WatchGuard Dimension™ v2.1.1 Update 3 Release Notes

Build Number	567758
Release Date	8 August 2018
Release Notes Revision Date	14 January 2019

On 8 August 2018, WatchGuard released the Dimension v2.1.1 Update 3 maintenance release. For information on the issues addressed in this update, see the Resolved Issues section. For more detailed information about the enhancements included in Dimension v2.1.1 Update 3, see the product documentation or review What's New in Dimension v2.1.1 Update 3.

WatchGuard is pleased to announce the release of Dimension v2.1.1. This release includes bug fixes and several feature enhancements, including:

- An update to the localization of the Dimension user interface and Dimension reports for our French (FR), Japanese, and Spanish (LA) users.
- A new Dimension Administrator role that enables you to restrict user privileges to monitoring and management of the Dimension system.

For information on bug fixes included in this release, see the Enhancements and Resolved Issues section. For more detailed information about the feature enhancements and functionality changes included in Dimension v2.1.1, see the product documentation or review What's New in Dimension v2.1.1.

New to Dimension?

WatchGuard Dimension must be installed on a virtual machine with a 64-bit OS. It can be installed on VMware or on Hyper-V. You can find installation instructions in *Fireware Help* at Get Started with WatchGuard Dimension.

If you are interested in installing Dimension in Amazon Web Services, please contact WatchGuard Technical Support for assistance.

Resolved Issues in Dimension v2.1.1 Update 3

General

- A conflict between Dimension Web UI and Firebox Web UI no longer logs users out when they connect to both with same browser. *[FBX-5305]*
- The Dimension web server process now starts correctly on hypervisors with AMD processors. *[FBX-9914]*
- The global monitor role now correctly restricts access to configuration history. *[FBX-10799]*
- Subject Alternative Name (SAN) entities are now correctly added to certificate signing requests. *[FBX-9873]*
- Backup files can now be correctly restored by manually uploading them to the Web UI. *[FBX-10501]*
- A change to the Start and End time range of a Dimension page now requires that you click Apply to apply the new time range to the displayed data. Previously, this time change immediately refreshed the displayed data. *[FBX-11614]*

Logging and Reporting

- This release resolves a memory leak in the wlcollector process. *[FBX-5584]*
- The Subscription Services dashboard now counts IPS Intrusions correctly. *[FBX-3297]*
- The log collector has been updated to handle new log attributes for DNS Forwarding, Host Header Redirection, and Geolocation. *[FBX-6665, FBX-9994]*
- From and To fields now appear correctly in spamBlocker exception log messages. *[FBX-6783]*
- External/VPN bandwidth report generation performance is improved. *[FBX-11559]*
- Labels in spam action report now match SMTP/POP3/IMAP proxy action labels. *[FBX-11653]*
- This release improves performance when the database purges expired log data. *[FBX-10958]*

Security

- This release updates the Web UI to present correct X-Frame-Options headers to resolve a clickjacking vulnerability. *[FBX-9682]*
- This release resolves an XSS vulnerability in the Web UI login page. *[FBX-11438]*

Resolved Issues in Dimension v2.1.1 Update 2

General

- APT Activity Summary report no longer prevents Tools and Reports menus from loading for cluster members. *[FBX-4920]*
- Log Server now correctly initializes if remote backup user does not have write permissions to create backup folders. *[FBX-4961]*
- A Log Collector issue has been fixed that caused incorrect logging status to be displayed for devices. *[FBX-5981]*
- Backup locations are now clearly indicated using sftp:// URLs instead of local mount points. *[FBX-8584]*
- This release resolves an issue in which the log collector process unexpectedly restarts due to large number of simultaneously connections. *[FBX-2591, FBX-3555]*
- The default setting for email encryption is now **Allow** instead of **None**. *[FBX-4614]*
- You can now correctly add devices to Dimension with the **Add online device** method. *[FBX-5513]*

