



Fireware

WatchMode Configuration Guide

About this Configuration Guide

The *Fireware WatchMode Configuration Guide* provides detailed information about how to install a WatchMode device in your customer's network. This enables you to gather information about the traffic in their networks and provide them with critical information about their network usage and possible threats to their network security.

More information about Fireware Web UI, WatchGuard System Manager, and Fireware OS is available in the *Fireware Help* on the WatchGuard web site at:

<http://www.watchguard.com/help/documentation/>.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 1/12/2023

Copyright, Trademark, and Patent Information

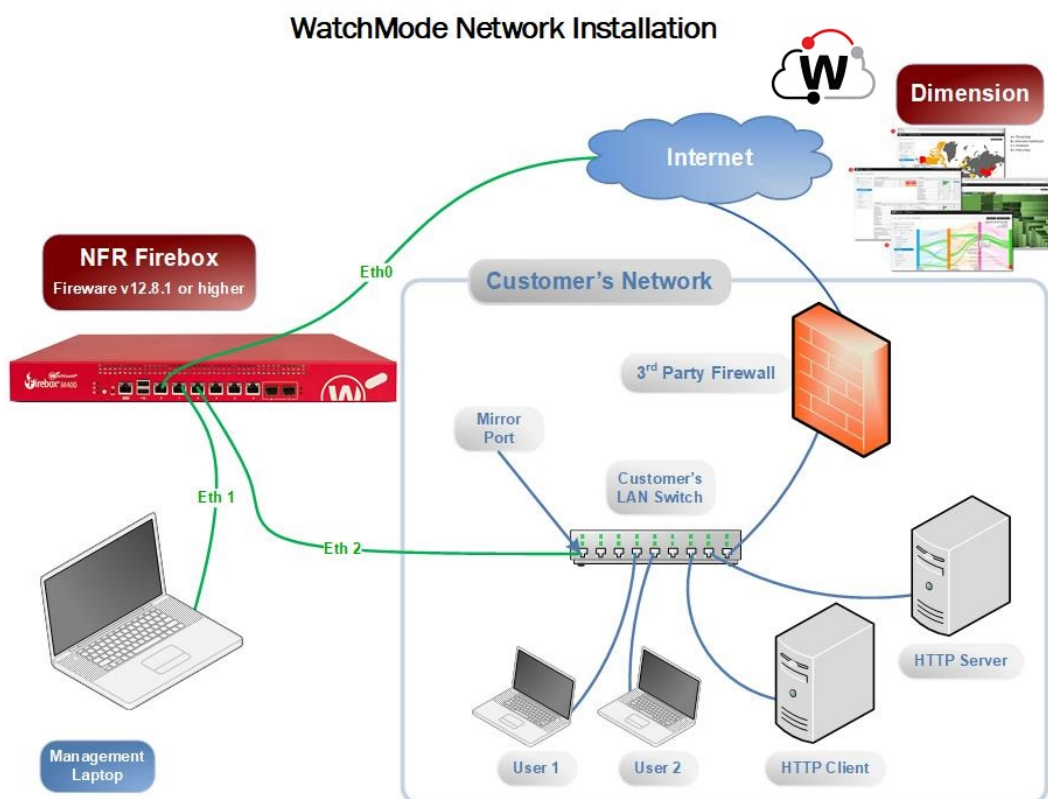
Copyright © 1998-2023 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at: <http://www.watchguard.com/help/documentation/>.

About WatchMode

WatchMode is a tool you can use to show your customers the indispensable value that a WatchGuard Firebox can add to their network security solution. When configured in WatchMode (an audit-only mode), the Firebox gathers information about network activity and sends log messages to WatchGuard Cloud or a WatchGuard Dimension Server for visibility and reporting.

To use WatchMode, enable WatchMode on the Firebox and install the Firebox in your customer's network behind a third-party device (a switch, tap device, or packet broker) that has a mirror port. The Firebox receives a mirror of the network traffic sent by the third-party device, and generates log messages with information about network activity. After the Firebox sends the log messages to WatchGuard Cloud or a WatchGuard Dimension Server, you can generate reports to demonstrate how the WatchGuard Firebox can provide superior security, as well as unparalleled, detailed visibility into the activity on their network.



With WatchMode enabled, the Firebox connects to the WebBlocker database over HTTP for URL categorization lookups. The Firebox reviews the traffic on your customer's network against the URL category information and provides information about what web sites users on your customer's network are visiting that could be blocked by the Firebox. The Firebox also connects to other WatchGuard servers for other security service updates.

To use WatchMode to show your customers the power of the WatchGuard Firewall solution you must:

1. Enable WatchMode on the Firebox and configure the device to send log messages to WatchGuard Cloud or an existing instance of Dimension.
2. Install the Firebox in your customer's network.
3. Make any necessary changes to the Firebox configuration.
4. Schedule and run reports of your customer's network traffic.
5. Present the reports to your customer.

Hardware, Software, and License Requirements

WatchMode is supported on these Fireboxes:

- Rack-mountable NFR Fireboxes (M Series)
- T70, T80, and T85 NFR Fireboxes



WatchMode is not supported on Firebox M440

To set up WatchMode in your customer's network, you must have:

- Firewall v12.8.1 or higher installed on the Firebox
- An NFR Firebox feature key that includes WatchMode and these subscription services:
 - WebBlocker
 - Gateway AV
 - IntelligentAV
 - Intrusion Prevention Service
 - Application Control
 - APT Blocker
- WatchGuard Cloud account or an instance of WatchGuard Dimension
- A management computer with WatchGuard System Manager v12.8.1 or higher installed
After you enable WatchMode, you can use Fireware Web UI or WatchGuard System Manager to manage and monitor the device.
- One Ethernet cable to connect Eth0 on the Firebox to the customer's network for Internet access
- One Ethernet cable to connect Eth1 on the Firebox to the laptop
- One Ethernet cable to connect Eth2 on the Firebox to the TAP port on the third-party switch (or TAP device)

About WatchMode on the Firebox T70

The Firebox T70 in WatchMode can handle mirrored traffic for 100 HTTP, HTTPS, or SMTP connections per second. When you choose which Firebox model to use with WatchMode, consider the expected volume of network connections.

Network Requirements

For WatchMode to work well, the firewall between the Firebox and the Internet must allow these ports:

- UDP port 53
- TCP port 80
- TCP port 443
- UDP port 10108

You must also connect the Firebox to a switch that is capable of port mirroring.

For security service updates to work, the network configuration must meet these requirements:

- The external network connected to Eth0 must not be on the same subnet as the Eth2 (TAP network).

