



WatchGuard® XCS

Extensible Content Security v9.1 Installation Guide

WatchGuard XCS
170, 370, 570, 770, 770R, 970, 1170

Copyright, Trademark, and Patent Information

Copyright © 2010 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.



This product is for indoor use only.

ABOUT WATCHGUARD

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

Table of Contents

Chapter 1	Getting Started	1
	Before You Begin	1
	Verify basic components	1
	Hardware installation	1
	Physical location	1
	Connect the network interfaces	2
	Get a WatchGuard device feature key	2
	Gather network addresses	3
	WatchGuard XCS Deployments	5
	WatchGuard XCS on the DMZ of a network firewall	5
	WatchGuard XCS in parallel with a network firewall	6
	WatchGuard XCS on the internal network	6
	Additional Configuration	7
	Network firewall configuration	7
	DNS configuration for mail routing	8
	Outbound mail routing	9
Chapter 2	Install the WatchGuard XCS	11
	Connect the WatchGuard XCS	11
	Default network settings	12
	Start the Installation Wizard	13
Chapter 3	Feature Key and Software Updates	21
	Feature Key	21
	Add a feature key	21
	Update a feature key	23
	Security Connection	24
	Software Updates	25
	Update Anti-Virus Pattern Files	26
Chapter 4	Configure Message Delivery	27
	Add Mail Routes	27
	Upload mail routes	28
	Trust Internal Mail Servers	29
	Modify Internal Mail Servers for Outbound Mail	30
	Exchange 2000 and 2003	30
	Multiple Exchange server configuration	30

Exchange 2007 and 2010	31
Start Messaging Services.....	31

1

Getting Started

Before You Begin

Before you begin the installation process, make sure you do the tasks described in the subsequent sections.

Verify basic components

Make sure that you have:

- A computer with an Ethernet network interface card and a web browser installed
- A WatchGuard XCS device
- Ethernet cables
- Power cables

You can also attach an optional monitor and keyboard (USB or PS/2) to get access to the WatchGuard XCS console.

Hardware installation

For detailed instructions on how to install the WatchGuard XCS device in an equipment rack, see the *Hardware Guide*.

Physical location

To safely install your WatchGuard XCS device, we recommend you select a physical location that meets these specifications:

- Install the device in a secure location, for example, in a locked equipment rack or a secure server room.
- Make sure that the network connections are secure, and the network hubs and switches are in the same secure location. Any network patch cables should be of the appropriate length (as short as possible).
- If a monitor and keyboard are attached to the device for console use, make sure that keystroke logging devices cannot be added to the keyboard connection. Connect the monitor and keyboard directly to the device.
- Use the Web UI only in a secure location at a trusted workstation. Do not use the Web UI in any location where the administrative session can be monitored physically or electronically.

Connect the network interfaces

Before installation, make sure that you physically connect at least one of the network interfaces to the network.

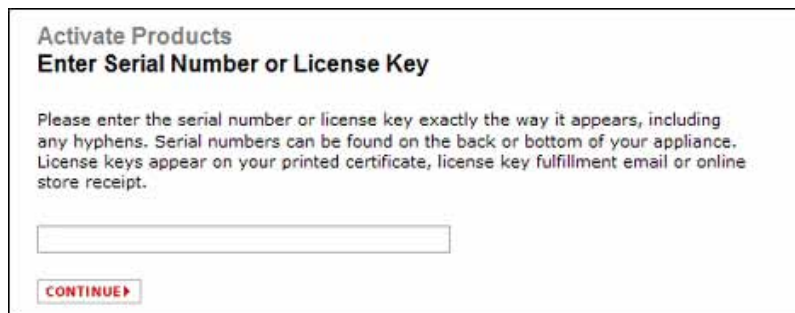
When you install your device, we recommend you use the first onboard Ethernet network interface at the left of the device (NIC 1) to connect to your network. This is the first default interface assigned by the WatchGuard XCS. After you complete the installation, you can configure additional network interfaces.

Get a WatchGuard device feature key

A feature key is a license that enables you to activate your purchased feature set on your WatchGuard XCS. You must register the device serial number with WatchGuard® LiveSecurity® to get your feature key.

To activate a serial number and get a feature key:

1. Open a web browser and go to <https://www.watchguard.com/activate>.
If you have not already logged in to the WatchGuard web site, the Log In page appears.
2. Type your LiveSecurity **User Name** and **Password**. Click **Log In**.
The Activate Products page appears.
3. Type the serial number for the product as it appears on your hardware device. Make sure to include any hyphens.



4. Click **Continue**.
The Choose Product to Upgrade page appears.
5. From the drop-down list, select the correct WatchGuard XCS.
6. Click **Activate**.
The Retrieve Feature Key page appears.
7. Copy the full feature key to a text file and save it on your computer.
8. Click **Finish**.

Gather network addresses

Before you start the installation, make sure you have this information about your network:

Hostname

The hostname assigned to the WatchGuard XCS. For example, if the FQDN (Fully Qualified Domain Name) is `hostname.example.com`, use `hostname`.

Domain Name

The domain name associated with the assigned hostname. This is the domain to which messages are sent. For example, `example.com`.

Internal IP Address

Select an IP address for the internal network interface. You use this address to connect remotely to the XCS device with a web browser.

External IP Address

Select an IP address for the external network interface (if required). This is the external interface that connects to a public network, such as the Internet.

Subnet Mask

The subnet mask for the IP addresses you selected.

Gateway Address

The default gateway for the XCS device. This is usually your network router.

Mail Domains

The mail domains for which the WatchGuard XCS processes messages.

Optional Network Cards

The IP address, Subnet Mask, and Gateway Address for any additional network cards required by your deployment.

DNS Servers

The addresses of your DNS (Domain Name Service) name servers. We recommend that you include both a primary and a secondary server.

