

# 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

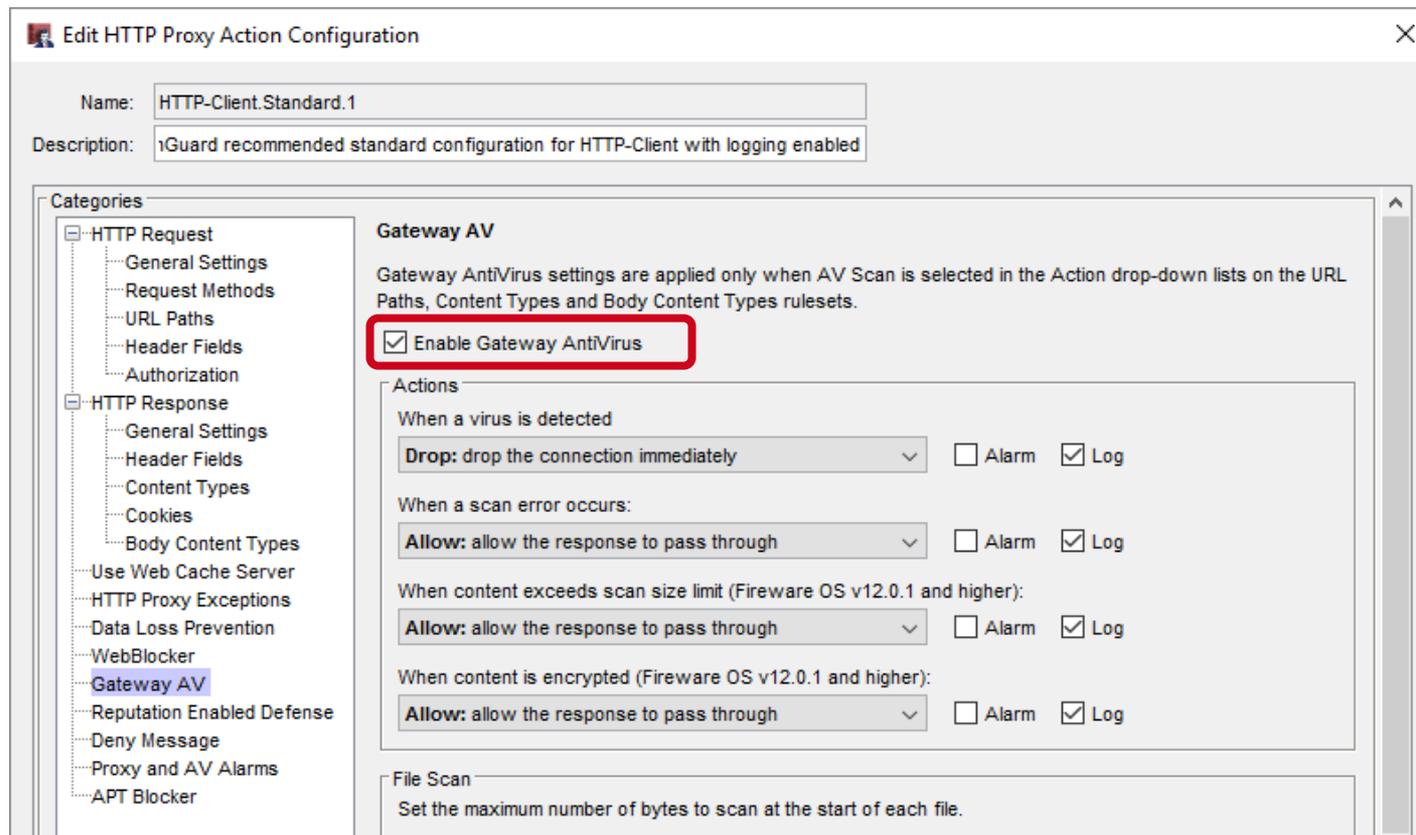




# Security Services Enhancements

# Enable Gateway AV Check Box Added

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



**Edit HTTP Proxy Action Configuration**

Name:

Description:

**Categories**

- HTTP Request
  - General Settings
  - Request Methods
  - URL Paths
  - Header Fields
  - Authorization
- HTTP Response
  - General Settings
  - Header Fields
  - Content Types
  - Cookies
  - Body Content Types
- Use Web Cache Server
- HTTP Proxy Exceptions
- Data Loss Prevention
- WebBlocker
- Gateway AV**
- Reputation Enabled Defense
- Deny Message
- Proxy and AV Alarms
- APT Blocker

**Gateway AV**

Gateway AntiVirus settings are applied only when AV Scan is selected in the Action drop-down lists on the URL Paths, Content Types and Body Content Types rulesets.

