What's New in Fireware v12.0.1

What's New in Fireware v12.0.1

- Security Services Enhancements
  - Gateway AntiVirus checkbox added to Proxy Action settings
  - Gateway AntiVirus scan size limit set automatically
  - Action for when scan size limit is exceeded
  - Action for encrypted files
  - Gateway AntiVirus file decompression is enabled by default
  - Subscription Service menus in alphabetical order

What's New in Fireware v12.0.1

- Technology Integration Enhancements
  - Autotask Integration
  - ConnectWise Integration
    - Use a new or existing ConnectWise configuration
    - Service board selection for Firebox tickets
    - Ability to edit configuration questions
- Policy Enhancements
  - YouTube for Schools removed

What's New in Fireware v12.0.1

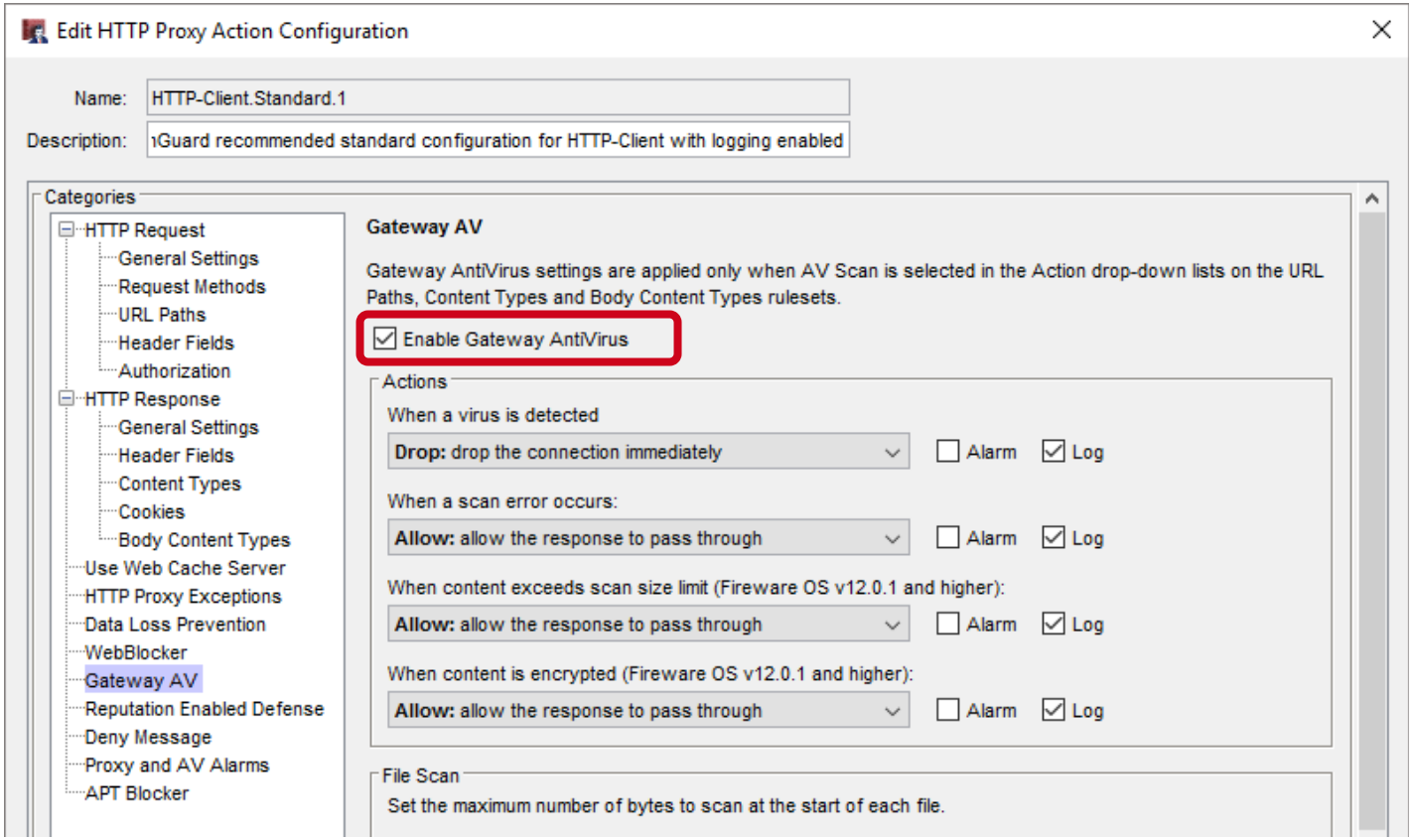
- Wireless Enhancements
  - KRACK WPA/WPA2 vulnerability mitigation
  - TKIP Option Removed for WPA2
- Other Enhancements
  - Support access for remote login
  - Quick Setup Wizard default stance settings updated
  - Enable configuration for a specific Fireware version in Policy Manager

Security Services Enhancements

WatchGuard Training

Enable Gateway AV Check Box Added

- **Enable Gateway AntiVirus** check box added to the Gateway AV settings in a proxy action



Added Gateway AV Enable Checkbox

- The **Enable Gateway AntiVirus** check box automatically enables or disables the **AV Scan** action in the proxy action
  - When you select the **Enable Gateway AntiVirus** check box, actions previously set to **Allow** are changed to **AV Scan**
  - When you clear the **Enable Gateway AntiVirus** check box, actions previously set to **AV Scan** are changed to **Allow**
- This new check box has the same effect as enabling or disabling Gateway AntiVirus for a proxy policy in the **Subscription Services > Gateway AntiVirus** settings

Gateway AV Scan Size Limits

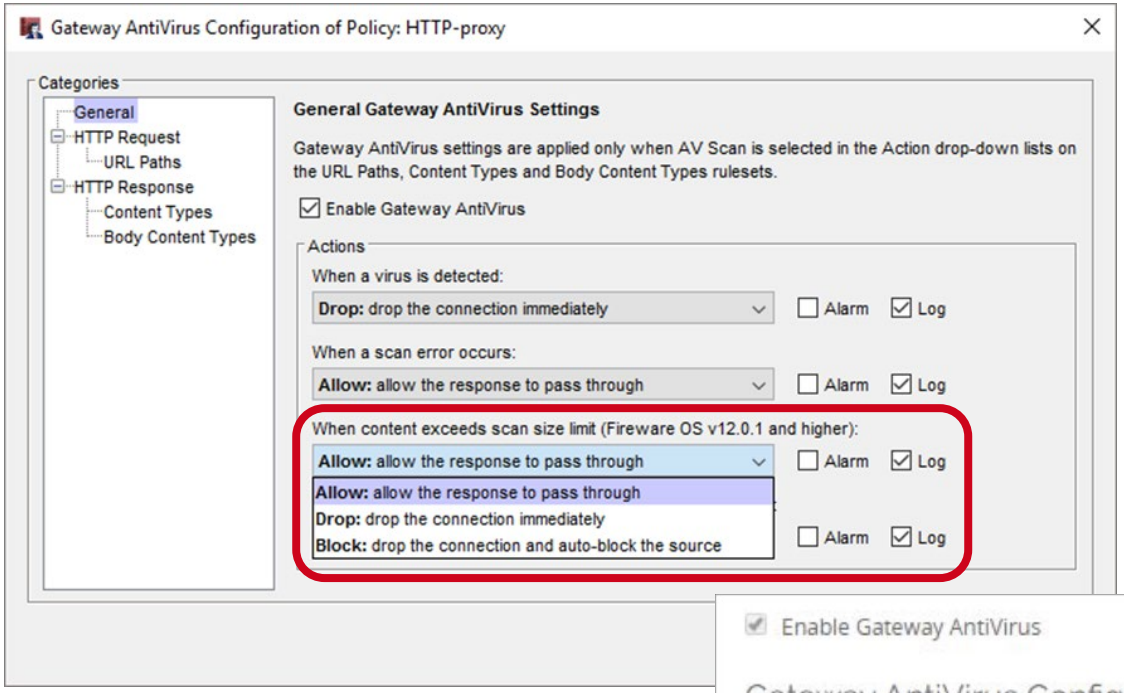
- The Gateway AV default and maximum scan size limits are set based on the hardware capabilities of each Firebox model
- Minimum scan size for all models is 1 MB

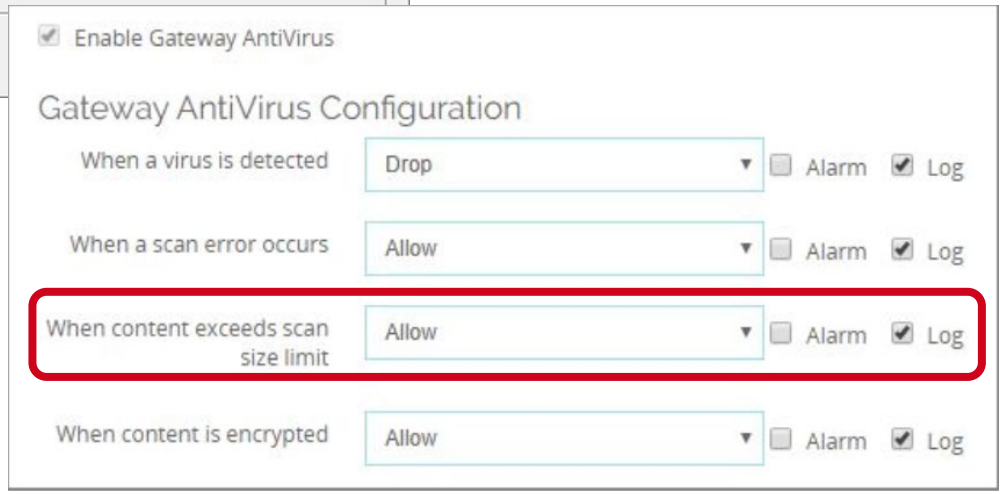
Default Scan Size Limit	Maximum Scan Size Limit	Model
1 MB	5 MB	Firebox T10, XTM 25, XTM 26
2 MB	10 MB	Firebox T30, XTM 33, XTM 330, Firebox Cloud Small, FireboxV Small, XTMv Small
5 MB	20 MB	Firebox T50, T70, M200, XTM 515, XTM 525, XTM 535, XTM 810, XTM 820, XTM 830, XTM 830-F, Firebox Cloud Medium, FireboxV Medium, XTMv Medium
10 MB	20 MB	All other models