NTP Servers

The addresses of your NTP (Network Time Protocol) servers for time synchronization. We recommend that you include both a primary and a secondary server.

Table 1: Basic Network Settings	Example
Hostname _____	hostname
Domain Name _____	example.com
Internal IP Address _____._____._____._____	10.0.0.1
Subnet Mask _____._____._____._____	255.255.255.0
External IP Address _____._____._____._____	100.100.100.10
Subnet Mask _____._____._____._____	255.255.0.0
Gateway Address _____._____._____._____	10.0.0.2

Table 1: Basic Network Settings	Example
Mail Domains _____ _____ _____	example.com example1.com
Internal Mail Servers _____._____._____._____ _____._____._____._____ _____._____._____._____	10.0.2.25 10.0.3.25
Optional Network Cards _____._____._____._____ _____._____._____._____	10.0.5.10
DNS Servers _____._____._____._____ _____._____._____._____	10.0.2.53 10.0.3.53
NTP Servers _____._____._____._____ _____._____._____._____	10.0.2.123 10.0.3.123

WatchGuard XCS Deployments

The WatchGuard XCS is designed to be installed between internal email servers and clients, and external servers on the Internet so that there are no direct connections between external and internal systems.

The WatchGuard XCS is installed in one of these locations:

- On the DMZ (Demilitarized Zone) of a network firewall
- In parallel with a network firewall
- Behind the existing firewall on the internal network

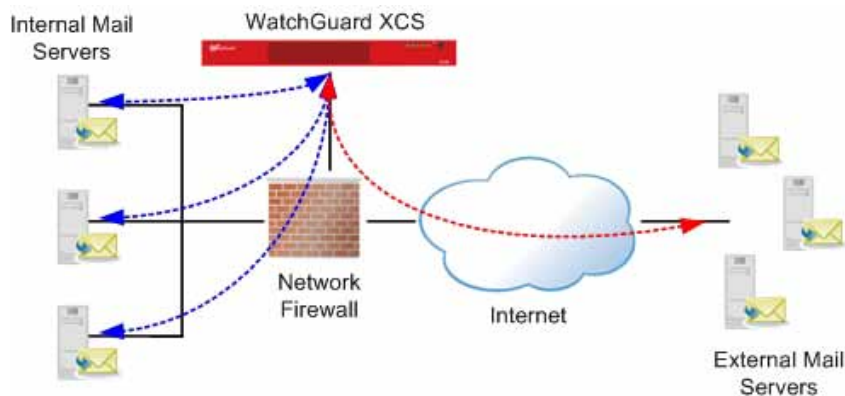
Messaging traffic is redirected from either the external interface of the network firewall or from the external router to the WatchGuard XCS. When the WatchGuard XCS accepts and processes a message, the device initiates a connection to the internal mail servers to deliver the message.

WatchGuard XCS on the DMZ of a network firewall

The most common deployment strategy for the WatchGuard XCS is to be situated on the DMZ of a network firewall. This type of deployment prevents any direct connections from the Internet to the internal mail servers, and makes sure the WatchGuard XCS is located on a secure network behind the firewall.

This deployment uses a single network interface connected to the DMZ network of the network firewall.

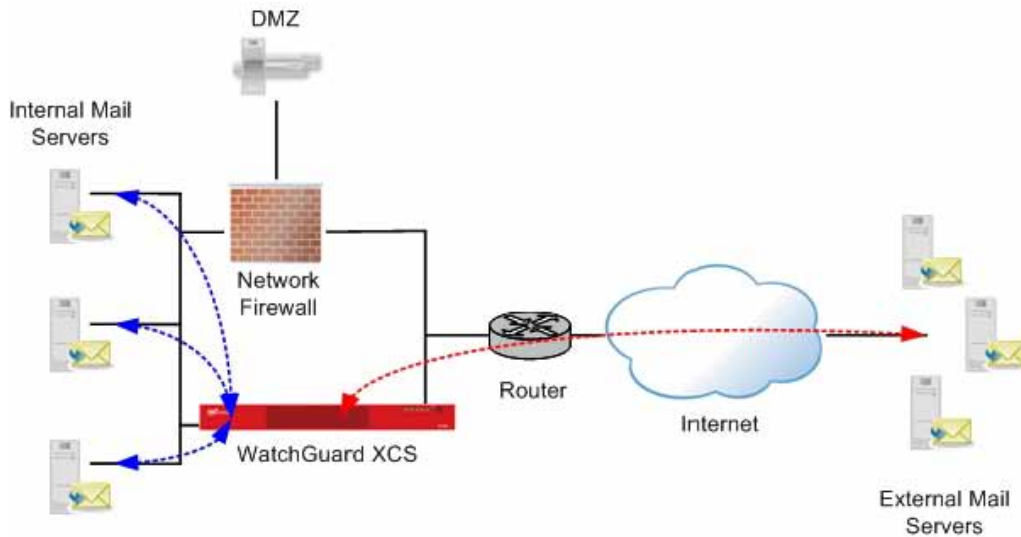
The Installation Wizard helps you install the WatchGuard XCS in this deployment configuration.



WatchGuard XCS in parallel with a network firewall

You can deploy the WatchGuard XCS in parallel with an existing network firewall. The firewall security of the XCS device architecture eliminates the risk associated with deployment on the perimeter of a network. This parallel deployment eliminates any messaging traffic on the network firewall and decreases its overall processing load.

