WatchGuard® XCS v9.2 Update 5 Release Notes

WatchGuard XCS Build	130322
Revision Date	March 28, 2013

Introduction

WatchGuard® is pleased to announce the release of WatchGuard XCS v9.2 Update 5. This update release provides several new features and enhancements, and resolves several issues reported by WatchGuard customers.

New Features and Enhancements

The WatchGuard XCS v9.2 Update 5 release provides these new features and enhancements.

Custom Quarantines

You can now create your own custom quarantine areas for specific types of quarantined messages. For example, you can create a quarantine specifically for messages quarantined because of a virus, or messages quarantined because they violate a Data Loss Prevention (DLP) policy rule.

When you create a custom quarantine, each message security feature that supports the quarantine option provides a quarantine action for the primary system quarantine and any defined custom quarantines. For example, you can create a custom quarantine called "Virus", and then set the Anti-Virus feature action to use that quarantine action. All messages quarantined by the Anti-Virus feature will then appear in the "Quarantine: Virus" quarantine area.

Custom quarantines can be managed by a Tiered Administrator with the appropriate permissions. This allows you to assign administrators for specific quarantine areas. For example, for compliance purposes, you can assign a user the role of administrator for the DLP quarantine.

You can also configure independent message expiry options for each custom quarantines.

There are two default pre-defined quarantines:

- **System** — The primary system quarantine. All quarantined messages are stored here except messages stored in a custom quarantine.
- **DLP** — You can use the DLP quarantine to store messages quarantined by Data Loss Prevention features.

To add and configure a custom quarantine, select **Activity > Queue/Quarantine > Custom Quarantines**.

To view the contents of the system quarantine and any custom quarantines, select **Activity > Queue/Quarantine > Message Quarantine**.

DKIM (DomainKeys Identified Mail) Support

DKIM (DomainKeys Identified Mail) is an enhanced version of DomainKeys that provides a means for authenticating the source of an email by querying the sending domain's DNS records and authenticating a unique domain name identifier. The protocol allows server administrators to add a digital signature to their emails which can be validated by looking at their DNS records. By verifying the signature in the headers of the email using the public key in the DNS record, the receiving host can verify that the email is originating from the legitimate mail server for that domain, and prevents spammers from sending forged emails.

As an enhancement to DomainKeys, DKIM offers additional parameters to the signing mechanism for enhanced security and spoofing protection, and allows authorized third-party signing of messages for a domain independent from the message author. When you use DKIM signing, you have the option of using ADSP (Author Domain Signing Practice). ADSP is an extension to DKIM where the domain name of the signing entity is included as part of the Author Domain Signature to prove that it is authorized to relay mail messages for the sending author address.

To configure DKIM authentication of inbound messages, select **Security > Anti-Spam > DKIM Authentication**.

DKIM signing can be applied independently to outbound messages based on policies. To enable DKIM signing of outbound message globally, select **Configuration > Mail > DKIM/DomainKeys**. You can then use policies to configure the signing policy for each domain. DKIM signing options appear in the Email tab of a policy. Sample DKIM DNS records are provided on the selector configuration page for DKIM and ADSP support.

> ***Note*** *The WatchGuard XCS supports DKIM RFC 6376 and RFC 5617.*

Allowed HTTPS Proxy Ports List

You can now configure a list of non-standard HTTPS Proxy ports that are allowed through the Web Proxy. This option is available on the HTTP/S Proxy configuration page at **Security > Configuration > HTTP/S Proxy**. The standard HTTPS port 443 is included by default.

Web Proxy IP Authentication Redirect

When you use the Web Proxy IP Proxy or Portal Authentication modes, you can now choose to redirect to the authentication page using the hostname or IP address of the Web Proxy. Select **Hostname** if you use a CA-signed certificate on your system to prevent a certificate warning error in the client browser. Otherwise, use **IP Address**. You must make sure that you add the Web Proxy hostname or IP address to your local web browser's proxy exclusion list to prevent a local proxy loop when you access the authentication page.

Download Problem Report

The Problem Report feature allows you to send important configuration and log information via email to WatchGuard Technical Support to help troubleshoot an existing support incident. You can now download a local copy of the report from the Problem Reporting configuration page at **Support > Problem Reporting**.

Pattern Filter ID Number Search in Message History

The advanced Message History search now allows you to search by Pattern Filter ID numbers when you select the "only show messages where PBMF is..." option.

