WatchGuard Dimension™ v2.1.1 Update 2 Release Notes

Build Number	549365
Release Date	20 December 2017
Release Notes Revision Date	20 December 2017

On 20 December 2017, WatchGuard released Dimension v2.1.1 Update 2 as a maintenance release. For information on the issues addressed in this update, see the Resolved Issues section. For more detailed information about the feature enhancements and functionality changes included in Dimension v2.1.1 Update 2, see the product documentation or review What's New in Dimension v2.1.1 Update 2.

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.

If you are interested in installing Dimension in Amazon Web Services, please contact WatchGuard Technical Support by opening a technical support case.

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.

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.

System Requirements

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 this document and in Fireware Help.

Dimension on VMware

Dimension is distributed as an OVA file for installation on VMware ESXi 5.x or 6.x. The vSphere client is used to provision and install the OVA file. We do not support the use of VMware client, Player, or any other non-ESXi server/client mechanisms to deploy the Dimension OVA file.

Dimension on Hyper-V

Dimension is distributed as a VHD file for installation on Hyper-V for Microsoft Windows Server 2008 R2, 2012, or 2012 R2. To deploy the VHD file, you can use a Hyper-V Manager on Microsoft Server, or another Hyper-V environment.

PostgreSQL Compatibility

Dimension installs by default with a PostgreSQL database, v9.2.8. If you choose to use an external PostgreSQL database, Dimension supports v9.2 or higher.

Browser Compatibility

The WatchGuard Dimension web UI supports the following browsers:

- Firefox v22 and later
- Internet Explorer 9 and later
- Safari 5 and later
- Safari on iOS 6 and later
- Chrome v29 and later
- Microsoft Edge

Upgrade to Dimension v2.1.1 Update 2

> You can upgrade to Dimension v2.1.1 Update 2 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_U2_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 (login required) 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 2 (549365).

Installation Instructions for VMware

WatchGuard Dimension is distributed as an OVA file for installation on VMware ESXi 5.x or 6.x (64-bit required). WatchGuard recommends you use the VMware vSphere Client to provision and install the OVA file.

After you install and start the virtual machine in vSphere, you run the web-based WatchGuard Dimension Setup Wizard to configure the basic settings for your new instance of Dimension.

Before You Begin

Before you can deploy the Dimension OVA file and set up your Dimension VM, you must:

- Download the WatchGuard Dimension OVA file.
  Download the `watchguard-dimension_2_1_1_U2.ova` file to install WatchGuard Dimension on your ESXi v5.x or v6.x host.
- Have a DHCP server configured in the network you choose for the Dimension virtual machine, if you want to use a DHCP server to get the initial IP address for Dimension. You can also manually set a static IP address for Dimension (instructions to set a static IP address are included in the *Dimension* section of the *Fireware Help*. You then use this initial IP address to connect to Dimension to run the Dimension Setup Wizard and complete your Dimension configuration.
- Have an ESXi host configured where you can deploy your Dimension VM.

Install the Dimension Virtual Machine

To deploy the WatchGuard Dimension VM:

1. Open VMware vSphere Client and connect to your ESXi host.
2. Select **File > Deploy OVF template**.
3. Browse to the location of the `watchguard-dimension_2_1_1_U2.ova` file you downloaded. Click **Next**.
4. On the **OVF Template Details** page, click **Next**.
5. Click **Accept** to accept the End User License Agreement. Click **Next**.
6. In the **Name** text box, type a descriptive name for your Dimension VM. Click **Next**.
7. Select an option for disk provisioning. Click **Next**.
   You can select any of the options to provision your disk, but WatchGuard recommends that you select **Thick Provision Lazy Zeroed**. This is the default option, provides more predictable performance, and enables the VM to increase the disk size as necessary.
8. On the **Network Mapping** page, select the destination network for the virtual machine.
   Make sure you select a network with a DHCP server.
   Click **Next**.
9. Verify your settings and click **Finish**.
   Your new Dimension VM appears in the vSphere Client.

When you deploy the OVF template to install the Dimension VM, the template automatically configures the amount of system memory for the VM. If you manually change the system memory value in the VM settings, make sure to specify a value of 2GB or higher.