Gateway AV Action for Scan Limit Exceeded

- Configure the action to take when content exceeds the Gateway AntiVirus scan size limit
- Actions when content exceeds the scan limit:
  - Allow
  - Drop
  - Block
- Notification options:
  - Alarm
  - Log (default)

Gateway AV Action for Scan Limit Exceeded

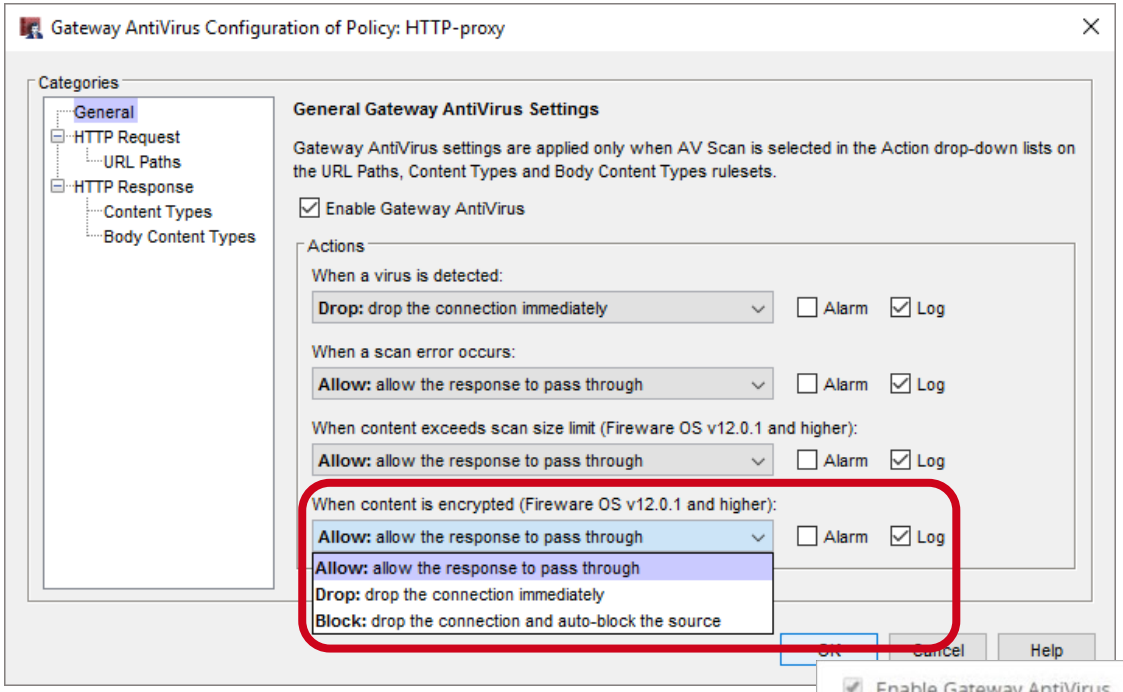


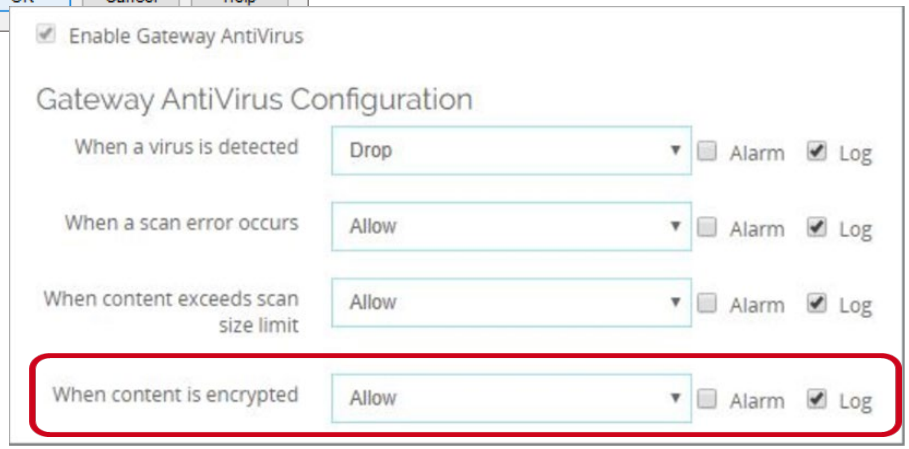


Gateway AV Action for Encrypted Content

- Configure the action to take when Gateway AntiVirus cannot scan a file because it is encrypted (password protected)
  - Encrypted files were previously handled by the scan error action
  - Scan failures for encrypted files can now be differentiated from other scan errors
- Actions when content is encrypted:
  - Allow
  - Drop
  - Block
- Notification options:
  - Alarm
  - Log (default)

Added Encrypted Content Options





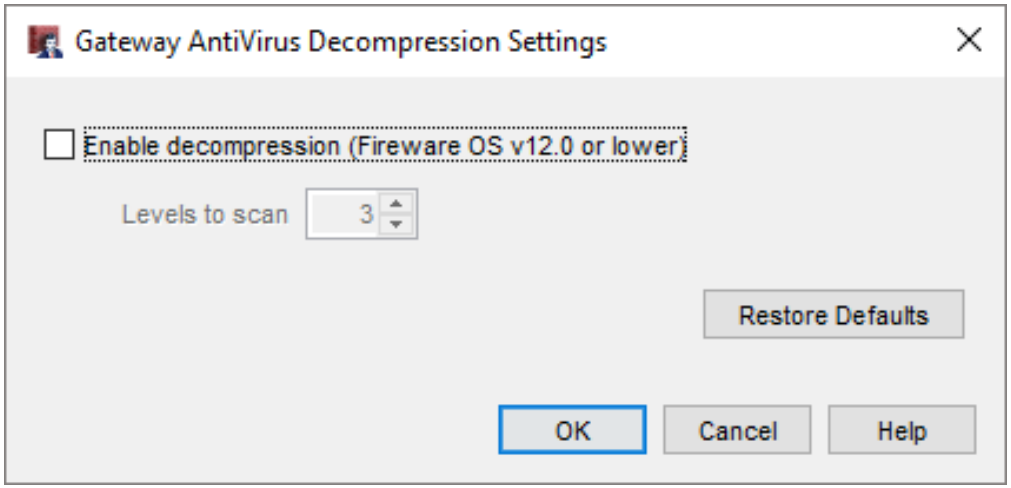
Gateway AV Decompression Enabled

- Gateway AntiVirus file decompression is always enabled in Fireware OS v12.0.1 or higher
- The scan depth depends on the amount of RAM
  - Firebox models with less then 2GB RAM use scan depth 8
  - Firebox models with 2GB or greater use scan depth 16

RAM	Decompression
Less than 2GB	Scan depth 8
2GB or greater	Scan depth 16

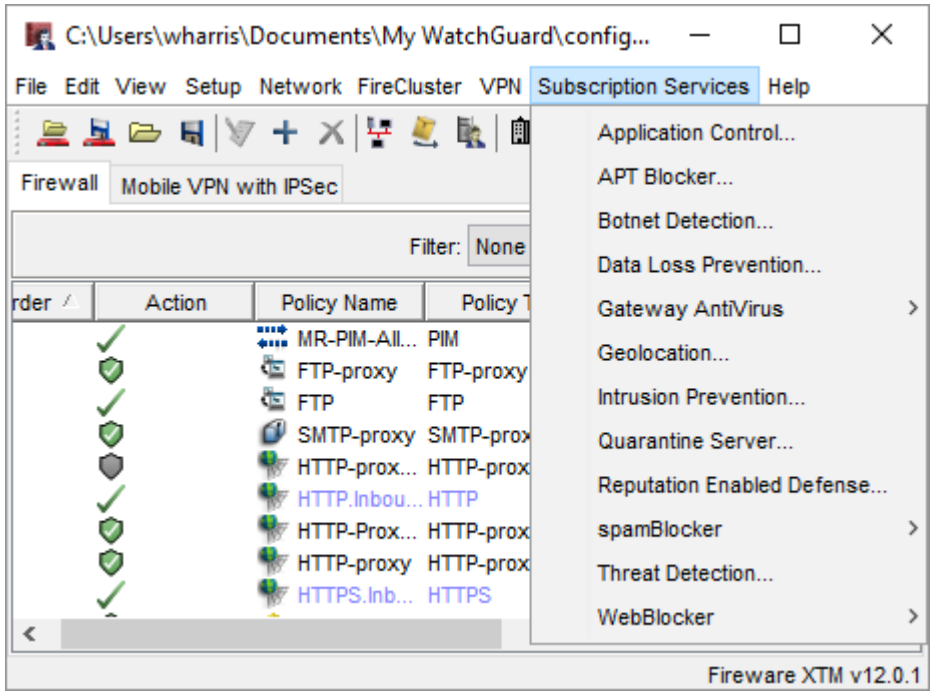
Gateway AV Decompression Enabled

- In Policy Manager, the **Gateway AntiVirus Decompression Settings** are retained for Fireware OS v12.0.0 or lower



