WatchGuard® XCS v10.0 Update 3 Release Notes

WatchGuard XCS Build	150203
Revision Date	February 6, 2015

Introduction

WatchGuard® is pleased to announce the release of WatchGuard XCS v10.0 Update 3. 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 3 release provides these new features and enhancements.

Search Mail Routes

The Mail Routes page has been redesigned so you can more easily manage your mail routing entries. A new Search field enables you to search your mail routes and filter your display.

Upload TLS Site Specific Policies

The TLS mail encryption page has been redesigned so you can more easily manage your TLS site policy entries. A new Search field enables you to search your TLS site policies and filter your display. You can also download and upload a list of TLS site policies.

Disable HTTP Proxy Caching

You can now disable the caching functionality of the HTTP Proxy. In some high-volume environments, the web cache can grow to sizes that result in reduced cache performance. In these cases, we recommend you disable HTTP caching.

Microsoft Office 2013 Document Support for Content Scanning

Microsoft Office Word, Excel, and Powerpoint 2013 document types are now supported by the Content Scanning feature.

Treat Abused Redirector and URL Shortener Links as Spam in URL Block Lists

A **Treat redirector links as spam** option has been added to the URL Block List page. This option, when enabled, treats abused legitimate redirection and URL shortener links found in email messages and web sites as spam.

URL Block List Checks Based on Name Server Lookup

In addition to the ability to check URL links in spam messages and web sites based on their domain name or IP address, the URL Block Lists feature can now also check the name server (NS) records of URL links. This Name Server block list contains the names and IP addresses of DNS servers used to host domains that are sources of spam.

In the UBL Domains page, you can now specify the lookup type as "Domain", "IP Address", or "Name Server".

IP address and Name Server lookups can provide additional security by detecting sources of spam before specific spam domains are added to popular block lists.

To utilize these new UBL block lists, you must add them to your current configuration. All three types of lists can be used at the same time.

- ubl.dnsbl.borderware.com – Domain type (current default)
- ublip.dnsbl.borderware.com – IP Address type (works with all XCS versions)
- ublns.dnsbl.borderware.com – Name Server type (requires 10.0 Update 3 or higher)

Treat Messages with MIME Decoding Errors as Malformed

You can now treat any messages that contain MIME decoding errors as a malformed message. This option prevents messages from passing through the system when the attachments cannot be decoded and scanned because of MIME decoding errors. Enabling this option can increase the number of messages identified as malformed. If you quarantine malformed mail, this can impact resource use and increase the amount of quarantined mail that requires management and review. This option is disabled by default.

SecureMail Support for Recipient Local Key Servers

SecureMail encrypted messages sent from the WatchGuard XCS now support local SecureMail key servers at the recipient's domain for decryption of the message.

McAfee Anti-Virus Engine Upgrade

The McAfee Anti-Virus engine has been upgraded to the most recent version (5700) to provide the latest security against current and emerging virus threats.

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:

- 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 http://software.watchguard.com/.
2. Select **XCS and QMS Devices**.
3. Select **XCS**.
4. Select and download the WatchGuard XCS v10.0 Update 3 software.
   The file is called *xcs100_update_3.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

- The following FreeBSD Security Advisories are resolved:
  - FreeBSD-SA-14:19.tcp *[82445]*
  - FreeBSD-SA-14:18.openssl *[82446]*
  - FreeBSD-SA-14:23.openssl *[83072]*
  - FreeBSD-SA-14:24.sshd *[83073]*
  - FreeBSD-SA-14:28.file *[83616]*
  - FreeBSD-SA-14:29.bind *[83617]*
- New permitted clients added to the SNMP configuration are now correctly applied. *[75870]*
- Reports are now generated correctly when email addresses in the data contain special characters. *[79738]*
- You can now correctly view quarantined mail messages with the Google Chrome browser (v37 and higher). *[82531]*
- LDAP user imports from multiple sources no longer cause system latency. *[82702]*
- Invalid HTTP requests no longer cause processing issues with the HTTP Web Proxy scanner. *[82993]*
- Time zones for Russia have been updated. *[83138]*
- Attachments that contain certain types of control characters no longer cause issues with report generation. *[82040]*
- Validation of the HTTP Proxy allowed networks setting is now correctly applied. *[82151]*
- LDAP bind attempts no longer fail with direct LDAP lookup features such as LDAP recipients, aliases, and routing. *[82537]*
- HTTP Proxy authentication portal errors no longer occur when you attempt to authenticate after the installation of v10.0 Update 2. *[82676]*
- A stack buffer overflow vulnerability in ntpd is resolved (CVE-2014-9295 / VU#852879). *[83794]*

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