> If you use an older version of the vSphere client, the .ova file may show an indicator that it is not correctly signed. This does not affect the installation of the client and this indicator does not show if you use a newer vSphere client such as v6.0.0.0.

Review the Dimension VM Settings

After you have deployed your new Dimension VM, you can power on the VM, review the settings for the VM, and find the IP address to use to connect to the WatchGuard Dimension web UI to run the Dimension Setup Wizard.

In the vSphere Client:

1. In the ESXi host tree, select the Dimension VM.
2. Select the **Summary** tab.
3. In the **General** section, review the settings for the VM and make sure everything is correct.
4. In the **Commands** section, power on Dimension.
   It can take a few moments for the Dimension VM to start up and get an IP address from the DHCP server.
5. In the **General** section, find the IP address for Dimension.
   This is the IP address you use to connect to the WatchGuard Dimension web UI to launch the Dimension Setup Wizard .

Run the WatchGuard Dimension Setup Wizard

After your Dimension VM is set up and powered on, you can connect to Dimension to run the Dimension Setup Wizard and complete the configuration for your Dimension system.

Before you start the Setup Wizard, make sure you have this information to add in the wizard:

- Host name for Dimension
- IPv4 address and settings for the Eth0 interface
- Administrator passphrase
- Log Server encryption key
- (Optional) External Log Server database location
- (Optional) Public FQDNs or IP addresses

To run the Dimension Setup Wizard:

1. Open a web browser and connect to Dimension at `https://<Dimension IP address>`.
   For example, if the IP address assigned to your instance of Dimension is 203.0.113.201, you connect to Dimension at `https://203.0.113.201`.
   The login page appears.
2. Type the default user credentials:
   - **User Name** — admin
   - **Passphrase** — readwrite
   You will change the administrator passphrase when you run the Setup Wizard.
3. Complete the wizard to configure Dimension.

   If you specify a static IP address for Dimension, when you click **Next**, you will be notified that you must log in to Dimension at the new IP address to complete the Wizard. Click the link to the new, static IP address to log in to Dimension again. It might take a few moments for Dimension to load at the new IP address.
   After you finish the wizard, the Dimension login page appears.
4. Use the new administrator passphrase that you specified in the wizard to log in to Dimension.

After you have completed the wizard and logged in to Dimension, you can complete the configuration settings for your Dimension system and Log Server, create report schedules, and manage users, as described in the *Dimension* section of the *Fireware Help*.

About the Dimension Database

The Dimension VM is deployed by default with a data disk size of 40GB. The data disk is fully reserved for the log database and the related overhead space required by PostgreSQL. After the Dimension VM is deployed, the data disk size cannot be reduced. If you want to limit the size to be less than 40GB, you must use this procedure before you power on the VM for the first time to avoid data loss:

1. In the Dimension VM Summary tab in the vSphere Client, click **Edit Settings**.
2. Delete **Hard Disk 2**.
3. Add a new Hard Disk with the appropriate size. Make sure **SCSI (0:1**) is selected in the Virtual Device Node section (this is the default selection).

The Dimension database maximum size is automatically set based on the size of the VM's data disk. Currently it is set to approximately 80% of the total file system size on the data disk, reserving some space for PostgreSQL's own disk space requirements to handle large queries and temporary tables. If you want to increase the database size, you can resize the data disk using vSphere and reboot. The reboot is necessary because the disk size increase is not made visible to the guest VM until the reboot occurs.

Installation Instructions for Hyper-V

WatchGuard Dimension is distributed as a VHD file for installation on Hyper-V for Windows Server 2008 R2, 2012, or 2012 R2 (64-bit required). WatchGuard recommends you use the Microsoft Server Hyper-V Manager to install your Dimension VM, but you can choose to use another Hyper-V environment.

To install Dimension on Hyper-V, you must complete these steps:

1. Deploy and start the Dimension virtual machine.
2. Add a data disk (IDE or SCSI) to use as the Dimension data disk.
3. Start the Dimension VM.
4. Run the web-based WatchGuard Dimension Setup Wizard to configure the basic settings for your new instance of Dimension.

