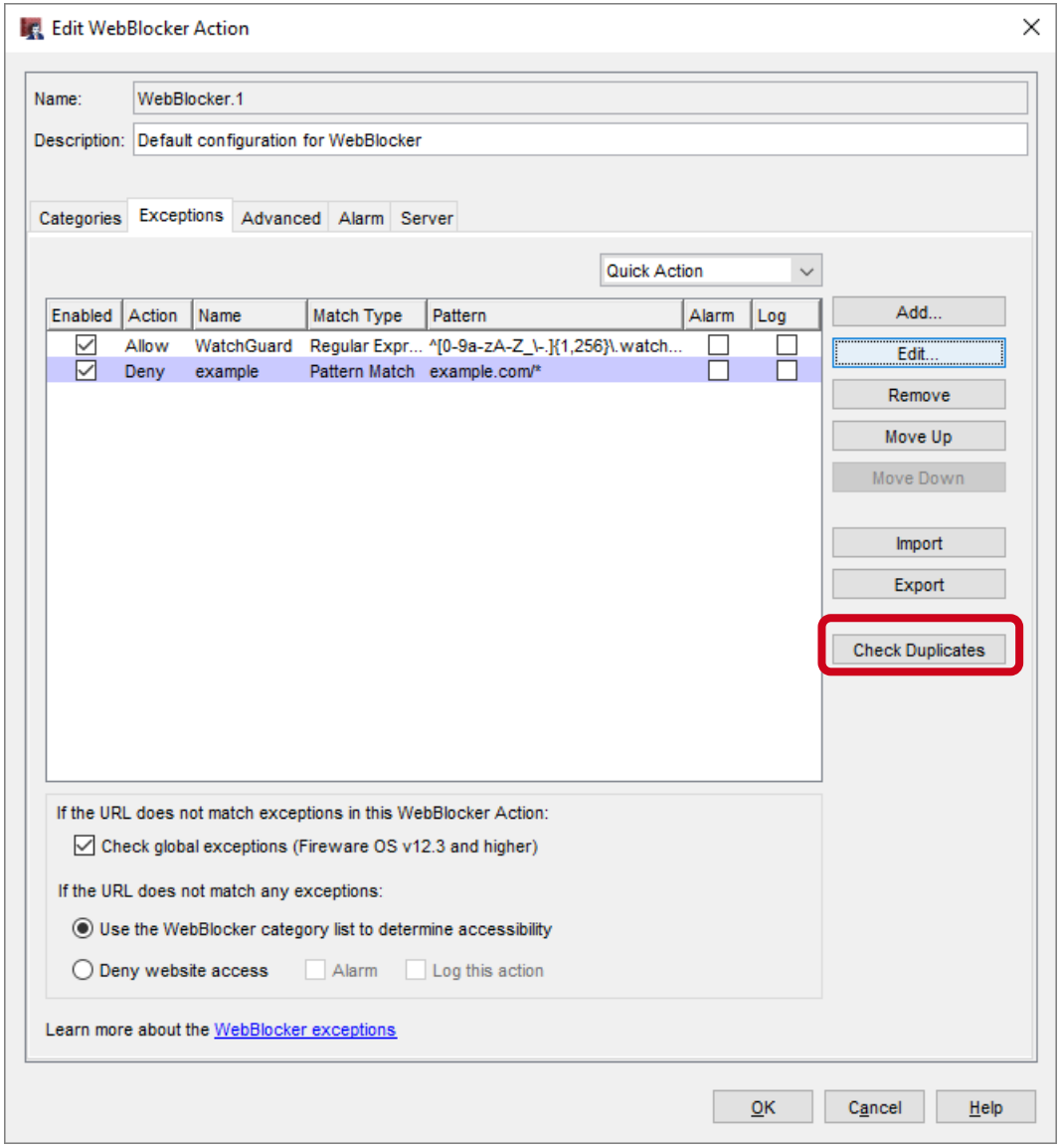
WebBlocker Enhancements

- 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



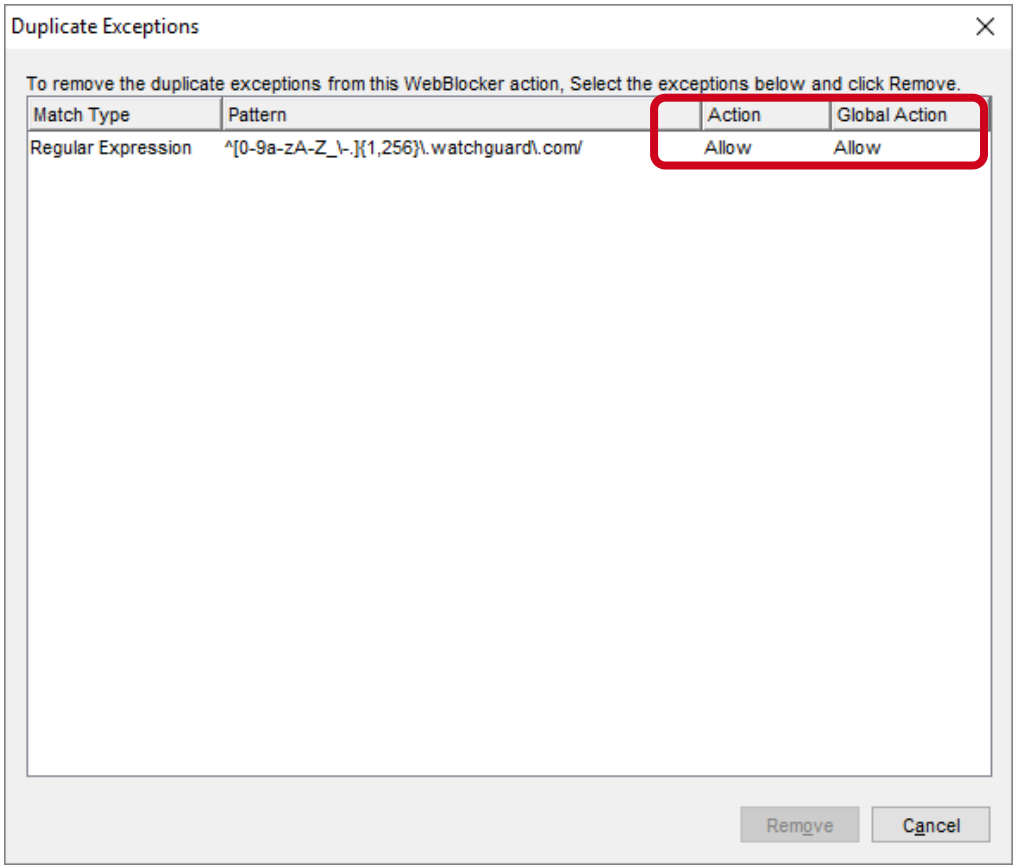
WebBlocker Enhancements

- 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



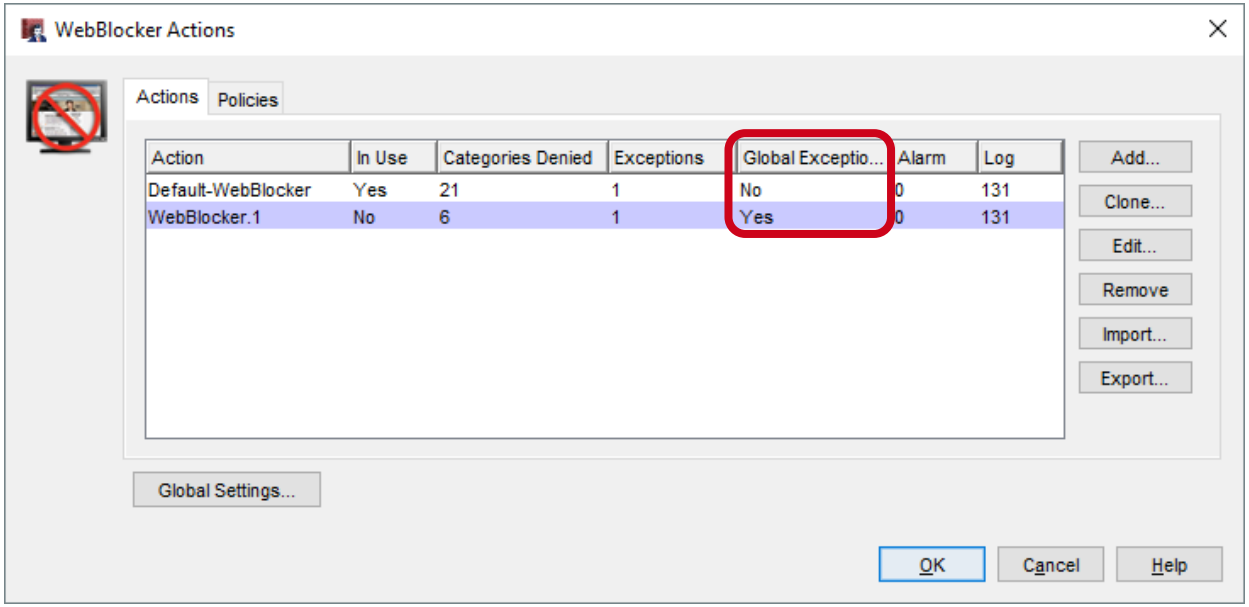
WebBlocker Enhancements

- 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**



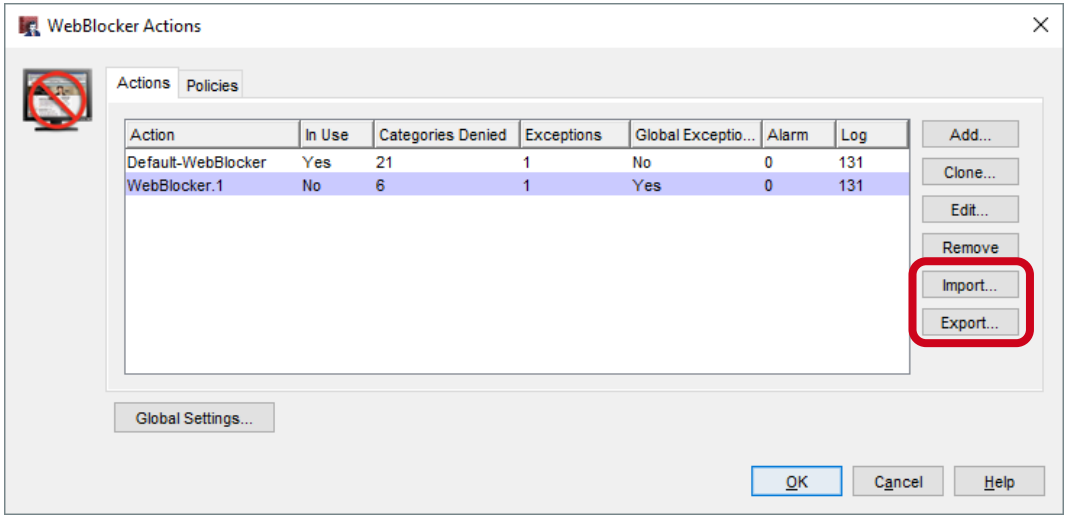
WebBlocker Enhancements

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



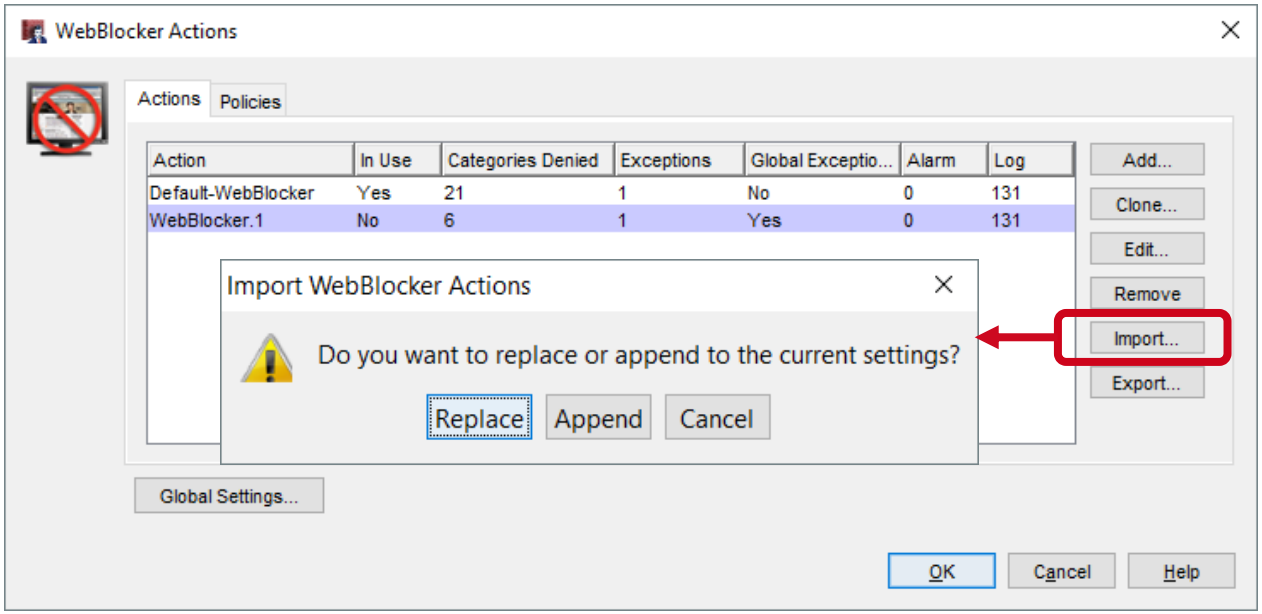
WebBlocker Enhancements

- 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\<username>\Documents\My WatchGuard



WebBlocker Enhancements