Subscription Service Menu

- The **Subscription Services** menu in the Web UI and WatchGuard System Manager now shows the services in alphabetical order

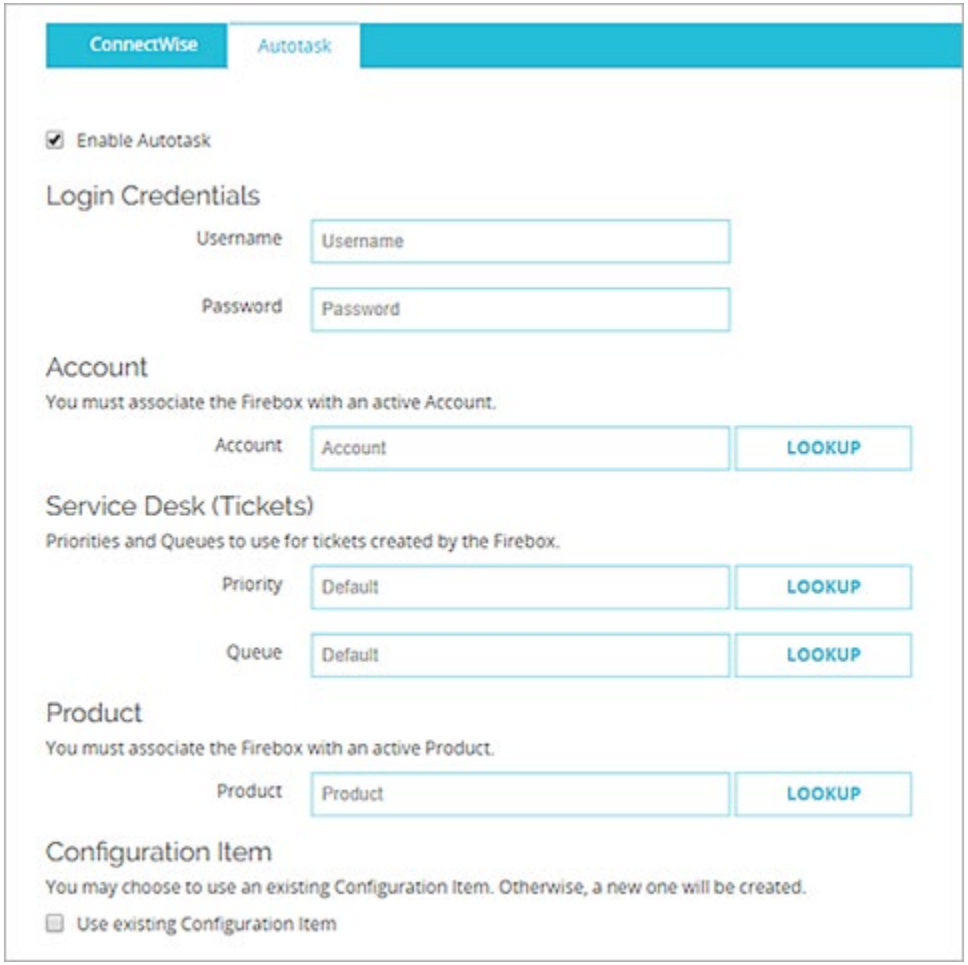


Technology Integration Enhancements

WatchGuard Training

Autotask Integration

- Support for Autotask integration
- Similar to the current ConnectWise integration
- In the Web UI in **System > Technology Integrations**
- In Policy Manager, in **Setup > Technology Integrations**

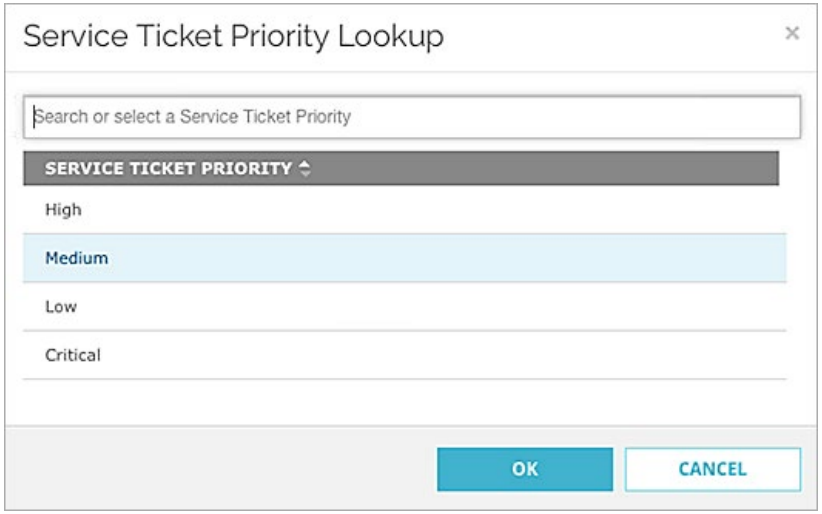


Autotask Integration

- To connect the Firebox to Autotask, you must specify:
  - An Autotask user name and password
    - Autotask does not use API keys
  - The name of an active Autotask account
  - A Product type
- You can select a default Priority and Queue for tickets created by Firebox events

Autotask Integration

- When you click **Lookup** for the Priority, Queue, and Product, default Autotask values appear
- On the Autotask website, you can add custom Priority levels, Queues, and Product types that appear on the Firebox when you click **Lookup**



Autotask Integration

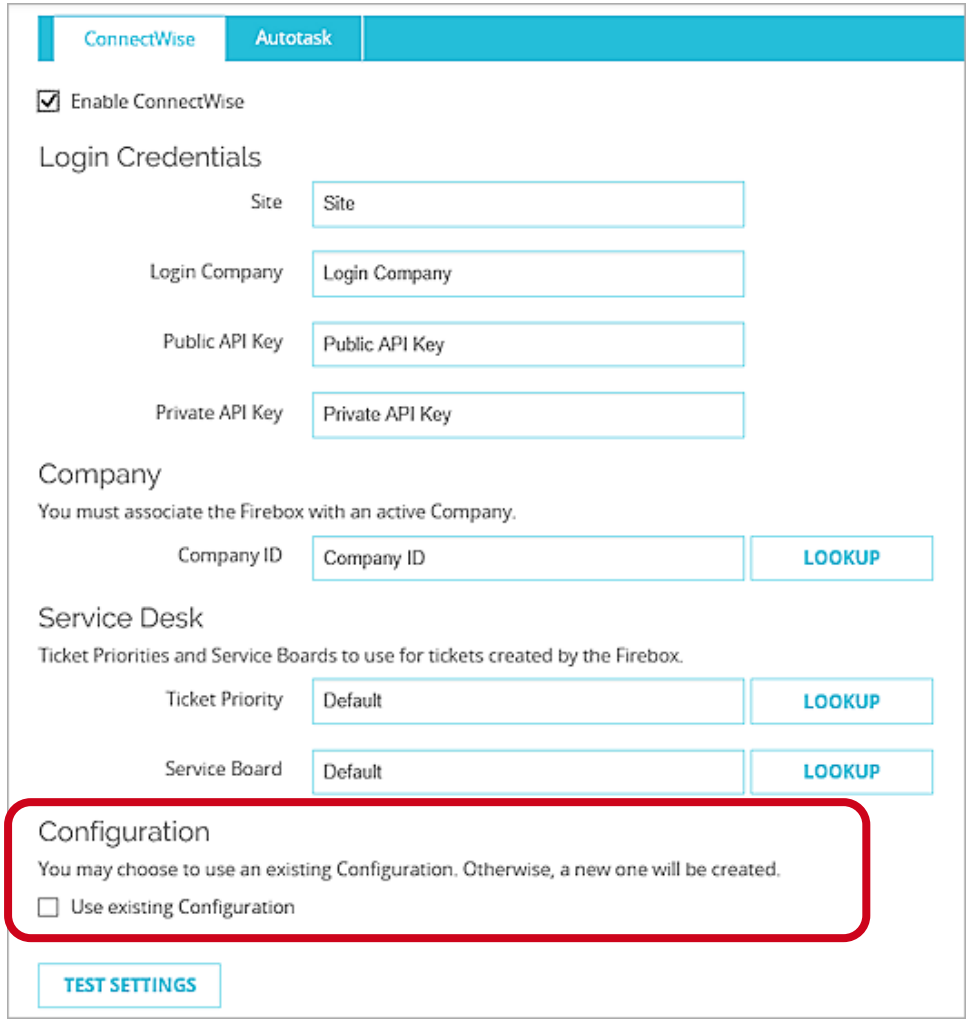
- After you save the configuration, Autotask automatically creates an object for the Firebox known as a *Configuration Item*
- Configuration Items are:
  - Assets that you manage in Autotask
  - Grouped by product type in Autotask

Autotask Integration

- In Autotask, if you edit the monitors for configuration items, you must use the same syntax as existing monitors
- For example, if you edit the **WG: Monitor CPU Usage** monitor, the syntax must be **> xx% over xx minutes**
  - **> 50% over 30 minutes** is valid
  - **50 percent > 30 mins** is invalid
- If you create a monitor with invalid syntax, the Autotask UI does not alert you, but error messages appear in the Firebox log messages