Before You Begin

Before you can deploy the Dimension VHD file and set up your Dimension VM, you must:

- Download the WatchGuard Dimension VHD file.
  Download the `watchguard-dimension_2_1_1_U2_vhd.zip` file and extract the `watchguard-dimension_2_1_1_U2.vhd` file to install WatchGuard Dimension on your Hyper-V server.
- Have a DHCP server configured in the network you choose for the Dimension virtual machine, if you want to use a DHCP server to get the initial IP address for Dimension. You can also manually set a static IP address for Dimension. You then use this initial IP address to connect to Dimension to run the Dimension Setup Wizard and complete your Dimension configuration.
- Have Hyper-V installed on a server where you can deploy your Dimension VM.

Install the Dimension Virtual Machine

When you install the Dimension VM, you must allocate the minimum amount of startup memory for Dimension. Dynamic memory allocation is not supported.

To deploy the WatchGuard Dimension VM:

1. On your Windows server, launch Hyper-V Manager.
2. In the Hyper-V Manager tree, right-click your Hyper-V server and select **New > Virtual Machine**.
   The New Virtual Machine wizard appears, with the Before You Begin page selected.
3. Read the instructions for the wizard and click **Next**.
   The Specify Name and location page appears.
4. In the **Name** text box, type a descriptive name for this instance of Dimension.
5. To store the virtual machine in a folder other than the default folder, select the **Store the virtual machine in a different location** check box. Click **Browse** and select the location to store the virtual machine.
6. Click **Next**.
   For Server 2012 R2 , the Specify Generation page appears.
7. *(2012 R2)* On the **Specify Generation** page, select **Generation 1**. Click **Next**.
   The Assign Memory page appears.
8. In the **Startup memory** text box, type the amount of memory to allocate to your Dimension VM. You must allocate a minimum of 2048 MB. Click **Next**.
   The Configure Networking page appears.

9. From the **Connection** drop-down list, select the virtual network adapter to use for the external interface, Eth0. Click **Next**.
   The Connect Virtual Hard Disk page appears.
10. Select **Use an existing virtual hard disk**.
11. Click **Browse** and select the location where you saved the Dimension VHD file.
12. Click **Next**.
    The Summary page appears.
13. Review the settings you specified for this instance of Dimension. Click **Finish**.
    The Dimension VM appears in the Virtual Machines list.

Add a Hard Disk to the Dimension VM

After you have deployed your Dimension VM, you must add a new virtual hard disk to the Dimension VM for the Dimension Log Server log database. You can add either a SCSI or an IDE virtual hard drive, but we recommend SCSI.

Option 1 — Add a SCSI Virtual Hard Disk

If you choose to add a SCSI virtual hard drive, for the most flexibility, make sure to add a dynamically expanding hard disk.

From the **Virtual Machines** list:

1. Right-click your Dimension VM and select **Settings**.
   The Settings page for your Dimension VM appears.
2. Select **Add Hardware > SCSI Controller** and click **Add**.
   The SCSI Controller page appears.
3. Select **Hard Drive** and click **Add**.
   The Hard Drive page appears.
4. In the **Media** section, select **Virtual hard disk** and click **New**.
   The New Virtual Hard Disk Wizard appears, with the Before You Begin page selected.
5. Read the instructions for the wizard and click **Next**.
   The Choose Disk Format page appears.
6. Select **VHD** or **VHDX**. Click **Next**.
   The Choose Disk Type page appears.
7. Select **Dynamically expanding**. Click **Next**.
   The Specify Name and Location page appears.
8. In the **Name** text box, type a descriptive name for this virtual hard disk.
9. To specify a location for the hard disk other than the default location, click **Browse** and select a location.
10. Click **Next**.
    The Configure Disk Size page appears.
11. Select **Create a new blank virtual hard disk**.
12. In the text box, type the size for the virtual hard disk in GB.
    Select a minimum of 40 GB.
13. Click **Next**.
    The Summary page appears.
14. Review the settings you specified for the hard disk. Click **Finish**.
    The wizard completes and the Hard Drive page in the Dimension VM Settings appears.
15. Click **OK**.
    The Settings dialog box closes.