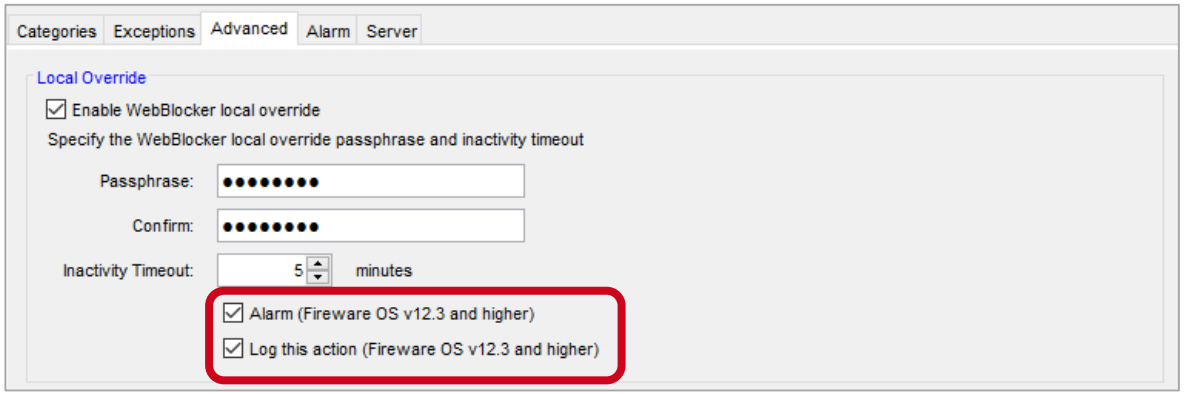
- When you import WebBlocker actions to your Firebox, specify whether to replace existing actions:
  - Replace — Add new actions and replace any existing actions with imported actions that have the same name
  - Append — Add new actions but do not replace existing actions



WebBlocker Enhancements

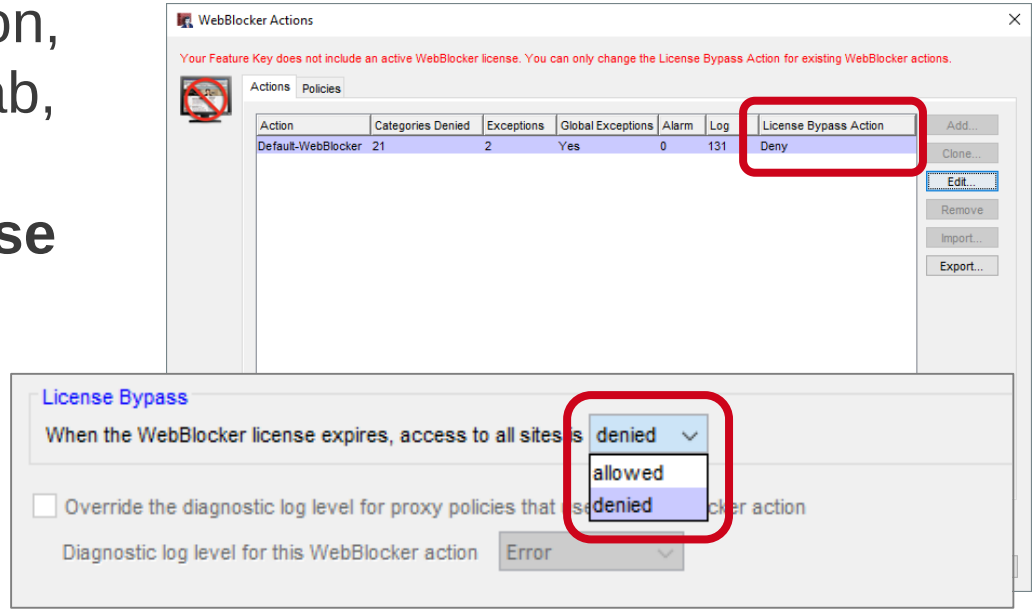
- In the WebBlocker action Advanced tab, you can now enable logs and alarms for WebBlocker local overrides:
  - Alarm — Select to send an alarm when a user enters the local override password
  - Log this action — Select to send a message to the log file when a user enters the local override password