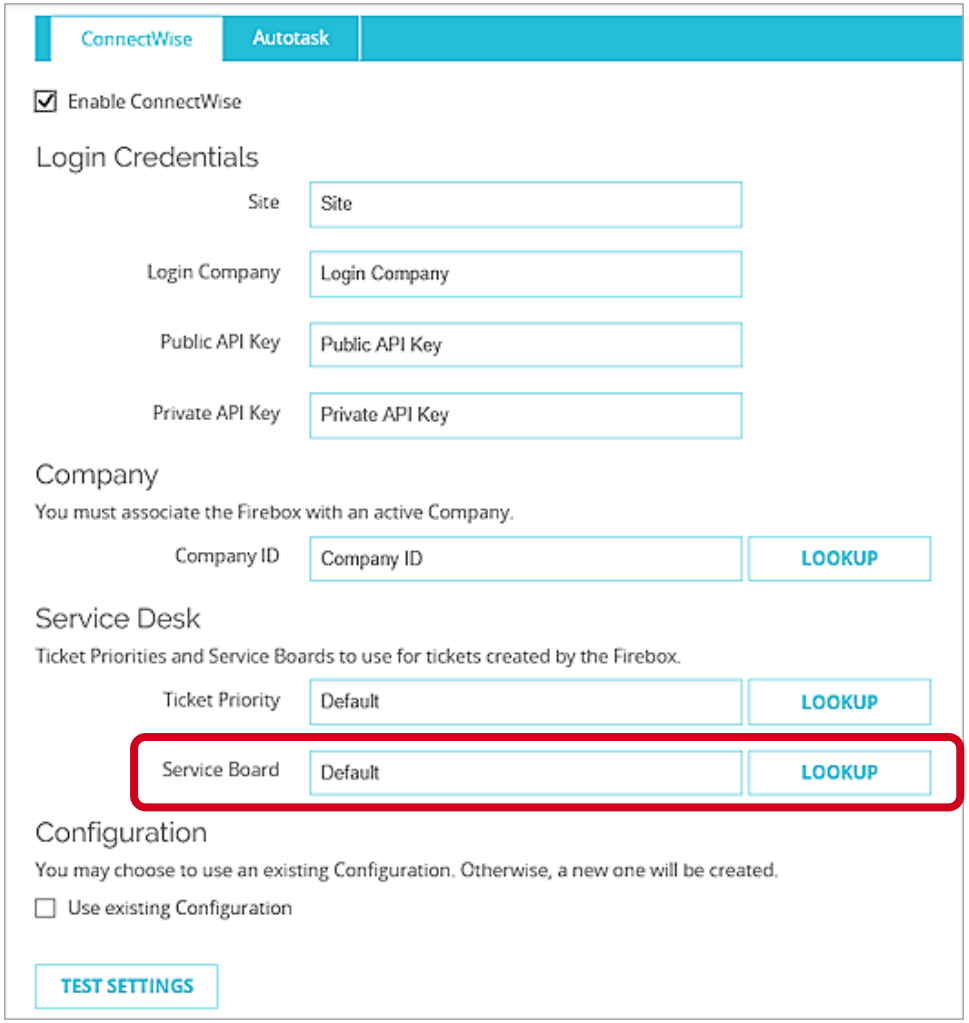
ConnectWise Configuration

- When you enable ConnectWise integration on a Firebox, you can now use a ConnectWise configuration that has already been set up for the Firebox (based on Firebox serial number)
- If you do not select to use an existing configuration, a new configuration is created in ConnectWise



ConnectWise Service Board

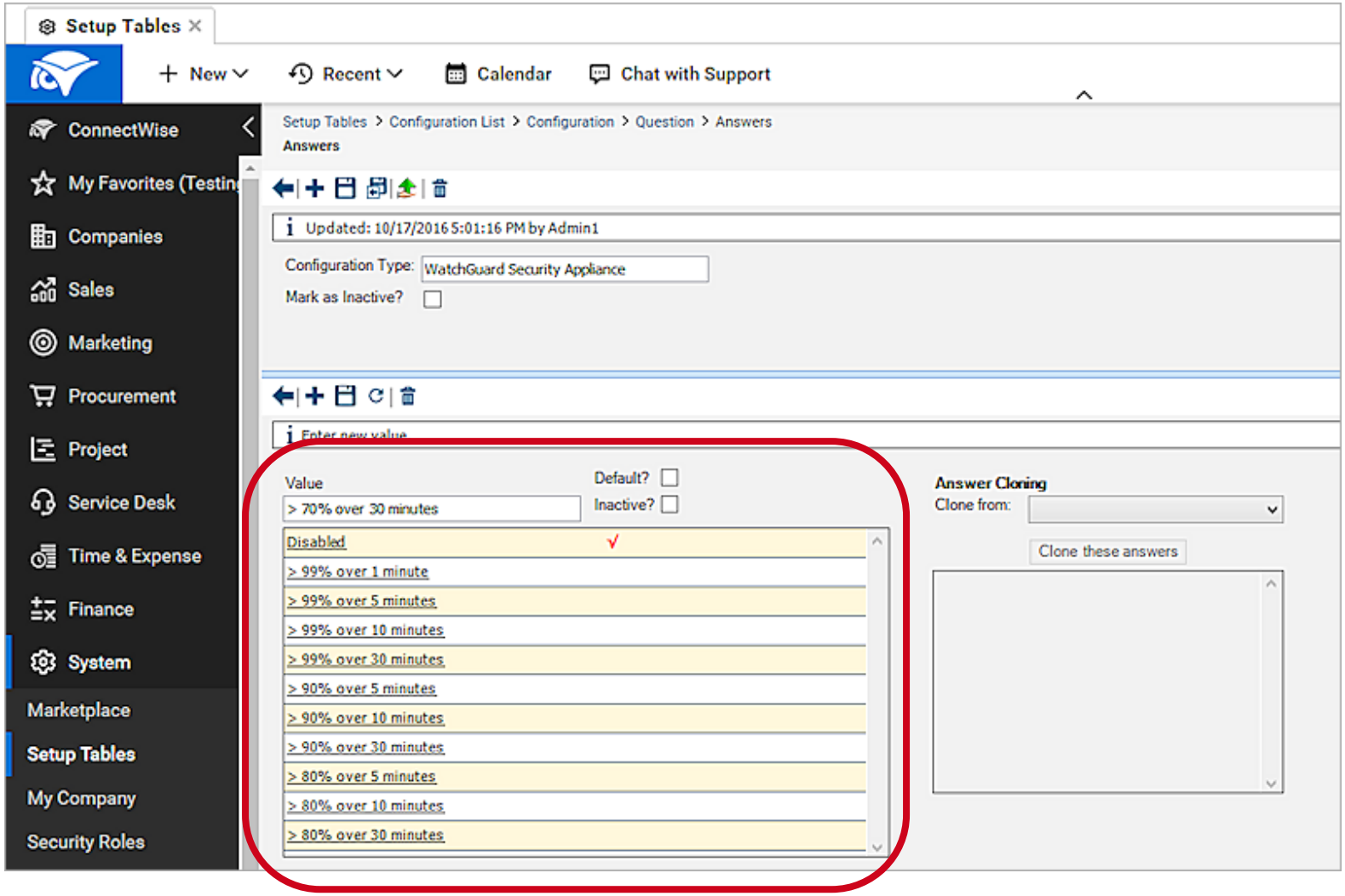
- You can now specify the Service Board where new Firebox tickets are created in ConnectWise
- Click Lookup to choose from a list of Service Boards in ConnectWise
- You can edit the Service Board selections in ConnectWise



Edit ConnectWise Configuration Questions

- In ConnectWise, you can now edit Firebox configuration question answers
- You must use the same syntax as existing configuration question answers
  - For example, for the monitor-based configuration questions such as **CPU Usage**, the syntax must be **> xx% over xx minutes**
    - **> 70% over 30 minutes** is valid
    - **70 percent > 30 mins** is invalid

Edit ConnectWise Configuration Questions



Technology Integrations and Config Report

- The Firebox Configuration Report now includes information on Technology Integrations (ConnectWise and Autotask)