XCSv Upgrade from an Evaluation

You can now perform an upgrade from an evaluation XCSv installation to a production model XCSv without having to reinstall the system. To upgrade your XCSv evaluation installation:

1. Log in to the WatchGuard LiveSecurity activation web site at https://www.watchguard.com/activate.
2. Register your new XCSv production model serial number and get a new feature key.
3. On your current evaluation XCSv installation, select **Administration > System > Feature Key**.
4. Click **Manual Update**.
5. Paste the new feature key text into the **Update Feature Key** text box.
6. Click **Update Key**.

You must reboot the system if the change in XCSv model requires a change to the number of CPU cores supported.

You must also update your performance settings if you update the feature key with an XCSv model different than your evaluation model. To update your performance settings:

1. Select **Configuration > Network > Performance**.
2. From the **Performance Option** drop-down list, select **Email scanning**.
3. Click **Apply**.

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 http://www.watchguard.com/archive/softwarecenter.asp.
2. Log in to the WatchGuard Portal and click the **Articles & Software** tab.
3. Search to see all available **Software Downloads** articles and find the **WatchGuard XCS Software Downloads** article.
4. Select and download the WatchGuard XCS v9.2 Update 5 software. The file is called `xcs92_update_5.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.

> ***Note*** *The installation process can take several minutes to complete.*

To Install the Software Update in a Cluster

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

> ***Note*** *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

- Attachment Control processing issues no longer occur when scanning extraneous data objects extracted from PDF documents. *[54836]*
- You can now enable the Trusted/Blocked Senders Lists feature on a cluster system. *[59379]*
- Secondary systems in a cluster no longer send an SNMP restart trap after each cluster synchronization. *[60588]*
- Mail processing issues no longer occur when an incorrect selector is used for DomainKeys signing. *[61660]*
- LDAP user routing now works properly with the Active Directory proxyAddresses attribute. *[65699]*
- The Session Timeout field in the HTTP/S Proxy page authentication configuration now properly accepts hour values from 0 to 23. *[66260]*
- Connection reset errors no longer occur when connecting through the Web Proxy to web sites that validate X-Forwarded-For: headers. *[66279]*
- Memory size errors no longer occur when you download and save large messages stored in the system quarantine. *[68853]*
- User and Tiered Admin settings are now properly replicated to cluster secondary systems. *[69021]*
- Mail processing issues no longer occur on XCS 970/1170 models that use Adaptec RAID controllers. *[69083]*
- Dictionary file names now properly appear in the "Top Content Control Occurrences" report field if a dictionary was created via text. *[69094]*
- You can now add Attachment Control MIME types that use the "+" or "++" characters. For example, "+xml". *[69429]*
- SCP backups now properly connect if the SCP server has a banner enabled. *[69527]*
- In certain cases, configuration changes to the Web Proxy could cause virtual interfaces to stop functioning. *[69606]*
- Content Scanning internationalization now fully supports the EUC_KR (Korean) and GB2312 (Simplified Chinese) character sets. *[69726]*
- Content Scanning internationalization now works consistently for HTTP/HTTPS traffic through the Web Proxy. *[69883]*
- International dictionaries are properly synchronized to entities in a Centralized Management federation. *[69964]*
- Edited dictionaries now properly display in the UI after an upgrade from 9.2 Update 2 or previous version. *[69984]*
- Local changes to dictionaries on a Centralized Management entity system are no longer overridden during synchronization. *[70139]*
- Changes to a dictionary are no longer lost in the event of a dictionary configuration error. *[70205]*
- Specific message detail fields now display properly when you show the log file from the Message History page. *[70244]*
- Proper dictionary type and weight options are now displayed when you create dictionaries for Domain Reports and HTTP Trusted/Blocked Sites lists. *[70246]*
- The security advisory FreeBSD-SA-12:06.bind has been resolved. *[70278]*
- Performance issues no longer occur when using the SMTP method of recipient verification. *[70347]*
- You can now properly add and edit group policies on systems with a very large amount of imported user groups. *[70391]*
- Queue file write errors no longer occur when the Analyze PDF Text option is enabled in the Token Analysis feature. *[70413]*
- Attachment filenames with backslash characters now appear properly in reports. *[70664]*

- Attachment Control processing issues no longer occur when scanning extraneous table objects extracted from Microsoft Word documents. *[70833]*

Known Issues and Limitations

These are the known issues for this release. Where available, we include a way to work around the issue.

- If you previously used DomainKeys signing with a selector key size less than 1024, and then switch to DKIM signing after the installation of Update 5, the signing configuration uses the same key size which is less than the minimum default size for DKIM. This configuration results in an invalid DKIM signature. *[71252]*

> **Workaround**
> Make sure you adjust the selector key size to be a minimum of 1024, and then regenerate your keys after you switch to DKIM signing.

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