**Enable Gateway AntiVirus**

**Actions**

When a virus is detected  
  Alarm  Log

When a scan error occurs:  
  Alarm  Log

When content exceeds scan size limit (Fireware OS v12.0.1 and higher):  
  Alarm  Log

When content is encrypted (Fireware OS v12.0.1 and higher):  
  Alarm  Log

**File Scan**

Set the maximum number of bytes to scan at the start of each file.

# 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 AntiVirus Configuration of Policy: HTTP-proxy

Categories

- General
- HTTP Request
  - URL Paths
- HTTP Response
  - Content Types
  - Body Content Types

**General Gateway AntiVirus Settings**

Gateway AntiVirus settings are applied only when AV Scan is selected in the Action drop-down lists on the URL Paths, Content Types and Body Content Types rulesets.

Enable Gateway AntiVirus

Actions

When a virus is detected:  
Drop: drop the connection immediately  Alarm  Log

When a scan error occurs:  
Allow: allow the response to pass through  Alarm  Log

When content exceeds scan size limit (Fireware OS v12.0.1 and higher):  
Allow: allow the response to pass through  Alarm  Log  
Drop: drop the connection immediately  Alarm  Log  
Block: drop the connection and auto-block the source  Alarm  Log

Enable Gateway AntiVirus

Gateway AntiVirus Configuration

When a virus is detected Drop  Alarm  Log

When a scan error occurs Allow  Alarm  Log

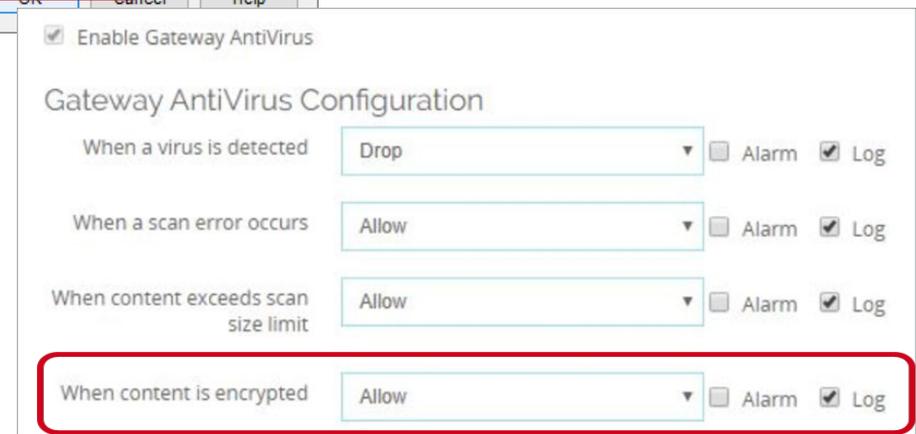
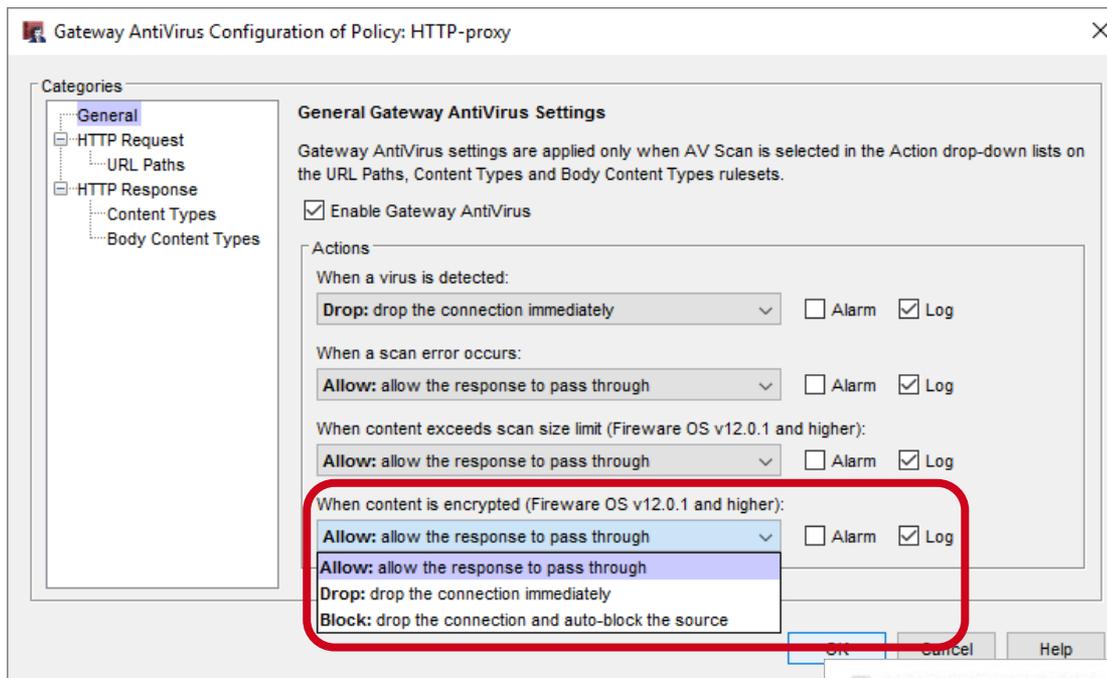
When content exceeds scan size limit Allow  Alarm  Log

