WatchGuard® XCS v10.0 Update 2 Release Notes

WatchGuard XCS Build	140911
Revision Date	11 November 2014

Introduction

WatchGuard® is pleased to announce the release of WatchGuard XCS v10.0 Update 2. This update release provides several new features and enhancements, and resolves several issues reported by WatchGuard customers.

New Features and Enhancements

The WatchGuard XCS v10.0 Update 2 release provides these new features and enhancements.

Message History Saved Search and Scheduled Report

When you perform a message history search, you can now save the search parameters as a saved search. This option is useful to store message history searches that you perform on a regular basis, and enables you to schedule a saved message history search as a report.

To search the message history, save your search parameters, and schedule a report, select **Activity > History > Message History**.

- Type a name for the search and enter your search parameters.
- Click **Save Search** to save the message history search.
- Click **Schedule as Report** to create a scheduled message history report for this search.

To manage your saved searches, select **Activity > History > Saved Searches**.

New Message Quarantine Actions

The Message Quarantine page now enables you to perform additional actions on quarantined messages. In addition to the ability to preview, delete, and release quarantined messages, you can now perform these actions:

- **Move to Quarantine** — Move the quarantined message to the selected quarantine area.
- **Rescan and Release** — Perform an anti-virus scan of the quarantined message and release the message if no viruses are detected, or drop the message if viruses are detected. Kaspersky Anti-Virus must be licensed and enabled to scan a quarantined message.
- **SecureMail Encrypt and Release** — Encrypt the quarantined message with SecureMail Email Encryption and release the message to the original recipient. SecureMail Email Encryption must be licensed and enabled to encrypt the message.
- **Encrypt and Release** — Encrypt the quarantined message with the configured External Email Encryption server and release the message to the original recipient. External Email Encryption must be enabled to encrypt the message.

To manage quarantined messages, select **Activity > Queue/Quarantine > Message Quarantine**.

HTML Annotation Support

You can now enable and customize both plain text and HTML annotations that are appended to all outbound messages. The annotation is a global option that you can use to append legal and policy notices, disclaimers, or a custom mail footer to all messages leaving your organization. You can also use policies to enable separate annotations for different users, domains, and groups.

To enable and configure plain text and HTML annotations, select **Configuration > Mail > More > Annotation**.

Configurable SMTP Recipient Verification Timeout

You can now configure the timeout values for SMTP Recipient Verification. You may need to modify the timeout and retry values in environments where network latency and other factors such as the Microsoft Exchange default tarpit time, can cause an SMTP probe to timeout when attempting to contact an SMTP server.

To configure SMTP timeout values for recipient verification, select **Security > Anti-Spam > Connection Control**.

McAfee Anti-Virus Update Alarm

An alarm is now generated if a McAfee Anti-Virus update fails for any reason, for example, a communications timeout or blocked connection. Previously, an alarm was generated only when the Anti-Virus update servers could not be contacted.

Resolved Issues

This release contains a number of defect fixes for issues reported by WatchGuard customers. See the Resolved Issues section below for a complete list of resolved issues.

Before You Begin

Before you install this update release:

- Read the information in the Known Issues and Limitations section of these Release Notes.
- 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 www.watchguard.com/help/documentation.

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 manually:

1. Go to the WatchGuard Software Downloads page.
2. Select the XCS device for which you want to download software.
3. Select and download the WatchGuard XCS v10.0 Update 2 software.
   The file is called *xcs100_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, enter 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

- Logout events now correctly appear in the system history. *[55789]*
- The network configuration page now correctly validates the subnet mask field. *[66236]*
- SMTP LDAP authenticated relay no longer fails if the password contains 8-bit non-ASCII characters. *[66346]*
- Report expiry now correctly deletes generated report files and database data. *[73907]*
- The "Networks that Bypass Authentication" field is now correctly validated when you enable authentication with the Web Proxy. *[78573]*
- Dashboard content now loads correctly when logged in as a Tiered Admin user. *[79921]*
- Error messages no longer appear on the CM Manager system after a Centralized Management configuration synchronization. *[79975]*
- OpenSSL libraries are updated to resolve the "Heartbleed" vulnerability (CVE-2014-0160). *[80031]*
- Attachment Control now correctly detects the MIME type of attachment sub-documents. *[80235]*
- The DNS status of a server in the Dashboard system summary now displays correctly. *[80254]*
- Web Proxy scanner issues no longer cause ICAP errors for client browsers. *[80268]*
- File handle management problems no longer cause issues with the Web Proxy. *[80311]*
- Password information no longer appears in the authentication log for local accounts accessed through IMAP. *[80383]*
- FreeBSD Security Advisory FreeBSD-SA-14:08.tcp (CVE-2014-3000) is resolved. *[80472]*
- A backup from an XCS v9.2 Centralized Management system applied to an XCS v10.0 system now correctly restores certain feature settings. *[80626]*
- Mail is now correctly fetched from a local account with POP3. *[80638]*
- TCP port access is now correctly configured when POP3 access is enabled. *[81009]*
- Connectivity issues no longer occur when you upgrade from a previous version to v10.0 and configure an IPv6 interface. *[81112]*
- Multiple OpenSSL vulnerabilities identified by security advisory FreeBSD-SA-14:14.openssl (CVE-2014-0224 and CVE-2014-3470) are resolved. *[81138]*
- SSLv2 is no longer enabled for use with IMAPS. *[81139]*
- The Web Proxy no longer stops responding when accessing web sites with IP Portal Authentication and HTTPS deep inspection enabled. *[81221]*
- The Web Proxy cache process no longer exits unexpectedly. *[81237]*
- The system no longer attempts delivery over IPv6 for a system configured only for an IPv4 network. *[81586]*
- Single sign-on authentication no longer fails if a user is a member of many Active Directory groups. *[81631]*

Known Issues and Limitations

There are no known issues for this release.

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