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



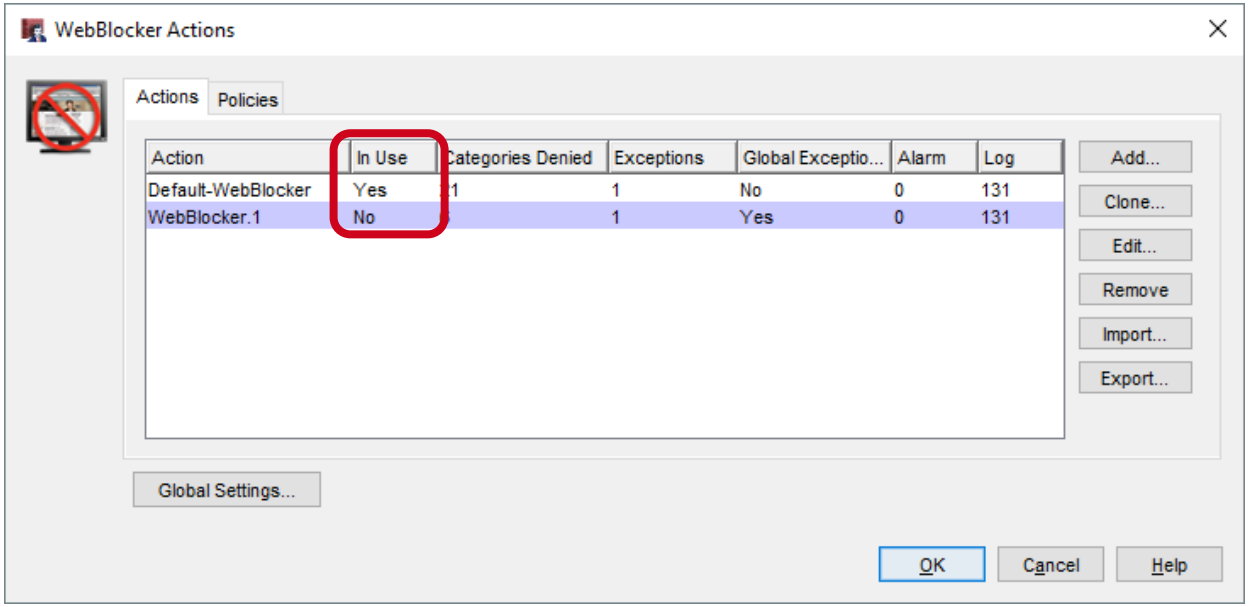
WebBlocker Enhancements

- 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



WebBlocker Enhancements

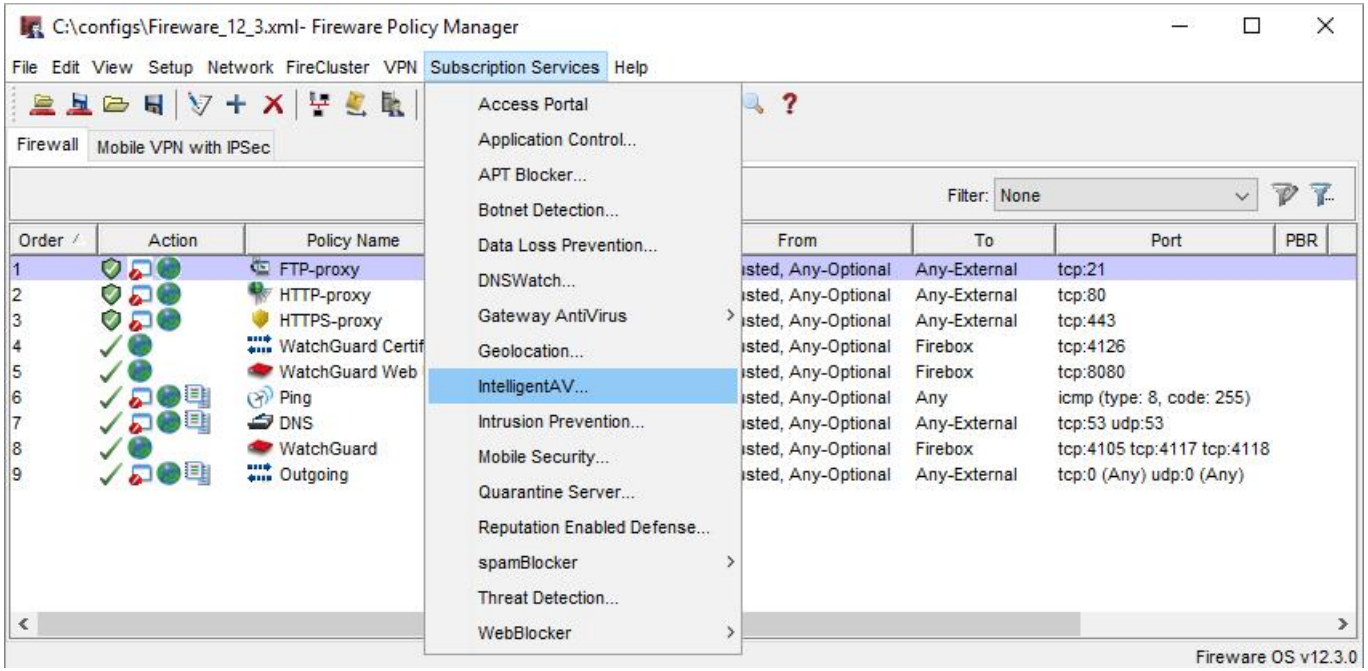
- In Policy Manager, in the WebBlocker Actions list, a new **In Use** column shows whether each WebBlocker action is used by a proxy action
- You can use this column to identify WebBlocker actions that are no longer used and can be removed