Known Issues and Limitations

WatchMode has these known issues and limitations:

- WatchMode is not supported on Firebox M440.
- WatchMode supports only one TAP interface.
- The FTP proxy policy does not work in WatchMode.
- The SIP and H.323 Application Layer Gateway components do not work in WatchMode.
- The IMAP proxy is not supported with WatchMode.

Enable WatchMode on Your Firebox

Before you can enable WatchMode on your Firebox, you must have Fireware v12.8.1 or higher installed on your Firebox and a feature key that includes WatchMode.

After you install Fireware v12.8.1 or higher and apply the feature key to the device, you can enable WatchMode and configure the device to send log messages to WatchGuard Cloud or an instance of Dimension that you have already installed and configured.

- For more information on how to set up Dimension, go to [Setup & Administer Dimension](#).
- For information on how to add a local-managed Firebox to WatchGuard Cloud, go to [Add a Locally-Managed Firebox to WatchGuard Cloud](#).

Connect to the Firebox

Before you can enable WatchMode in the Firebox configuration, you must physically connect the Firebox to a computer, such as your laptop. After your laptop is connected to the Firebox, you can connect to Fireware Web UI or use Firebox System Manager to enable WatchMode and configure the Firebox to send log messages to WatchGuard Cloud or Dimension.

If your Firebox is in factory-default mode, the IP address of the Eth1 interface is *10.0.1.1*, the *Status* user account passphrase is *readonly*, and the *Admin* user account passphrase is *readwrite*.

To connect to the Firebox:

1. Power on the Firebox.
2. To make a management connection to the Firebox, connect your laptop to the Eth1 interface on the Firebox.
3. To enable the Firebox to monitor traffic on your customer's network, connect the Eth2 interface to the switch in your customer's network.
For more information about the network connections to your device and the customer's network, see [Network Installation — Mirror Customer Traffic](#).
4. To enable the Firebox to connect to the Internet, connect the Eth0 interface port on the Firebox to the switch in your customer's network. Make sure that the network you connect to Eth0 is on a separate subnet from the network you want to monitor.
5. If you use Dimension, ping the IP address of your instance of Dimension to make sure your laptop can connect to it.
6. Connect to Fireware Web UI for your Firebox and log in with a user account that has Device Administrator privileges (*admin*):
`https://<device-IP-address>:8080`.
If your device uses default network settings, connect to it at `https://10.0.1.1:8080`.
7. If required, use the Web Setup Wizard to set up the Firebox with a basic configuration.
8. (Optional) Start WatchGuard System Manager and connect to the Firebox.

You can now use Fireware Web UI to enable WatchMode and make any configuration changes to the configuration. You can also start Firebox System Manager to monitor the activity on the device in real-time. If you must make changes to the network configuration, make sure that you modify only the Eth0 interface.

Upgrade the Firebox

If your Firebox does not already run Fireware v12.8.1 or higher, you must upgrade the Firebox before you can enable the latest update for WatchMode.

1. Connect your laptop to the Eth1 interface on the Firebox.
2. On your laptop, connect to Fireware Web UI for your Firebox.
If your device is in factory-default mode, the IP address is 10.0.1.1 and the Admin user account passphrase is readwrite.
If your device is not in factory-default mode, use the current IP address and passphrase of the Firebox to connect to it with Fireware Web UI.
3. Select **System > Upgrade OS** to start the upgrade process.
The Upgrade dialog box appears.
4. Select the Fireware v12.8.1 or higher upgrade file for your Firebox model.
5. Complete the upgrade process to install the OS on your device.

After you have upgraded your Firebox to the correct Fireware OS build, you can connect to the device and enable WatchMode.

Enable WatchMode and Configure Logging

To enable WatchMode on your Firebox, you must have an NFR Firebox feature key installed on your device that includes WatchMode and these subscription services:

- WebBlocker
- Gateway AV
- IntelligentAV
- Intrusion Prevention Service
- Application Control
- APT Blocker

When the feature key on your Firebox includes these items, you can enable WatchMode and configure your device to send log messages to WatchGuard Cloud or an existing Dimension Log Server.

Verify WatchMode in the Feature Key

To verify your feature key includes WatchMode:

1. Open a web browser and connect to Fireware Web UI for your device at `https://<IP address of your device>`.
2. Select **System > Feature Key**.
The Feature Key page appears.
3. Scroll down to the **Features** section and find the *WatchMode* item in the **Features** list.
4. If *WatchMode* does not appear in the **Features** list, click **Update Feature Key** and add a feature key that includes WatchMode.
5. Save the changes to your device.

Enable WatchMode on the Firebox

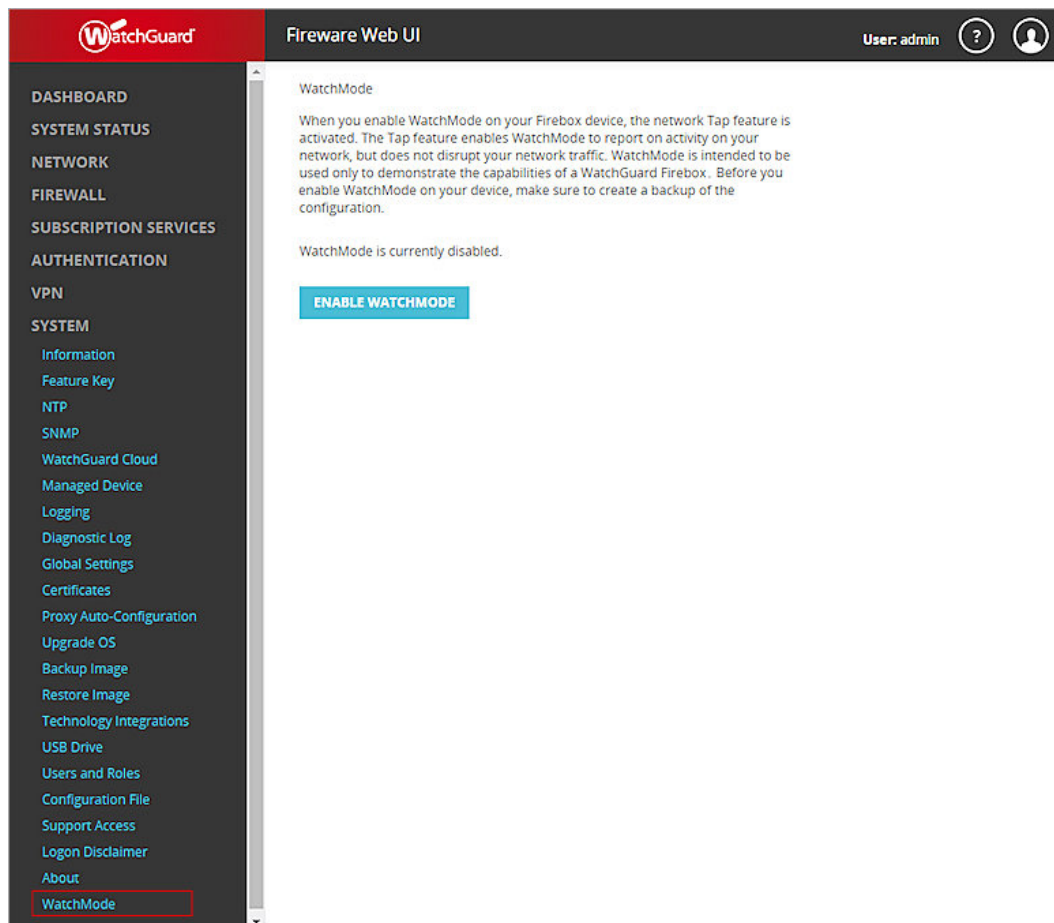
Before you enable WatchMode, you might want to create a backup image.