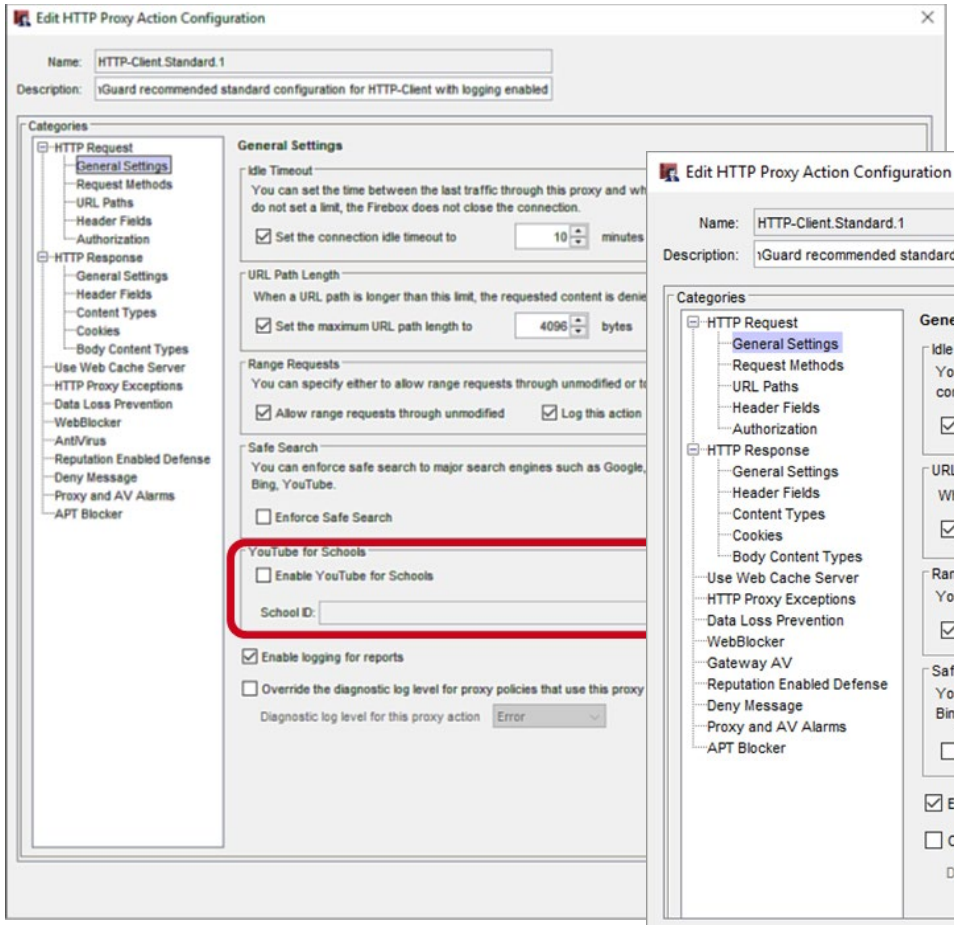
Policy Enhancements

WatchGuard Training

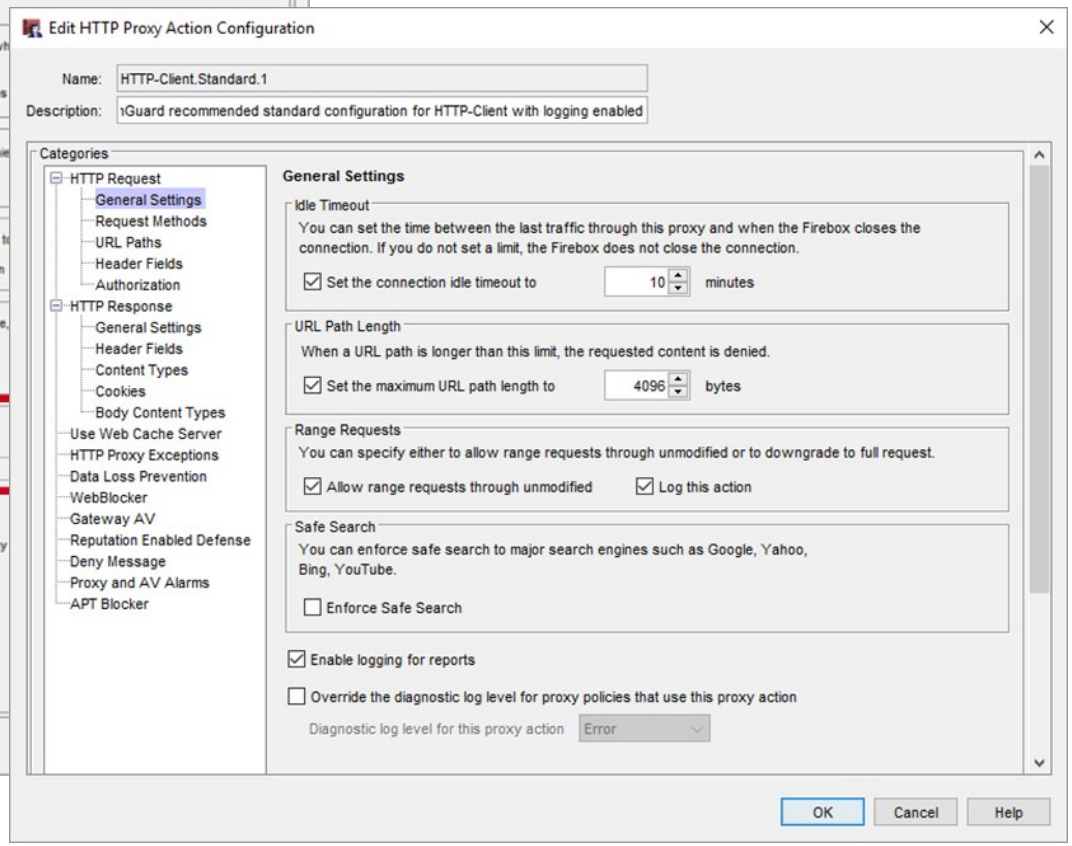
YouTube for Schools Removed

- Google has discontinued the YouTube for Schools service
- The **YouTube for Schools** option is removed from the HTTP proxy action General Settings

YouTube for Schools Removed



v12.0



v12.0.1

Wireless Enhancements

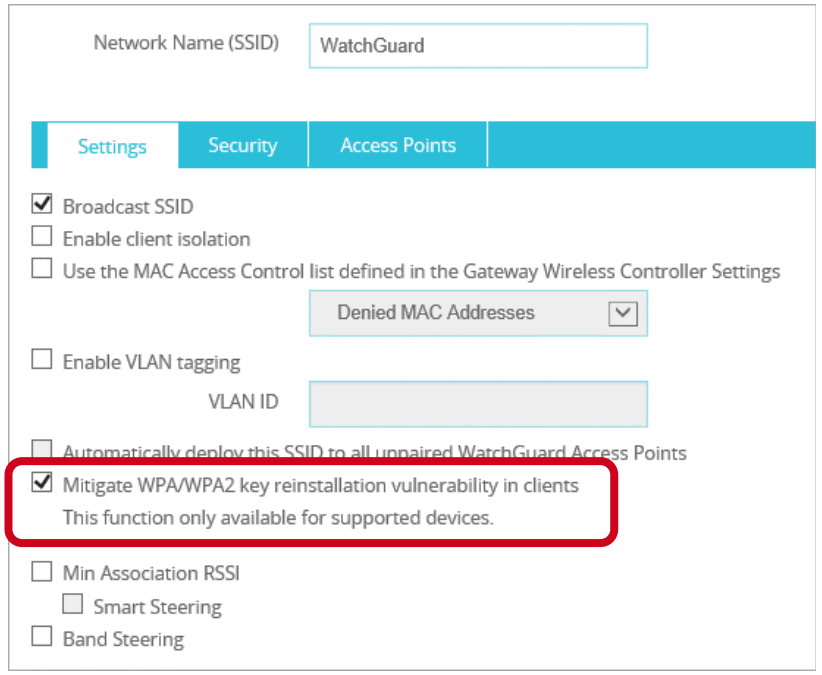
WatchGuard Training

KRACK WPA/WPA2 Vulnerability Mitigation

- WPA/WPA2 key reinstallation vulnerabilities
  - Addressed in XTM and Firebox Wireless devices:
    - XTM 25-W, 26-W, 33W
    - Firebox T10-W, T15-W, T30-W, T35-W, T50-W, T55-W
  - Addressed in AP firmware:
    - AP120, AP320, AP322, AP420: 8.3.0-657
    - AP100, AP102, AP200: 1.2.9.14
    - AP300: 2.0.0.9
  - Client vulnerabilities must be addressed on each client

KRACK WPA/WPA2 Vulnerability Mitigation

- Mitigate client WPA/WPA2 key reinstallation vulnerabilities with the Gateway Wireless Controller
- Blocks handshake messages that can potentially exploit clients and forces clients to reauthenticate
- Configured for each SSID
- AP120, AP320, AP322, AP420 support only



Gateway Wireless Controller Enhancements

- You now cannot select the deprecated and insecure TKIP option for the WPA2 only wireless security mode
  - Only AES is supported with WPA2
  - You can still select TKIP for WPA/WPA2 mixed mode for legacy support
- Fast Roaming is now disabled and not supported on AP300 for WPA/WPA2 vulnerability prevention
- The list of available channels in the Preferred Channel list only shows channels available to you in your region for your selected Frequency Band and Channel Mode

