WatchGuard Dimension™ v2.1.2 Update 4 Release Notes

Build Number	v2.1.2 Update 4 -- 622159 v2.1.2 Update 3 -- 608183 v2.1.2 Update 2 -- 596545 v2.1.2 Update 1 -- 590784 v2.1.2 -- 588050
Release Date	v2.1.2 Update 4 -- 24 June 2020 v2.1.2 Update 3 -- 9 January 2020 v2.1.2 Update 2 -- 27 June 2019 v2.1.2 Update 1 -- 13 May 2019 v2.1.2 -- 14 March 2019
Release Notes Revision Date	4 May 2021

On 24 June 2020, WatchGuard released Dimension v2.1.2 Update 4. This release adds support for IMAP Mail and Detailed reports, support for PostgreSQL 11 and 12, and includes several important bug fixes.

On 9 January 2020, WatchGuard released Dimension v2.1.2 Update 3. This release corrects several issues with incorrect domain and email sender names in reports, and a PCI compliance failure. This release includes several other bug fixes and feature enhancements.

On 27 June 2019, WatchGuard released Dimension v2.1.2 Update 2. This release addresses the TCP SACK kernel vulnerability, and includes several other important bug fixes and feature enhancements.

On 13 May 2019, WatchGuard released Dimension v2.1.2 Update 1. This release includes several important bug fixes.

WatchGuard is pleased to announce the release of Dimension v2.1.2. This release includes bug fixes and several feature enhancements, including:

- Dimension now correctly creates reports for ConnectWise.
- Dimension can now accept connections from a Firebox configured in FIPS mode.

- Dimension now uses a new IP database release for Threat Map..
- New Dimension instances will be supported by Ubuntu 16.04 LTS

For information on bug fixes included in this release, see the Enhancements and Resolved Issues section.

New to Dimension?

WatchGuard Dimension is distributed as a VHD file for installation on Hyper-V for Microsoft Windows Hyper-V Server 2008 R2, 2012, 2012 R2 (64-bit required), 2016, or 2019.

WatchGuard Dimension is distributed as an OVA file for installation on VMware ESXi 5.5, 6.0, or 6.5 (64-bit required).

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 v2.1.2 Update 4

General

- The UI labels on the Per Client Support and Most Popular Domains reports are updated to be more descriptive. *[FBX-3171]*
- This release adds support for IMAP Mail and Detailed reports. *[FBX-7235]*
- Unnecessary log messages that include "iptables denied" have been suppressed so log files do not fill as quickly. *[FBX-18720]*
- This release adds support for PostgreSQL 11 and 12. *[FBX-18751]*
- This release resolves a problem that caused Dimension to stop accepting log messages. *[FBX-18828]*
- This release adds support for TDTS IPS/AppID engine for Fireware v12.6.1 and T20, T40, and T80 Firebox models. *[FBX-18130]*

Resolved Issues in Dimension v2.1.2 Update 3

General

- Dimension now supports PostgreSQL versions up to v10.8. *[FBX-14969, FBX-16784]*
- This release resolves a PCI compliance failure due to behavior of HTTP redirect to HTTPS connection feature. *[FBX-16543]*
- Quick Setup Wizard no longer stalls on administrator passphrase step on Hyper-V. *[FBX-16103]*
- This release improves performance with multiple connected devices. *[FBX-11322]*
- This release resolves a log collector memory leak issue. *[FBX-17228]*

Logging and Reporting

- Authenticated users now correctly appear as the source for connections in HTTP and HTTPS proxy connnections. *[FBX-15333]*
- The **User Expiration** time now correctly appears in local browser time zone. *[FBX-17025]*
- The **Policy Usage Report** now appears in local browser time zone. *[FBX-17301*]
- ConnectWise reports no longer fail with message `Task failed: _CWReportGeneration_align_to_ maxlines is not defined.` *[FBX-17953]*

- Geolocation data is now correctly included in Log Search results. *[FBX-17970]*
- The phrase `app_cat_id` no longer appears in domain name or IP address fields in some Dimension reports. *[FBX-18071, FBX-18098]*
- This release resolves an issue that caused SMTP proxy report to show `app_cat_ID=5` as the email sender. *[FBX-17634]*