Services Usability Enhancements

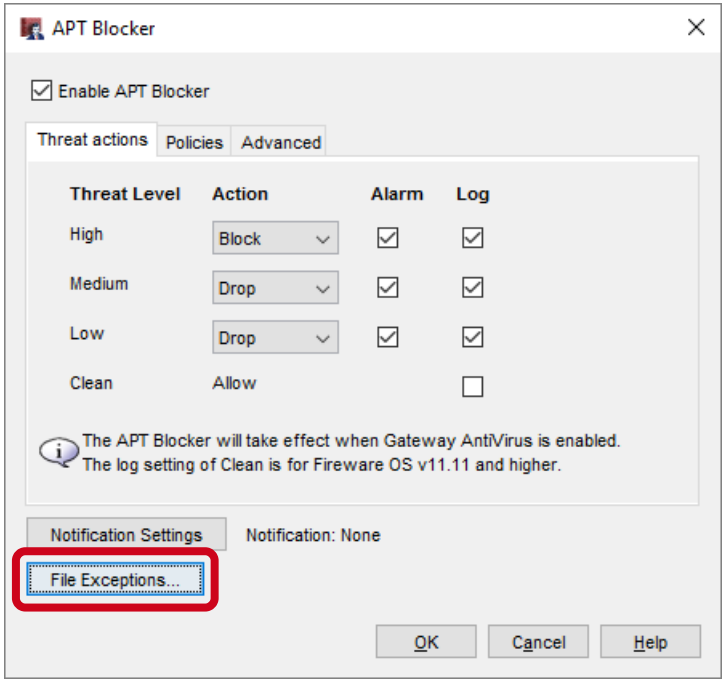
IntelligentAV

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



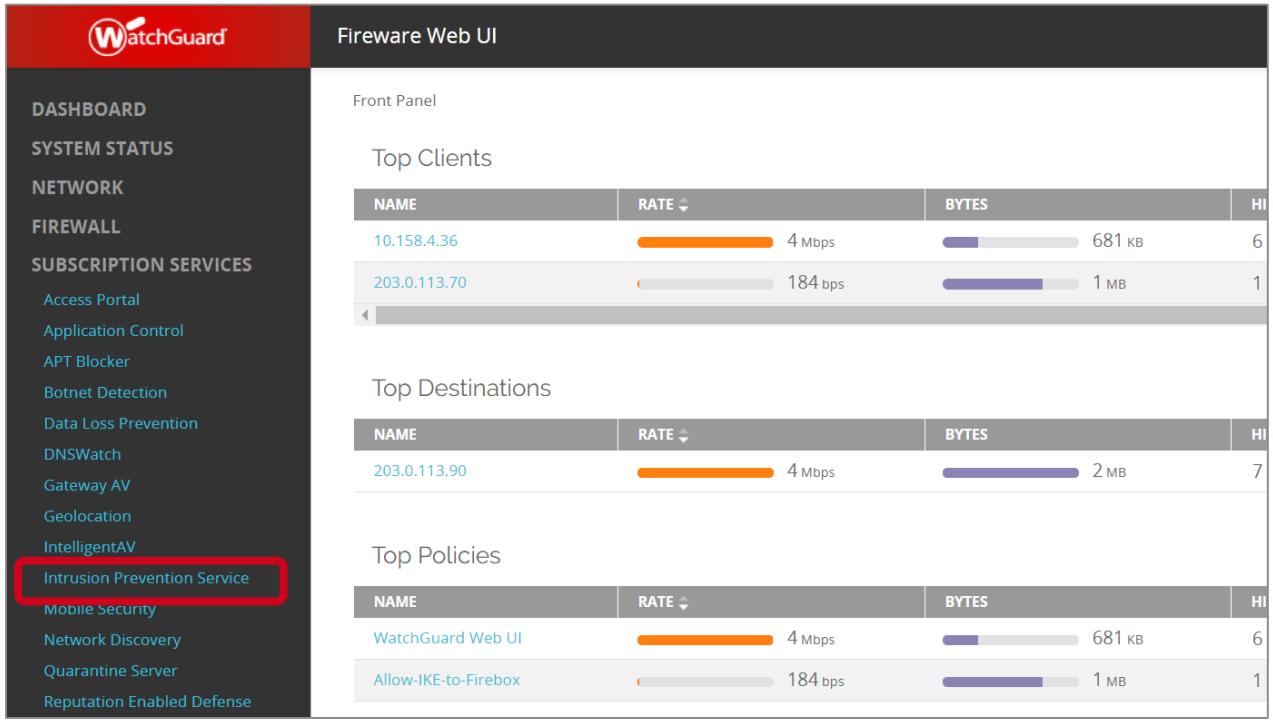
File Exceptions

- 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



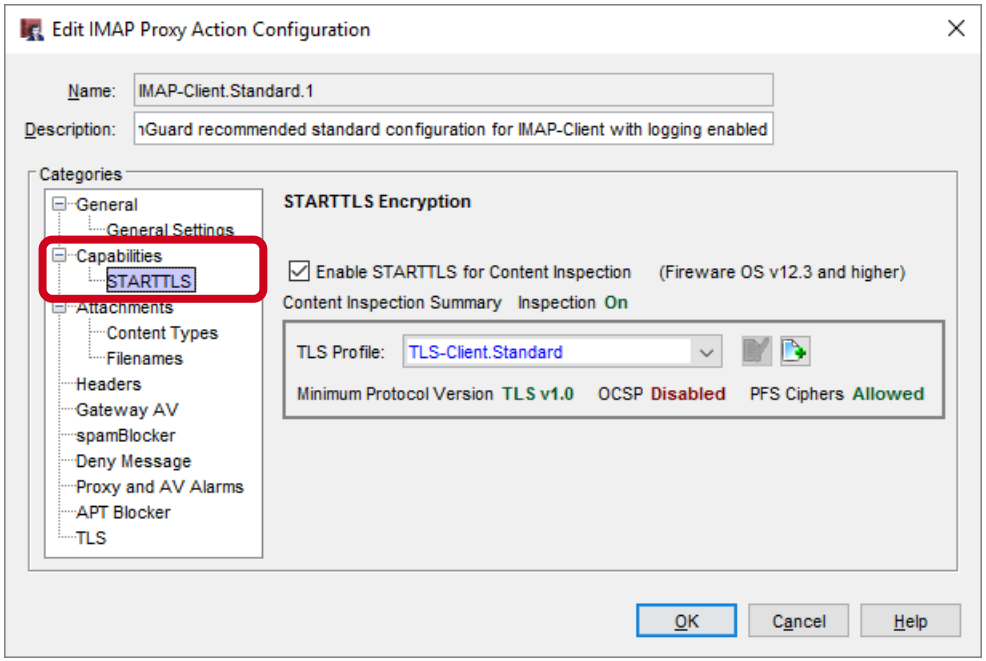
STARTTLS in the IMAP Proxy

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

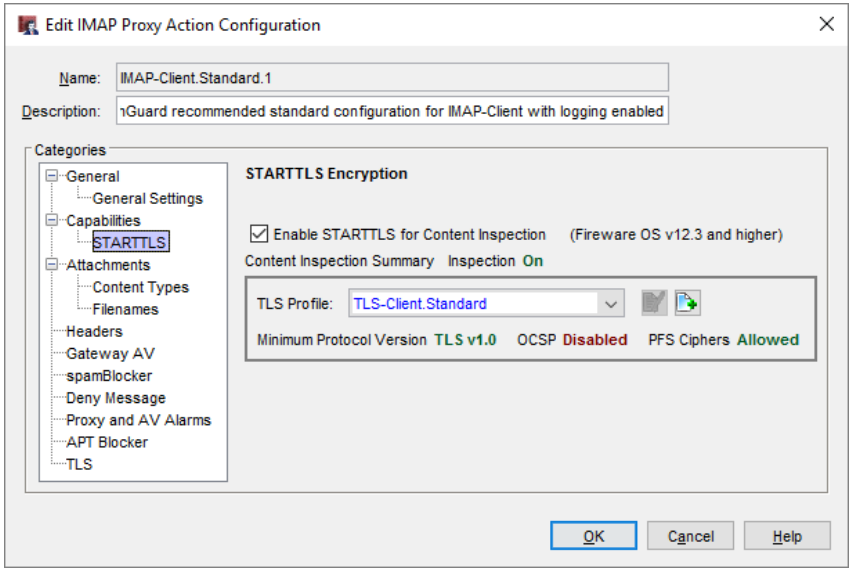
STARTTLS in the IMAP Proxy

- 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



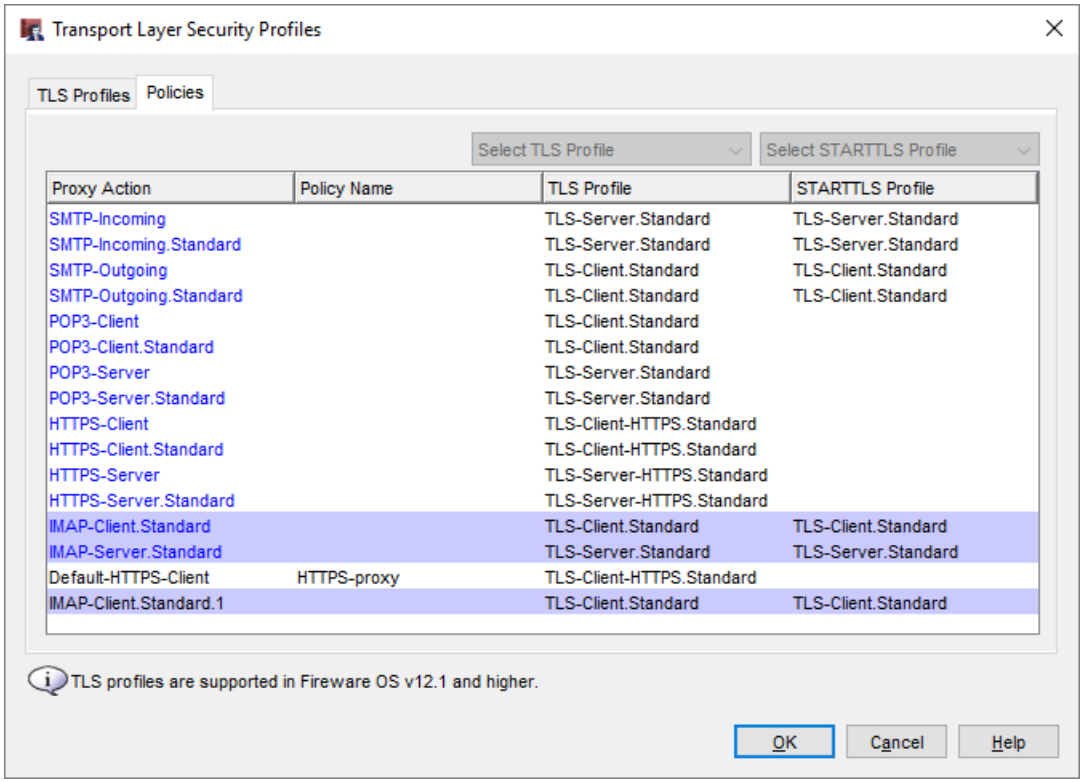
STARTTLS in the IMAP Proxy

- 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

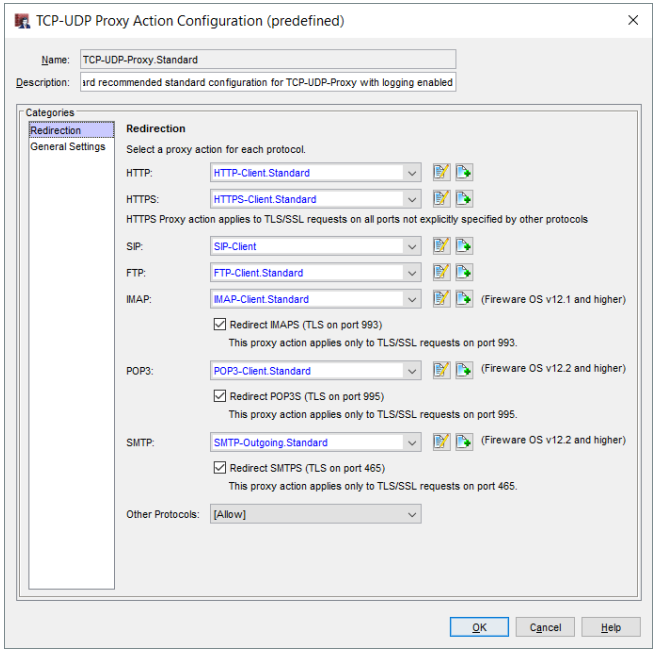