When content is encrypted Allow  Alarm  Log

# 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



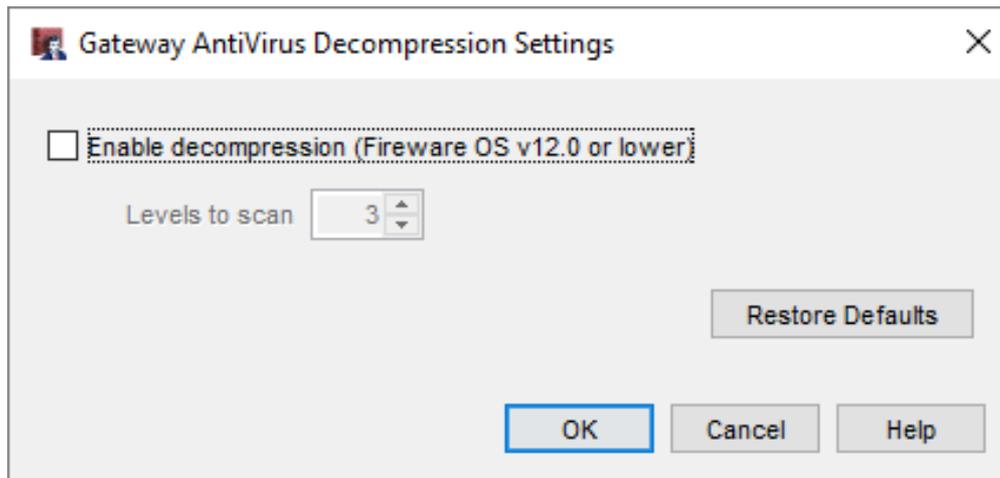
# Gateway AV Decompression Enabled

- 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 than 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

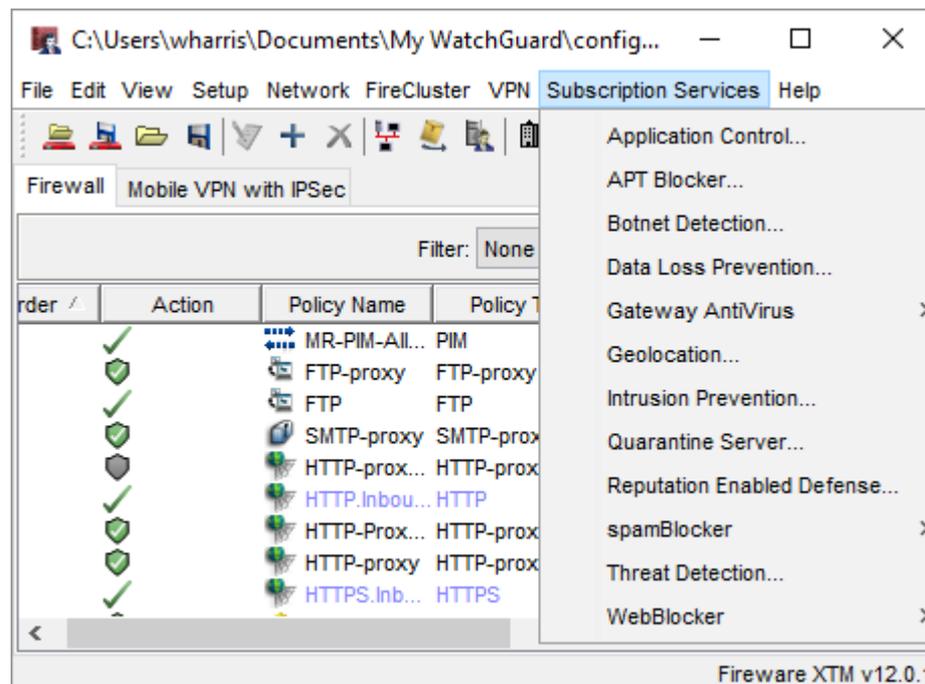
# Gateway AV Decompression Enabled

- 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

# 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**

The screenshot shows the 'Autotask' configuration page within the 'ConnectWise' section of the WatchGuard web UI. The page is titled 'Autotask' and features a blue header bar with 'ConnectWise' and 'Autotask' tabs. The main content area is white and contains several sections for configuration:

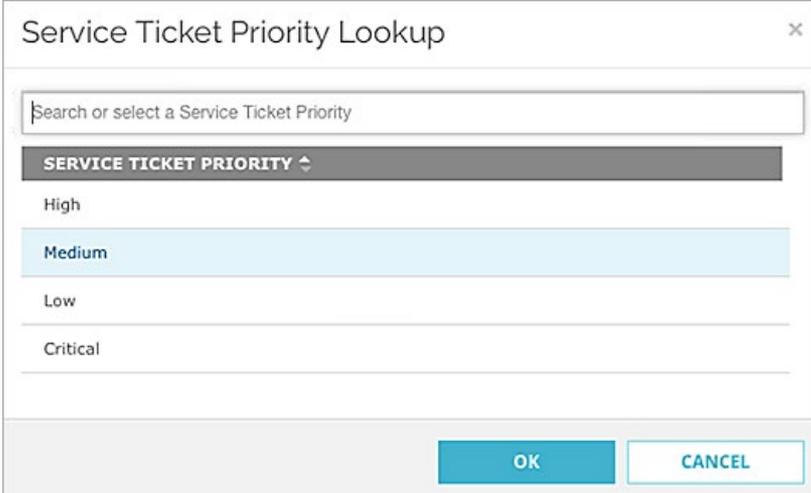
- Enable Autotask:** A checkbox labeled 'Enable Autotask' is checked.
- Login Credentials:** Two input fields are provided: 'Username' and 'Password'.
- Account:** A section titled 'Account' with the instruction 'You must associate the Firebox with an active Account.' It includes an 'Account' input field and a 'LOOKUP' button.
- Service Desk (Tickets):** A section titled 'Service Desk (Tickets)' with the instruction 'Priorities and Queues to use for tickets created by the Firebox.' It includes two rows: 'Priority' and 'Queue', each with a 'Default' input field and a 'LOOKUP' button.
- Product:** A section titled 'Product' with the instruction 'You must associate the Firebox with an active Product.' It includes a 'Product' input field and a 'LOOKUP' button.
- Configuration Item:** A section titled 'Configuration Item' with the instruction 'You may choose to use an existing Configuration Item. Otherwise, a new one will be created.' It includes a checkbox labeled 'Use existing Configuration Item' which is currently unchecked.

# 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**



The screenshot shows a dialog box titled "Service Ticket Priority Lookup" with a close button (X) in the top right corner. Below the title bar is a search input field containing the placeholder text "Search or select a Service Ticket Priority". Underneath the search field is a dropdown menu with the header "SERVICE TICKET PRIORITY" and a downward arrow. The dropdown menu is open, showing four options: "High", "Medium", "Low", and "Critical". The "Medium" option is currently selected and highlighted in light blue. At the bottom right of the dialog box, there are two buttons: "OK" and "CANCEL".

# 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 Autotask

Enable ConnectWise

Login Credentials

Site

Login Company

Public API Key

Private API Key

Company

You must associate the Firebox with an active Company.

Company ID  [LOOKUP](#)

Service Desk

Ticket Priorities and Service Boards to use for tickets created by the Firebox.

Ticket Priority  [LOOKUP](#)

Service Board  [LOOKUP](#)

Configuration

You may choose to use an existing Configuration. Otherwise, a new one will be created.

Use existing Configuration

[TEST SETTINGS](#)

# 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

The screenshot shows the configuration page for ConnectWise in the Autotask system. The page has a blue header with 'ConnectWise' and 'Autotask' tabs. Below the header, there is a checkbox for 'Enable ConnectWise' which is checked. The 'Login Credentials' section contains four input fields: 'Site', 'Login Company', 'Public API Key', and 'Private API Key'. The 'Company' section has a text input for 'Company ID' and a 'LOOKUP' button. The 'Service Desk' section has two dropdown menus: 'Ticket Priority' (set to 'Default') and 'Service Board' (set to 'Default'), each with a 'LOOKUP' button. The 'Service Board' dropdown and its 'LOOKUP' button are highlighted with a red rectangular box. The 'Configuration' section has a checkbox for 'Use existing Configuration' which is unchecked. At the bottom, there is a 'TEST SETTINGS' button.