- This release updates the name of the **Encryption Key** to the **Authentication Key**, in parity with Firebox interface updates. *[FBX-6512]*
- Dimension no longer shows **Not Licensed** status for Fireboxes with renewed feature keys. *[FBX-6518]*
- Top Blocked Advanced Malware (APT) now consistently displays in Security Dashboard. *[FBX-7422]*
- This release adds support for external postgreSQL servers hosted on Azure. *[FBX-7725]*
- This release creates additional indexes for data to improve performance with large numbers of logging devices. *[FBX-2584]*
- The Dimension system now more accurately reports the number of connected users. *[FBX-8466]*

Reports

- Subscription Services reports now export correctly to PDF on web browsers configured for French. *[FBX-5762]*
- The Executive Summary report can now be successfully exported to PDF in the Japanese locale. *[FBX-8117, FBX-2574]*
- Log data summarization no longer causes some report generation to fail. *[FBX-8119]*
- The Scheduled Executive Summary no longer fails when APT results have extremely long names. *[FBX-5732]*
- This release resolves an issue in which APT content names with reserved characters would cause PDF reports to fail. *[FBX-6740]*
- Double-quotes (") and other reserved characters no longer cause email notifications to be truncated. *[FBX-6756]*
- The Subscription Service Summary report descriptions for RED Good and Bad scores are no longer reversed. *[FBX-5747]*
- All reports now correctly display the End Time value. [FBX-8234]

Security

- You no longer see XSS error messages on some report pages. *[FBX-9439]*
- Dimension SSH service now correctly rejects weak ciphers. *[FBX-7894]*
- This release updates the Apache server to v2.4.28 and Postgres client to v9.6.5 to avoid vulnerability to CVE-2016-8743. *[FBX-5206]*
- The Web UI is now protected against the CSRF vulnerability. *[FBX-8224]*

Resolved Issues in Dimension v2.1.1 Update 1

- The version of OpenSSL used by Dimension has been updated to v1.0.2j with this release. *[92233]*
- This release includes fixes to address several reported command injection vulnerabilities. *[92305]*
- This release includes a fix related to arbitrary file read vulnerabilities associated with the Dimension Web UI. *[92306]*
- This release addresses a cross-site scripting vulnerability in the Dimension Web UI. *[92307]*
- This release address a server-side request forgery vulnerability in the Dimension Web UI. *[92308]*

Enhancements and Resolved Issues in Dimension v2.1.1

Dimension Administration

- This release provides updates to the French (FR), Japanese, and Spanish (LA) localization.
- This release introduces a new Dimension Administrator role, which restricts user privileges to monitoring and management of the Dimension system. *[91842]*

- You can now connect directly to your instance of WatchGuard Wi-Fi Cloud from Dimension. *[91843]*
- This release adds support for the new Firebox T70 appliance, being released by WatchGuard in October. *[91478]*
- You can no longer input invalid characters when generating a Web Server CSR. *[91349]*
- The time stamp of APT Blocker-detected events no longer shows in UTC in Log Manager. *[90947]*
- A problem that caused the Dimension database to fail to upgrade when upgrading Dimension from v1.3 to v2.1 has been resolved in this release. *[91289]*

Reports

- Reports now show the IP addresses of clients behind the Explicit Proxy. *[91937]*
- Scheduled reports delivered through email now open correctly when the email client has the "display attachments inline" option enabled. *[87587]*
- When traffic is sent to a Botnet site, it is no longer included in the Top Blocked Destinations list when using the filtered view on the Security Dashboard. Similarly, if traffic originates from a Botnet Site, that site is no longer included in the Top Blocked Clients list. *[91098]*

Dimension Command

- The License tab no longer shows incorrect expiration information for a managed FireCluster. *[91870]*

Known Issues and Limitations

Known issues for Dimension v2.1.1 and updated versions, including workarounds where available, can be found on the Technical Search > Knowledge Base tab. To see known issues for a specific release, from the **Product & Version** filters you can expand the Dimension version list and select the check box for v2.1.1.

Upgrade to Dimension v2.1.1 Update 3

You can upgrade to Dimension v2.1.1 Update 3 directly from Dimension v1.2 or higher. It is not possible to upgrade from v1.0 or v1.1 directly to Dimension v2.1.1 or higher. You must upgrade to v1.3 first.