- The IMAP proxy action can now use two different TLS profiles, one for TLS and one for STARTTLS
- In the TLS Profiles configuration, the Policies list now shows both the TLS and STARTTLS profiles configured in each IMAP proxy action

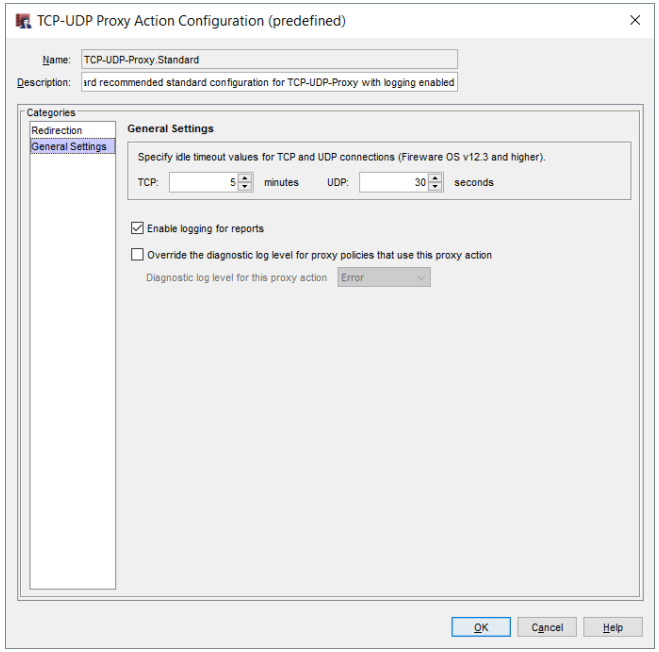


TCP-UDP Proxy Action Enhancements

TCP-UDP Proxy Action Enhancements

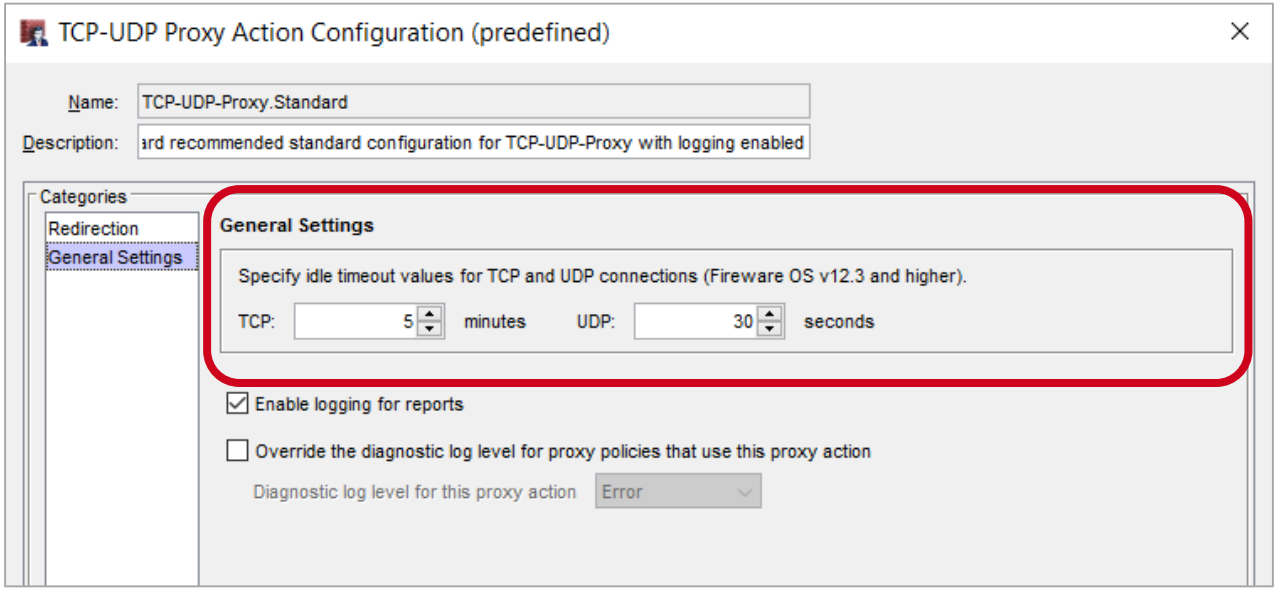
- TCP-UDP Proxy Action settings are now reorganized into two categories:
  - **Redirection:** Configure proxy actions to redirect traffic
  - **General Settings:** Configure timeout values and logging settings





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)

