WatchGuard® XCS v10.0 Release Notes

WatchGuard XCS Build	131010
Revision Date	3 December 2015

After you install WatchGuard XCS v10.0, make sure you install any additional software updates available for this release.

See these release notes for information about updates to WatchGuard XCS v10.0:

- WatchGuard XCS v10.0 Update 1 Release Notes
- WatchGuard XCS v10.0 Update 2 Release Notes
- WatchGuard XCS v10.0 Update 3 Release Notes
- WatchGuard XCS v10.0 Update 4 Release Notes
- WatchGuard XCS v10.0 NTP Hotfix Release Notes (included in Update 3)
- WatchGuard XCS v10.0 Security Hotfix Release Notes (included in Update 4)

Introduction

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

New Features and Enhancements

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

IPv6 Support

WatchGuard XCS now supports the IPv6 protocol. You can assign an IPv6 address to any network interface, and most XCS features support the use of IPv6 addresses in their configuration. The **Configuration > Network > Interfaces** page features a redesigned interface for IPv4 and IPv6 configuration.

- Static IPv6 addresses can be assigned to a network interface.
- IPv6 static routes can be configured.
- WatchGuard XCS now support Dual Stack Mode where network interfaces can have both IPv4 and IPv6 addresses and both IPv4 and IPv6 connections can be made simultaneously.
- At least one interface must be designated as IPv4 or IPv4 and IPv6 interface mode.

IPv6 Support Notes

- Auto-configuration of IPv6 addresses from compatible IPv6 routers is not supported.
- Cluster IP configuration is local to the cluster network, and uses only IPv4.
- IPv6 configuration is not available in the Installation Wizard.
- IPv6 configuration is not available on the system console.
- IPv6 to IPv4 tunneling is not supported.

These XCS features and third-party services currently do not support IPv6.

- Anti-virus software pattern updates
- Brightmail Anti-Spam updates
- SecureMail email encryption server
- URL Categorization IP address checking
- Centralized Management
- Threat Prevention static lists and push to an F5 device
- Web Proxy Single Sign-on Agent
- WatchGuard RED (Reputation Enabled Defense) network queries and data submission
- WatchGuard Security Connection for XCS software updates

WatchGuard XCSv Microsoft Hyper-V Support

WatchGuard XCSv is an email and web security solution that provides all the security features of our WatchGuard XCS technology optimized for a virtual machine environment. The WatchGuard XCSv virtual machine can now be installed in a Windows Hyper-V environment.

Installation Prerequisites

You must install the XCSv virtual device in a Microsoft Hyper-V environment that meets these requirements:

- **Hyper-V**
  - Hyper-V role on Windows Server 2008 R2 or Windows Server 2012, or stand-alone version of Hyper-V Server 2008 R2 or Hyper-V Server 2012.
  - Make sure your Windows Server or Hyper-V Server software is updated to the latest patch level.
  - You can use the Hyper-V Manager on Windows Server 2012 to deploy, configure , and provision the XCSv virtual machine in the Hyper-V environment. You can also use System Center Virtual Machine Manager (VMM) interface, or a Hyper-V role on a client computer instead of Hyper-V Manager.
- **Hardware**
  - The hardware requirements for XCSv are the same as the hardware requirements for Hyper-V on Windows Server 2008 R2 or Windows Server 2012.
- **Network**
  - You can configure a maximum of 8 interfaces.

Features Not Supported with WatchGuard XCSv on Hyper-V

- XCSv does not support the dynamic memory setting on Hyper-V.
- The Data Exchange and Volume Backup features are not supported.
- Time synchronization is not supported. We recommend you use an NTP server in the XCSv network configuration.

Installation Overview

For XCSv on Hyper-V, WatchGuard distributes XCSv as a virtual hard disk (.vhd) file. To deploy an XCSv virtual hard disk in a Hyper-V environment:

1. Use Hyper-V Manager or System Center VMM to deploy the XCSv virtual machine and select the *.vhd* file to use.
2. Assign network adapters and configure appropriate resources (processor, memory, disks) for your XCSv edition.
3. Power on the XCSv virtual machine.
4. Connect to the XCSv virtual machine to run the Setup Wizard.