Device Management

- The Dimension no longer displays feature keys for devices after you remove them. *[FBX-16678, FBX-17155]*
- Your Dimension will no longer create a new entry for a resolved FQDN that is already a configured static IP address. *[FBX-3462]*

Resolved Issues in Dimension v2.1.2 Update 2

General

- This release addresses the TCP SACK kernel vulnerabilities (CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479) *[FBX-16844]*
- System Status page now has a tooltip message for `Web Server Certificate Expiration` message. *[FBX-16235]*
- Dimension no longer enforces a maximum size limit on external database. *[FBX-3283]*

Logging and Reporting

- Virus Found log messages now included in GAV reports. *[FBX-16440]*
- Dimension now correctly includes `sent_bytes` field in summarized data in reports when Application Control is enabled. *[FBX-15697]*
- Log Search results now include the `info` field from IAV log messages. *[FBX-15544]*
- The Executive Report now displays all hostnames in scheduled reports for multiple devices. *[FBX-15474]*
- Most Popular Domain reports now includes HTTPS traffic as well as HTTP. *[FBX-15453, FBX-11038]*

Resolved Issues in Dimension v2.1.2 Update 1

- Dimension v2.1.2 instances hosted by AWS no longer fail to connect to the data disc. *[FBX-16036]*
- Dimension can now correctly display status of VPNs for Fireboxes managed by Dimension. *[FBX-15590]*
- The Dimension System Status page now displays time in the local time zone for the client web browser. *[FBX-15591]*
- Dimension now uses the required ClientID for ConnectWise integration. *[FBX-15651]*

Resolved Issues in Dimension v2.1.2

General

- Non-ASCII characters in the Dimension notification email subject no longer cause emails to have an unreadable subject line. *[FBX-14657]*
- Dimension now correctly uses IPv4 IP addresses to deliver emails to an IPv4-only network when the recipient has an IPv6 IP address. *[FBX-3446]*
- Dimension now shows the correct uptime value for the system and database. *[FBX-12744]*
- This release resolves a disk error issue that caused Dimension systems in Hyper-V to stop unexpectedly. *[FBX-13400]*
- This release includes an update to the IP database for Threat Map. *[FBX-15062]*

Logging and Reporting

- Dimension now supports connections from a Firebox configured in FIPS mode. *[FBX-14821]*
- The Dashboard no longer fails to display complete data with the message `COPY cluster_pe, column in_octets value is out of range for type bigint error` in Dimension database log messages. *[FBX-14914]*
- This release resolves an issue that caused PCI Compliance report generation to fail in French, Spanish, and Japanese. *[FBX-15045, FBX-14571]*
- Dimension Web UI can now display External and VPN Bandwidth reports with a 10 minute interval. *[FBX-13250]*
- Dimension can now correctly create reports for ConnectWise. *[FBX-13067]*
- This release improves how quickly Dimension creates on-demand Services reports for large report periods. *[FBX-12243]*
- A scheduled task now correctly generates the APT Malware Activity Trend report. *[FBX-2880]*

Security

- New Dimension systems deployed with this release will be supported by Ubuntu 16.04 LTS *[FBX-13487]*
- This release resolves the reported vulnerability to CVE-2015-9251. *[FBX-11558]*
- The Dimension system now automatically renews the self-signed web server certificate. *[FBX-5984]*

User Interface and Configuration

- This release resolves the error *An error occurred refreshing the VPN status: Invalid device ID* that appears when you refresh the VPN Hub view. *[FBX-13784]*
- You can now edit configuration history comments after the first page. *[FBX-13761]*
- Help links in the Dimension Web UI are updated to the current Fireware documentation pages. *[FBX-14086]*
- The dialog boxes for backup and restore of historical data now correctly display the backup location. *[FBX-9797]*
- The Dimension setup wizard now checks whether your configured default gateway is on the same subnet as the IP address for the Dimension system. *[FBX-9526]*
- The System Settings page now displays the expiration of the current Web Server Certificate. [FBX-6612]

Known Issues and Limitations

Known issues for Dimension v2.1.2 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 v2.1.2.

WatchGuard Technologies, Inc.

Upgrade to Dimension v2.1.2 Update 4

> You can upgrade to Dimension v2.1.2 Update 4 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 opens.
3. Click **Upgrade** and click **Browse** to select the Dimension upgrade file: `watchguard-dimension_2_1_2_U4_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 2.1.2 Update 4 (622159).

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