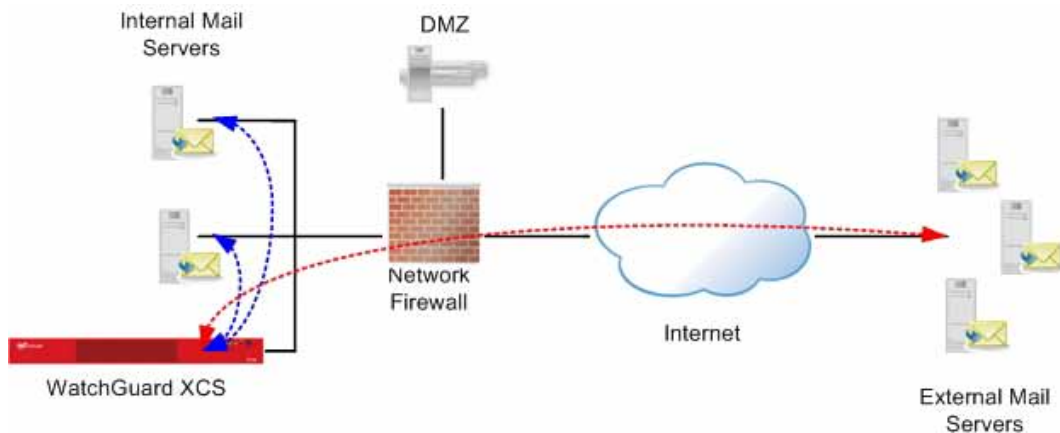
A second network interface must be configured to connect to the Internet-facing network.



WatchGuard XCS on the internal network

The WatchGuard XCS can also be deployed on the internal network. Although this configuration allows a direct connection from the Internet to the internal network, it is a legitimate configuration when required by existing network resources.

This deployment uses a single network interface connected to the DMZ network of the network firewall.



Additional Configuration

When you have decided on a deployment strategy, you must gather this information about your environment:

- Any ports that must be opened on the network firewall (if the system is deployed behind a firewall)
- Any DNS changes necessary to route incoming email messages to the WatchGuard XCS
- Any changes required to the internal mail servers to route outbound email messages through the WatchGuard XCS

Network firewall configuration

To enable the WatchGuard XCS to effectively process messages when it is located behind a network firewall, you must correctly configure the network ports on your network firewall.

This table describes the ports required for each feature. If you do not use a feature in the table, you do not have to open the port for that feature:

Port	Description	From Internet	To Internet	From Internal Network	To Internal Network	Protocol
21	FTP for System Backups				X	TCP
22	SCP (Backup or Offload)				X	TCP
25	SMTP (standard port used to send and receive mail)	X	X	X	X	TCP
53	DNS and RED Queries		X		X	TCP/UDP
80	Anti-Virus Updates (also requires port 443)		X			TCP
80	URL Categorization Updates		X			TCP
80	Web Mail Access (OWA, iNotes, etc.) See port 443 for Secure WebMail access.	X		X		TCP
110	POP3	X		X		TCP
123	Network Time Protocol (NTP)		X		X	UDP
143	IMAP Proxy	X		X		TCP
161	SNMP			X		UDP
162	SNMP trap				X	UDP
389	LDAP				X	TCP
443	WatchGuard XCS Software Updates		X			TCP

Port	Description	From Internet	To Internet	From Internal Network	To Internal Network	Protocol
443	Anti-Virus Updates (also requires port 80)		X			TCP
443	Secure Web Mail Access	X		X		TCP
443	Web UI connections	X		X		TCP
443	RED Statistics Sharing		X			TCP
514	Syslog				X	UDP
636	LDAPS				X	TCP
993	Secure IMAP	X		X		TCP
995	Secure POP3	X		X		TCP
1812	RADIUS Server				X	UDP
5500	RSA Secure ID ACE Server				X	UDP
10101	Support Access	X	X			TCP
10106	Centralized Management	X	X	X	X	TCP
10108	Web Reputation		X			UDP

DNS configuration for mail routing

DNS services are used to route mail messages from the Internet to the WatchGuard XCS. DNS configurations can be complex and are dependant on your specific network environment.

These instructions represent the minimum changes required for mail routing:

- Add an MX (mail exchanger) record to your DNS configuration to forward incoming messages to the WatchGuard XCS:

```
example.com. IN MX 0 hostname.example.com
```
- Add an A record to resolve the domain name to an IP address:

```
hostname.example.com. IN A 10.0.0.1
```
- Add a PTR record to allow reverse look-ups to succeed and prevent messages sent from the WatchGuard XCS from being marked as suspected spam:

```
1.0.0.10.in-addr.arpa. IN PTR hostname.example.com
```
- It can be useful to keep an MX record with a higher preference pointed at your current mail server in the integration phase. If the WatchGuard XCS is taken out of service, the messages automatically route directly to the mail server. This entry must be deleted before you move to a production environment because spammers could find this alternate route and bypass the WatchGuard XCS.

```
example.com. IN MX 10 mailserver.example.com
```

Outbound mail routing

You must modify existing internal mail servers to route outbound messages through the WatchGuard XCS.

After the installation is complete, you must configure all internal mail servers to use the WatchGuard XCS for mail delivery. This allows the WatchGuard XCS to scan outbound message content and file attachments to prevent the spread of viruses introduced locally, and to improve the spam detection capabilities of the Intercept Anti-Spam features.

See “Modify Internal Mail Servers for Outbound Mail” on page 30 for more detailed information on how to integrate your internal mail servers with the WatchGuard XCS after installation.