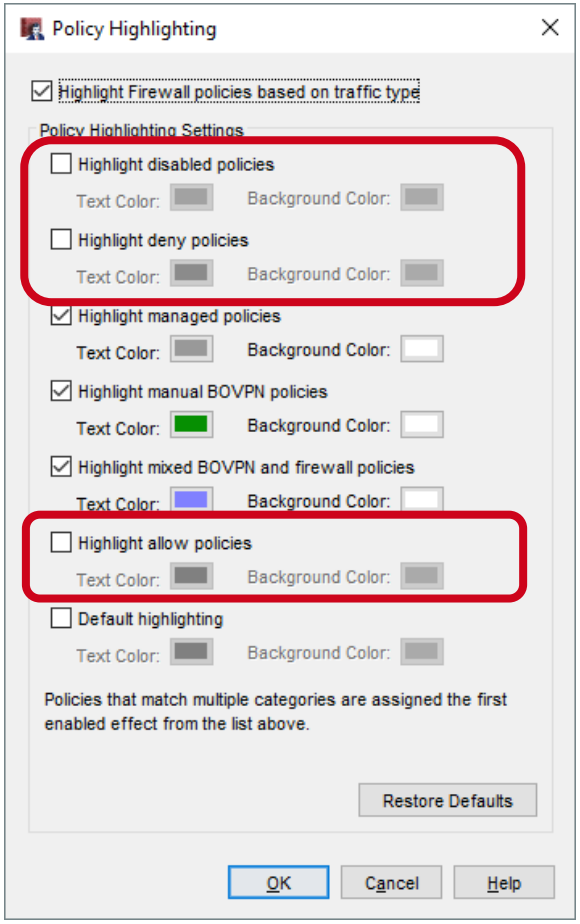


Policy Highlighting Enhancements

WatchGuard Training

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

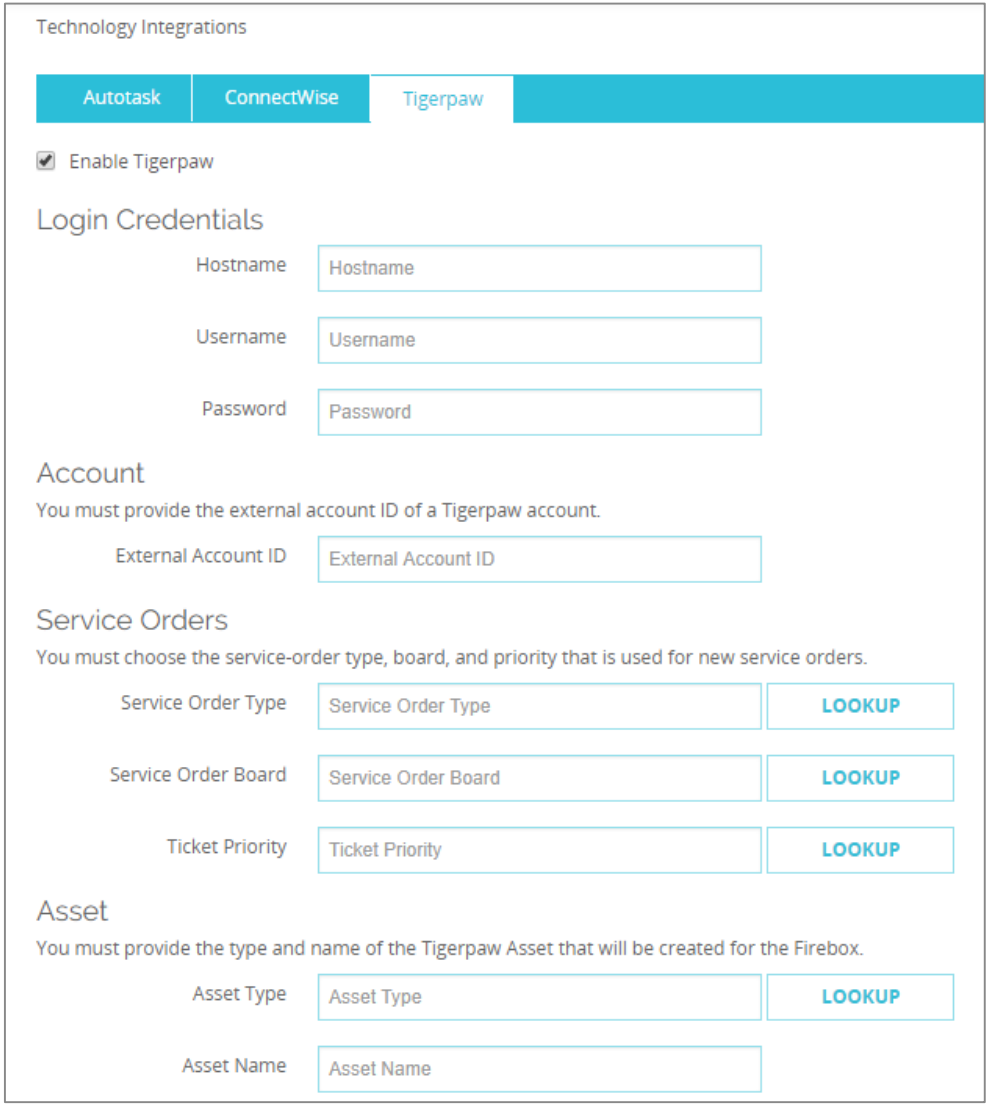
WatchGuard Training

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

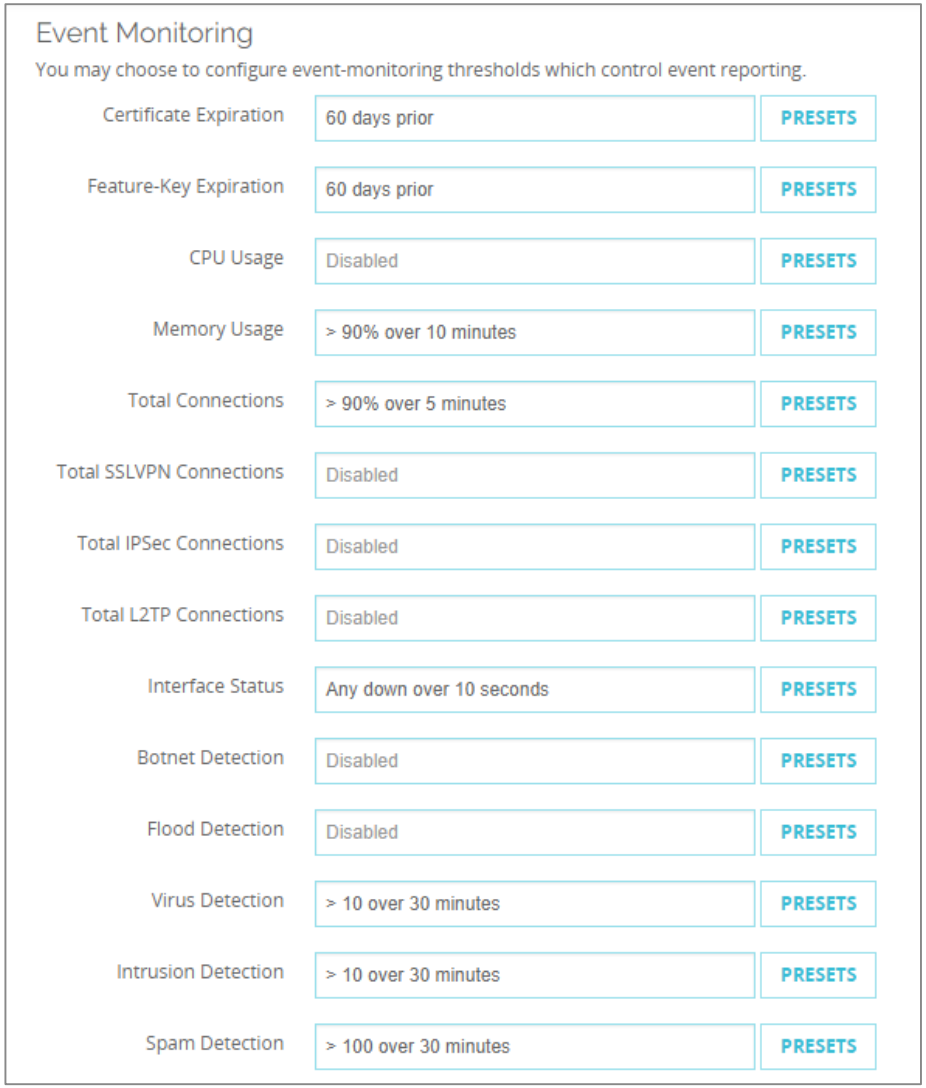
Tigerpaw Integration

- 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



Tigerpaw Integration

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



USB Backup Enhancements

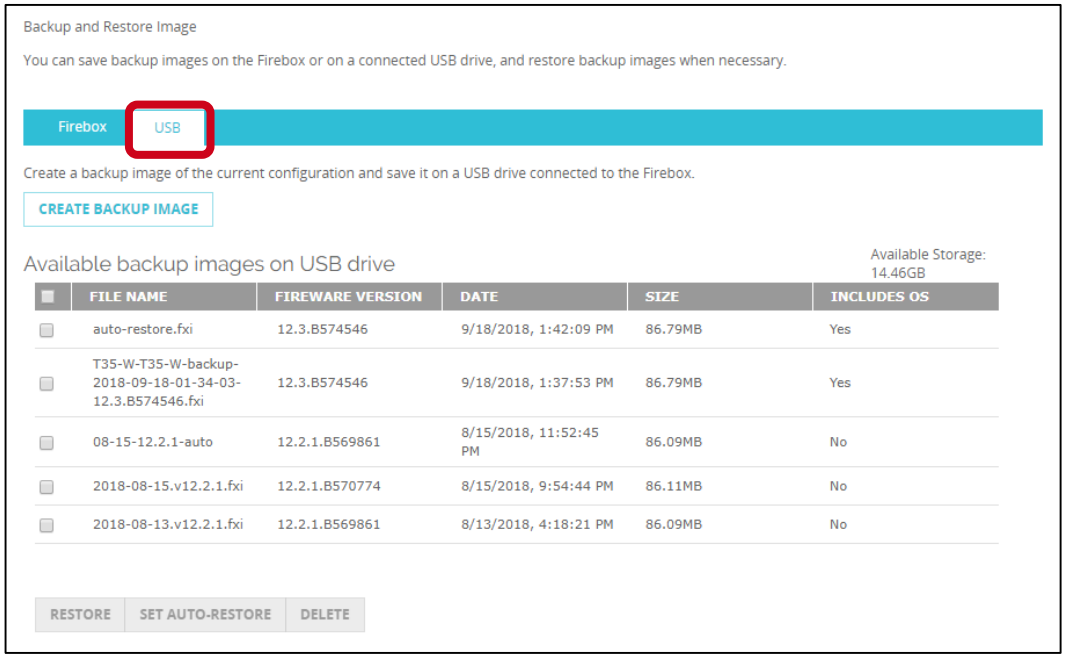
USB Backup Enhancements

- 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

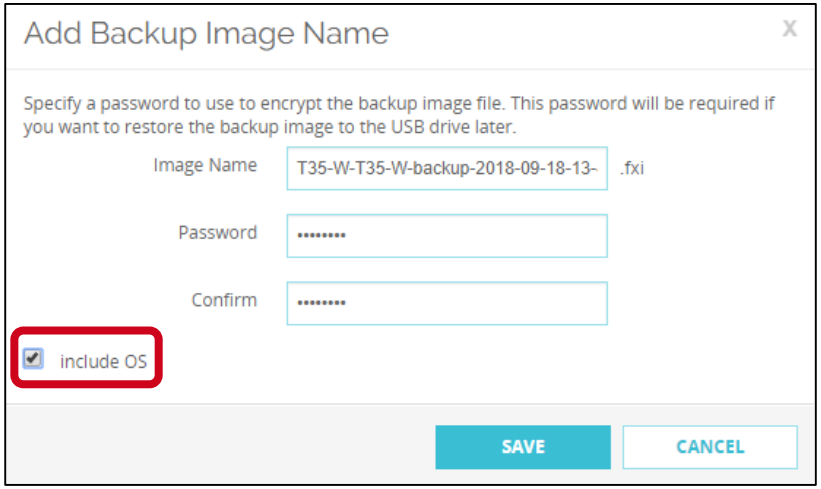
- You can now use the Backup and Restore Image page in Fireware Web UI to see and manage backup images saved on a USB drive connected to the Firebox

1. Select **System > Backup and Restore**
2. Select the **USB** tab



Include Fireware OS in USB Backup Images

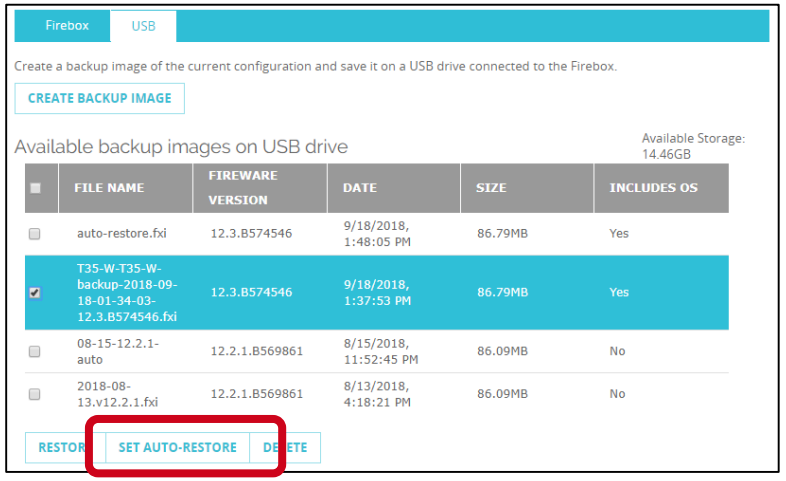
- You can now choose whether to include the Fireware OS in backup images saved to the USB drive
- To save backup images to the USB drive:
  - Fireware Web UI: Select **System > Backup and Restore Image**. Click **Create Backup Image**.
  - Firebox System Manager: Select **Tools > USB Drive**. Click **Create**.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



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



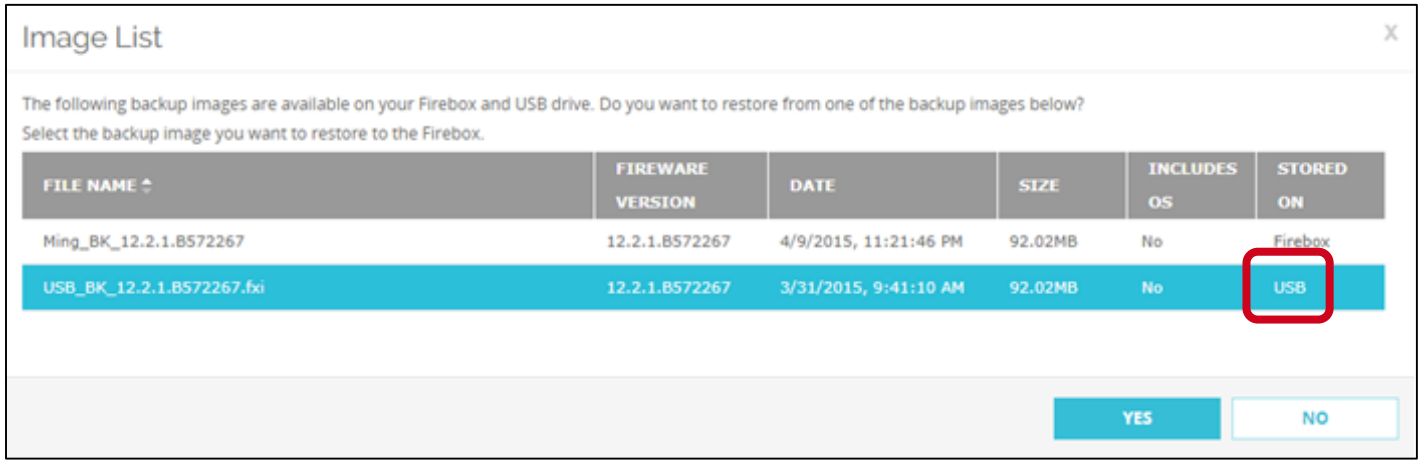
A duplicate of the selected image is saved on the USB drive at: /pending/usb/auto-restore/<Firebox Model>/auto-restore.fxi

