



WatchGuard® Quarantine Management Server v2.0 Installation Guide

QMS 500, 1000

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Part Number: 275-3679-001

Document Version: 1.0

Revised: 2/9/10

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.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online:

<http://www.watchguard.com/help/documentation/>



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.

For more information, please call 206.613.6600 or visit www.watchguard.com.

ADDRESS

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

SALES

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Table of Contents

| | | |
|------------------|--|-----------|
| Chapter 1 | Getting Started | 1 |
| | Before You Begin | 1 |
| | Verify basic components | 1 |
| | Hardware installation | 1 |
| | Physical location..... | 1 |
| | Connect the monitor and keyboard..... | 2 |
| | Connect the network interfaces | 2 |
| | Get a WatchGuard device feature key | 2 |
| | Internal deployment..... | 5 |
| Chapter 2 | Install the Quarantine Management Server | 9 |
| | Use the Console to Install the Server..... | 9 |
| | Supported web browsers..... | 13 |
| | Connect to the Web UI..... | 13 |
| Chapter 3 | Licensing and Software Updates | 15 |
| | Feature Key | 15 |
| | Add a feature key to the Quarantine Management Server..... | 15 |
| Chapter 4 | Quarantine Server Configuration | 19 |
| | Network Configuration..... | 19 |
| | Network interface configuration..... | 20 |
| | Start Mail System | 26 |
| Chapter 5 | User Accounts | 27 |
| | Create User Accounts..... | 27 |
| | LDAP User Accounts | 31 |
| | Define directory servers..... | 31 |
| | Import Settings | 34 |
| | Mirror LDAP accounts as local users..... | 35 |
| | Remote Authentication | 35 |
| | Configuring LDAP Remote Authentication | 35 |
| Chapter 6 | WatchGuard XCS Configuration | 37 |
| | Add Mail Routes to the Quarantine Server | 37 |

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 Quarantine Management Server (QMS) device
- A keyboard and monitor
- Ethernet cables
- Power cables

Hardware installation

For detailed instructions on how to install the Quarantine Management Server device in an equipment rack, see the *Hardware Setup Guide*.

Physical location

To safely install your Quarantine Management Server device, we recommend you select a physical location that has these specifications:

- Install the server 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 server for console use, to make sure that keystroke logging devices cannot be added to the keyboard connection, connect the monitor and keyboard directly to the server.
- 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 monitor and keyboard

For the initial installation, you must connect a monitor and keyboard (USB or PS/2) to the server to operate the system console. After the initial console configuration is complete, you can use the Web UI to manage the server remotely.

Connect the network interfaces

Before installation, make sure that at least one of the network interfaces is physically connected to the network. This enables you to easily confirm that you have correctly identified the server on the network and confirm the connectivity status.

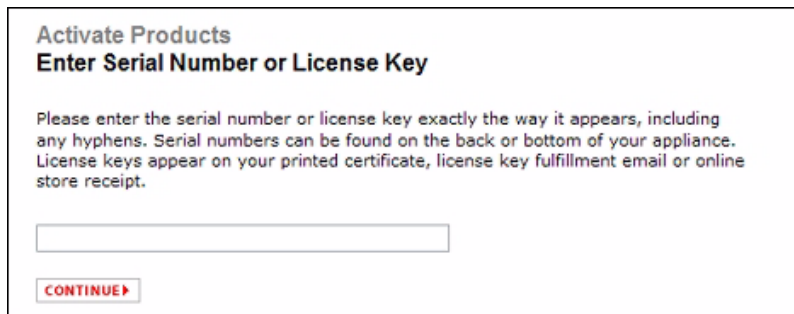
When you install your server, for all hardware models, we recommend that you use the first onboard Ethernet network interface (NIC 1) at the left of the device to connect to your LAN. This is the first default interface assigned by the system. After the installation is complete, you can configure an additional network interface as your external interface that connects to the Internet.

Get a WatchGuard device feature key

A feature key is a license that enables you to activate your purchased feature set on your Quarantine Management Server. You must register the device serial number on the WatchGuard LiveSecurity® web site 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 Quarantine Management Server.
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 Quarantine Management Server, such as `hostname` in the FQDN (Fully Qualified Domain Name) `hostname.example.com`.

Domain Name

The domain name associated with the assigned hostname. This is the domain where messages are sent (for example, `example.com`).

