WatchGuard® XCS v10.0 Update 1 Release Notes

WatchGuard XCS Build	140312
Revision Date	11 November, 2014

Introduction

WatchGuard® is pleased to announce the release of WatchGuard XCS v10.0 Update 1. 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 1 release provides these new features and enhancements.

Block Password-Protected Attachments with Attachment Control

You can now control how password-protected file attachments are processed by the Attachment Control feature. You can use this feature if you have disabled the "Treat As Virus - Password-protected attachments" option in the Kaspersky Anti-Virus configuration, but still want control of how to process password-protected attachments. In some spam campaigns, viruses and malware are concealed within a password-protected attachment and the password is given to the user within the message itself. This feature allows you to block or strip this attachment before it reaches the end user's mailbox.

A new extension called **[password protected]** appears in the Attachment Control **Email File Extensions** types list. Configure the action for this file extension to *Allow*, *Block*, or *Strip* password-protected attachments. By default, this extension is set to "Allow".

You must have Kaspersky Anti-Virus enabled to be able to detect that an attachment is password-protected. The Kaspersky Anti-Virus "Treat as Virus - Password-protected attachments" option, if enabled, takes precedence over Attachment Control actions.

Dashboard and Menu Internationalization

You can now select the language in which to display the WatchGuard XCS menu system, the Dashboard page, and the Frequent Tasks page. Each Tiered Admin user can have their own specific language settings. The WatchGuard XCS currently supports English, French, Spanish, and Chinese (Simplified).

From the Web UI, select a language from the drop-down list in the top-right corner of the page. Choose **Auto-Select** to automatically detect the language based on the current browser settings.

Multiple Branding Profiles for SecureMail Email Encryption

You can now configure multiple branding profiles for SecureMail Email Encryption. Branding services allow you to display your organization's logo and branding text on all encrypted messages. With the addition of multiple profile support, you can configure a separate branding profile for each mail domain that you process mail on a per-policy basis. Your default primary branding profile is defined on the main SecureMail configuration page, and the use of other branding profiles can be defined in the SecureMail policy configuration located in a policy's Email settings.

Updated HTTP Proxy Engine

The WatchGuard XCS HTTP Proxy engine has been updated to provide the latest security and performance enhancements, and includes these new features:

- Improved IPv6 support
- Full support for HTTP 1.1

In addition, these changes have been made to the Web UI:

- The "Prefer IPv4 over IPv6" advanced network setting is now automatically enabled if you do not have any IPv6 interfaces configured.
- The "Ignore HTTP/1.1 Expect Header" advanced HTTP Proxy option is deprecated and has been removed.

Extended IPv6 Support

These WatchGuard XCS features now support IPv6:

- Web RED reputation lookups and URL Reputation
- Threat Prevention Status
- WatchGuard QMS Trusted/Blocked Senders List import

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 1 software. The file is called *xcs100_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, 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.

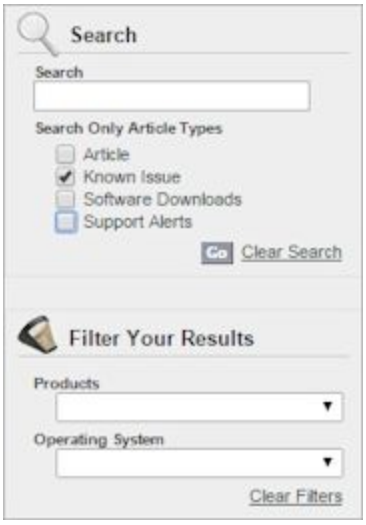
Resolved Issues

- The WatchGuard XCS now properly halts an LDAP users import operation if it is interrupted. *[54206]*
- The system now logs which tiered admin user releases a message from the message quarantine. *[54630]*
- 3ware RAID controller diagnostics information from XCS 770R and 970 systems now appear in a problem report. *[74684]*
- The Reports name filter drop-down list now properly displays full report type names. *[74685]*
- Web RED networking rules for IPv6 addresses are now properly synchronized to cluster members. *[76396]*
- Scanning issues no longer occur when the DNS Block List component is set to check all relays. *[76862]*
- Logs are now properly displayed when you view the log for a message on a clustered CM Manager system. *[76894]*
- Web RED reputation lookups and URL Reputation now fully support IPv6. *[76956]*
- Errors no longer occur in the DLP Wizard if a dictionary contains a single quote character in its name. *[77133]*
- The DLP Wizard now properly sets the default direction for certain types of rules. *[77134]*
- You can now properly assign a user policy if the user address contains a subdomain of a hyphenated domain. *[77231]*
- Weighted thresholds are now properly applied when using Spam Words for Outbound Anti-Spam scanning. *[77249]*
- You can now properly import the Trusted/Blocked Senders List from a WatchGuard QMS with an IPv6 address. *[77416]*
- The Message Header and Summary of Content sections now properly display for a message located on a remote system in a Cluster Quarantine. *[77496]*
- Content Scanning "InDictionary" matching now works properly when international document capability is disabled. *[77608]*
- Adaptec RAID controller diagnostics information now appear in a problem report. *[77644]*
- Web Proxy process crashes no longer occur due to memory issues. *[77649]*
- Executable files are now properly detected by Attachment Control as "application/x-dosexec" instead of "application/octet-stream". *[77670]*
- PHP page errors no longer appear when you edit a dictionary and there is a file location issue. *[77671]*
- Adaptec RAID Controller status now properly appears on the Dashboard System Summary page. *[77672]*
- The Spam Quarantine Disk Full expiry mode is applied properly when mail is expired from quarantine. *[77885]*
- Processing issues no longer occur when a message with a large number of addresses in the To: field is sent for DKIM signing. *[77985]*
- CPU resource issues no longer occur when you use a Content Scanning rule with a null regex rule condition. *[77860]*
- In certain cases, messages in the Spam Quarantine could not be processed correctly. *[78014]*
- You can now properly upload Content Rules from a previous XCS version to XCS v10.0. *[78086]*
- The XCS can now properly communicate with systems that use multicast MAC addresses. *[78153]*
- The HTTPS Deep Inspection Bypass Domains list is now properly configured if you add overlapping domains and subdomains. *[78222]*
- The Threat Prevention Status search field now accepts valid IPv6 address queries. *[78247]*
- You can now properly upload attachments to a new message with the WebMail interface. *[78298]*

- The correct custom notification text is now properly sent when you use custom actions in Content Rules. *[78388]*
- You can now properly add Domain and IP content to phrase list dictionary types. *[78428]*
- XCS local mailboxes no longer cause mailbox corruption when accessed from Apple-based mail clients. *[78613]*
- Memory errors no longer occur when you display a large number of groups on the Group Policy page. *[78618]*
- In certain cases, the Outgoing Connections counter displayed in the Mail Resources section of the Dashboard was not accurate. *[78900]*
- Intercept threshold values defined in a policy are now properly validated. *[78973]*
- The XCS is no longer identified as an open relay when SMTP Authenticated Relay is enabled. *[79270]*

Known Issues and Limitations

You can find information about known issues for this release, including workarounds, where available, , in the WatchGuard Knowledge Base. You must log in to the WatchGuard Portal to search for Known Issues. Known Issues are not available in the public version of the Knowledge Base. After you log in, you can use the filters available in the WatchGuard Portal > Knowledge Base tab to find articles about 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