To create a backup file:

1. Select **System > Backup Image**.
The Backup and Restore Image page appears.
2. Click **Create Backup Image**.
3. Type a name for the backup file.
4. Click **Save**.
The backup image is saved on the Firebox.

To enable WatchMode on your Firebox, from Fireware Web UI:

1. Select **System > WatchMode**.
The WatchMode page appears.



2. Click **Enable WatchMode**.
A confirmation message appears.
3. Click **Yes**.
WatchMode is enabled on the device and the device reboots. When the device reboots, the interface settings are changed and you cannot connect to the device at the same IP address.

4. Connect to Fireware Web UI on port 8080 over one of these interfaces:
 - Eth0 — DHCP assigned address (if DHCP is unavailable on the customer's network, assign a static IP address)
 - Eth1 — 10.199.1.1

When WatchMode is enabled on your Firebox, a default WatchMode configuration is automatically created for the device.

To verify WatchMode is enabled on the device, use one or more of these methods:

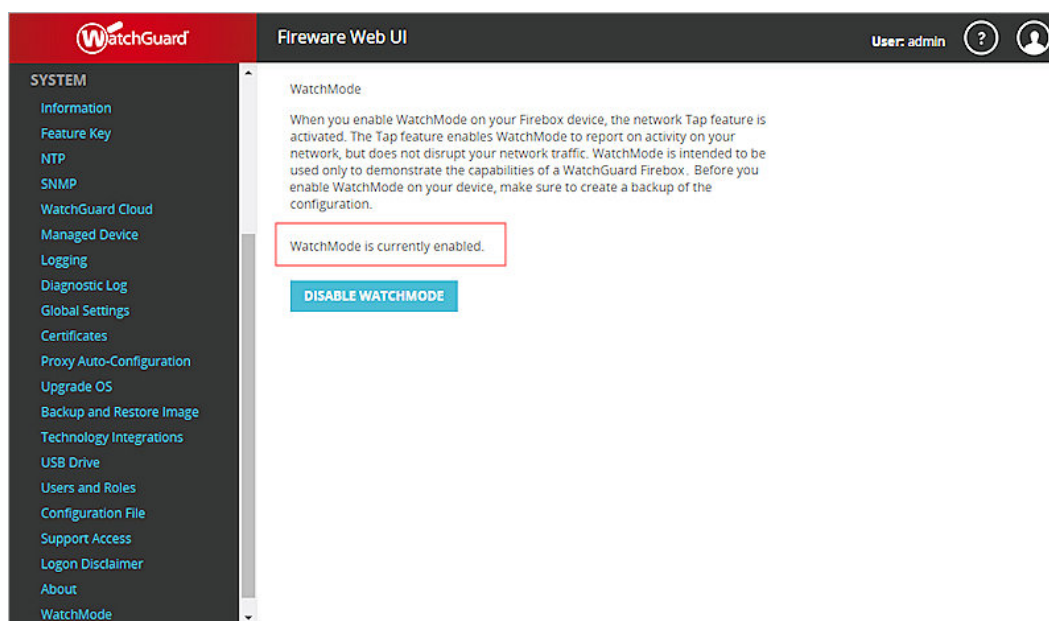
- Select **Dashboard > Front Panel** and verify that the System **Name** is the Firebox model number with *-WatchMode* appended.

The screenshot shows the Fireware Web UI interface. The left sidebar contains navigation links: DASHBOARD, Front Panel, Subscription Services, FireWatch, Interfaces, Traffic Monitor, Gateway Wireless Controller, Geolocation, Mobile Security, Network Discovery, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area is titled 'Front Panel' and displays 'Top Clients' and 'Top Destinations' tables. On the right, the 'System' section is highlighted with a red box, showing the following information:

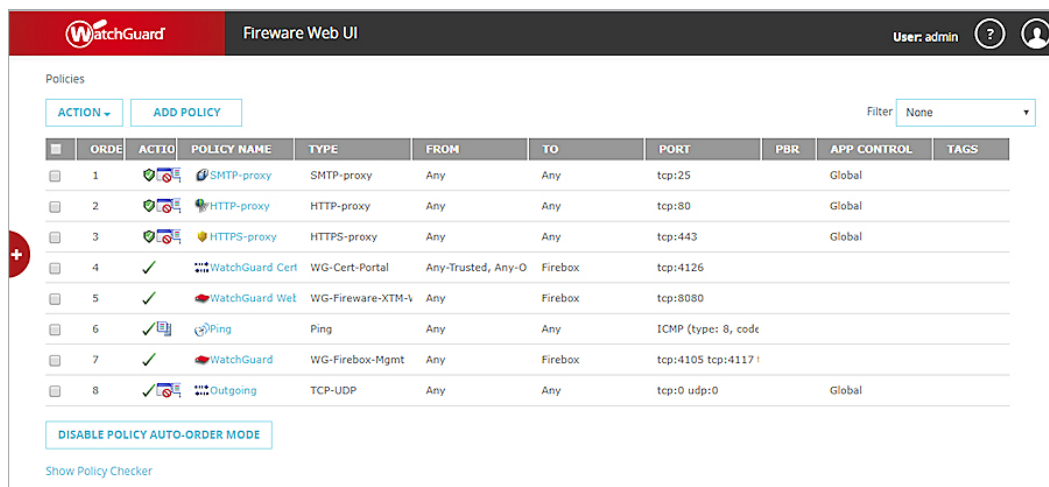
System	
Name	M270 WatchMode
Model	M270
Version	12.2.1.B569657
Serial Number	8014008C5809
System Time	22:56 Greenwich
System Date	2018-08-09
Uptime	0 days 00:15

Below the system information, there are sections for 'Servers' (Log Server, DNSWatch, Dimension, all Disabled), 'WatchGuard Cloud' (Status: Disabled), and 'External Bandwidth' (a graph showing sent and received data over 20 minutes).

