WatchGuard Dimension™ v2.3 Release Notes

Build Number	717220
Release Date	29 May 2025
Release Notes Revision Date	13 November 2025

Introduction

WatchGuard is pleased to announce the release of Dimension v2.3. This release updates the version of the Ubuntu operating system used by Dimension and also includes bug fixes.

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*.

Enhancements and Resolved Issues in Dimension v2.3

Enhancements

- This release updates the version of Ubuntu used by Dimension to v24.04 LTS. *[FBX-28616]*

Resolved Issues

- Dimension now successfully retrieves the Filter-Id (RADIUS attribute 11) when RADIUS Access-Accept includes the Message-Authenticator attribute. *[FBX-29524]*

Known Issues and Limitations

Known issues for Dimension v2.3 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 v2.3.

Upgrade to Dimension v2.3

To upgrade to Dimension v2.3, we strongly recommend you deploy a new instance. This upgrades the operating system to Ubuntu v24.04 LTS. If you do not deploy a new Dimension v2.3 instance, you will not be able to upgrade to future Dimension releases.

Ubuntu v20.04 LTS reached end-of-life (EOL) in April 2025. When you deploy a new instance of Dimension v2.3, you also upgrade to the newer version of Ubuntu (v24.04 LTS), which is necessary for security updates and for future Dimension upgrades.

To upgrade to future Dimension releases with an upgrade file, you must run a Dimension v2.3 instance that you deployed through the OVA template. To confirm this, select **System Settings > Dimension System Information** and make sure that the Linux version is v6.8.x.

Before You Begin

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

Because of a database schema update, to migrate the Dimension database to a new Dimension instance, or to connect your new Dimension instance to an external database, you must have Dimension v2.1.2 Update 4 installed.

Upgrade from Dimension v2.1.2 Update 4 or Higher to Dimension v2.3

To upgrade from Dimension v2.1.2 Update 4 or higher to Dimension v2.3:

1. Deploy a new v2.3 instance. For detailed instructions about how to install a new Dimension instance on VMware or Hyper-V, see Install WatchGuard Dimension.

You must complete the Setup Wizard for the new Dimension v2.3 instance before you migrate your data. If you migrate your existing database disk to the new instance before you run the Setup Wizard, all data is deleted.

When you run the Setup Wizard on the new Dimension instance, you must set the Log Server Authentication Key to the same one that was set on your old instance. The key is not stored on the data disk.

2. Migrate your database to the new v2.3 instance. For more information about how to migrate your database, see Move the Dimension Database to a New Dimension Server.

If you are running an external database, follow the steps in Move External Dimension Database in VMware or Hyper-V.

Upgrade from Dimension v2.1.2 Update 3 or Lower to Dimension v2.3

If you have Dimension v2.1.2 Update 3 or lower installed, you must complete the steps below to upgrade to Dimension v2.3. You must upgrade to Dimension v2.1.2 Update 4, then deploy Dimension v2.3 and migrate your data to the new v2.3 instance. After you complete these steps, you will have a Dimension v2.3 instance that runs Ubuntu v24.04 LTS and uses your migrated database.

To upgrade your instance of Dimension from v2.1.2 Update 3 or lower to Dimension v2.3, you must complete these steps:

1. From the WatchGuard Software Downloads Center, download the `watchguard-dimension_2_1_2_U4_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_1_2_U4_apt.tgz`.
6. Wait for the upgrade to complete.
   If the upgrade requires the Dimension services to restart, you will be redirected to the Login page.
7. 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).

If your v2.1.2 Update 4 upgrade fails, go to Upgrading from Dimension 2.1.2 to Dimension 2.1.2 Update 4 fails due to lack of free disk space.

8. Deploy a new v2.3 instance and complete the Setup Wizard with an empty database. For more information, go to Install WatchGuard Dimension.

You must complete the Setup Wizard for the new Dimension v2.3 instance before you migrate your data. If you migrate your existing database disk to the new instance before you run the Setup Wizard, all data is deleted.

When you run the Setup Wizard on the new Dimension instance, you must set the Log Server Authentication Key to the same one that was set on your old instance. The key is not stored on the data disk.

9. Migrate your database to the new v2.3 instance. For more information, go to Move the Dimension Database to a New Dimension Server.

If you are running an external database, follow the steps in Move External Dimension Database in VMware or Hyper-V.

Dimension Command

Because the web server certificate is unique to each Dimension instance, to restore Dimension Command tunnels after migrating a database to a new instance, you must download the management settings (.wgd) file and import it to each Firebox or FireCluster. For more information, see Add a Firebox to Dimension for Management.

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, VMware, and Proxmox.

Hyper-V

- WatchGuard Dimension is distributed as a VHD file for installation on Hyper-V for Microsoft Windows Server 2019, 2022, or 2025, 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.

Proxmox

- WatchGuard Dimension is distributed as an OVA file for installation on Proxmox VE v9.0.1 or higher. For more information, go to Install Dimension on Proxmox.

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