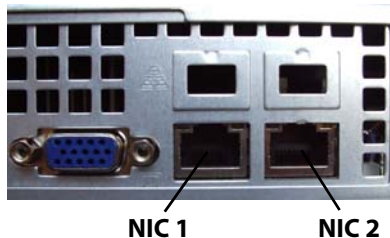
2

Install the WatchGuard XCS

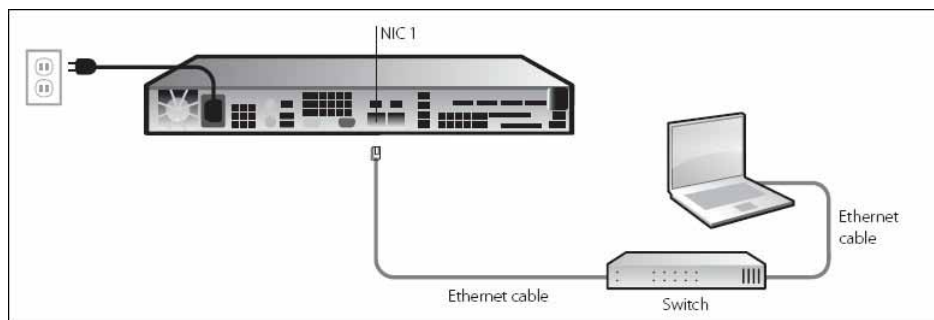
Connect the WatchGuard XCS

To connect the WatchGuard XCS:

1. Unpack the device, cables, and documentation from the shipping carton.
2. Connect the power cable to the system and a power source, preferably a UPS (Uninterruptible Power Supply).
3. Connect the first onboard Ethernet network interface on the left of the device (NIC 1) to the network.
For the initial installation, you only need to connect the internal network interface to be able to connect to the device with a web browser. You can configure additional network interfaces after the installation.



4. Use one of these methods to get access to the Web UI Installation Wizard:
 - Connect your computer to the same network as the WatchGuard XCS through a network switch. Connect the WatchGuard XCS to the network switch using the first onboard Ethernet connector (NIC 1) at the left side of the back panel.



- Connect your computer directly to the WatchGuard XCS with a cross-over Ethernet cable connected to the first onboard Ethernet connector (NIC 1) at the left side of the back panel.

Default network settings

The default network settings for the WatchGuard XCS are:

- IP address: 10.0.0.1
- Netmask: 255.255.255.0
- Gateway: 10.0.0.2

To connect to the WatchGuard XCS Web UI, we recommend you configure your computer to use the IP address 10.0.0.2.

The WatchGuard XCS supports these web browsers:

- Internet Explorer 7 (Windows XP, Windows 2000, Windows 2003, Windows Vista, Windows 7)
- Internet Explorer 8 (Windows XP, Windows 2000, Windows 2003, Windows Vista, Windows 7)
- Firefox 3 and greater (Windows, Linux, Mac)

Use a minimum screen resolution of 1024x768.

Start the Installation Wizard

1. Power on your device.

Wait at least 5 minutes for the system to initialize before you try to connect to the WatchGuard XCS with a web browser. Ping is enabled on the configured network interface. You can ping the default address 10.0.0.1 to check connectivity before you connect with a web browser.

2. Launch a web browser on your computer and type the IP address of the WatchGuard XCS as the URL in the location bar. For example, `https://10.0.0.1`

The login page appears.



A security certificate notification appears in the browser because the system uses a self-signed certificate. It is safe to ignore the warning (Internet Explorer) or to add a certificate exception (Mozilla Firefox).

3. Type the default **Username** and **Password**.

When you access the system for the first time after installation, the default settings are **admin** for the username, and **admin** for the password.

4. The Installation Wizard introduction page appears. Click **Continue** to start the installation. Make sure you register your device serial number with the WatchGuard® LiveSecurity® web site and receive a feature key before you continue with installation.

- In the **Regional Settings** page, configure these options:
 - Time Settings** — Type the current **Time** and **Date**. For the time, use 24-hour format hh:mm:ss. For the date, use this format: YYYY-MM-DD.
 - Time Zone** — Select the closest city to your location and time zone.
 - Keyboard** — Select the keyboard layout for your location. You can attach a keyboard and monitor to the WatchGuard XCS to get access to the console.

Regional Settings

Time Settings

Time: 15:25:06 ✓
Date: 2010-04-17 ✓

Time Zone

Region: America
Country: Canada
City: Toronto

Keyboard

Layout: USA/Canada

Help

Time Settings: Set the current date and time. For the time, use 24-hour format hh:mm:ss. For the date, use the format YYYY-MM-DD. Configure an NTP Time Server in the Network Settings step of the installation wizard to make sure the system time is always synchronized.

Time Zone: Select the location for your time zone.

Keyboard: Select the keyboard layout for your location. The keyboard is used to access the system console.

[Continue](#)

- Click **Continue**.
- On the **Networks Settings** page, configure the first network interface. This is the first onboard Ethernet connector (NIC 1) at the left side of the back panel of your device.

Network Settings

Hostname: hostname ✓
Domain: example.com ✓
Gateway: 10.0.0.2 ✓
Name Server: 10.0.2.53 ✓
Name Server 2: 10.0.3.53
NTP Server: 10.0.2.123

Interface 1

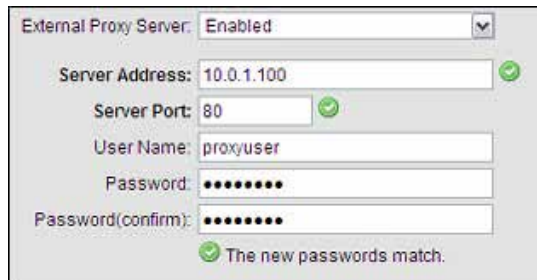
IP Address: 10.0.0.1 ✓
Netmask: 255.255.255.0 ✓
External Proxy Server: Disabled

[continue \(reboot required\)](#)

You can configure these options:

- Hostname** — Type the hostname for the device. For example, if your fully qualified domain name is hostname.example.com, type `hostname`.
- Domain** — Type your domain. For example, type `example.com`.
- Gateway** — Type the gateway (typically the router) for your network. For example, type `10.0.0.2`.
- Name Server** — Type the IP address of your DNS Name Server. For example, type `10.0.2.53`.