- Select **System > WatchMode**, and verify WatchMode is enabled.

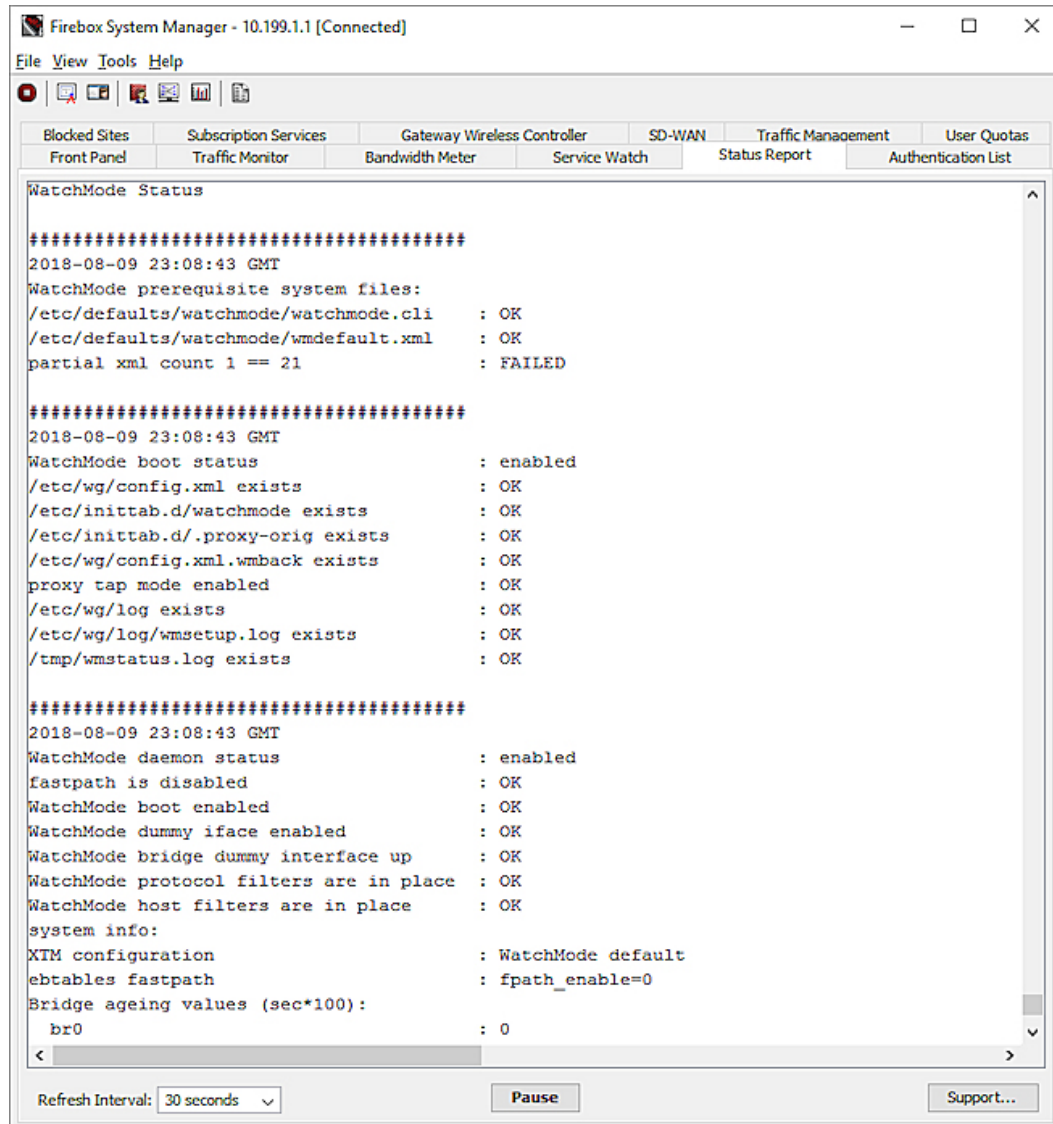


- Select **Firewall > Firewall Policies** and verify that most policies allow traffic from *Any* to *Any*, and that the Firebox management policies allow connections to the Firebox from *Any*.



- Select **System Status > Diagnostics** and complete two diagnostic tasks:
 - DNS lookup — Try to resolve a host name on the local network and one on the Internet
 - Ping — Ping a host name or IP address on the Internet
- Select **Dashboard > Subscription Services** and click **Update** for one or more of the services to verify that signature downloads can occur.

- From Firebox System Manager, select the **Status Report** tab and verify:
 - If you use WatchGuard Cloud, the *WatchGuard Cloud Status* section shows if the Firebox has WatchGuard Cloud enabled and if the Firebox is connected to WatchGuard Cloud.
 - If you use Dimension, the *Log Configuration* section shows the *WatchGuard Log Server* status as **Enabled** for the IP address of your Dimension instance.
 - The *WatchMode Status* section appears in the Status Report.

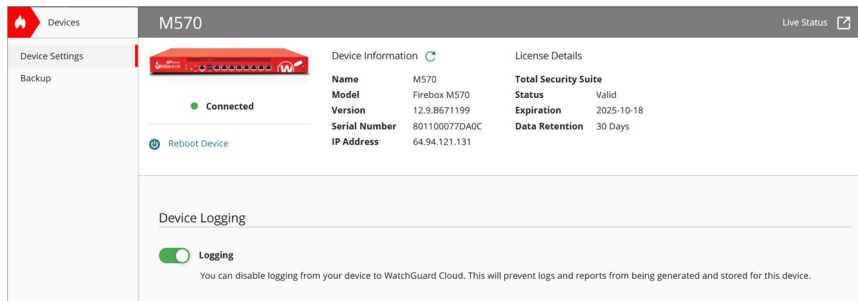


Enable Logging to WatchGuard Cloud

If your Firebox is currently not added to WatchGuard Cloud, you must add the Firebox to WatchGuard Cloud before you can send logs. For information on how to add a locally-managed Firebox to WatchGuard Cloud, go to [Add a Locally-Managed Firebox to WatchGuard Cloud](#).

