WatchGuard® XCS v10.1 Release Notes

WatchGuard XCS Build	151009
Revision Date	May 25, 2017

After you install WatchGuard XCS v10.1, make sure you install any additional software updates available for this release.

See these release notes for information about updates to WatchGuard XCS v10.1:

- WatchGuard XCS v10.1 Update 1 Release Notes
- WatchGuard XCS v10.1 Update 2 Release Notes
- WatchGuard XCS v10.1 Update 3 Release Notes
- WatchGuard XCS v10.1 OpenSSL Hotfix Release Notes
- WatchGuard XCS v10.1 OpenSSL Hotfix 2 Release Notes

Introduction

WatchGuard® is pleased to announce the release of WatchGuard XCS v10.1. This update release provides many new features and enhancements, and resolves several issues reported by WatchGuard customers.

New Features and Enhancements

The WatchGuard XCS v10.1 release provides these new features and enhancements.

Kaspersky Security Network Support

This release adds support for the Kaspersky Security Network and cloud protection when scanning messages for viruses. The Kaspersky Security Network (KSN) improves scanning effectiveness, reduces false positives, and protects against new threats by checking the reputation of files with Kaspersky cloud-based services. A file is first scanned with the local signature database, and if there is no match to an existing signature, an MD5 checksum of the file is sent to the Kaspersky Security Network for additional reputation checks with cloud-based data. Connections to the Kaspersky Security Network are performed over HTTPS port 443.

The Kaspersky cloud protection option is enabled by default.

DMARC Authentication Support

Domain-based Message Authentication, Reporting and Conformance (DMARC) is a mechanism that allows a message sender to indicate to the receiver that the sender's messages are protected by SPF and/or DKIM, and informs the receiver what action to perform if SPF and DKIM authentication fails for the message.
DMARC provides domain-specific feedback, including failure reports, to the sender to verify the accuracy of their published SPF and DKIM authentication configuration.

The XCS device can use DMARC authentication as part of your Anti-Spam configuration to authenticate incoming mail that uses SPF or DKIM, and send DMARC reports back to domain owners. You can use the results of DMARC processing as part of the overall Intercept Anti-Spam decision for the message, or you can use the specified action of the domain owner as published in their DMARC DNS records. This option is available on the **Security > Anti-Spam > Anti-Spam** page.

If you want to publish DMARC authentication records for your own organization's mail in your DNS, you can create your own DMARC DNS records on the **Activity > Status > Utilities** page.

Manage Trusted and Blocked Senders Lists

The WatchGuard XCS administrator can now view and manage all trusted and blocked senders created by end users. You can search and filter the display for specific users or senders, and view, edit, delete, and add entries.

SecureMail Email Decryption

You can now perform decryption of inbound SecureMail-encrypted email messages for message recipients that have their mail processed by the WatchGuard XCS. A new default pattern filter is available that searches for "X-IBE-Encrypted" in the mail header that identifies the message as encrypted by SecureMail. You can enable this pattern filter and use it in your configuration to identify and decrypt messages for your recipients.

SecureMail Server Alarm

You can now enable an alarm notification in the SecureMail configuration to generate an alarm if the SecureMail server cannot be contacted because of network issues or an outage with the SecureMail service. This alarm notification option is disabled by default.

Attachment Control Conditions for Content Rules

You can now use Attachment Control conditions in your Content Rules. This enables you to create conditions based on the attachment content type and attachment filename and extension. You can also search the attachment filename for *[passwordprotected]* to look for password-protected attachments with your content rules.

Detect Macros in Office Documents with Attachment Control

The Attachment Control feature can now detect macros inside of Microsoft Office document attachments. These attachments are detected with the content type of "application/x-vbscript".

If you want control the deliver of attachments that contain macros, create an Attachment Control content type called "application/x-vbscript" and select an action to perform on the attachment.

TLS 1.1 and 1.2 Support

TLS versions 1.1 and 1.2 are now supported and enabled by default for TLS mail delivery encryption, the XCS web server configuration, and POP/IMAP configuration. Earlier versions of SSL and TLS contain known security vulnerabilities, but may need to be enabled for compatibility with older email servers.

RC4 Ciphers Disabled

RC4 ciphers are now configurable and disabled by default for TLS mail delivery encryption, the XCS web server configuration, and the POP/IMAP configuration. RC4 ciphers contain known security vulnerabilities, and you should only enable RC4 ciphers for backwards compatibility.

SHA2 Algorithm for Certificate Generation

The default XCS system certificate and new self-signed certificates, including those generated for HTTPS content inspection, can now be generated with the SHA2 signature algorithm. The SHA1 algorithm is considered insecure and is slowly being phased out, and can result in web browser warnings for end users.

WatchGuard XCS Operating System Upgrade

The WatchGuard XCS secure operating system has been upgraded to provide the latest updates in security, performance, and hardware compatibility support.