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

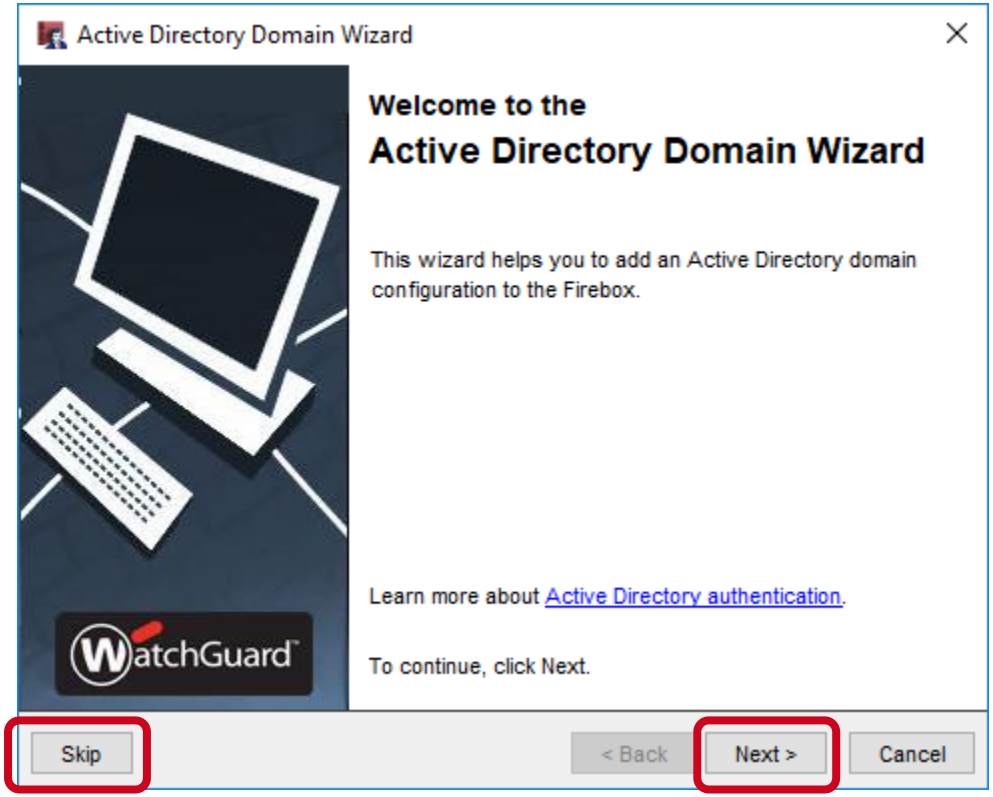
WatchGuard Training

Active Directory Wizard

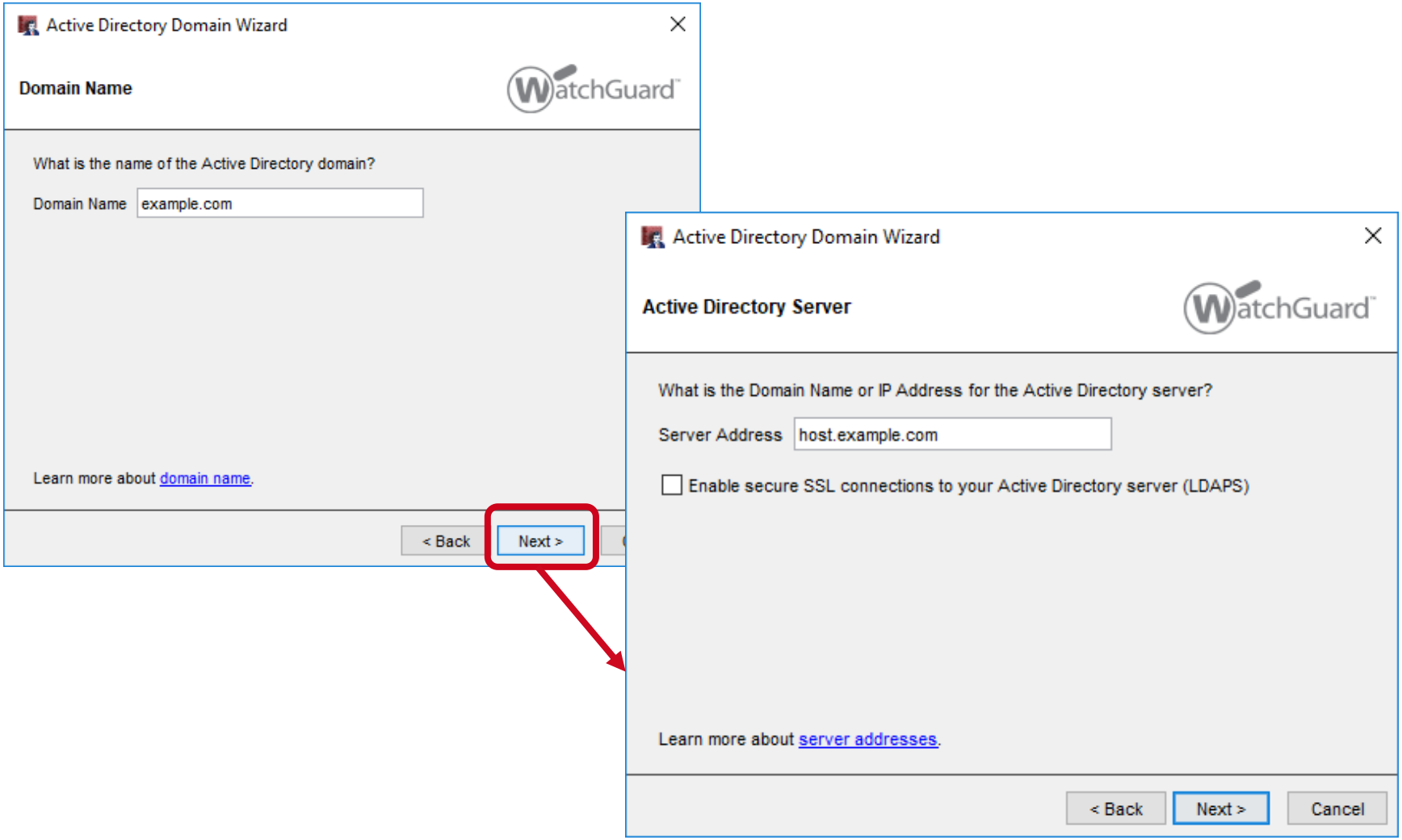
- You can now use a wizard to configure Active Directory server settings on your Firebox
- The wizard simplifies the configuration process because it automatically determines these settings based on the domain name you specify:
  - Search base settings
  - Active Directory server address
- After you 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

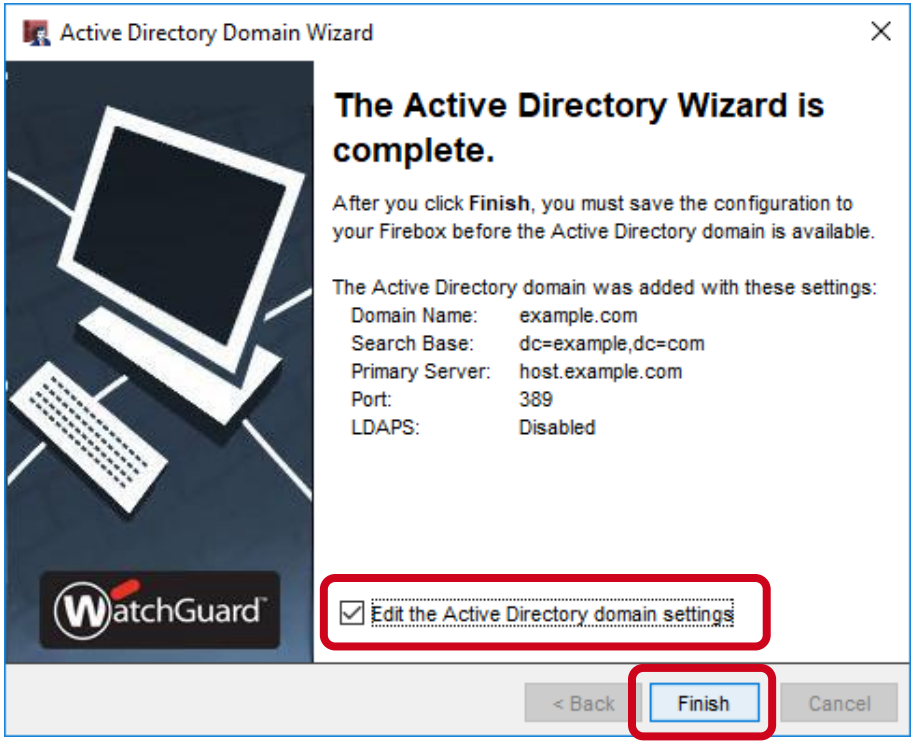


Active Directory Wizard



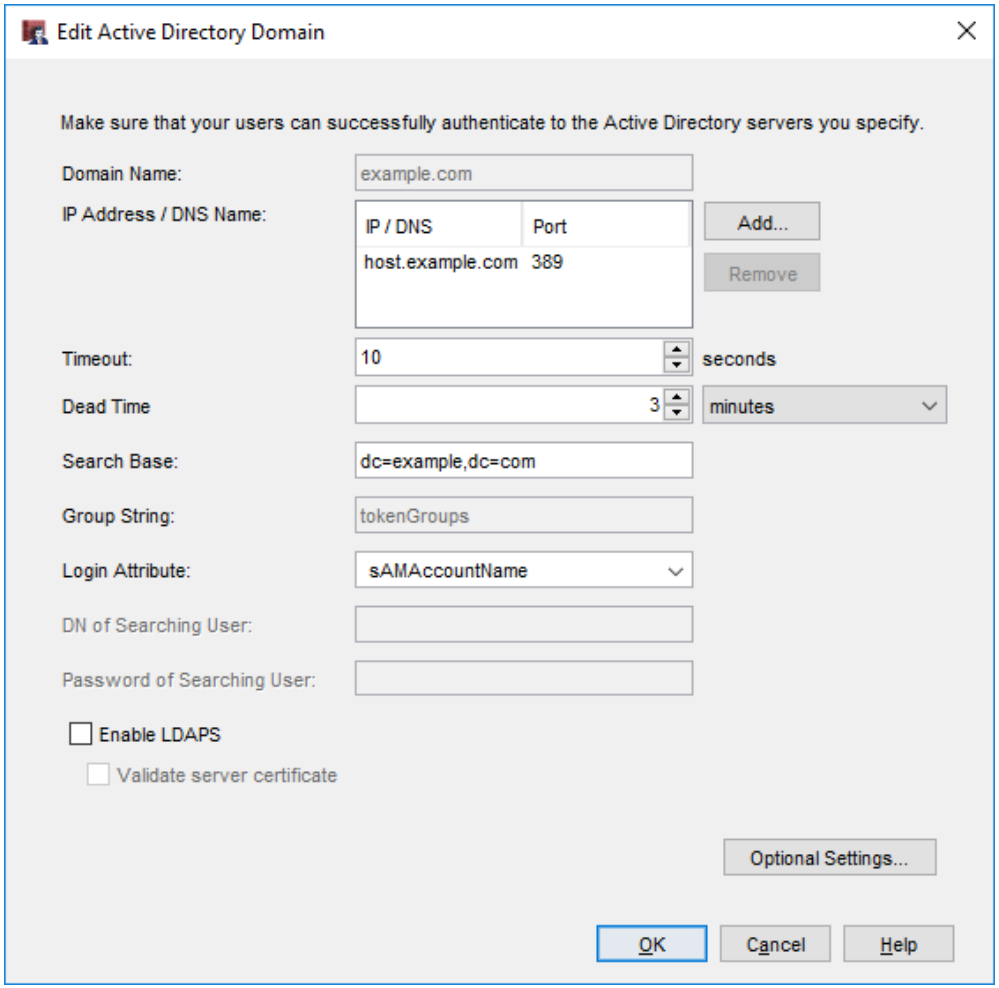
Active Directory Wizard

- 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

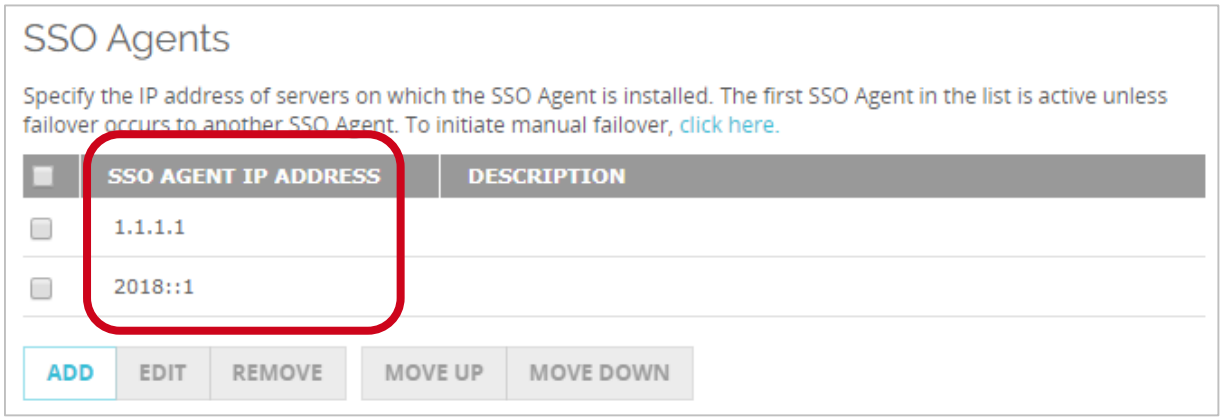


IPv6 Support for Active Directory SSO

WatchGuard Training

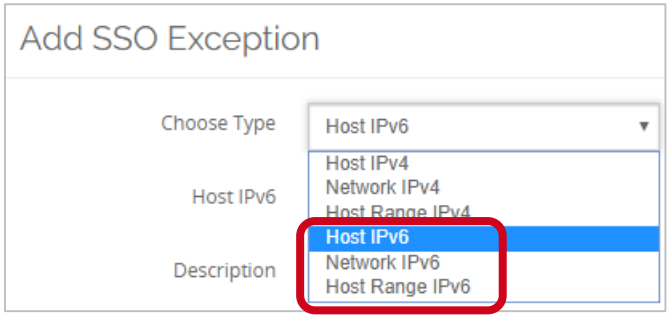
IPv6 Support for Active Directory SSO

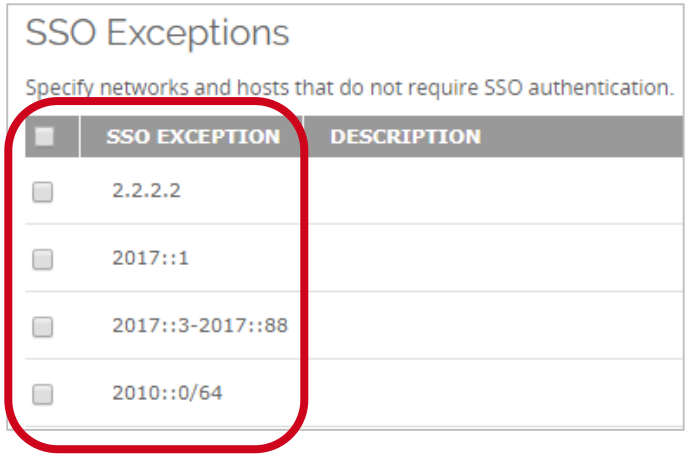
- Most Active Directory single sign-on (SSO) components now support IPv6
  - The Firebox, SSO Agent, SSO Client, and Event Log Monitor support IPv6
  - Exchange Monitor does not support IPv6 in Fireware v12.3
- On the Firebox, you can configure either an IPv4 or IPv6 address for the SSO agent if the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



