WatchGuard Dimension™ v1.0 Release Notes

Build Number	432456
Revision Date	October 15, 2013

WatchGuard Dimension is the next-generation cloud-ready management solution for our Unified Threat Management (UTM) appliances. With Dimension, you get innovative, insightful, and interactive dashboard views of your network security, as well as visual and responsive logging and reporting. New features include:

- New ways to visualize network data
- Dashboards with simple drill-down into detailed log and report information
- A new flexible deployment model that can be deployed on-premise, or in a private cloud or public cloud.
- Customizable reports that can be sent to different users via e-mail automatically on a pre-defined schedule

You now have a choice. You can continue to use the standard WatchGuard System Manager Log Server/Report Server functionality to monitor the activity of your XTM device. Or, you can use WatchGuard Dimension and its intuitive, interactive interface to take advantage of our new, innovative set of visibility tools and a simplified report console.

WatchGuard Dimension includes new dashboards that are designed to complement the real-time Front Panel and FireWatch visibility tools in Fireware XTM v11.8 Web UI. WatchGuard Dimension's Executive, Security, Threat Map and FireWatch dashboards provide similar user experiences but add the ability to report on historical data.

WatchGuard Dimension highlights include:

- **Executive Dashboard** - provides insightful views to monitor and analyze network security related to user, application and threat activity.
- **Security Dashboard** - provides an interactive experience for exploring denied connections.
- **Threat Map** - uses IP address geolocation to build a visualization of the dangers in our connected world.
- **FireWatch** - an interactive report tool that groups, aggregates, and filters firewall traffic in an easy-to-understand form. FireWatch includes many options to pivot, drill-down, and filter firewall connections.
- **Executive Summary Report** - shows a high level summary of network use and blocked threats for a given period. The report can be viewed or scheduled for email delivery.
- **Standard XTM reports** - including compliance reports for PCI and HIPAA, Web reports, Application Control reports, Authentication reports, and more.

For more information about WatchGuard Dimension, review the product Help or the Introduction to WatchGuard Dimension presentation.

Browser Compatibility

WatchGuard Dimension Web UI supports the following browsers:

- Firefox v22 and later
- Internet Explorer 9 and later
- Safari 5 and later
- Safari on iOS6 and later
- Chrome v29 and later

Additionally, you can successfully use the WatchGuard Dimension Web UI on most mobile phone and tablet devices.

Installation Instructions

WatchGuard Dimension is distributed as an .ova file for installation on VMWare ESXi 5.x (64-bit required). The vSphere client is used to provision and install the .ova file. We do not recommend that you use VMWare Client, Player, or any other non-ESXi server/client mechanisms to deploy the Dimension .ova. There is a web based wizard that is used to configure WatchGuard Dimension after you install and start the virtual machine in vSphere.From the WatchGuard Portal > Articles & Software tab, find and download the `watchguard-dimension_1_0.ova` file to install WatchGuard Dimension on your ESXi v5.x host.

Use these instructions to deploy WatchGuard Dimension and start the Dimension Setup Wizard:

1. Open vSphere and connect to ESXi. Select **File > Deploy OVF template**.
2. Browse to the location of the `watchguard-dimension_1_0.ova` file you downloaded from the WatchGuard Portal. Click **Next**.
3. On the **OVF Template Details** page, click **Next**.
4. Accept the End User License Agreement. Click **Next**.
5. Name your VM and click **Next**.
6. Select any option for disk provisioning and click **Next**.
7. On the **Network Mapping** page,select the destination network for the virtual machine you want to create. There must be a DHCP server in the network you choose for the virtual machine. Dimension must get its initial IP address with DHCP. When the Dimension VM successfully obtains an IP address, you can see this IP address in the Dimension VM Summary tab > General pane in the vSphere client.
8. Click **Next**.
9. Verify your settings and click **Finish**. Power on your device.
10. Connect to `https://<hostIP>` to launch WatchGuard Dimension. Use the default credentials of *admin/readwrite*. You will change this administrator passphrase during the Setup Wizard. You also configure these settings:
    a. Host name
    b. IPv4 settings for Eth0
    c. Log encryption key

About the Dimension Log Server 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 log 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.