# 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

The screenshot displays the WatchGuard ConnectWise configuration interface. The left sidebar shows the navigation menu with 'Setup Tables' selected. The main content area shows the configuration details for a specific question. The 'Value' column is highlighted with a red circle, showing a list of performance thresholds. The 'Disabled' option is selected, indicated by a red checkmark.

Configuration Type: WatchGuard Security Appliance  
 Mark as Inactive?

Value

Value	Default?	Inactive?
> 70% over 30 minutes	<input type="checkbox"/>	<input type="checkbox"/>
<b>Disabled</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
> 99% over 1 minute	<input type="checkbox"/>	<input type="checkbox"/>
> 99% over 5 minutes	<input type="checkbox"/>	<input type="checkbox"/>
> 99% over 10 minutes	<input type="checkbox"/>	<input type="checkbox"/>
> 99% over 30 minutes	<input type="checkbox"/>	<input type="checkbox"/>
> 90% over 5 minutes	<input type="checkbox"/>	<input type="checkbox"/>
> 90% over 10 minutes	<input type="checkbox"/>	<input type="checkbox"/>
> 90% over 30 minutes	<input type="checkbox"/>	<input type="checkbox"/>
> 80% over 5 minutes	<input type="checkbox"/>	<input type="checkbox"/>
> 80% over 10 minutes	<input type="checkbox"/>	<input type="checkbox"/>
> 80% over 30 minutes	<input type="checkbox"/>	<input type="checkbox"/>

Answer Cloning  
 Clone from:   
 Clone these answers

# Technology Integrations and Config Report

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

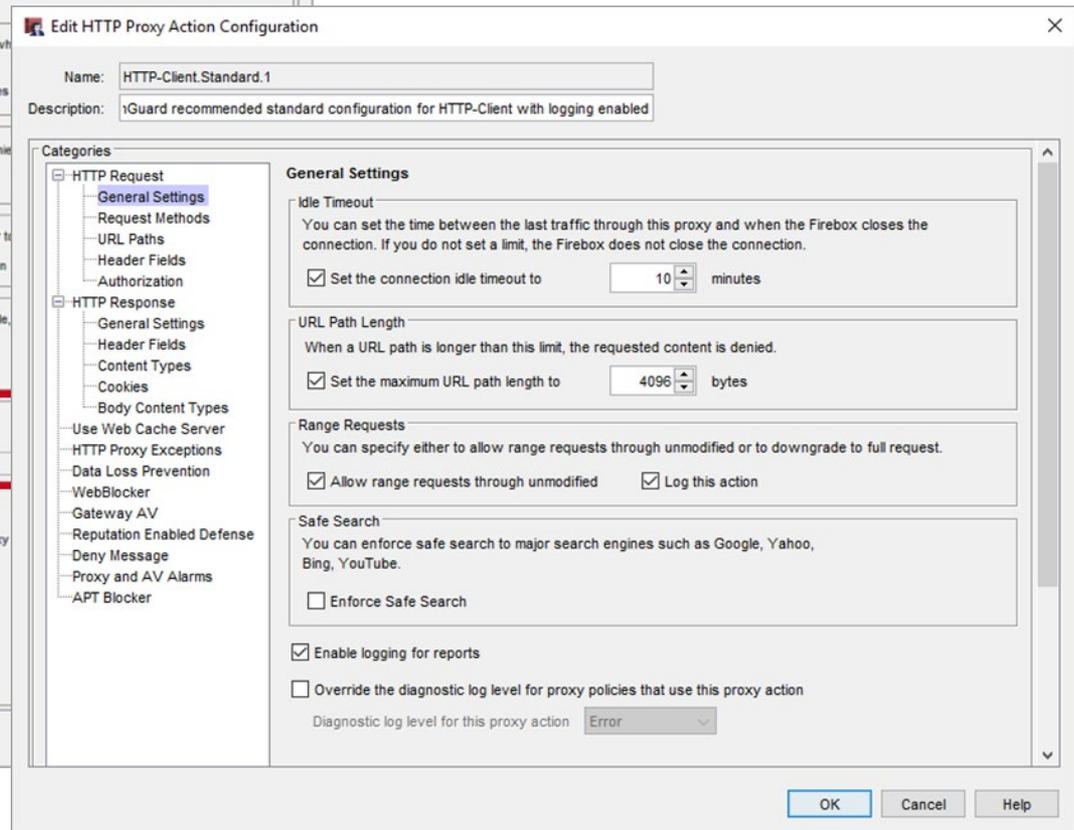
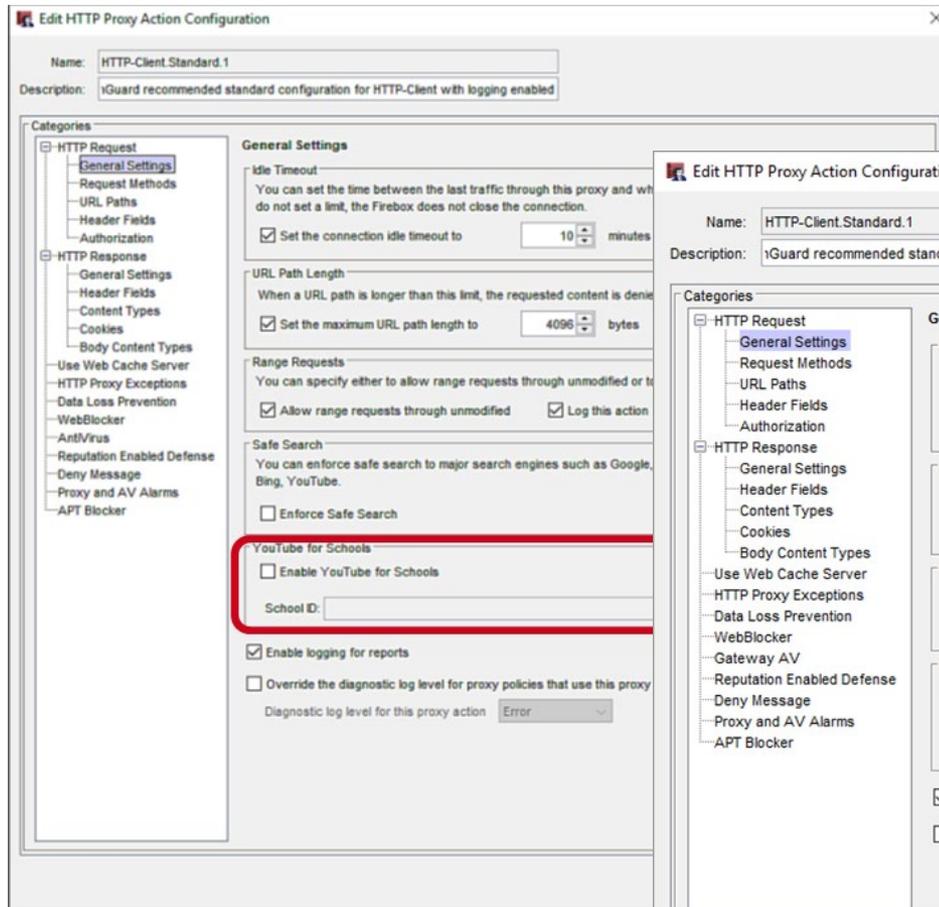