For detailed information on installation and configuration, please see the ***WatchGuard XCSv Setup Guide***.

Perform XCS v10.0 System Upgrade from the Web UI

With the WatchGuard XCS v10.0 release, you can now perform a full upgrade of your WatchGuard XCS system software without the use of the system console. The software upgrade is distributed as a *.pf* file just like a software update. You can upload the v10.0 upgrade file on the **Administration > Software Updates > Updates** page. The system upgrade will appear in a new *System Upgrades* section on the **Software Updates** page.

When you perform a system upgrade, the system retains its original IP address and network settings, time zone, admin user login names and passwords, and feature key information. When the system restarts after the upgrade, you can connect to the system using its original IP address. As part of the upgrade process, you are also prompted to back up and restore your configuration.

Upgrade Notes

- You must be running WatchGuard XCS 9.2 Update 5 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, Transparent Mode) will be reset to their default value. You must re-enable these options after the upgrade is complete. Note that in v10.0, many of these options are now in the **Show Advanced Options** section of the network configuration page.
- 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.

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.

For more information, see the Install the Software section of these release notes.

Per-Domain Recipient Verification

The Recipient Verification feature is used to reject mail based on recipient address checks to an LDAP server or recipient address SMTP probe to the configured MTA. This check ensures that the recipient address is verified to be deliverable. You can now configure how to perform recipient verification based on the domain of the recipient. For each domain, you can disable recipient verification, or choose between the LDAP or SMTP verification methods. If a domain is not configured, the default recipient verification method is used.
To configure Per-Domain Recipient Verification, select **Security > Anti-Spam > Connection Control**.

Per-Policy Anti-Virus Options

You can now configure these "Treat as Virus" Anti-Virus options on a per-policy basis:

- **Attachments containing unknown viral code** — The Anti-Virus scanner can detect code that resembles the patterns of a virus.
- **Corrupt attachments** — The Anti-Virus scanner may not be able to scan corrupted attachments which can contain viruses.
- **Password-protected attachments** — Attachments protected by a password cannot be opened by the Anti-Virus scanner and could contain viruses. Disable this option if you use password-protected files and archives in your organization.

- **Attachments causing scan errors** — Attachments that cause errors while being scanned by the Anti-Virus scanner can contain viruses.

SMTP Mail Submission on SMTP Port 587

The WatchGuard XCS now supports message submission on SMTP port 587. When message submission is enabled, the system listens on SMTP port 587 (in addition to port 25) for SMTP authenticated relay. To enable Message Submission, select **Configuration > Mail > Access**. Message Submission must also be enabled on a specific network interface on the **Configuration > Network > Interfaces** page.

Outbound Anti-Spam

Outbound Anti-Spam controls are used to prevent trusted users from sending spam outbound. You can use the Spam Rules, Spam Words, and URL Block List Anti-Spam features to scan outbound mail for spam messages.

You can also use the new **Mail Surge Detection** feature to identify internal mail users who are sending an unusually large amount of mail messages which can indicate spam activity. When a mail surge is detected, you can prevent the user from sending further emails for the duration of a specified hold period. Outbound Anti-Spam features are available within policies to define actions and notifications for different users, groups, and domains.

To configure Outbound Anti-Spam and Mail Surge Detection, select **Security > Anti-Spam > Outbound Anti-Spam** on the menu.

Adaptive Default Anti-Spam Strategy

Adaptive is now the default Intercept Anti-Spam strategy. This strategy is very effective for most environments and provides an excellent spam catch rate with a very low chance of false positives. The **Adaptive** strategy combines the abilities of **Heuristic 1** and **Heuristic 2** and monitors the initial message training period. When the system has trained a suitable amount of spam and legitimate mail, it adjusts its internal aggressiveness strategy accordingly to utilize the trained mail.

Internationalization Support for Objectionable Content Filter and Spam Words

The WatchGuard XCS now supports international languages when you use the Objectionable Content Filter (OCF) and Spam Words features to scan messages that use Unicode or other supported international character sets.You must specifically enable international character support on the OCF or Spam Words feature pages. If you do not require international character support, we recommend you leave this option disabled to improve message processing performance.