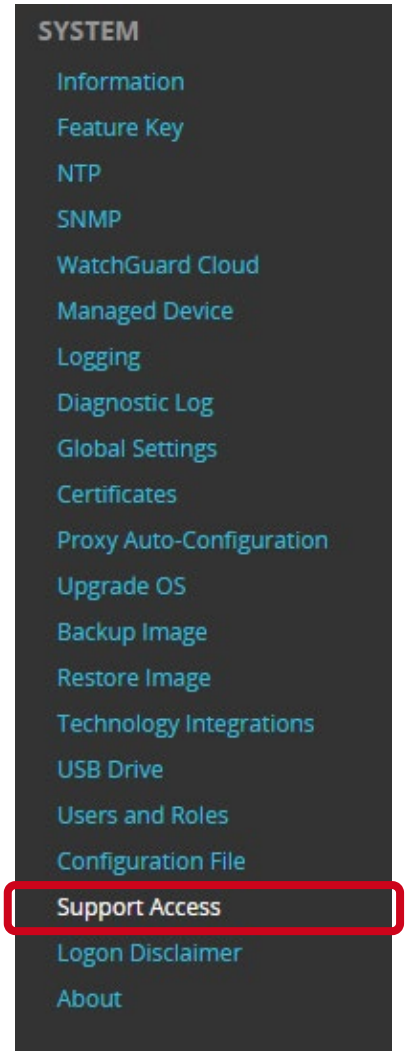
Other Enhancements

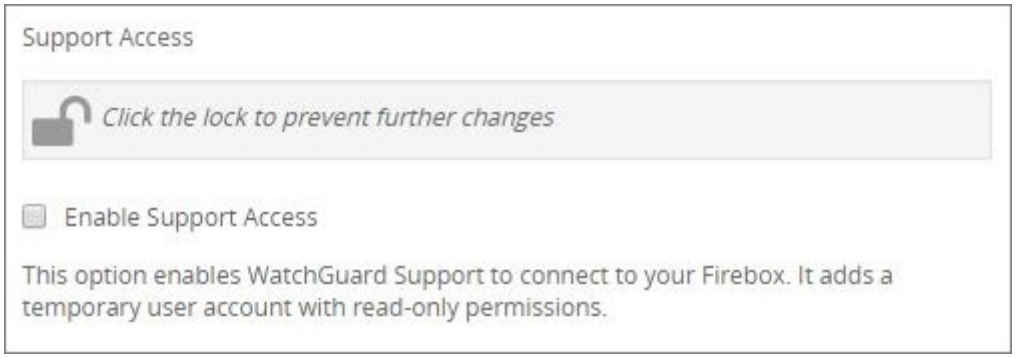
WatchGuard Training

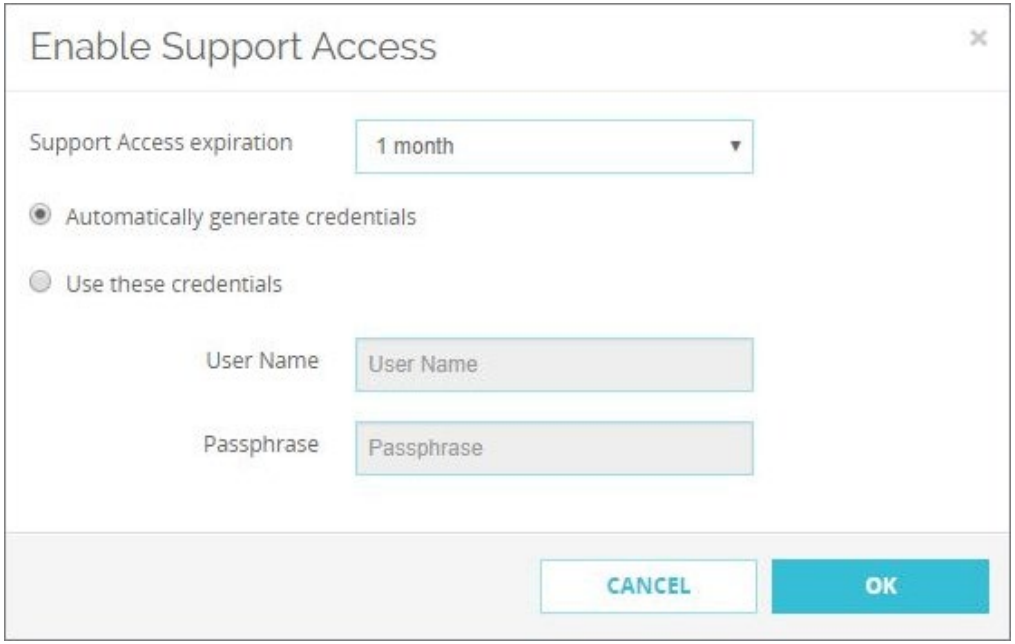
Support Access for Remote Login

- The **Enable Support Access** checkbox and options to define credentials and expiration have been added
- This option enables WatchGuard support to connect to the Firebox with read-only permission
- It adds a temporary hidden policy that allows connections to the Firebox from **ts.watchguard.com**
- It adds a temporary user account with read-only permissions
  - You can automatically generate credentials, or specify a user name and password
  - You can define the expiration for the temporary account
  - Options for support access account expiration: None, 3 months, 1 month, 1 week, and 1 day

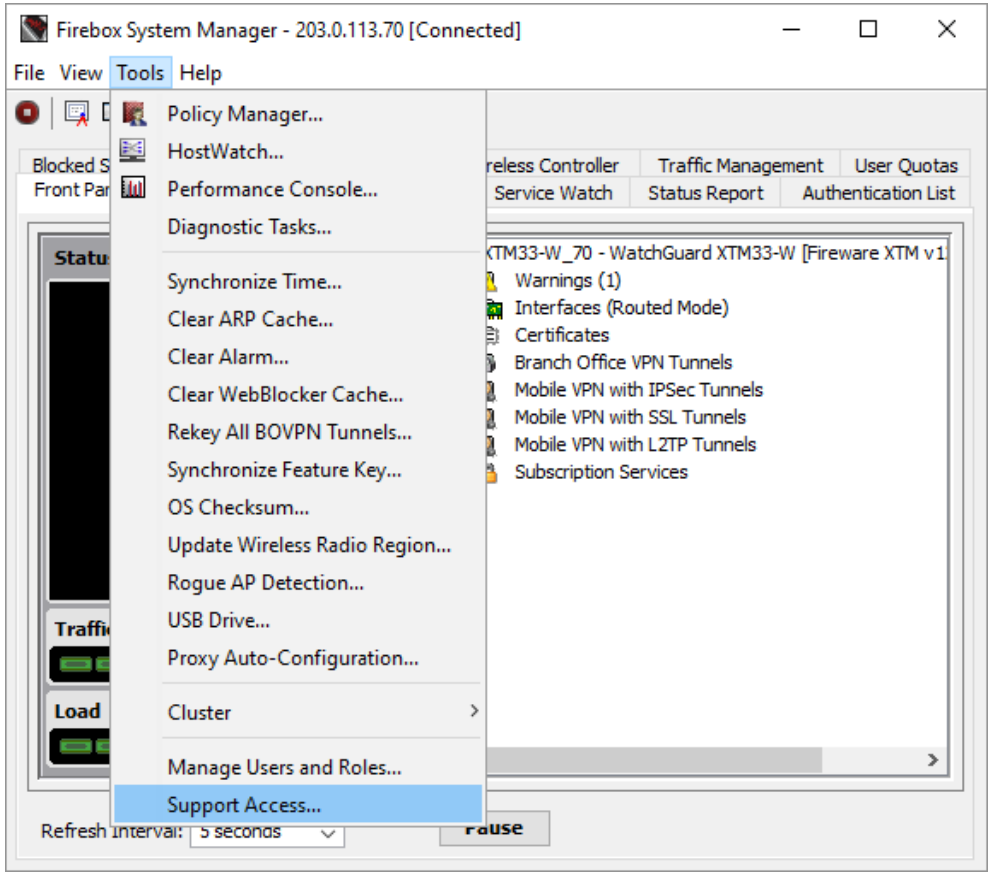
Support Access for Remote Login

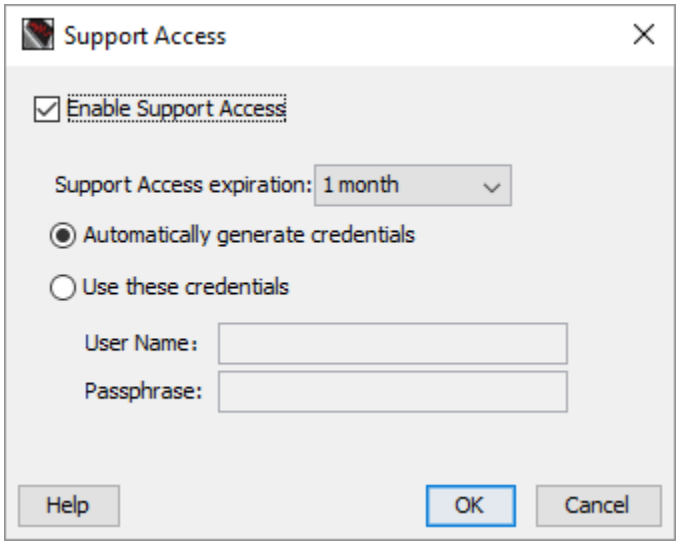






Support Access for Remote Login



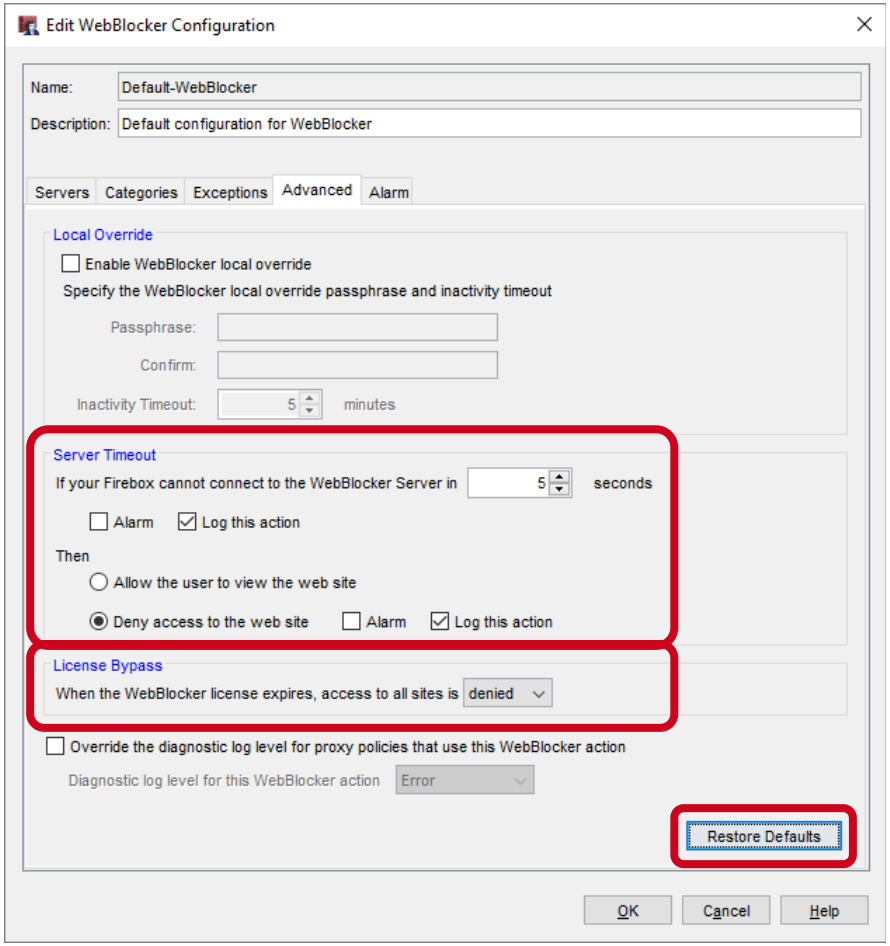


Setup Wizard Default Settings

- The default settings configured by the Web Setup Wizard and Quick Setup Wizard have been updated for improved security and usability
  - If Gateway AntiVirus is licensed, in the Default-HTTP-Client proxy action, the action for the **Windows EXE/DLL** Body Content Rule is set to **AV Scan** instead of **Deny**
  - In the APT Blocker configuration, the action for **High** level threats is set to **Drop** instead of **Block** regardless of whether APT Blocker is enabled
  - In the Intrusion Prevention configuration, the action for **Low** level threats is set to **Drop** instead of **Allow**, regardless of whether IPS is enabled