To configure the Firebox to send logs to WatchGuard Cloud:

1. Log in to your WatchGuard Cloud account.
2. Select the Firebox.
3. Click **Configure > Devices**.
4. In the **Device Logging** section, make sure **Logging** is enabled.



Enable Logging to Dimension

After WatchMode is enabled on your Firebox, you can enable logging to your existing instance of Dimension. This instance of Dimension must already be installed and configured, and in a location you can connect to from your client's network.

Though you can only enable WatchMode from Fireware Web UI, you can configure the logging settings for your device from any of the WatchGuard management tools. In this section, we only provide instructions from Fireware Web UI.

From Fireware Web UI:

1. Select **System > Logging**.
The Logging page appears with the WatchGuard Log Server tab selected.

Logging

WatchGuard Log Server Syslog Server Settings

☐ Send log messages to these Dimension or WSM Log Servers

Your device can send log messages to a maximum of two primary Log Servers at the same time.

Log Servers 1 Log Servers 2

LOG SERVERS 1	PRIORITY
ADD EDIT REMOVE MOVE UP MOVE DOWN	

On each **Log Servers** tab, the first address in the list is for the primary Log Server. This can be an instance of Dimension or a WSM Log Server. Additional addresses in each list are for backup servers that are used when the primary server is unavailable. If the Firebox cannot connect to the first backup server in a list, it tries to connect to the next backup server in that list. The Firebox falls back to the primary server when it becomes available.

SAVE

2. Select the **Send log messages to these WatchGuard Log Servers** check box.
3. Select **Log Servers 1**.
4. To add the IP address of the Dimension server, below the **Log Servers 1** list, click **Add**.
The Add WatchGuard Log Server dialog box appears.
5. Specify the IP address and the encryption key for the Dimension server.
6. Click **Add**.
The IP address of the Dimension server appears in the Log Servers 1 list.
7. Click **Save**.

After you add the IP address for the Dimension server, the IP address appears on the **Dashboard** > **Front Panel** page in the **System** section.

Front Panel

Top Clients View all

NAME	RATE	BYTES	HITS
10.158.4.19	651 kbps	1 MB	8
192.168.43.81	704 bps	6 MB	1
192.168.42.162	272 bps	173	1
192.168.42.163	160 bps	162	1
192.168.43.79	144 bps	342 KB	2
192.168.42.209	80 bps	174	1
192.168.42.214	64 bps	171	1
192.168.42.213	56 bps	72	1

System

Name: M270-WatchMode
 Model: M270
 Version: 12.2.1.B569657
 Serial Number: 80140008C5809
 System Time: 19:42 Greenwich
 System Date: 2018-08-10
 Uptime: 0 days 21:01

Servers

Log Server: 203.0.113.122
 DNSWatch: Disabled
 Dimension: Disabled

WatchGuard Cloud

Status: Disabled

REBOOT

Verify the Connection to the Dimension Server

To verify that the Firebox is connected to the Dimension server:

1. Open a web browser and connect to Dimension at <https://<IP address of Dimension>>.
2. Log in with the Administrator credentials.
The Dimension Home > Devices page appears with the list of connected devices.
3. Verify that your Firebox appears in the **Devices** list with a **Connected** status of **Yes**.

WatchGuard Dimension User: admin

Devices Groups VPNs Servers Wi-Fi Cloud

List Health License Map Search

NAME	LOGGING	MANAGED	IP ADDRESS	SERIAL NUMBER	VERSION
M270-WatchMode	Yes	Disabled	192.168.42.183	80140008C5809	12.2.1.B569657
M400_50	Yes	Disabled	203.0.113.50	80DA034D65886	12.1.1.B558423
M400_cluster_100 (Member2)	Yes	Disabled	203.0.113.100	80DA02BD37DA6	12.0.2.B546738
M470_20	Yes	Disabled	203.0.113.20	801000070C94C	12.2.1.B569657
M500_90	Yes	Disabled	203.0.113.90	80DB02D9CFB66	12.3.B570012
T35-W	No	Disabled	192.168.42.105	D02102718C5FC	12.2.B555031
T50-W_80	Yes	Disabled	203.0.113.80	70AF0283EF534	12.1.3.B563398
T55-W_70	Yes	Disabled	203.0.113.70	D02302754E2FF	12.2.B563486

View 1 - 8 of 8 Page 1 of 1

ADD **EDIT** **REMOVE**

4. If your device does not appear in the **Devices** list, wait a few minutes and click  to refresh the list.

If the device still does not appear in the list, connect to the Firebox with Fireware Web UI and verify that the IP address and Authentication Key you specified for the Dimension server are correct.

After you have the Firebox configured, you can connect the device to your customer's network. For more information, see [Network Installation — Mirror Customer Traffic on page 18](#).

Change the DNS Server

If you do not use DHCP for Eth0, and a local DNS server is available, WatchGuard recommends that you change the DNS server settings on your device to the IP address of the local DNS server.

To change the DNS server IP address for your device, from Fireware Web UI:

1. Select **Network > Interfaces**.
The Interfaces page appears.
2. Scroll down to the **DNS Servers** list.
3. In the **DNS Server** text box, type the IP address of the local DNS server.
4. Click **Add**.
The IP address appears in the DNS Servers list.
5. Click **Save**.

Verify Monitoring Activity

To make sure that your WatchMode Firebox is monitoring the activity on your customer's network, you can use Traffic Monitor in Fireware Web UI or Firebox System Manager to see the log messages in real-time.

To see log messages in **Traffic Monitor**, from Fireware Web UI:

1. Connect to Fireware Web UI for your device.
2. Select **Dashboard > Traffic Monitor**.
The Traffic Monitor page appears.
3. At the top of the page, specify any options to sort and filter the log messages.



You can also connect to WatchGuard Cloud or Dimension to see the log messages from your WatchMode device.

WatchMode Configuration Details

When you enable WatchMode, the Firebox is configured with default settings. You can edit these settings and enable additional policies and services.



We recommend that you do not modify the configuration of the Eth0 and Eth1 interfaces.