- **Name Server 2** — Type the IP address of a secondary DNS name server.
For example, type 10.0.3.53.
- **NTP Server** — Type the IP address or hostname of your NTP server.
For example, type 10.0.2.123.
- **IP Address** — Type IP address for this interface.
For example, type 10.0.0.1.
- **Netmask** — Type the netmask.
For example, type 255.255.255.0.
- **External Proxy Server** — If your network uses a proxy server to access the Internet, you must set this option to **Enabled** and enter your external proxy server configuration. The WatchGuard XCS requires access to the Internet through the proxy server to retrieve license information and software updates. If you do not use an external proxy server, keep this option set to **Disabled**.



- **Server Address** — Type the IP address of your external proxy server.
- **Server Port** — Type the server port used by the external proxy server. The default is TCP port 80.
- **User Name** — If your proxy server requires authentication, type the user name to log in to the proxy server.
- **Password** — Type and confirm a password.

8. Click **Continue**.

If you make any network changes, you must restart the device and reconnect to the WatchGuard XCS with the new IP address you assigned to the network interface.



Make sure your computer is configured to get access to the new IP address settings on the WatchGuard XCS.

9. On the **Customer Information** page, type the **Organization Name** and **Server Admin Email**.
Device alerts and notifications are sent to the Server Admin Email address.



10. Click **Continue**.

11. On the **Change Password** page, type and confirm a new admin password.
We recommend that you choose a secure password of at least 8 characters in length and include a mixture of upper and lowercase letters, numbers, and special characters.



12. Click **Continue**.
13. On the **Feature Key** page, select one of these options to add your feature key:
- Click **Update** to manually add a feature key. Paste your feature key into the text box and click **Apply**.
 - Click **Get Feature Key** to automatically download and apply your feature key from the WatchGuard LiveSecurity service. This option requires an Internet connection and an existing LiveSecurity account. Make sure you can get access to the Internet if the device is installed behind a network firewall, or connects through an external proxy server.
 - Click **Enter Feature Key Later** to manually add the feature key after installation. To enter the feature key manually, from the Web UI, select **Administration > System > Feature Key**.



If you do not enter a valid feature key in this step, the Mail Configuration and Start Processing steps of the wizard are not displayed.



If you see errors when you add your feature key, try this:

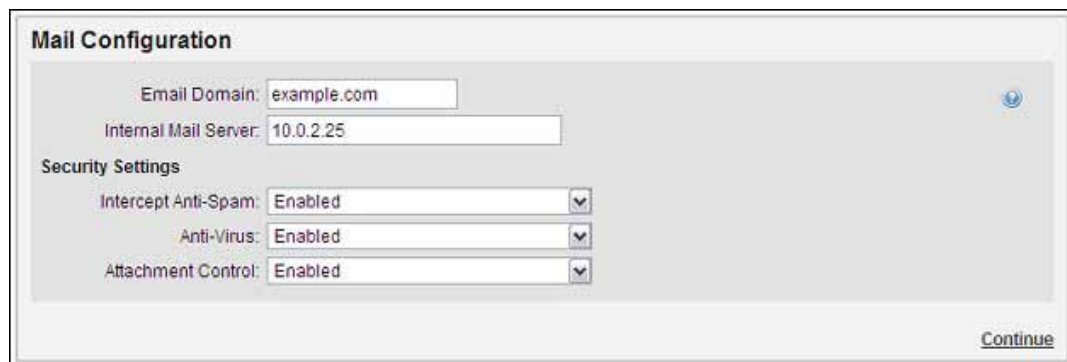
For Automatic Update:

- Make sure you have a valid LiveSecurity account and that you have registered your device serial number.
- You must have an Internet connection to retrieve your feature key.
- Make sure communications are not blocked by a network firewall.

For Manual Update:

- Make sure you cut and paste the entire feature key text.
- The first line must be "Serial Number: B0Exxxxxxxxx".
- The last line is a long line that starts with "Signature: ".

14. On the **Mail Configuration** page, type your mail domain and server details, and select the initial status of the WatchGuard XCS security scanning features.



Mail Configuration

Email Domain:

Internal Mail Server:

Security Settings

Intercept Anti-Spam:

Anti-Virus:

Attachment Control:

[Continue](#)

- In the **Email Domain** text box, type the domain for which the WatchGuard XCS processes messages. For example, `example.com`.
- In the **Internal Mail Server** text box, type the IP address of the internal mail server that receives and sends mail through the WatchGuard XCS.

The WatchGuard XCS automatically configures a mail route for the domain and internal mail server you enter on this page. To configure additional domains for mail routing after the installation is complete, from the Web UI, select **Configuration > Mail > Routing**.

The WatchGuard XCS also automatically configures a Specific Access Pattern to trust your internal mail server address to allow the mail server to relay mail outbound through the WatchGuard XCS. Mail that originates from the internal mail server is also trusted for Anti-Spam processing. To configure Specific Access Patterns after the installation is complete, from the Web UI, select **Configuration > Mail > Access**.

15. In the **Security Settings** section of the **Mail Configuration** page, you can enable or disable **Intercept Anti-Spam**, **Anti-Virus**, and the **Attachment Control** features.

If you enable these features in the Installation Wizard, mail scanning is active when the installation is complete and mail processing is started.