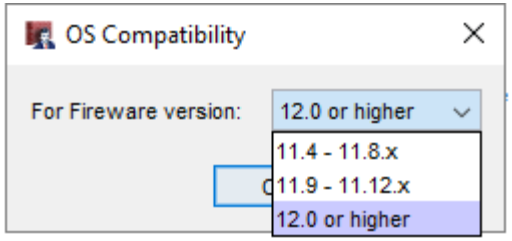
Setup Wizard Default Settings

- Changes in the **Default-WebBlocker** action:
  - **Server Timeout** denies access if the Firebox cannot connect to the WebBlocker Server
  - **License Bypass** denies access when the WebBlocker license expires
- To restore these default settings, click **Restore Defaults**



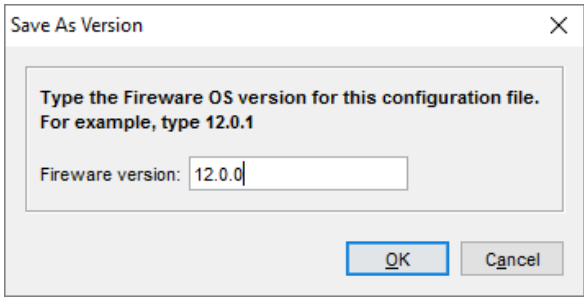
Policy Manager — Save As Version

- You can now use Policy Manager to save a configuration file for a specific version of Fireware
  - This makes it easier to create configuration files for RapidDeploy
  - The version you specify must be in the range of versions in the configured OS Compatibility setting
    - This is to make sure that the configuration settings are compatible with the selected Fireware version
- To see or change the OS Compatibility setting, from Policy Manager select **Setup > OS Compatibility**



Policy Manager — Save As Version

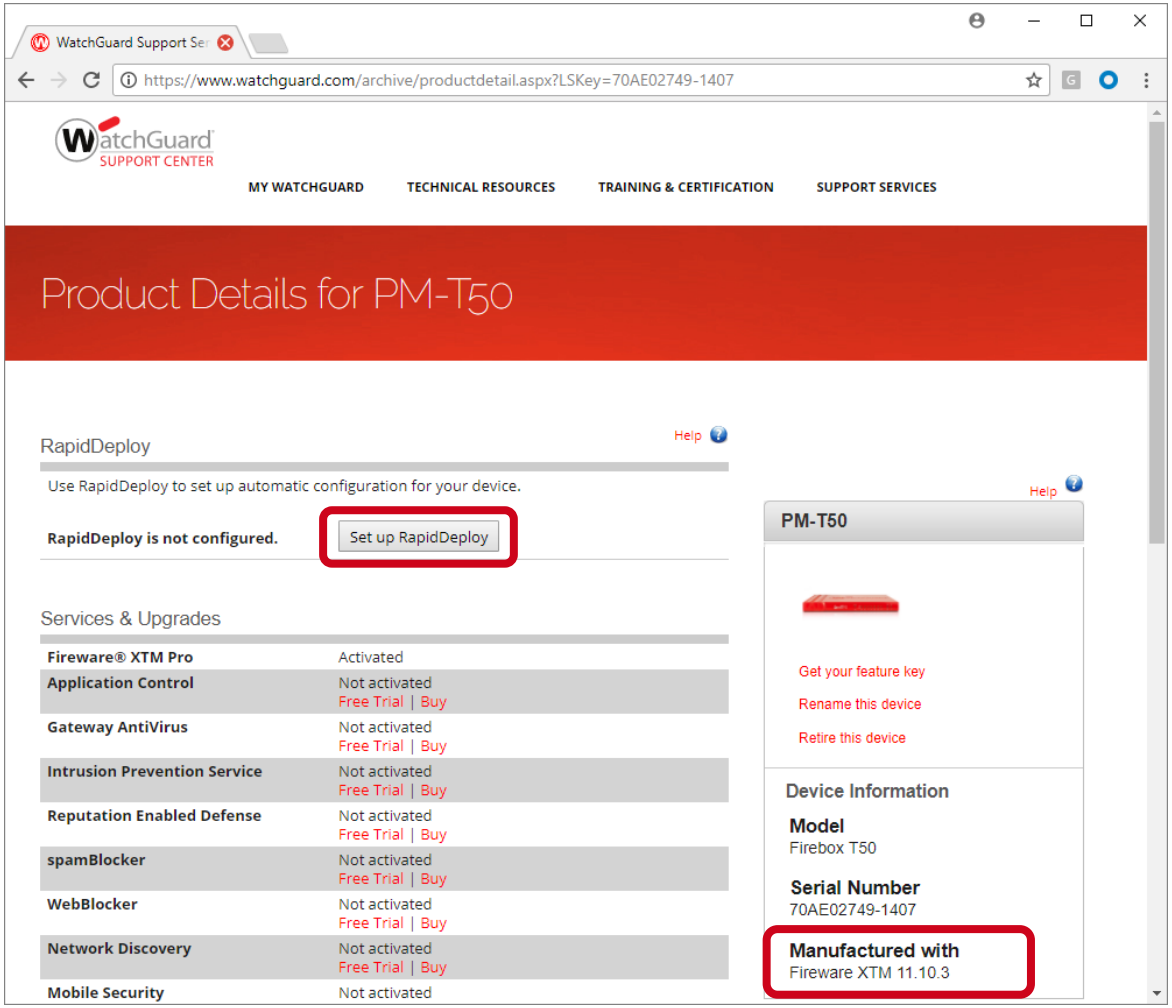
- To save a configuration file for a specific Fireware version, from Policy Manager:
  1. Select **File > Save > As Version**
  2. Type the Fireware Version
  3. Specify the file name and location
- If any feature in the configuration is not compatible with the version you specify, an error message appears with information about what you must change before you can save the configuration as the specified version



Policy Manager — Save As Version

- To create a configuration file that you can use for RapidDeploy for a new Firebox, save the configuration file as the version of Fireware the Firebox was manufactured with
- You can find the **Manufactured with** version on the **Product Details** page in the WatchGuard portal
- To upload the saved configuration file, click **Set up RapidDeploy**