Default Configuration Settings

In WatchMode, your Firebox is configured with these default settings:

Networking Settings

- Eth0 (External) — DHCP
- Eth1 (Management) — 10.199.1.1/24 (DHCP Server)
- Eth2 (TAP)

System and Security Services Settings

- Intrusion Prevention Service and Application Control are enabled globally
- Signature auto-download is enabled
- NTP is enabled (important for meaningful, time-based reports)
 - Uses the *pool.ntp.org* NTP servers (Fireware default)
 - (Optional) You can configure different NTP servers
- Default Packet handling blocks dangerous activities and prevents distributed denial of service attacks

Firewall Policies

The default is set to From: Any, To: Any, but you can restrict this by subnet, IP address, or IP address range

- Ping — For management
- WatchGuard — For management
- WatchGuard Web UI — For management
- Outgoing — Intrusion Prevention Service and Application Control are enabled; for log message generation

Proxy Policies

The default is set to From: Any, To: Any, but you can restrict this by subnet, IP address, or IP address range

- SMTP
- HTTP
- HTTPS — For WebBlocker services

Modify the Configuration

WatchGuard recommends that you do not modify the settings for the Eth1 and Eth2 interfaces. Instead, restrict your edits to these areas of the configuration:

- Policies
- System and Security settings
- Network access for the Eth0 interface
- Global network settings (such as local DNS/WINS/NTP servers)

WatchMode does not support these features of Fireware OS:

- Dynamic routing
- FireCluster
- Multi-WAN
- Single Sign-On

Supported Security Services

In WatchMode, the Firebox supports these security services for inspection of network traffic:

	HTTP Proxy	HTTPS Proxy without content inspection	SMTP Proxy	Packet Filter Policies
Reputation Enabled Defense	✓			
Botnet Detection	✓	✓	✓	✓
Geolocation	✓	✓	✓	✓
spamBlocker			✓	
WebBlocker	✓	✓		
Application Control	✓	✓	✓	✓
Intrusion Prevention	✓		✓	✓
Data Loss Prevention	✓		✓	
Gateway AV	✓		✓	
IntelligentAV	✓		✓	
APT Blocker	✓		✓	
Threat Detection and Response				
DNSWatch				

Services operate with traffic from tagged VLANs.

Threat Detection and Response and DNSWatch are not supported in WatchMode.

Network Installation — Mirror Customer Traffic

When you install the Firebox in your customer's network, you connect the device to a third-party switch on the customer's network that is capable of port mirroring. With the port mirroring method, you connect the Eth2 interface port on the Firebox to a mirror port on the customer's third-party switch. A mirror, or copy, of the traffic from your customer's network then passes through the Firebox so the device can collect log messages related to the network traffic, without having any effect on the network traffic. You can then generate reports of the traffic.

In addition to the connection to the Eth2 interface port, connect your laptop to the Eth 0 or Eth1 interface port. The connection to the Eth0 or Eth1 interface port enables you to use Fireware Web UI or WSM to manage the Firebox and to connect to WatchGuard Cloud or Dimension to review log messages and generate reports. Make sure that you do not connect Eth1 to your customer's network.

Because you must connect the Eth0 interface port on the Firebox to your customer's network, you can also use one of your customer's computers to connect to Fireware Web UI to manage the Firebox, and to connect to WatchGuard Cloud or Dimension to review log messages and generate reports. The Eth0 interface port connection also enables you to connect to the Internet for WebBlocker URL category lookups and signature update services.

WatchGuard recommends that you make these interface port connections to your Firebox:

- Connect Eth0 on the Firebox to the customer's network for Internet access
- Connect Eth1 on the Firebox to the laptop
- Connect Eth2 on the Firebox to the TAP port on the third-party switch (or TAP device)



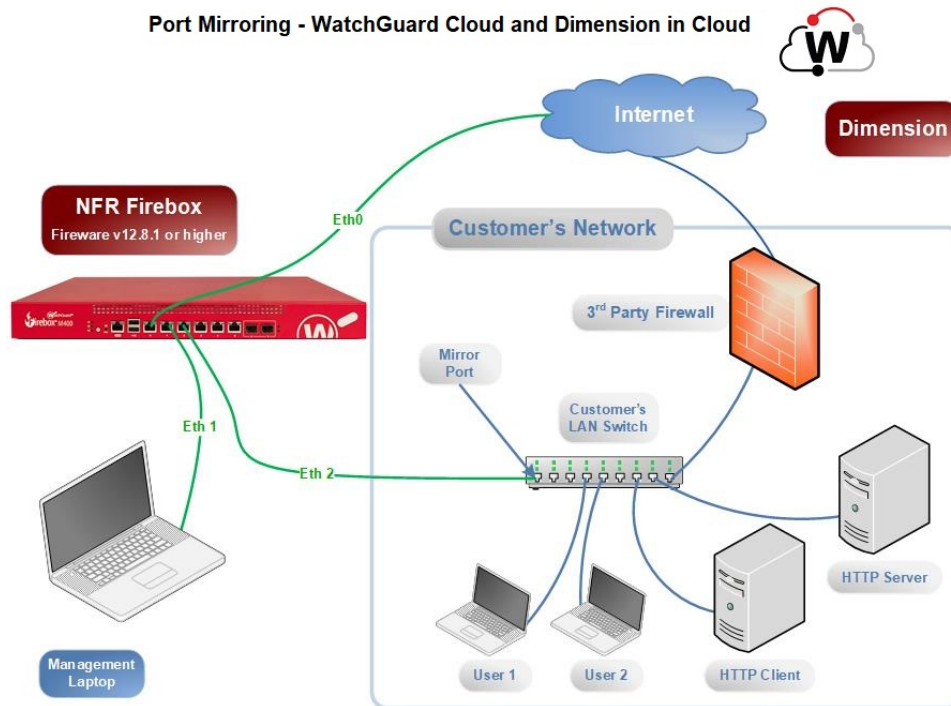
Make sure to connect Eth0 to a different subnet than Eth2 so that subscription services can connect to the update server. For more information, see the *Known Issues* section of [About WatchMode](#)

If you use Dimension, your instance of Dimension must be installed and configured before you configure your Firebox for WatchMode and install it in your customer's network. You can run your instance of Dimension in any of these locations, as long as you can get access to them from your customer's network:

- In a cloud
- On a VMware or Hyper-V server already in the datacenter
- On a laptop server that you provide