This table describes the default **Intercept Connection Control** settings when you enable Intercept Anti-Spam:

Feature	Default Setting
Reject on Reputation (Reputation Enabled Defense)	Enabled (Threshold: 90)
Reject on infection (Reputation Enabled Defense)	Enabled
Reject connections from dial-ups (Reputation Enabled Defense)	Off
Reject on DNSBL	Off
Threat Prevention	Enabled
Reject on unknown sender domain	Enabled
Reject on missing sender MX	Off
Reject on non FQDN sender	Enabled
Reject on unauth pipelining	Enabled
Reject on missing addresses	Off
Reject on missing reverse DNS	Off

This table describes the default settings for the **Intercept Anti-Spam** features:

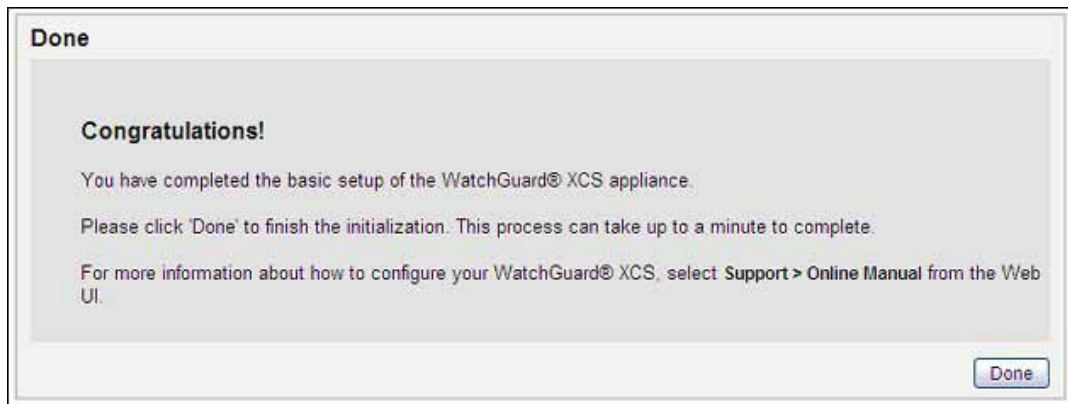
Intercept Option	Default Setting
Certainly Spam	Reject (Threshold: 99)
Probably Spam	Modify Subject Header (Threshold: 90)
Maybe Spam	Just Log (Threshold: 60)
Decision Strategy	Heuristic 1
Spam Words	Enabled
Mail Anomalies	Enabled
DNS/URL Block List	Enabled
Reputation Enabled Defense	Enabled
Token Analysis	Enabled
SPF	Enabled
DomainKeys	Enabled
Backscatter	Off

16. Click **Continue**.

17. From the **Email Traffic** drop-down list, select **Enabled** to start email traffic processing after the installation is complete.
If you select **Disabled**, you can start mail processing manually from **Activity > Status > Utilities** after the installation is complete.



18. Click **Continue**.
19. Click **Done** to complete the installation.
This process can take up to a minute to complete.



The main Dashboard appears.



3

Feature Key and Software Updates

Feature Key

A feature key is a license that enables you to activate your purchased feature set on your WatchGuard XCS. You must register the device serial number on the WatchGuard LiveSecurity® web site and retrieve your feature key before you can add it to the WatchGuard XCS. If you have not yet obtained a feature key, see “Get a WatchGuard device feature key” on page 2

If you did not enter your feature key in the Installation Wizard, you must add a feature key to the WatchGuard XCS to enable your purchased features and to start the processing and scanning of email messages.

Add a feature key

To add a new feature key:

1. Select **Administration > System > Feature Key**.
The Feature Key page appears.

The screenshot shows a web interface titled "Feature Key". It is divided into two main sections: "Summary" and "Features".

Summary

Appliance Model: XCS170
Appliance Serial: B0E842A6EF002
Download your feature key through LiveSecurity

Buttons: Remove, Update, Get Feature Key

Features

Features	Expiration	Time Left
No licensed features available.		

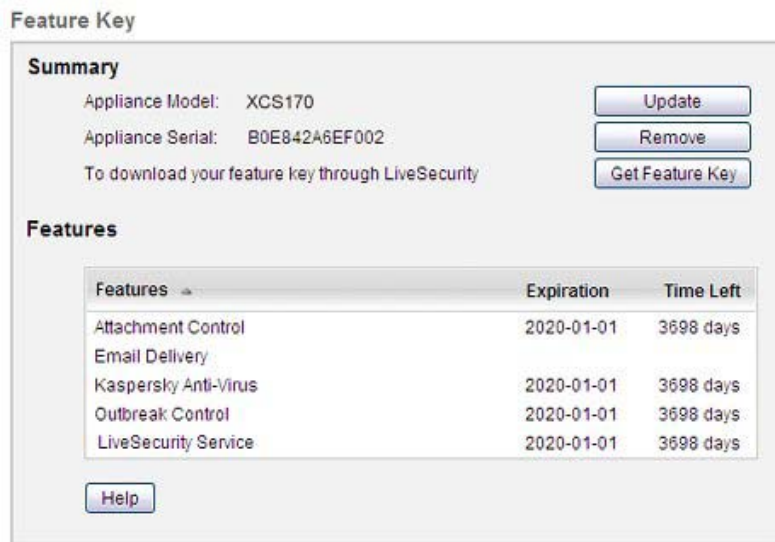
Buttons: Help

2. Click **Update**.
The Update Feature Key page appears.



The dialog box has a title bar 'Update Feature Key'. Below the title bar is a text prompt: 'Please enter your feature key:'. This is followed by a large, empty rectangular text input field. At the bottom of the dialog, there are two buttons: 'Update Key' and 'Cancel'.

3. Copy the text of the feature key file and paste it in the text box.
4. Click **Update Key**.
The Feature Key page appears with the new feature key information.



The 'Feature Key' page is divided into two main sections: 'Summary' and 'Features'.

Summary

Appliance Model: XCS170
Appliance Serial: B0E842A6EF002
To download your feature key through LiveSecurity

Buttons: Update, Remove, Get Feature Key

Features

Features	Expiration	Time Left
Attachment Control	2020-01-01	3698 days
Email Delivery		
Kaspersky Anti-Virus	2020-01-01	3698 days
Outbreak Control	2020-01-01	3698 days
LiveSecurity Service	2020-01-01	3698 days

Buttons: Help

Update a feature key

If you already have a LiveSecurity web site login and your WatchGuard device serial number is registered, you can update your feature key automatically.