Policy Manager — Save As Version



Import and Export Alias Members

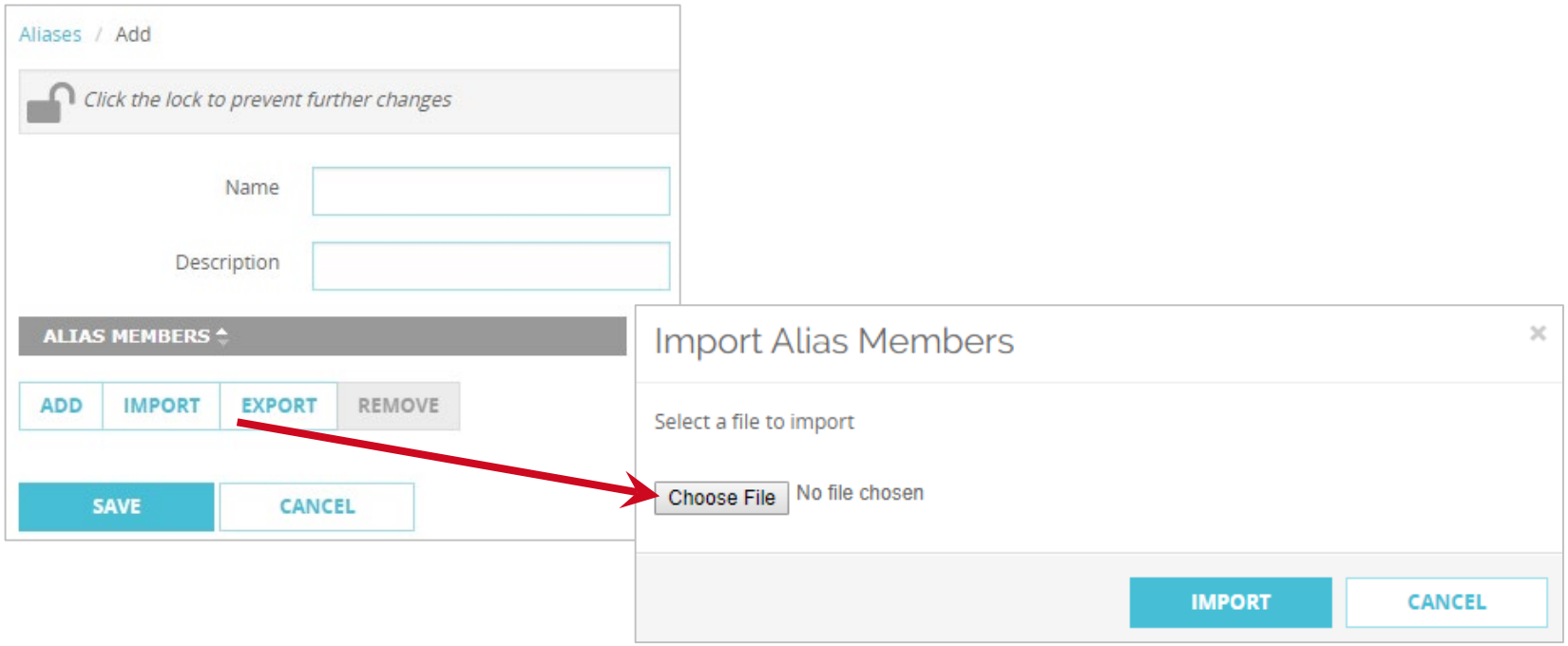
WatchGuard Training

Import and Export Alias Members

- In Fireware Web UI, you can now import or export a list that contains these alias member types:
  - IPv4 (hosts, networks, ranges, and wildcard IP addresses)
  - IPv6 (hosts, networks, ranges, and wildcard IP addresses)
  - FQDN
  - alias
  - fw-user
  - sslvpn-user
  - fw-group
  - sslvpn-group
  - device
- *This enhancement will be available in Policy Manager in Fireware v12.1*

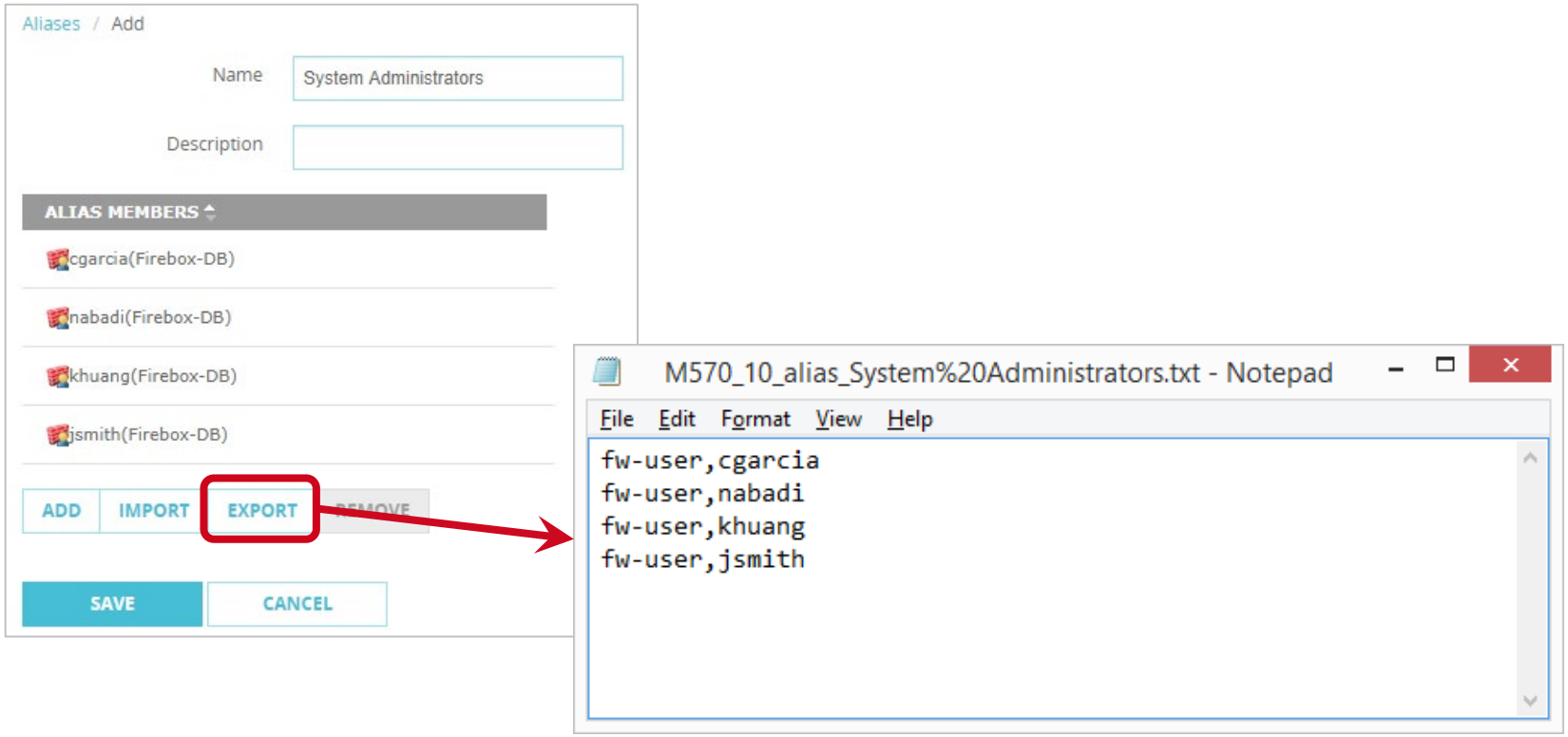
Import and Export Alias Members

- To import a list of alias members, from the **Add** alias page, click **Import** and select the file with the list of alias members



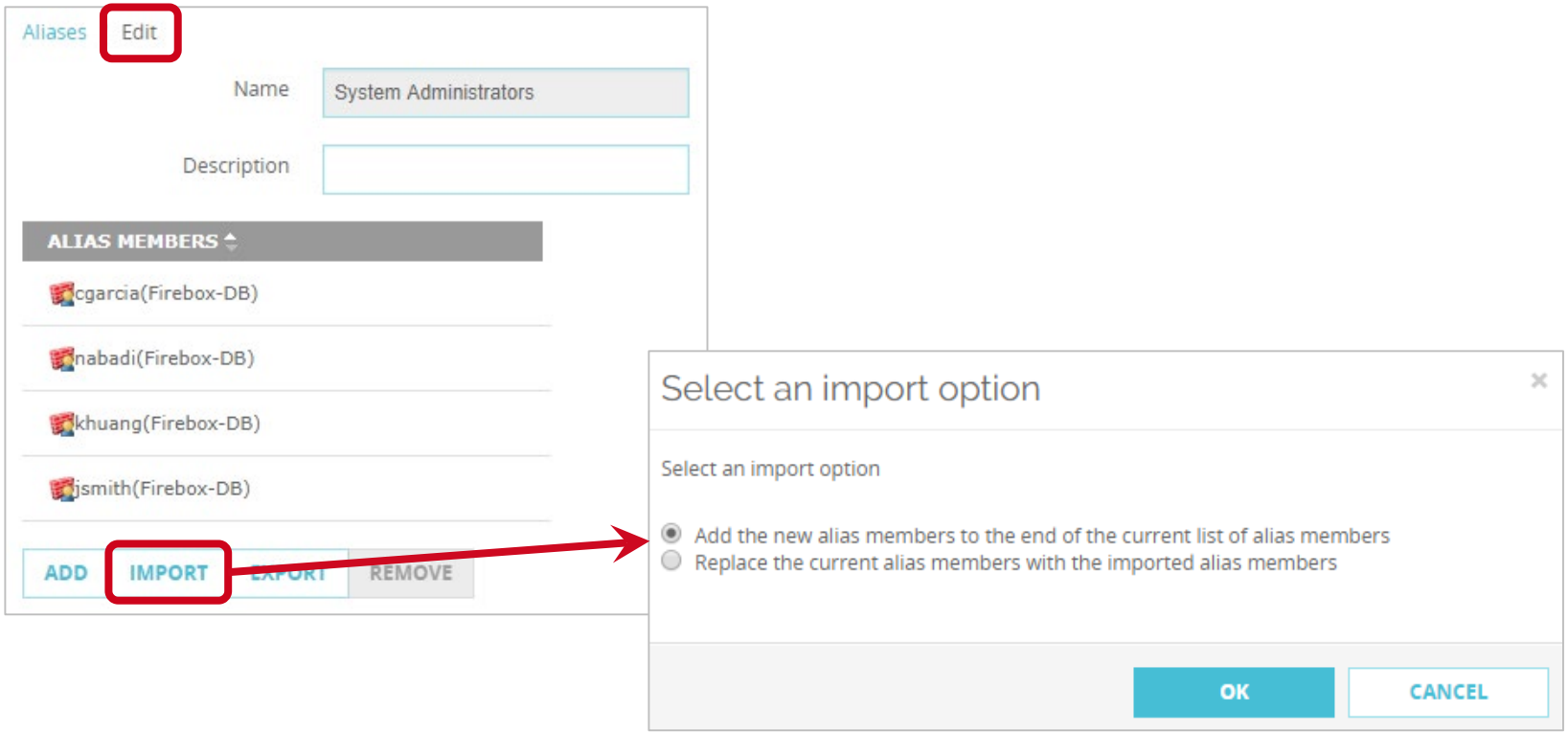
Import and Export Alias Members

- To export a list of alias members, from the **Add** alias page, click **Export**



Import and Export Alias Members

- If you select to edit an Alias and click **Import**, you must select whether to add to or replace the list of alias members



Thank You!

NOTHING GETS PAST RED.

WatchGuard Training