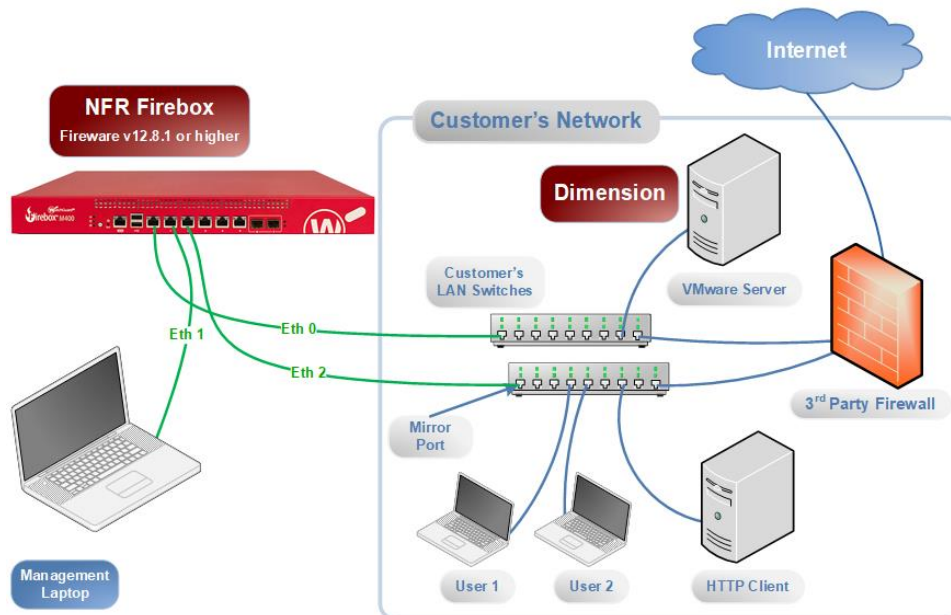
WatchMode Network Installation

Port Mirroring - WatchGuard Cloud and Dimension in Cloud



WatchMode Network Installation

Port Mirroring — Dimension on Virtual Machine



After you have verified the network configuration settings are correct, connect the Eth2 interface on the Firebox to the mirror port on the third-party switch for the network you want to monitor. The Firebox should begin to receive the mirrored traffic from your customer's network.

Connect the Firebox to the Network

To connect your Firebox to your customer's network for port mirroring, connect the mirror interface port on your customer's switch to the Eth2 interface port on the Firebox. You can also connect Eth0 or Eth1 on the Firebox to your customer's network to manage the Firebox and connect to WatchGuard Cloud or Dimension.

Traffic can now pass through the Firebox so it can monitor the traffic in your customer's network.

View Log Messages & Reports

After you complete the installation and configuration processes for your Firebox, and have waited sufficient time for the device to have sent enough log messages, you can view the log messages and available reports that you need to show your customer.

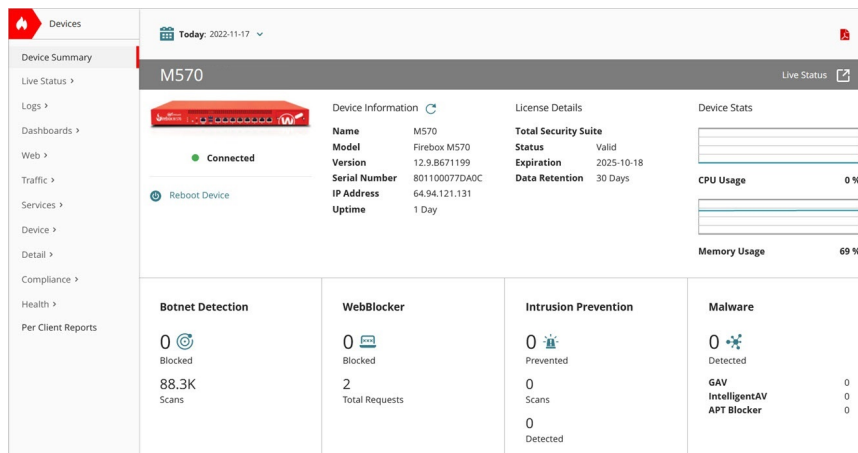
You can view log messages and reports in:

- [WatchGuard Cloud](#)
- [Dimension](#)

WatchGuard Cloud

To see log messages and reports in WatchGuard Cloud:

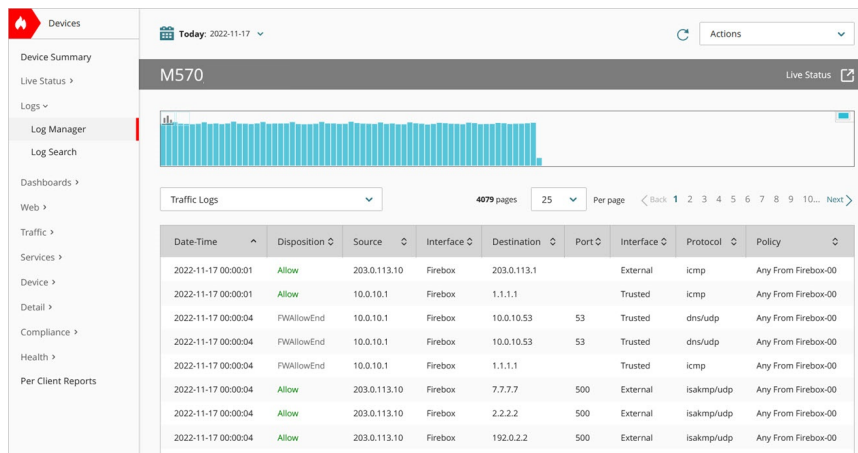
1. Log in to your WatchGuard Cloud account.
2. Select **Monitor > Devices**.
3. From the devices list, select the Firebox.
The Device Summary for the Firebox appears.



WatchGuard Cloud Log Manager

To see the log messages for the device:

1. Select **Logs > Log Manager**.
The Log Manager page appears for the device.
2. At the top of the **Log Manager** page, select the options to sort and filter the log messages.




Search WatchGuard Cloud Logs

From WatchGuard Cloud, you can view and search log messages for your Firebox devices:

1. From the list of reports, select **Logs > Log Search**.
The Log Search page opens for the selected device.



2. To specify which type of log messages to include in the search, from the drop-down list at the right side of the page, select the log message type (Traffic Logs, Alarm Logs, Event Logs, or Statistic Logs). To search all log message types, select **All Logs**.
3. In the **Search** text box, type the search query.
4. To run the search, press **Enter** or click .