# Policy Enhancements

# 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





# Wireless Enhancements

# 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

Network Name (SSID) WatchGuard

Settings Security Access Points

Broadcast SSID

Enable client isolation

Use the MAC Access Control list defined in the Gateway Wireless Controller Settings

Denied MAC Addresses

Enable VLAN tagging

VLAN ID

Automatically deploy this SSID to all unpaired WatchGuard Access Points

Mitigate WPA/WPA2 key reinstallation vulnerability in clients  
This function only available for supported devices.

Min Association RSSI

Smart Steering

Band Steering

# 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

# 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

**SYSTEM**

- Information
- Feature Key
- NTP
- SNMP
- WatchGuard Cloud
- Managed Device
- Logging
- Diagnostic Log
- Global Settings
- Certificates
- Proxy Auto-Configuration
- Upgrade OS
- Backup Image
- Restore Image
- Technology Integrations
- USB Drive
- Users and Roles
- Configuration File
- Support Access**
- Logon Disclaimer
- About

## Support Access



*Click the lock to prevent further changes*

Enable Support Access

This option enables WatchGuard Support to connect to your Firebox. It adds a temporary user account with read-only permissions.

## Enable Support Access

Support Access expiration

1 month

Automatically generate credentials

Use these credentials

User Name

User Name

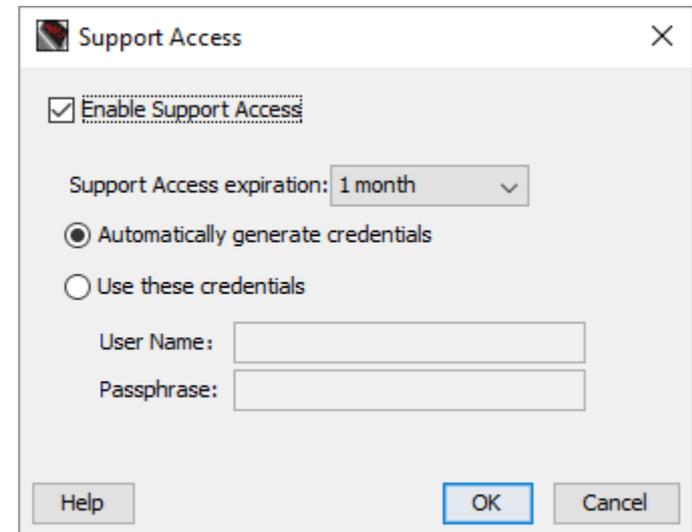
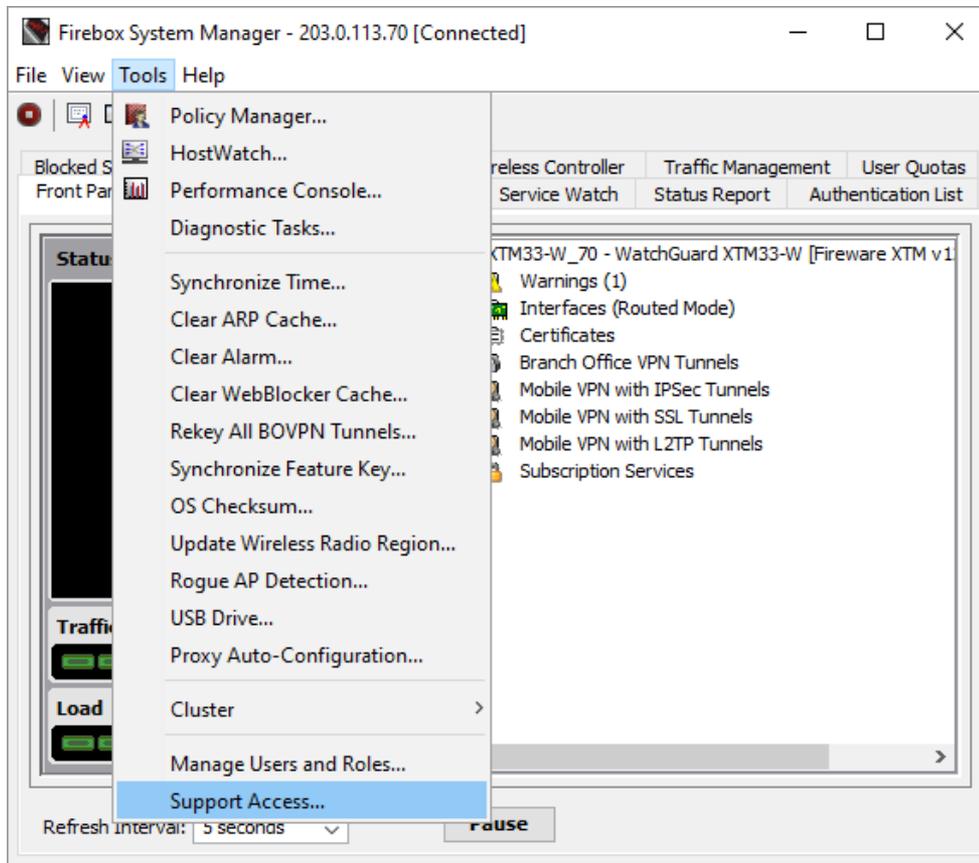
Passphrase

Passphrase

CANCEL

OK

# 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**

**Edit WebBlocker Configuration**

Name: Default-WebBlocker  
Description: Default configuration for WebBlocker

Servers Categories Exceptions **Advanced** Alarm

**Local Override**

Enable WebBlocker local override  
Specify the WebBlocker local override passphrase and inactivity timeout

Passphrase:   
Confirm:   
Inactivity Timeout: 5 minutes

**Server Timeout**

If your Firebox cannot connect to the WebBlocker Server in 5 seconds

Alarm  Log this action

Then

Allow the user to view the web site  
 Deny access to the web site  Alarm  Log this action

**License Bypass**

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

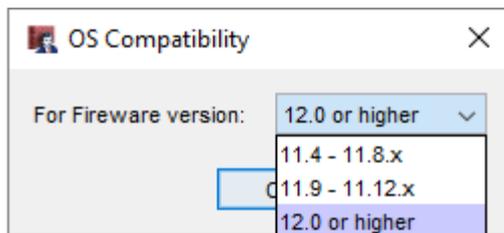
Override the diagnostic log level for proxy policies that use this WebBlocker action  
Diagnostic log level for this WebBlocker action: Error