To automatically update a feature key:

1. Select **Administration > System > Feature Key**.
The Feature Key page appears.

Feature Key

Summary

Appliance Model: XCS170

Appliance Serial: B0E842A6EF002

To download your feature key through LiveSecurity

Features

Features	Expiration	Time Left
Attachment Control	2020-01-01	3698 days
Email Delivery		
Kaspersky Anti-Virus	2020-01-01	3698 days
Outbreak Control	2020-01-01	3698 days
LiveSecurity Service	2020-01-01	3698 days

2. Click **Get Feature Key**.
Your feature key is downloaded from the LiveSecurity site and automatically updated on your XCS device.

Security Connection

Security Connection is a service that polls WatchGuard's support servers for new updates, security alerts, and Anti-Spam database updates. The WatchGuard XCS sends a notification to the administrator when new information and updates are available.

The Security Connection service is enabled by default after you install the WatchGuard XCS to make sure you automatically receive notifications for the latest software updates. After the initial installation, Security Connection immediately checks for new available updates. The Security Connection downloads any available updates for your system, but does not automatically install them.

To install software updates, from the Web UI, select **Administration > Software Updates > Updates**. For more detailed information on Software Updates, see "Software Updates" on page 25.



For security purposes, all Security Connection files are encrypted and contain an MD5-based digital signature that is verified after the file is decrypted.

To configure Security Connection:

1. Select **Administration > Software Updates > Security Connection**.

Security Connection

Security Connection

Enabled:

Frequency: daily

Auto Download:

Display Alerts:

Send Email:

Send Emails To: admin@example.com

Connect Now Apply Help

2. Select the **Enabled** check box.
3. From the **Frequency** drop-down list, select how often to run the Security Connection service: **daily**, **weekly**, or **monthly**.
4. To enable software updates to be downloaded automatically, select the **Auto Download** check box. *Updates are automatically downloaded, but not automatically installed. You must use Software Updates to manually install the updates.*
5. To enable Security Connection alert messages to appear on the system console, select the **Display Alerts** check box.
6. To send an email to the address specified in the **Send Emails To** text box, select the **Send Email** check box.
7. In the **Send Emails To** text box, type the email address to receive notifications.
8. Click **Apply**.
9. Click **Connect Now** to run Security Connection and check for new software updates.

Software Updates

To make sure your device software is up to date with the latest patches and upgrades, you must install any updates released for your version of software.

After the installation of the WatchGuard XCS, Security Connection immediately checks for new software and automatically downloads any available updates. The Security Connection does not automatically install these updates. You must manually install them on the **Software Updates** page.

Updates appear in two sections: *Available Updates* (on the device, but not yet installed) and *Installed Updates* (installed and active). You can install an available update, or delete an installed update. Software updates downloaded from Security Connection appear in the *Available Updates* section.

To install software updates:

1. Select **Administration > Software Updates > Updates**.

The Software Updates page appears.

The screenshot shows the 'Software Updates' interface. It is divided into two main sections: 'Installed Updates' and 'Available Updates (not installed)'. The 'Installed Updates' section is currently empty, displaying the message 'No updates or options have been installed.' The 'Available Updates (not installed)' section contains a table with one update entry. Above the table are controls for selecting updates, including 'Select All | None', 'Selected Updates', and 'Install' and 'Delete' buttons. Below the table is an 'Upload a Software Update' section with a text input field for the 'Software update file', a 'Browse...' button, and an 'Upload' button.

Name	Description	Version
<input type="checkbox"/> support_access	Enables Support Access	Release 8.0-0

2. If you manually downloaded your software update:
 - Click **Browse** and select the software update.
 - Click **Upload**.

The software update appears in the Available Updates section.
3. In the **Available Updates** section, select the software update.
4. Click **Install**.

After you install updates, you must restart the device.

Update Anti-Virus Pattern Files

If licensed, the Anti-Virus service is automatically enabled and started.

After the initial installation of the WatchGuard XCS, it may take up to the default of one hour to update your Anti-Virus pattern files to the most recent version. We recommend you update your pattern files immediately after installation.

To update your pattern files:

1. Select **Security > Anti-Virus > Anti-Virus**.
2. Go to the **Virus Pattern Files** section.



The screenshot shows a configuration window titled "Virus Pattern Files". It contains the following elements:

- "Kaspersky User-defined Server:" followed by an empty text input field.
- "Kaspersky User-defined Alternate Server:" followed by an empty text input field.
- "Update Interval:" followed by a dropdown menu currently set to "1 hour".
- "Manual Update:" followed by a button labeled "Get Pattern Now".
- "Kaspersky Anti-Virus Status:" followed by the text "Not updated".

3. Click **Get Pattern Now**.

4

Configure Message Delivery

Add Mail Routes

If you configured a primary email domain and an internal mail server during the initial installation of the WatchGuard XCS, a mail route is automatically set up for that mail server.

Use the *Mail Routing* page to configure additional domains for which to accept mail, and identify the destination mail servers to which to route messages.

To add and configure mail routes:

1. Select **Configuration > Mail > Routing**.

Sub. Domain	Route-to...	Port	MX	KeepOpen
example.com	10.0.2.25	25	X	✓
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: LDAP Routing, Upload File, Download File, Help, Add, Cut

2. To accept and relay mail for subdomains of the specified domain, select the **Sub** option.
3. In the **Domain** text box, type the domain for which mail is to be accepted.
For example, `example.com`.
4. In the **Route-to** text box, type the IP address for the mail server to which mail is delivered.
For example, `10.0.2.25`.
5. In the **Port** text box, type the port on which to deliver mail to this server.
The default is SMTP port 25.
6. If you need to look up the mail routes in DNS before delivery, select the **MX** option.
If this option is not enabled, MX records are ignored. You do not need to select this item unless you use multiple mail server DNS entries for load balancing and failover purposes. When you check the MX record, DNS sends the request to the next mail server in the list.