Before You Begin

- WatchGuard recommends that you take a snapshot of your Dimension VM in VMware or Hyper-V before you start the upgrade process.
- Do not reboot the VM while a Dimension upgrade is in process.

Upgrade Instructions

Estimated time to upgrade: < 8 minutes

1. In a web browser, connect to your existing instance of Dimension at `https://<IP address of Dimension>`, and log in.
2. Select **Administration > System Settings**.
   The System Settings > Status page appears.
3. Click **Upgrade** and click **Browse** to select the Dimension upgrade file: `watchguard-dimension_2_1_1_U3_apt.tgz`.
4. Click **OK**. Wait for the upgrade to complete.
   If the upgrade requires the Dimension services to restart, you will be redirected to the Log In page.

There are several reasons that could cause a Dimension upgrade to fail. If your upgrade fails, read these Important Notes. We also recommend that you search the Known Issues in the Knowledge Base for more information. If you do not find the solution to your upgrade problem, please contact WatchGuard Technical Support.

To verify that the upgrade was successful, make sure the **System Settings > Dimension System Information** shows that the **Version** is 2.1.1 Update 3 (549365).

Important Notes

As you get started with Dimension it is important to understand:

Appliances supported for logging and reporting

WatchGuard Dimension can accept log messages and generate reports for any appliance that runs Fireware v11.x or higher that has a current Support subscription. Dimension can also accept log messages for WatchGuard System Manager Management Server and Quarantine Server. You must make sure that Dimension can resolve and connect to *services.watchguard.com* for support subscription verification for any Firebox running v11.11 or earlier. Dimension will not accept log messages for any Firebox or XTM device that does not have an active Support subscription (a 30-day grace period is provided before log messages are refused).

Appliances supported by Dimension Command for centralized management

WatchGuard Dimension can centrally manage any Firebox that runs Fireware v11.10.1 or higher that has a current Support subscription and a feature key that includes Dimension Command. Dimension Command licenses can be purchased through authorized WatchGuard resellers.

Deploying Dimension behind a Firebox

To provide an extra layer of security to your Dimension system, you can deploy your instance of Dimension behind a Firebox. When you configure the settings for this Firebox, make sure that it meets several key requirements, as defined here. It is especially important that Dimension is configured to resolve DNS and make successful HTTP connections to *services.watchguard.com* and to the Ubuntu repository server. Dimension is based on Ubuntu Linux. Your Dimension system must be able to resolve DNS and make periodic HTTP requests to the Ubuntu servers to check for updates to the Linux OS to correct security and system stability issues. The Ubuntu domains are:
- archive.ubuntu.com

- security.ubuntu.com

If you use a Firebox with restrictive HTTP proxy settings, you may need to create an HTTP proxy exception to allow Dimension to reach these addresses, or create packet filter policies to specifically allow traffic between Dimension and **.ubuntu.com* and Dimension and *services.watchguard.com*.

Using Dimension Command through a firewall

If your instance of Dimension is behind a firewall (Firebox or another NAT device), before you add your Firebox to Dimension for management, make sure the firewall is set for correct port-forwarding to Dimension, and then make sure your Dimension instance is configured to use the fully qualified domain name (or external IP address)of the firewall in the Public Accessibility settings. For more information about how to configure Public Accessibility settings for Dimension, go here.

Collect report data

To see reporting data related to Fireware policies you must enable logging in your policies. To see reporting data for your subscriptions services (WebBlocker, spamBlocker, Gateway AV, IPS, RED, Application Control, DLP, or APT Blocker), you must:

- Enable the subscription service in your Firebox configuration.

- Enable logging in the policies that use the subscription service and make sure the **Enable logging for reports** check box is selected.

- Enable the **Send Security Services Statistics** check box in your Logging settings.

- Make sure that there has been traffic to which these services apply

To collect data for reports for your AP devices, you must:

- Make sure the Gateway Wireless Controller logging setting **Enable logging for reports** is enabled.

- Make sure the Gateway Wireless Controller Firebox or XTM device is running Fireware v11.10.1 or later.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard website at https://www.watchguard.com/support. When you contact Technical Support, you must supply your registered Product Serial Number or Partner ID.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375