WatchGuard® XCS v10.1 Update 1 Release Notes

WatchGuard XCS Build	160201
Revision Date	February 9, 2016

Introduction

WatchGuard® is pleased to announce the release of WatchGuard XCS v10.1 Update 1.

This release resolves several issues reported by WatchGuard customers. See the Resolved Issues section below for a complete list of resolved issues.

This update requires that you have WatchGuard XCS v10.1 installed.

Before You Begin

Before you install this update release:

- For more information about how to configure WatchGuard XCS, from the Web UI, select **Support > Online Manual**.
- The latest versions of the product documentation are available at http://www.watchguard.com/wgrd-help/documentation/overview.

Download Software

If Security Connection is enabled, the software update is downloaded automatically to your XCS device. The update is not automatically installed. You must manually install software updates on the **Software Updates** page.

See the Install the Software Update section below for detailed instructions.

To download the software:

1. Go to the WatchGuard Software Download Center.
2. Select and download the WatchGuard XCS v10.1 Update 1 software.
   The file is called *xcs101_update_1.pf*.

Install the Software Update

To install this update release:

Back Up the WatchGuard XCS Configuration

1. Select **Administration > Backup/Restore > Backup and Restore.**
2. Select your backup method (**FTP**, **SCP**, or **Local Disk**), then click **Next**.
3. Select which information to back up. If you do not want to restore reporting data, clear the **Backup reporting db data** check box. We recommend you select all options.

   For the **FTP** and **SCP** methods, type your server information.
4. Click **Next** to confirm your selections.
5. Click **Create backup now**.

Install the Software Update

1. Select **Administration > Software Update > Updates**.
2. If you use Security Connection, the software update already appears in the **Available Updates** section.

   If you manually downloaded your software update:

   - Click **Browse** and select the software update.
   - Click **Upload**.
3. In the **Available Updates** section, select the software update.
4. Click **Install**.
   The device will restart when the installation is complete. This process may take several minutes.

To Install the Software Update in a Cluster

1. On all devices in the cluster, change the cluster run mode to **Standalone** mode.

We recommend that you stop message processing on any **Client** systems before you switch them to **Standalone** mode. This prevents the system from processing mail with a default configuration when you change the mode back to **Client**. The **Client** needs time to update its configuration from the **Primary** system when the **Client** is added to the cluster again after the update.

2. Install the update on the **Primary**, and then restart the device.
3. Change the run mode of the **Primary** device from **Standalone** back to **Primary** mode.
4. Install the update on the **Secondary**, and then restart the device.
5. Change the run mode of the **Secondary** system from **Standalone** back to **Secondary** mode.
6. Install the update on any **Client** devices, and then restart the device.
7. Change the run mode of the **Client** devices from **Standalone** back to **Client** mode.

Resolved Issues

- Brightmail settings can now be modified in a Centralized Management configuration set. *[56726]*
- Message History results now return a timeout message if the search takes longer than five minutes to complete. *[57660]*
- The Dashboard status of an alternate domain is now correctly checked and displayed if the DNSBL, RED, or UBL domain timeout mode is disabled. *[59058]*
- Outbound and Inbound virus statistics are now correctly displayed in reports. *[64971]*
- Permission errors no longer occur when a delegated domain administrator logs in to the WatchGuard XCS. *[71671]*
- Syslog now correctly sends logs to a syslog server after a cluster synchronization. *[81225]*
- Daily backups now correctly include reporting data. *[81367]*
- In certain cases, a backup could not be restored to a new XCS system. *[84181]*
- In the TLS settings, the allow SSL renegotiation option must be enabled if you allow SSLv2. *[84235]*
- The domain field for a mail route is no longer limited to 50 characters. *[85960]*
- The McAfee Antivirus engine is upgraded to version 5800. *[87417]*
- Delegated Domain Administration (DDA) quarantine management and access permissions are now correctly applied in a cluster. *[87605]*
- Mail is no longer temporarily rejected if you disable incoming queue monitoring after the significant queuing threshold is exceeded. *[87848]*
- The RAID status for LSI RAID controllers no longer reports a degraded status when RAID is rebuilding. *[87906]*
- The error message "Setting locale failed" no longer appears in the web server logs after you upload a root CA certificate bundle. *[88177]*
- FreeBSD security advisory FreeBSD-SA-15:25.ntp that identifies multiple NTP vulnerabilities is resolved. *[88367]*
- Attachment size limits are now correctly applied based on the proper size of the attachment. *[88440]*
- Mail processing now correctly starts after upgrading from version 10.0 to 10.1 in a cluster. *[88465]*
- Cluster systems running different XCS software versions no longer cause mail processing issues after configuration synchronization. *[88567]*
- Base64 encoded text/HTML messages are now correctly annotated in the proper format. *[88569]*
- Extra <CR> carriage return characters are no longer added to HTML annotations. *[88630]*
- Quarantine searches by a delegated domain administrator in a cluster can now find patterns with single quote or backslash characters. *[88631]*
- In certain cases after an upgrade to 10.1, the "Show Log" button did not appear for messages to view the corresponding log message. *[88668]*
- Configuration synchronization in a cluster no longer occurs when cluster systems run different XCS software versions. *[88869]*
- TLS settings in a Centralized Management global configuration set can no longer be applied on an Entity system. *[88928]*
- Comma characters in attachment filenames no longer result in formatting issues in CSV reports. *[88984]*
- The security advisory FreeBSD-SA-15:26.openssl that identifies multiple OpenSSL vulnerabilities is resolved. *[89026]*
- DMARC failure and aggregate report email addresses are now correctly validated. *[89027]*
- Kaspersky AntiVirus signatures now update correctly through an external proxy server. *[89228]*
- The security advisory FreeBSD-SA-16:07.openssh that identifies an OpenSSH vulnerability is resolved. *[89523]*

Known Issues and Limitations

Known issues, including workarounds where available, can be found on the WatchGuard website. To see Known Issues, log in to the WatchGuard website and use the filters available on the Technical Search > Knowledge base tab.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or 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