Kaspersky Anti-Virus Upgrade

The Kaspersky Anti-Virus engine has been upgraded to the most recent version to provide the latest security against current and emerging virus threats. This upgrade also adds support for the Kaspersky Security Network.

SecureMail Email Engine Upgrade

The SecureMail Email Encryption engine has been upgraded to provide the latest software updates and add support for the SecureMail Email Decryption feature.

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 http://www.watchguard.com/wgrd-help/documentation/overview.

Download Software

To download the software:

1. Go to http://software.watchguard.com.
2. Select and download the appropriate WatchGuard XCS v10.1 software package:
    - **xcs101_upgrade.pf** — This is a software update file that you can upload directly to the XCS on the Software Updates page.
        - This is the recommended method to upgrade to v10.1.
        - You must be running WatchGuard XCS v10.0 Update 3 or higher to use this software upgrade method.
        - This method can be used for both XCS and XCSv.
    - **xcs-101.zip** — This package contains an upgrade image file (.img) and the BTIweb software so you can perform a network image upgrade from the system console.
        - This method requires a minimum version of WatchGuard XCS v9.2 Update 5 or higher.
    - **XCSv-101.ova** — This package contains an OVA template for an installation of XCSv v10.1 on VMware.
    - **XCSv-101-HyperV.zip** — This package contains the files required to install XCSv v10.1 on Microsoft Hyper-V.

Install the Software

There are two ways to install the XCS v10.1 software:

- Install the Software Upgrade from the Web UI — Use the software upgrade file packaged as a software update *(xcs101_upgrade.pf)*. You can install this file from the Software Updates page on the Web UI. You must be running WatchGuard XCS v10.0 Update 3 or higher to use this software upgrade method. This method can be used for both XCS and XCSv.
- Install the Software Upgrade from the Console — Use the full software image file *(xcs-101.img)* for a network upgrade installation from the system console. This method requires a minimum version of WatchGuard XCS v9.2 Update 5 or higher.

We recommend that you use the Web UI to upload the *xcs101_upgrade.pf* file on the Software Updates page to install this upgrade. This method preserves your system IP address and network information, admin login name and passwords, time zone information, and feature key. As part of the upgrade process, you will also be prompted to backup and restore your configuration.

If you install a full system upgrade, your current configuration and data will be deleted. Make sure you perform a backup of your system before you perform a full system upgrade.

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 Upgrade from the Web UI

You can install a full system upgrade from the **Software Updates** page. The upgrade is distributed as a *.pf* file just like a software update. When you upload a full system software upgrade, it appears in the *System Upgrades* section. When you perform a system upgrade, the system retains its original IP address and network settings, time zone, admin user logins and passwords, and feature key information. When the system restarts, you can connect to the system using its original IP address. You can then perform a restore of your configuration from backup.

You must be running WatchGuard XCS v10.0 Update 3 or higher to use this software upgrade method.

- This upgrade method requires that you have at least 2 GB free space in the *System Data Storage* disk area. To check your free disk space, select **Activity > Dashboard > System Summary > Disk Usage**.

- Any network interface specific features that you enabled before the upgrade (for example: Large MTU, Respond to Ping, Trusted Subnet, Admin & Web User Login, WebMail, SNMP Agent, Centralized Management, HTTP/HTTPS Proxy, Queue Replication, Bridging, and Transparent Mode) will be reset to the default setting. You must re-enable these options after the upgrade is complete.
- Cluster status is preserved, but the system will restart in Standalone mode after the upgrade. You must manually change the run mode to the system's previous mode, such as Primary, Secondary, or Client.

To install the software upgrade from the Software Updates page on the Web UI:

1. Select **Administration > Software Update > Updates**.
   The Software Updates page appears.
2. Click **Browse** and select the software upgrade file. The file name is `xcs101_upgrade.pf`.
3. Click **Upload**.
   The software update appears in the System Upgrades section.
4. In the **System Upgrades** section, select the software upgrade you want to install.
5. Click **Upgrade**.
   You will be prompted to perform a backup of your system. After you install the software upgrade, you must restart the device.

The installation process can take several minutes to complete. The system will reboot three times before you will be able to access it via the Web UI.

6. Log in to the system as the primary admin user.
   You will be prompted to perform a restore of your configuration.
7. Select your restore method (**FTP**, **SCP**, or **Local Disk**), then click **Next**.
8. Select which information to restore.
   For the FTP and SCP methods, enter your server information.
9. Click **Next** to confirm your selections.
10. Click **Restore now**.

Reapply Network Settings

To make sure that your network settings are correctly applied after you upgrade the device and restore your configuration, you must reapply the network settings.

1. Select **Configuration > Network > Interfaces**.
2. Click **Apply**.
3. After you apply the settings, you must reboot the XCS device.

Install the Software Upgrade from the Console

To install the software upgrade from the system console using a *.img* file:

You must be running WatchGuard XCS v9.2 Update 5 or higher to use this software upgrade method.