Option 2 — Add an IDE Virtual Hard Disk

From the **Virtual Machines** list:

1. Right-click your Dimension VM and select **Settings**.
   The Settings page for your Dimension VM appears.
2. Select **Add Hardware > IDE Controller 0** and click **Add**.
   The IDE Controller page appears.
3. From the **IDE Controller 0** list, select **Hard Drive** and click **Add**.
   The Hard Drive page appears.
4. Select **Virtual hard disk** and click **New**.
   The New Virtual Hard Disk Wizard appears, with the Before You Begin page selected.
5. Read the instructions for the wizard and click **Next**.
   For Server 2008, the Choose Disk Type page appears. For Server 2012 and 2012 R2, the Choose Disk Format page appears.
6. *(Server 2012 and 2012 R2)* Select **VHD** or **VHDX**. Click **Next**.
   The Choose Disk Type page appears.
7. Select **Dynamically expanding**. Click **Next**.
   The Specify Name and Location page appears.
8. In the **Name** text box, type a descriptive name for this virtual hard disk.
9. To specify a location for the hard disk other than the default location, click **Browse** and select a location.
10. Click **Next**.
    The Configure Disk Size page appears.
11. Select **Create a new blank virtual hard disk**.
12. In the text box, type the size for the virtual hard disk in GB.
    Specify a minimum of 40 GB.
13. Click **Next**.
    The Summary page appears.
14. Review the settings you specified for the hard disk. Click **Finish**.
    The wizard completes and the Hard Drive page in the Dimension VM Settings appears.
15. Click **OK**.
    The Settings dialog box closes.

Start the Dimension VM

After you add a virtual hard disk to your Dimension VM, you can start the Dimension VM.

1. From the Hyper-V Manager **Virtual Machines** list, select your Dimension VM.
2. Right-click the Dimension VM and select **Start**.
   The Dimension VM starts.

Find the External IP Address

If the external network has a DHCP server, the Dimension external interface is automatically assigned an IP address. If you want to assign a static IP address for Dimension, you can find the instructions in the *Dimension Help*. To find the DHCP-assigned IP address to use to connect to the Dimension, you can use the command line.

To use the command line to find the IP address for Dimension:

1. In the **Virtual Machines** list , select the Dimension VM.
2. Right-click the VM and select **Connect**.
3. At the login prompt, type `wgsupport`. Press **Enter** on your keyboard.
4. At the passprhase prompt, type `readwrite`. Press **Enter** on your keyboard.
   This is the default admin account passphrase. A prompt to change the passphrase appears.
5. Type the new passphrase to use for the *wgsupport* account. Press **Enter** on your keyboard.
   The passphrase is changed.
6. To show the IP address for the external interface again, type `ifconfig` or `ip addr`. Press **Enter** on your keyboard.
   The IP address for the external interface appears.
7. To log out, type `exit`. Press **Enter** on your keyboard.

Run the WatchGuard Dimension Setup Wizard

After your Dimension VM is set up and powered on, you can connect to Dimension to run the Dimension Setup Wizard and complete the configuration for your Dimension system.

Before you start the Setup Wizard, make sure you have this information to add in the wizard:

- Host name for Dimension
- IPv4 address and settings for the Eth0 interface
- Administrator passphrase
- Log Server encryption key
- (Optional) External Log Server database location
- (Optional) Public FQDNs or IP addresses

To run the Dimension Setup Wizard:

1. Open a web browser and connect to Dimension at `https://<Dimension IP address>`.
   For example, if the IP address assigned to the external interface of your instance of Dimension is 203.0.113.201, you connect to Dimension at `https://203.0.113.201`.
   The login page appears.
2. Type the default user credentials:
   - **User Name** — admin
   - **Passphrase** — readwrite
   You will change the administrator passphrase when you run the Setup Wizard.
3. Complete the wizard to configure Dimension.

   If you specify a static IP address for Dimension, when you click **Next**, you will be notified that you must log in to Dimension at the new IP address to complete the Wizard. Click the link to the new, static IP address to log in to Dimension again. It might take a few moments for Dimension to load at the new IP address.
   After you finish the wizard, the Dimension login page appears.
4. Use the new administrator passphrase that you specified in the wizard to log in to Dimension.

After you have completed the wizard and logged in to Dimension, you can complete the configuration settings for your Dimension system and Log Server, create report schedules, and manage users, as described in the *Dimension* section of the *Fireware Help*.

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]*

WatchGuard Technologies, Inc.

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.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard website at http://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