WatchGuard Cloud Device Reports

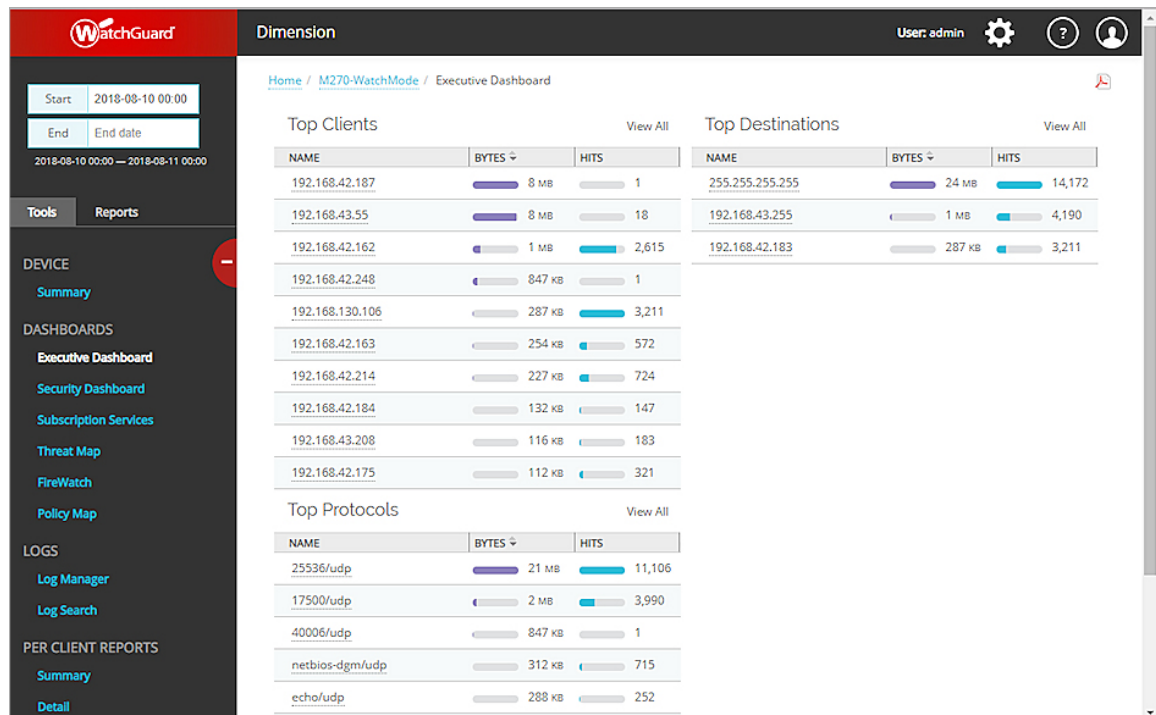
To view device reports in WatchGuard Cloud:

1. Log in to WatchGuard Cloud.
2. Select **Monitor > Devices**.
3. Select the Firebox.
4. To select the report date range, click .
5. From the list of reports, select a report.
The selected report data opens.
6. Click  to download the report.

Dimension

To see log messages and reports in Dimension:

1. Open a web browser and connect to Dimension at `https://<IP address of Dimension>`.
2. Log in with the *Administrator* credentials.
The Dimension Home > Devices page appears with the list of connected devices.
3. From the **Devices** list, select the Firebox.
The Dashboard reports page appears for the Firebox.



4. From the **Start** and **End** drop-down calendars, select the start and end date and time for the log message and report data.

To see the log messages for the device:

1. On the **Tools** tab, select **Log Manager**.
The Log Manager page appears for the device.
2. At the top of the **Log Manager** page, select the options to sort and filter the log messages.



To see the available reports for the device:

1. Select the **Reports** tab.
2. From the **Reports** list, select a report to review.
The selected report appears.
3. From the drop-down list at the top of the report, select an option to pivot the report data.

Export a Report as a PDF

To save the results from most reports in a format that you can print and share with your customer, you can convert the report to a PDF file that you can view electronically or print.

To generate a PDF of a report:

1. At the top right of the report page, click .
If the report cannot be converted to PDF format,  does not appear.
2. Specify a name for the PDF file and a location to save it.

Disable WatchMode on Your Firebox

After you have run all the necessary reports for your customer, have demonstrated all the features and benefits of a Firebox protecting their network, and are ready to remove your Firebox from their network, you can disable WatchMode on your device. When you disable WatchMode, any configuration changes you made to support WatchMode in your customer's network are removed, and the previous configuration settings on the device are restored.

You can only disable WatchMode from Fireware Web UI, and you must be logged in with a user account that has Device Administrator privileges, such as the default *admin* user account.

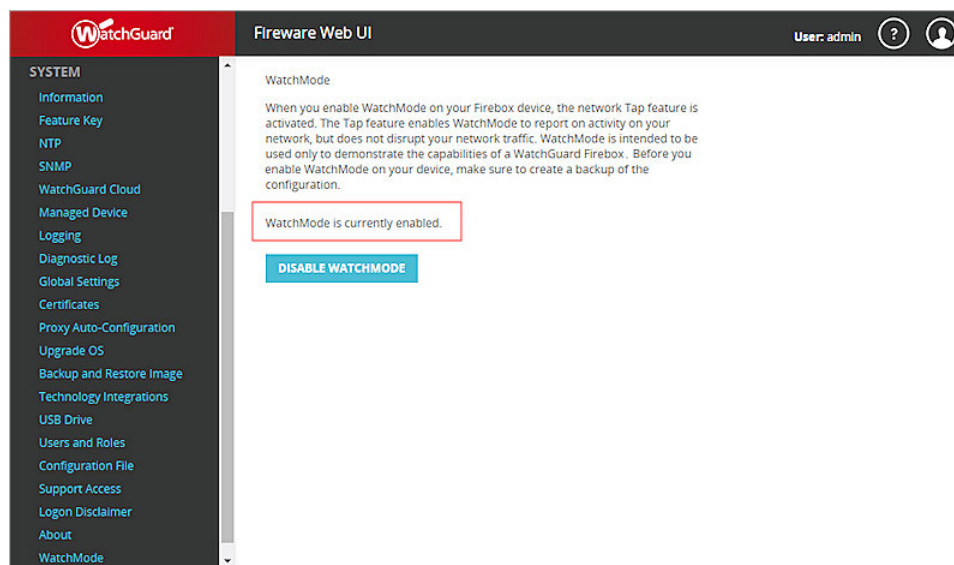
You can choose from these methods to disable WatchMode:

- Disable WatchMode in the Firebox System settings
- Restore a backup image to the Firebox that does not have WatchMode enabled
- Upgrade the OS on the Firebox

To disable WatchMode from the System settings:

1. Select **System > WatchMode**.

The WatchMode page appears.



2. Click **Disable WatchMode**.

WatchMode is disabled and the device automatically reboots.

To restore a backup image to the device and disable WatchMode:

1. Select **System > Backup and Restore Image**.
The Backup and Restore Image page appears.
2. From the **Available backup images** list, select the backup image to restore.
To restore a backup image that is not stored on the Firebox, you must first click Import Backup Image to import it.
3. Click **Restore**.
The backup image is restored and the device reboots.

To upgrade the OS and disable WatchMode:

1. Select **System > Upgrade OS**.
The Upgrade OS page appears.
2. Click **Choose File** and select the OS upgrade file installed on your computer for your Firebox model.
3. Click **Upgrade**.
The device reboots to complete the upgrade. After the upgrade, WatchMode is disabled