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



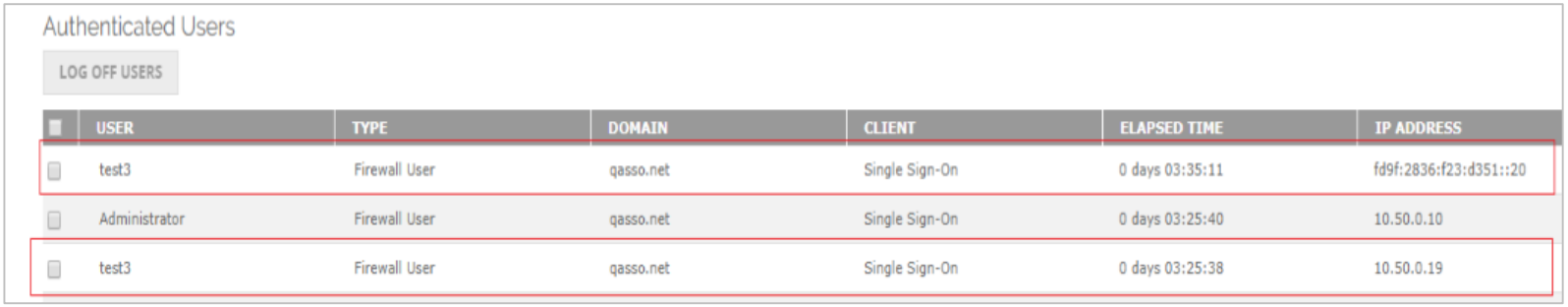


IPv6 Support for Active Directory SSO

- 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:*



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

WatchGuard Training

SSO Agent Debug Info

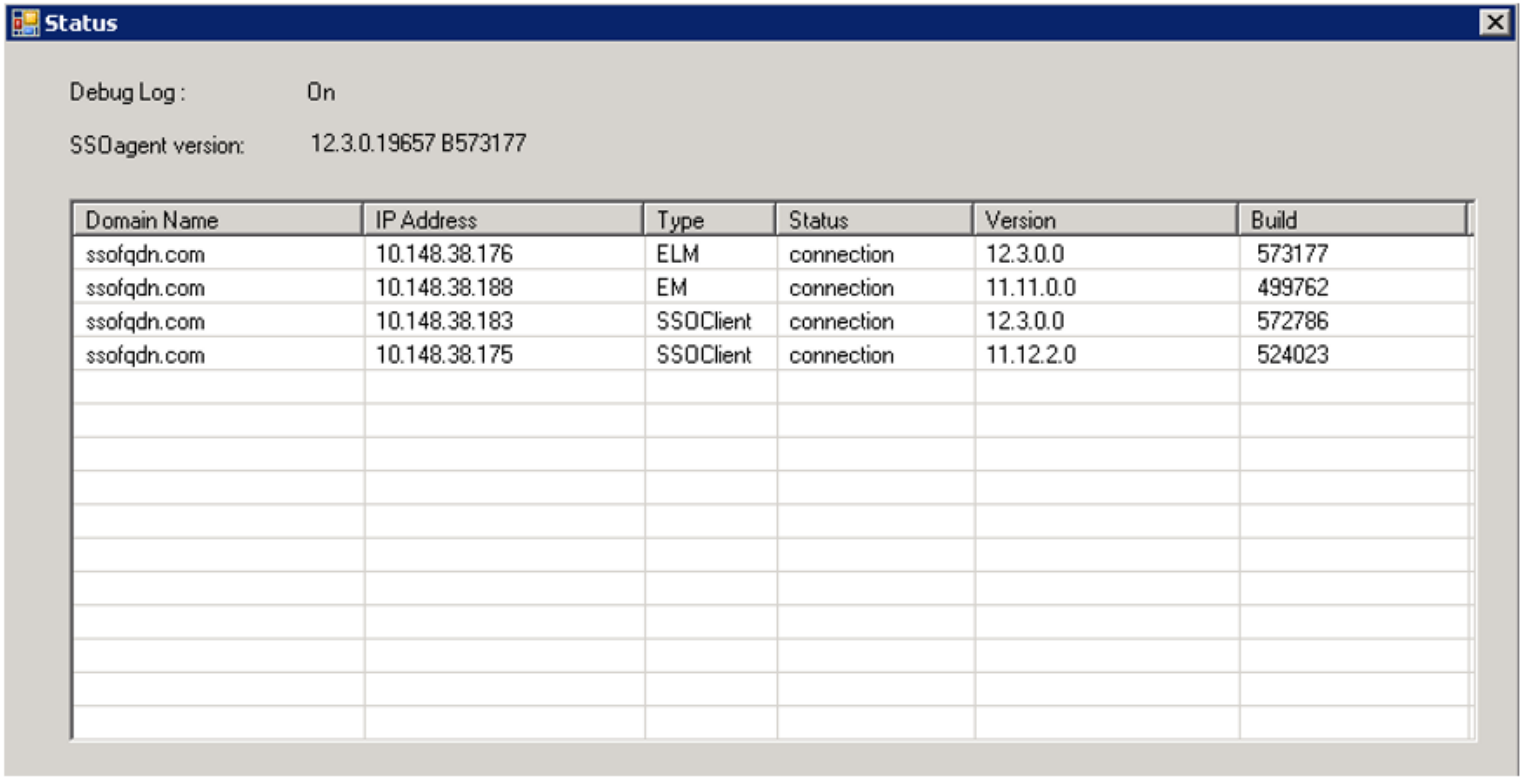
- Real-time information about single sign-on components helps you troubleshoot SSO issues on your network

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

SSO Agent Debug Information

- In the SSO Agent, select **Information > Status**

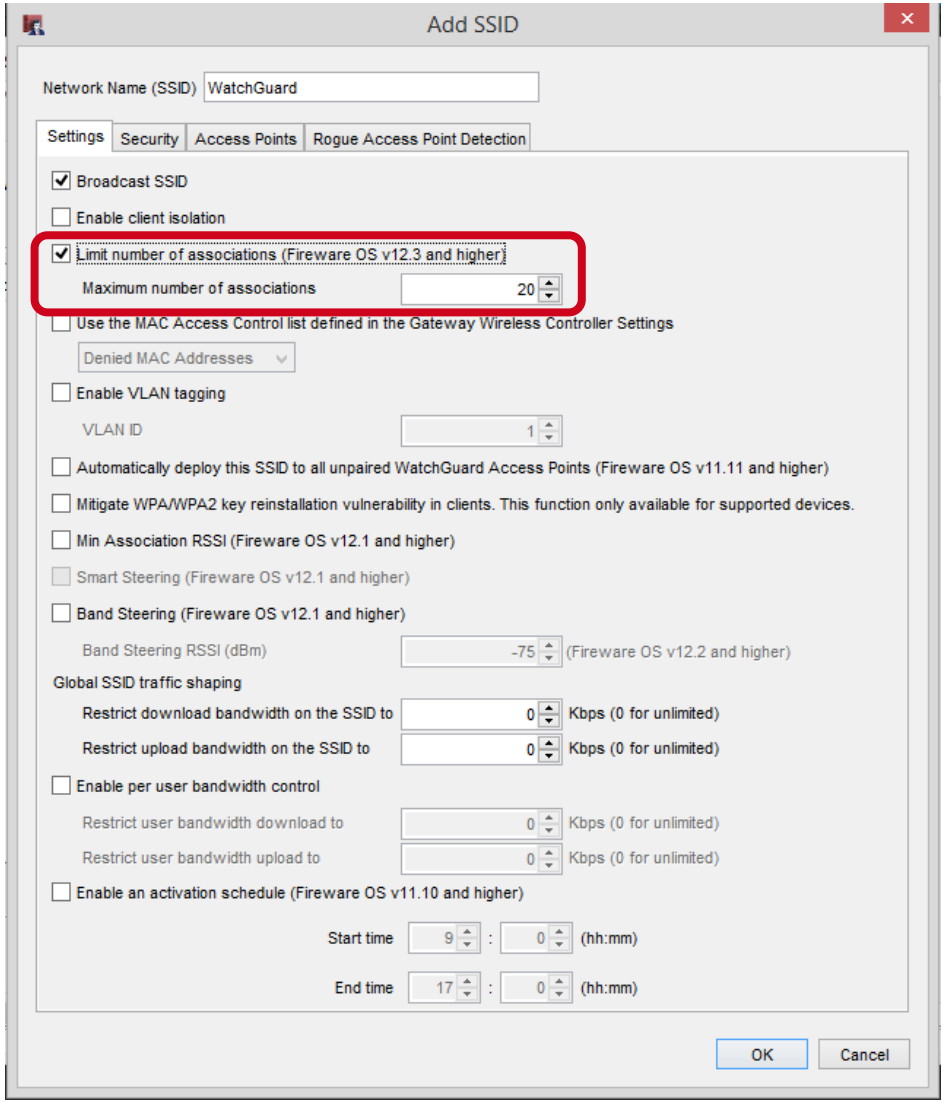


Gateway Wireless Controller Enhancements

WatchGuard Training

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



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 Training

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