**Restore Defaults**

OK Cancel Help

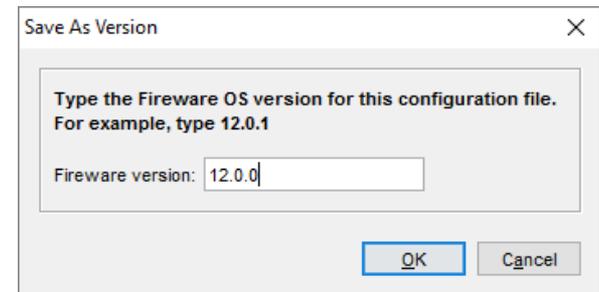
# Policy Manager — Save As Version

- 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

WatchGuard Support Center

MY WATCHGUARD TECHNICAL RESOURCES TRAINING & CERTIFICATION SUPPORT SERVICES

## Product Details for PM-T50

RapidDeploy [Help](#)

Use RapidDeploy to set up automatic configuration for your device.

RapidDeploy is not configured. [Set up RapidDeploy](#)

Services & Upgrades

Fireware® XTM Pro	Activated
Application Control	Not activated <a href="#">Free Trial</a>   <a href="#">Buy</a>
Gateway AntiVirus	Not activated <a href="#">Free Trial</a>   <a href="#">Buy</a>
Intrusion Prevention Service	Not activated <a href="#">Free Trial</a>   <a href="#">Buy</a>
Reputation Enabled Defense	Not activated <a href="#">Free Trial</a>   <a href="#">Buy</a>
spamBlocker	Not activated <a href="#">Free Trial</a>   <a href="#">Buy</a>
WebBlocker	Not activated <a href="#">Free Trial</a>   <a href="#">Buy</a>
Network Discovery	Not activated <a href="#">Free Trial</a>   <a href="#">Buy</a>
Mobile Security	Not activated

PM-T50 [Help](#)



[Get your feature key](#)

[Rename this device](#)

[Retire this device](#)

Device Information

**Model**  
Firebox T50

**Serial Number**  
70AE02749-1407

**Manufactured with**  
Fireware XTM 11.10.3



# Import and Export Alias Members

# 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

The screenshot displays the 'Aliases / Add' page in the WatchGuard interface. At the top, there is a breadcrumb 'Aliases / Add' and a lock icon with the text 'Click the lock to prevent further changes'. Below this are input fields for 'Name' and 'Description'. A section titled 'ALIAS MEMBERS' contains four buttons: 'ADD', 'IMPORT', 'EXPORT', and 'REMOVE'. At the bottom of this section are 'SAVE' and 'CANCEL' buttons. A red arrow points from the 'IMPORT' button to a dialog box titled 'Import Alias Members'. The dialog box has a close button (X) in the top right corner. It contains the text 'Select a file to import' and a file selection area with a 'Choose File' button and the text 'No file chosen'. At the bottom of the dialog box are 'IMPORT' and 'CANCEL' buttons.

# Import and Export Alias Members

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

Aliases / Add

Name

Description

**ALIAS MEMBERS** ↑

-  cgarcia(Firebox-DB)
-  nabadi(Firebox-DB)
-  khuang(Firebox-DB)
-  jsmith(Firebox-DB)

M570\_10\_alias\_System%20Administrators.txt - Notepad

File Edit Format View Help

```
fw-user,cgarcia
fw-user,nabadi
fw-user,khuang
fw-user,jsmith
```

# 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

The image shows a screenshot of the WatchGuard interface. On the left, the 'Aliases' section is open, and the 'Edit' button is highlighted with a red box. The 'Name' field contains 'System Administrators' and the 'Description' field is empty. Below the fields is a section titled 'ALIAS MEMBERS' with a list of members: 'cgarcia(Firebox-DB)', 'nabadi(Firebox-DB)', 'khuang(Firebox-DB)', and 'jsmith(Firebox-DB)'. At the bottom of this section, the 'IMPORT' button is highlighted with a red box, and a red arrow points from it to the 'Select an import option' dialog on the right.

The 'Select an import option' dialog has a title bar with a close button (X). The main content area is titled 'Select an import option' and contains two radio button options:

- Add the new alias members to the end of the current list of alias members
- Replace the current alias members with the imported alias members

At the bottom of the dialog, there are two buttons: 'OK' and 'CANCEL'.



# Thank You!

***NOTHING GETS  
PAST RED.***



**WatchGuard Training**

Copyright ©2017 WatchGuard Technologies, Inc. All Rights Reserved