Internationalized scanning supports these character sets for use with the Content Scanning, Objectionable Content Filter, and Spam Words features:

- Thai, Windows-874
- Japanese Shift-JIS, Windows-932
- Chinese simplified GBK, GB2312, GB18030, Windows-936
- Korean, EUC-KR, Windows-949
- Chinese Traditional, Big5, Windows-950
- Central Europe, Windows-1250
- Cyrillic, Windows-1251
- Latin 1, Windows-1252
- Greek, Windows-1253

- Turkish, Windows-1254
- Hebrew, Windows-1255
- Arabic, Windows-1256
- Baltic, Windows-1257
- Russian, KOI8-R
- Japanese EUC, ISO-2022-jp
- Latin 1, ISO-8859-1
- Latin 2, ISO-8859-2
- Latin 3, ISO-8859-3
- Baltic, ISO-8859-4
- Cyrillic, ISO-8859-5
- Latin/Arabic, ISO-8859-6
- Greek, ISO-8859-7
- Latin/Hebrew, ISO-8859-8
- Turkish, ISO-8859-9
- Latin/Thai, ISO-8859-11
- Latin 7, ISO-8859-13
- Latin 9, ISO-8859-15

Pattern Match Counting

In the Pattern Filter and Content Rules features, you can now specify a **Match Threshold** that indicates the number of times a pattern must appear in the message before an action is performed. This field only appears when you select the *Raw Mail Body*, *Mail Content*, *STA Token*, or *Content Scanning* message parts. For example, if you set this field to 3, a pattern must appear at least 3 times before an action is performed. The default is 1.

Copy Policy

You can now copy the contents of an existing policy and use it as a base template for a new policy. On the Policy page, click the **Copy** link for the specific policy you want to duplicate. A new policy page will open containing the same settings as the original policy.

Data Loss Prevention Wizard Updates

New rule types have been added to the Data Loss Prevention Wizard to provide greater coverage for magnetic track credit card types and national identification numbers.

- **New Financial Identification Numbers**
  - Credit card magnetic track 1 - International Air Transport Association (IATA). This track is sometimes used by airlines when securing reservations with a credit card.
  - Credit card magnetic track 2 - American Banking Association (ABA). This track is read by ATMs and credit card verification systems.
- **New National Identification Numbers**
  - Social Insurance Number (UK)
  - National identification numbers (Denmark)
  - National Identification Number (Brazil)
  - Social Insurance Number (Germany)
  - Personal Public Service numbers (Ireland)
  - Fiscal code numbers (Italy)
  - Fiscal identification numbers (Spain)
  - National identity card (Hong Kong)

- Permanent account numbers (India)
- National registration identity card (Singapore)

Data Loss Prevention Wizard and Content Scanning Phrase Length

Depending on the ID number you search for, you must set the Content Scanning phrase length to an appropriate value to match that pattern. The default Content Scanning phrase length is 4. These types of ID numbers require a longer minimum phrase length:

- IBAN (International Bank Account Number) – 7
- INSEE (Social Insurance Number - France) – 7
- National Identification Number (Brazil) – 8
- Social Insurance Number (UK) – 5

To set the Content Scanning phrase length, select **Security > Content Control > Content Scanning** on the menu. Longer Content Scanning phrase lengths result in greater processing time.

Cluster Message Quarantine Management

You can now manage the message quarantine for a cluster from any cluster host. Within the message quarantine, each message indicates the host in the cluster where the quarantined message is located. You can preview, release, or delete any quarantined message in the cluster from any cluster host.

Kaspersky Anti-Virus Update Alarm

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

Centralized Management Purge Local Settings Action Moved

In Centralized Management, the **Purge Local Settings** action has been moved to the CM configuration screen for an Entity system (**Administration > Multi-System Management > Centralized Management > Configure**). You will also be asked for confirmation before the purge action is started.

Feature Key Automatic Synchronization

You can now keep your feature key automatically synchronized with your WatchGuard LiveSecurity account. If you purchase new feature options or renew your product, your feature key will be automatically updated on the XCS device. To enable this option, select **Configuration > System > Feature Key**.

