WatchGuard Dimension™ v2.2.2 Release Notes

Build Number	684479
Release Date	7 September 2023
Release Notes Revision Date	14 September 2023

Introduction

On 17 October 2023, we re-released the OVF template file (.ova) for Dimension v2.2.2 . This was an update to the signing certificate only and does not affect functionality.

WatchGuard is pleased to announce the release of Dimension v2.2.2. This release includes bug fixes and several feature enhancements.

For information about the enhancements and bug fixes included in this release, go to the Enhancements and Resolved Issues section.

New to Dimension?

For system requirements, go to Operating System Requirements.

For installation instructions, go to Get Started with WatchGuard Dimension in *Fireware Help*.

If you want to install Dimension in Amazon Web Services, please contact WatchGuard Technical Support for assistance.

Enhancements and Resolved Issues

Enhancements

- When Dimension uses the built-in PostgreSQL database as its database location, an Advanced Settings section now provides the ability to tune the built-in PostgreSQL settings, with guidance from WatchGuard Support. For more information, go to Configure the Database Location. *[FBX-15374]*

Resolved Issues

General

- This release resolves an issue where the system root partition filled with system logs. *[FBX-3092]*
- Dimension now correctly uses the MAC address instead of the client ID in DHCP requests. *[FBX-21816]*
- This release adds support for PostgreSQL v13 and v14. *[FBX-23395]*
- In Dimension Command, the VPN tunnel mode no longer defaults to Aggressive. *[FBX-20678]*

- The FTP test connection no longer fails when a password contains special characters. *[FBX-24402]*
- Dimension instances that run Hyper-V no longer outputs fd0I/O errors to the console for floppy disk devices that do not exist. *[FBX-25471]*

Logging and Reporting

- This release resolves an issue where users could not download the PCI Compliance PDF report. *[FBX-25481]*
- Dimension now prevents unsupported characters and key length entries outside of the allowed range for the logging Authentication Key. *[FBX-19774]*
- The French PDF Executive Summary Report no longer has a space missing in the generated date. *[FBX-20192]*
- The IPS Signature Report now shows an embedded link instead of the full HTML URL in the Signature column. *[FBX-21453]*
- Health reports now generate successfully and show the correct time range in the PDF report. *[FBX-22276]*

Security

- This release updates OpenSSL to v3.0.8 to address CVE-2023-0286, CVE-2023-0215, CVE-2022-4450, and CVE-2022-4304. *[FBX-24720]*
- The Dimension Log Collector now supports TLS v1.2 as the minimum protocol version. *[FBX-23412]*
- This release resolves a DoS DHEat attack vulnerability and addresses CVE-2002-20001. *[FBX-24879]*

Known Issues and Limitations

Known issues for Dimension v2.2.2 and updated versions, including workarounds where available, can be found on the Technical Search > Knowledge Base tab. To view known issues for a specific release, from the **Product & Version** filters you can expand the Dimension version list and select the check box for v2.2.2.

Upgrade to Dimension v2.2.2

You can upgrade to Dimension v2.2.2 directly from Dimension v2.2 or v2.2.1 only. It is not possible to upgrade from v2.1.2 Update 4 or lower directly to Dimension v2.2.1 or higher. You must upgrade to v.2.2 first. To upgrade to v2.2, go to Upgrade to Dimension v2.2.

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.

Estimated time to upgrade: < 8 minutes

1. From the WatchGuard Software Downloads Center, download the `watchguard-dimension_2_2_2_apt.tgz` upgrade file.
2. In a web browser, connect to your existing instance of Dimension at `https://<IP address of Dimension>`, and log in.
3. Select **System Settings**.
   The System Settings page opens.
4. In the **System Maintenance** section, click **Upgrade**.
   The Upgrade Dimension dialog box opens.
5. Click **Choose File** and select the Dimension upgrade file `watchguard-dimension_2_2_2_apt.tgz`.
6. Click **OK**. Wait for the upgrade to complete.
   If the upgrade requires the Dimension services to restart, you will be redirected to the Login 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, select **System Settings > Dimension System Information** and make sure that the **Version** is 2.2.2 (684479).

Operating System Requirements

To send log messages to Dimension, your Firebox must:

- Run Fireware v11.x or higher
- Have a current Support subscription

For more information, go to Set Up & Administer Dimension in *Fireware Help*.

You can install Dimension on Hyper-V or VMware.

Hyper-V

- WatchGuard Dimension is distributed as a VHD file for installation on Hyper-V for Microsoft Windows Server 2019 or 2022, and Hyper-V Server 2019. For more information, go to Install Dimension on Hyper-V.

VMware

- WatchGuard Dimension is distributed as an OVA file for installation on VMware ESXi 6.5, 6.7, 7.0, or 8.0. For more information, go to Install Dimension on VMware.

For detailed installation instructions, including system memory allocation requirements and instructions to determine disk size for storage, go to Install WatchGuard Dimension.

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. You can purchase Dimension Command licenses 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 might have 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 view reporting data related to Fireware policies you must enable logging in your policies. To view reporting data for your subscription services (WebBlocker, spamBlocker, Gateway Antivirus, IntelligentAV, 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 runs 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