Install and Run BTIweb

BTIweb is a small web server that hosts the software image file for a network upgrade installation.

1. On your local workstation, extract the files from the *xcs-101.zip* archive.
2. In the *btiweb* directory, double-click **btiweb.exe**.
3. To start the web server service, click **Start**.

Install the Software Upgrade from the Console

1. Attach a monitor and keyboard (PS/2 or USB) to the connectors on the back panel of your XCS device.
2. Log in to the console.
3. Select **Admin > Reboot**, and then select **Yes** to confirm.
4. When the device restarts, press **F1** to start the installation process.
5. Press **Enter**.
6. Select your **Keyboard Type** for your location.
7. Select **Auto**, and then select **OK**.
8. Select **Network**.
9. Configure the settings for the first network interface of your device.
10. In the **Install Path** field, type the URL of the computer on which you installed BTIweb. For example, `http://10.0.0.2/`
    Make sure you type the trailing "/" character.
11. Select **xcs-101.img**.
12. Select **Save Image to Hard Disk**.
    The software image is copied to the local disk.
13. Press **Enter**.
    The software installs automatically. Wait at least 5 minutes for the device to initialize.
14. Open a web browser and type the IP address of the device to start the Web UI Setup Wizard.
15. For example, `https://10.0.0.1`.
16. On the Login page, type the default user ID **admin**, and the default password **admin**.
17. Follow the instructions on the screen and complete the Wizard.
18. Make sure you update the feature key during the Wizard.

Restore the Configuration

1. Select **Administration > Backup/Restore > Backup and Restore**.
2. Select your restore method (**FTP**, **SCP**, or **Local Disk**), then click **Next**.
3. Select which information to restore. 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 **Restore now**.
   The XCS device reboots when the restore is complete.

To Install the Software Upgrade 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 to **Primary** mode.
4. Install the update on the **Secondary**, and then restart the device.
5. Change the run mode of the **Secondary** system to **Secondary** mode.
6. Install the update on any **Client** devices, and then restart the device.
7. Change the run mode of the **Client** device to **Client** mode.

Resolved Issues

- The Message Quarantine pagination settings are now consistent when you manage the quarantine. *[70260]*
- Attachment Control processing issues no longer occur when scanning extraneous data objects extracted from PDF documents. *[73192]*
- Web connections now properly complete and ICAP failure errors are no longer displayed in the client web browser. *[81060]*
- Tiered administrators with individual quarantine access can now correctly view the details of a quarantined message. *[81263]*
- The HTTP proxy allowed networks list is no longer reset after an automatic feature key update. *[81574]*
- In some cases the Recent Mail Activity on the Dashboard did not correctly display or update data. *[81773]*
- Per-domain LDAP recipient verification checks no longer fail if the default recipient verification method is not set to LDAP. *[81923]*
- Pattern filter rules for mailer-daemon and postmaster are now correctly updated to the configured system domain after installation. *[82272]*
- The number of items per page selection on the Pattern Filters page is now preserved when you sort filters. *[82671]*
- The Trusted Senders List no longer has precedence over Content Rule actions. *[82979]*
- Content scanning phrase length checking is now applied correctly when scanning for phrases. *[84084]*
- Scanning certain types of messages with regular expressions no longer results in scanning engine latency. *[84151]*
- Messages released from the User Spam Quarantine through the WebMail interface are no longer blocked by Outbound Anti-Spam. *[84819]*
- Errors no longer occur when a Delegated Domain Administrator modifies an email action for a domain. *[85157]*
- Scheduled Message History reports are now correctly generated. *[85220]*
- In certain cases, the message quarantine default disk full expiry setting resulted in quarantined messages filling the mail partition. The default quarantine disk full expiry setting is now set to 85%. *[85714]*
- This release resolves four potential security vulnerabilities in the WatchGuard XCS Web UI and management script functions, including a SQL injection flaw and other elevation of privilege issues. We thank Daniel Jensen of Security-Assessment.com for identifying these vulnerabilities and helping us protect our customers. *[85846-50]*
- Validation is improved for the Mail Routing Route-To field. *[86040]*
- After you enable SecureMail, the Dashboard status display no longer shows the message "Urgent - Encryption failed - configuration error". *[86233]*
- Spam Rule updates no longer overwrite content rules if you have more than 200 defined content rules. *[86385]*
- The Dashboard no longer intermittently reports RED status as down when it is working correctly. *[86672]*
- Very Malformed Mail messages are now correctly sent to the configured quarantine. *[86717]*
- Spam Rules are now properly disabled when you disable the feature in the Anti-Spam or Outbound Anti-Spam configuration. *[86789]*

Known Issues and Limitations

Known issues for XCS 10.1 including workarounds where available, can be found on the Technical Search > Knowledge Base tab. To see known issues for a specific release, from the Product & Version filters you can expand the XCS version list and select the check box for v10.1.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or on the Web at http://www.watchguard.com/wgrd-support/overview. 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