7. Select the **KeepOpen** option to make sure that each mail message to the domain is not removed from the active queue until delivery is attempted, even if the preceding mail failed or was deferred. *This option makes sure that local mail servers receive high priority.*



You must only use the KeepOpen option for reliable domains. If the domain is unavailable, it can result in system performance problems because of excessive error conditions and deferred mail.

8. Click **Add**.
9. Repeat the procedure for any additional domains and mail servers.

Upload mail routes

You can upload a list of mail routes in a text file. The file must contain comma or tab separated entries with one entry per line.

Use this format:

```
[domain],[route],[port],[ignore_mx],[subdomains_too],[keepopen]
```

For example:

```
example.com,10.0.2.25,25,on,off,off
```

You must use a text editor to create the file domains.csv.

To update a mail route file:

1. To download the mail route list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the mail route list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

Trust Internal Mail Servers

To allow internal mail systems to relay mail outbound through the WatchGuard XCS, you must configure a Specific Access Pattern. A Specific Access Pattern makes sure that your mail servers and their messaging traffic is trusted and not processed for spam.

If you configured an internal mail server during the initial installation of the WatchGuard XCS, a specific access pattern is automatically set up for that mail server.

To configure Specific Access Patterns for additional mail servers:

1. Select **Configuration > Mail > Access**.
2. Click **Add Pattern**.



The screenshot shows a dialog box titled "New Access Pattern". It contains the following fields and controls:

- Pattern:** A text box containing "10.0.2.25".
- Client Access:** A checked checkbox.
- HELO Access:** An unchecked checkbox.
- Envelope-From Access:** An unchecked checkbox.
- Envelope-To Access:** An unchecked checkbox.
- If pattern matches:** A dropdown menu with "Trust" selected.
- Buttons:** "Apply", "Cancel", and "Help" buttons at the bottom.

3. In the **Pattern** text box, type the IP address of the internal mail server.
For example, 10 . 0 . 2 . 25.
4. Select the **Client Access** check box.
5. From the **if pattern matches** drop-down list, select **Trust**.
6. Click **Apply**.

Modify Internal Mail Servers for Outbound Mail

Changes are required to your existing internal mail servers to route outbound mail through the WatchGuard XCS. You must configure your internal mail servers to use the hostname or IP address of the XCS device for SMTP delivery of outbound mail. The procedure depends on the type of internal mail server you use. See the instructions for your specific mail server to route outgoing mail through the WatchGuard XCS.

The instructions below are for a Microsoft® Exchange mail server.

Exchange 2000 and 2003

To add the WatchGuard XCS to the outbound configuration on an Exchange 2000 or Exchange 2003 server:

1. Open Exchange System Manager.
2. Select **Connectors**.
3. Go to the **Internet Mail SMTP Connector**.
4. Select the **Forward all mail through this connector to the following smart hosts:** option.
5. Type the IP address of your WatchGuard XCS system in square brackets.
For example, [10.0.1.25]
To add multiple systems, separate them with commas.
For example, [10.0.1.25], [10.0.2.25]
6. Click **OK**.

Multiple Exchange server configuration

In an environment with multiple Microsoft Exchange servers (not in a clustered configuration), you must configure each system to route outbound mail through the WatchGuard XCS. This can be performed on a per-server basis with the SMTP connector configuration on each server.

To provide a more efficient configuration, add an *SMTP Connector* to the **Exchange Routing Groups** configuration instead of the **Servers** configuration item. The Routing Group configuration applies to all your Exchange servers.

To configure the SMTP Connector in a routing group of Exchange servers:

1. Open the Exchange System Manager.
2. Select **Routing Groups**.
3. Select the **First Routing Group**.
4. Select **Add**.
5. Select **SMTP Connector**.
6. Type a name for the SMTP Connector.
For example, XCSConnector.
7. Select the **Forward all mail through this connector to the following smart hosts:** option.
8. Type the IP address of your WatchGuard XCS system in square brackets.
For example, [10.0.1.25]
To add multiple systems, separate them with commas.
For example, [10.0.1.25], [10.0.2.25]
9. In the **Local bridgeheads** section, click **Add**.
10. Add each Exchange server that must send mail through the WatchGuard XCS to the list.
Make sure you add all servers and not just the primary Bridgehead server.

11. Select the **Address Space** configuration tab.
12. Use the default values of **Type: SMTP**, **Address: ***, and **Cost: 1**.
13. Click **OK**.

Exchange 2007 and 2010

To add the WatchGuard XCS to the outbound configuration on an Exchange 2007 or Exchange 2010 server:

1. Open the Exchange Management Console.
2. Expand the **Organization Configuration** option.
3. Select **Hub Transport**.
4. Select the **Send Connectors** tab.
5. Right-click on the existing **Send Connector**.
6. Select **Properties**.
7. Go to the **Network** tab.
8. Select **Route mail through the following smart hosts:**.
9. Click **Add**.
10. Type the IP address of the WatchGuard XCS system to forward outbound mail to, such as: 10.0.1.25
Repeat this procedure to add the addresses of all of your WatchGuard XCS systems.
11. Click **OK**.

Start Messaging Services

When you have configured the WatchGuard XCS with your required networking information and mail routes, you can start the messaging system and start to process messages.

To start the messaging system:

1. Select **Activity > Status > Utilities**.
2. In the **Messaging System Control** section, click **Start**.
The status message changes from "Messaging System is stopped" to "Messaging System is running".

