WatchGuard® XCS v10.1 Update 2 Release Notes

WatchGuard XCS Build	160607
Revision Date	June 10, 2016

Introduction

WatchGuard® is pleased to announce the release of WatchGuard XCS v10.1 Update 2.

This release provides these enhancements:

- Updates the web proxy server to add support for SHA-256 when resigning certificates for HTTPS content inspection.
- For enhanced security, SSL v2 support has been removed from the product.

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 Update 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 2 software.
   The file is called *xcs101_update_2.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

- Annotations are now inserted into base64 messages in the correct encoding when the messages are sent from mobile devices. *[55522]*
- Restoring a cluster backup to a secondary cluster system no longer causes "duplicate key value" errors in the system logs. *[62045]*
- PHP errors are no longer displayed when viewing a message with a null subject header in WebMail. *[69456]*
- Validation is improved so that you can no longer assign the same IP address to multiple network interfaces. *[76889]*
- Attachments with duplicate multi-part MIME boundaries are now correctly detected as a malformed message. *[82646]*
- Mail surge detection no longer counts some inbound messages towards the volume total that are from the same domain as outbound messages. *[82682]*
- Some special international characters in WebMail are now correctly displayed. *[82845]*
- The TLS specific site policy upload page now displays correctly with 1024x768 resolution. *[84361]*
- The backup and restore process now performs correctly after uploading large local disk backups over 2Gb in size. *[84527]*
- Log messages "gethostby*.gethostanswer" no longer appear in the message logs with DMARC enabled. *[88204]*
- Email addresses that start with an underscore or dash character are now allowed in user policy mappings. *[88865]*
- Message History results are now correctly displayed in ascending order on subsequent pages after the first results page. *[89633]*
- SPF checks no longer fail for IPv6 addresses. *[89744]*
- Alarm email notifications are now correctly generated for cluster Secondary systems. *[89805]*
- You can now correctly release a message from the quarantine preview page in the Google Chrome browser. *[89811]*
- Attachment Filename and Content Type options now work correctly as part of a nested Content Rule. *[90289]*
- Slash characters in the comments field of a Threat Prevention lists no longer result in incorrect IP address matches. *[90383]*
- The names of pattern filters in PDF reports no longer appear URL encoded. *[90491]*
- Annotations are now correctly appended to base64 encoded messages that contain an empty body. *[90609]*
- HTML message parts are now correctly annotated with an HTML annotation in base64 encoded messages. *[90611]*
- Long From headers no longer cause errors with SPF, DKIM, and DMARC processing. *[90776]*
- Previews of large quarantined messages now display correctly in a cluster quarantine. *[90864]*
- Trusted and Blocked Sender limits are now correctly applied when adding Trusted Senders from a spam summary notification. *[90922]*
- Security advisory FreeBSD-SA-16:17.openssl (CVE-2016-2107, CVE-2016-2105, CVE-2016-2106, CVE-2016-2109, CVE-2016-2176) is resolved. *[91039]*

Known Issues and Limitations

Known issues for WatchGuard XCS, including workarounds where available, can be found on the WatchGuard website.

To see the known issues:

1. Log in to the WatchGuard website at login.watchguard.com.
2. Click the Technical Search icon to go to the Technical Search page.

3. On the Technical Search page, select the **Knowledge Base** tab.
   Knowledge Base filters appear on the left side of the page.
4. To see known issues for a specific release, use these filters:
   - From the **Category** filters, select the **Known Issues** check box.
   - From the **Status** filters, select the **Open** check box.
   - From the **Product & Version** filters, expand the XCS version list and select the check box for v10.x.

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