XTM Device Configuration Requirements

WatchGuard Dimension can accept log messages and generate reports for any device running Fireware XTM. WatchGuard Dimension can also accept log messages from WatchGuard System Manager Management Server and the Quarantine Server.

In the WatchGuard Log Server configuration settings, use the IP address and log encryption key you used when you set up WatchGuard Dimension. Use this same IP address and log encryption key in your WatchGuard Server Center settings.

Log-to-Report Mapping

Some reports rely on particular log messages that must be enabled in your XTM device configuration. The following table includes all log messages that should be sent from an XTM device to WatchGuard Dimension for different types of reports. The table shows which report categories use the associated log message.

Logs	Reports	Dashboards
Packet Filter Allowed Logs	Web, Packet Filter, Top Client, Application Control	Executive, Threat Map, FireWatch
Packet Filter Denied Logs	Web, Packet Filter, Denied Packet, Top Client, Application Control	Security, Threat Map
Intrusion Prevention Logs	IPS, Denied Packet	Security, Threat Map
Always On/Enabled by default	Authentication/Audit	
All Proxies: 'Enable logging for reports'	Gateway AV, IPS, SPAM, Application Control, DLP	Executive, Security, Threat Map, FireWatch
* HTTP Proxies: 'Enable logging for reports'	Web, Firebox Statistics, RED	Executive, Security, Threat Map, FireWatch
FTP Proxies: 'Enable logging for reports'	Firebox Statistics	Executive, Security, Threat Map, FireWatch
SMTP Proxies: 'Enable logging for reports'	SMTP, Firebox Statistics	Executive, Security, Threat Map, FireWatch
POP3 Proxies: 'Enable logging for reports'	POP3, Firebox Statistics	Executive, Security, Threat Map, FireWatch
Any alarms	Gateway AV, Alarms	

** For Web Audit reports, make sure that WebBlocker Action > Categories: 'Log this action'is enabled.*

Known Issues and Limitations

Some planned Dimension functionality is not available in this initial v1.0 release:

- Backup to an external location. The backup/restore feature supports data backup only to local disk space in this release.
- Audit trail and log messages for administration activities.
- Schedule generation and publication of CSV files for detail reports to a remote location.
- Use of an external PostgreSQL database.

Known Issues

- WatchGuard does not support migration of log data from a Windows-based Log Server to WatchGuard Dimension.
- Dimension does not support the reverse DNS lookup of IP addresses in reports. If the XTM device has firewall authentication enabled, Dimension will display the user names instead of source IP addresses in reports.
- To make sure that you can see all fields in the UI correctly, you may need to disable Ad Block Plus, NoScript, or any other Java blocking browser plug-ins and extensions for the IP address of your Dimension instance. *[76994]*

- The dashboard and executive reports will include bandwidth data if it is available. Fireware XTM v11.7.x and earlier generated bandwidth data only for connections handled by proxy policies, if the underlying proxy action had logging for reports enabled . Fireware XTM v11.8 will also log this data for connections handled by packet filter policies, if logging for reports is enabled.*[56957]*
- When you print a PDF report, the top portion of the report is cropped. You can select the **Fit Size** or **Shrink Oversized Pages** option if you want to see this content. *[75833]*
- The Executive Dashboard may fail to load correctly in a Mac OS X/Safari 6 environment. *[76933]*
- The Web Audit and WebBlocker reports are shown as available when there are only allowed logs (for Web Audit) or denied logs (for WebBlocker) for a specified time period. *[75957]*
- In the PCI compliance report, the Gateway AV-Host report data shows on the Gateway AV-Protocol report and vice versa. *[76972]*
- You cannot specify a per-client filter for DLP rulenames in this release. *[76367]*
- The Intrusion Prevention Summary report is missing the category name, description and WatchGuard Security Portal link for signatures. *[76656]*
- Compliance reports for device groups may not be accurate. *[76996]*

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web 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