Operating System Upgrade

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

Content Scanning Engine Upgrade

The Content Scanning engine has been updated to provide the latest security, performance, and product updates for the latest types of documents.
These new document types are supported:

- Microsoft Word 2013, Microsoft Excel 2013, Microsoft PowerPoint 2013, Microsoft Outlook 2013
- Microsoft Word 2011 for Mac, Microsoft Excel 2011 for Mac, Microsoft PowerPoint 2011 for Mac
- Microsoft Word 2010, Microsoft Excel 2010, Microsoft PowerPoint 2010, Microsoft Project 2010
- Adobe Photoshop CS6, Illustrator CS6, InDesign CS6
- DICOM (Digital Imaging and Communications in Medicine) files

McAfee Anti-Virus Upgrade

The McAfee Anti-Virus engine has been upgraded to the most recent version (5600) 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:

- 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

To download the software:

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 appropriate WatchGuard XCS v10.0 software package:
    - **xcs100_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 v10.0. You must be running WatchGuard XCS 9.2 Update 5 to use this software upgrade method. This method can be used for both XCS and XCSv.
    - **xcs_100.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. For this method you must have a minimum of WatchGuard XCS v9.1 Update 3.
    - **XCSv-100.ova** — This package contains an OVA template for an installation of XCSv v10.0 on VMware.
    - **XCSv-100-HyperV.zip** — This package contains the files required to install XCSv v10.0 on Microsoft Hyper-V.

Install the Software

There are two ways to install the XCS v10.0 software:

- Install the Software Upgrade from the Web UI — Use the software upgrade file packaged as a software update *(xcs100_upgrade.pf)*. You can install this file from the Software Updates page on the Web UI. You must be running WatchGuard XCS v9.2 Update 5 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-100.img)* for a network upgrade installation from the system console. This method requires a minimum version of WatchGuard XCS v9.1 Update 3.

We recommend that you use the Web UI to upload the *xcs_100_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 9.2 Update 5 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, Transparent Mode) will be reset to their default value. You must re-enable these options after the upgrade is complete. Note that in v10.0, many of these options are now in the **Show Advanced Options** section of the network configuration page.
- 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 `xcs_100_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**.

Install the Software Upgrade from the Console

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

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-100.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-100.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

- Configuration values on the Mail Access settings page are now correctly synchronized in a Centralized Management configuration set. *[49019]*
- Extraneous log file entries no longer appear when you install support access on a Centralized Management Entity system. *[54061]*
- A memory size error no longer occurs when you view reports on systems with a large database of reporting data. *[54138]*
- Dictionaries viewed with a Windows-based text editor now appear with correct CR/LF characters. *[55163]*
- Hardware performance settings are now correctly set if the feature key is not applied during the initialization wizard. *[59898]*
- In certain cases, the Dashboard no longer displays incorrect service status and dates. *[60515]*
- The security advisory FreeBSD-SA-11:05.unix has been resolved. *[63677]*
- File names with multiple RFC2047 encoded words in the same line are now correctly detected by Attachment Control. *[64548]*
- Processing latency and high CPU utilization no longer occurs when using the Web Proxy. *[69288]*
- Internationalized content scanning now works correctly with the Web Proxy. *[69883]*
- The Show Log function now correctly displays details for messages processed in a previous year. *[70785]*
- Centralized Management systems no longer restart because of memory usage issues. *[71833]*
- Corrupted archive files no longer cause errors with the Content Scanning engine. *[71863]*
- Mail processing errors no longer occur when special characters are used in the Anti-Spam Email Action Data field. *[71969]*
- Connection errors no longer occur when you use URL Categorization to scan web traffic. *[71977]*
- Content rule and filter dictionary matches for email addresses are no longer case sensitive. *[72013]*
- Very large UBL whitelists no longer causes issues with communications to the Security Connection service. *[72249]*
- You can now use a backslash character in the folder path for SCP log offload. *[72543]*

Known Issues and Limitations

Known issues for this release, including workarounds where available, can be found on the WatchGuard website. To see Known Issues, log in to the WatchGuard website and use the filters available on the Technical Search > Knowledge base tab.

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