Internal IP Address

Select an IP address for the internal LAN trusted network interface. This address is used to connect remotely to the server with the Web UI.

External IP Address

Select an IP address for the external network interface (if required). This is the WAN 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 server. This is usually your network router.

WatchGuard XCS address

The domain name or IP address of your WatchGuard XCS device that sends quarantined mail to the Quarantine Management Server.

Optional Network Cards

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

DNS Servers

The addresses of your DNS (Domain Name Service) name servers. This includes both a primary and a secondary server.

NTP Servers

The addresses of your NTP (Network Time Protocol) servers for time synchronization. This includes both a primary and a secondary server.

Before you configure your device, write your network information in this table:

| Table 1: Basic Network Settings | | Example |
|--|---------------------|----------------|
| Hostname | _____ | hostname |
| Domain Name | _____ | example.com |
| Internal IP Address (LAN, Trusted) | ____.____.____.____ | 10.0.1.20 |
| Subnet Mask | ____.____.____.____ | 255.255.0.0 |
| Gateway Address | ____.____.____.____ | 10.0.1.1 |

| Table 1: Basic Network Settings | Example |
|--|--------------------------|
| WatchGuard XCS address ____.____.____.____ | 10.0.1.10 |
| 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 |

Quarantine Management Server Deployment

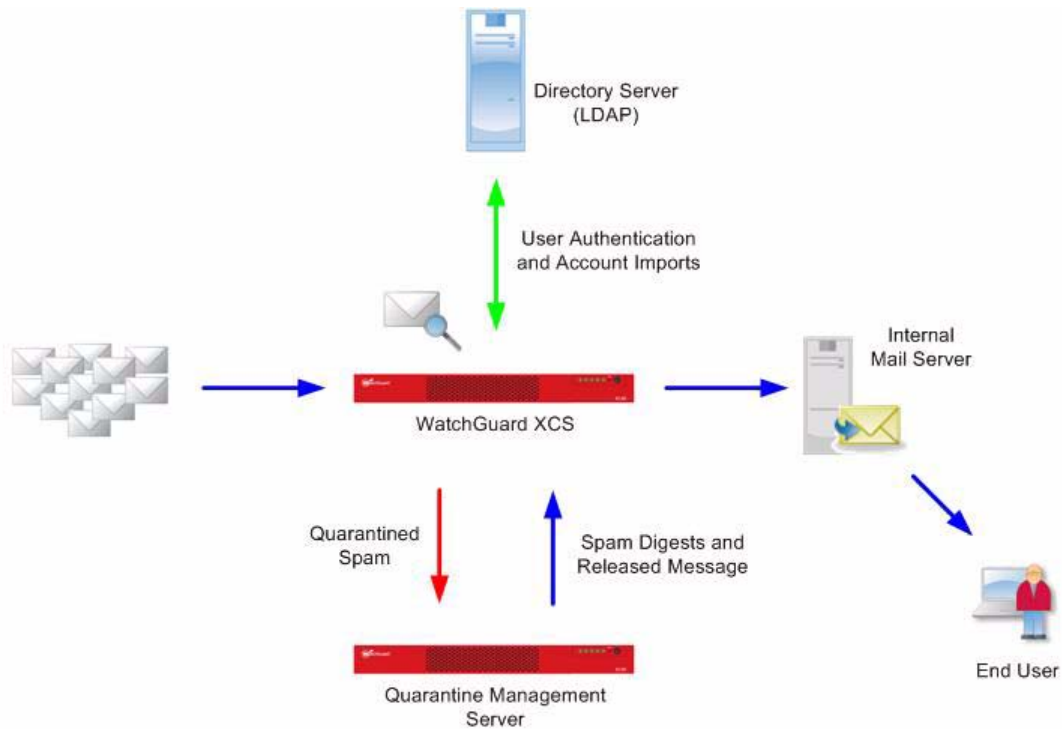
You can choose from two deployment methods for your Quarantine Management Server: internal deployment or hosted deployment.

Internal deployment

In a basic internal deployment, the Quarantine Management Server is installed on the same network as the WatchGuard XCS device. Incoming mail is processed by the WatchGuard XCS device and any spam to be quarantined is redirected from the WatchGuard XCS device to the Quarantine Management Server.

Spam digest notification messages and messages released from the Quarantine Server are sent from the WatchGuard XCS device to the internal mail servers, where they are received by the end user.

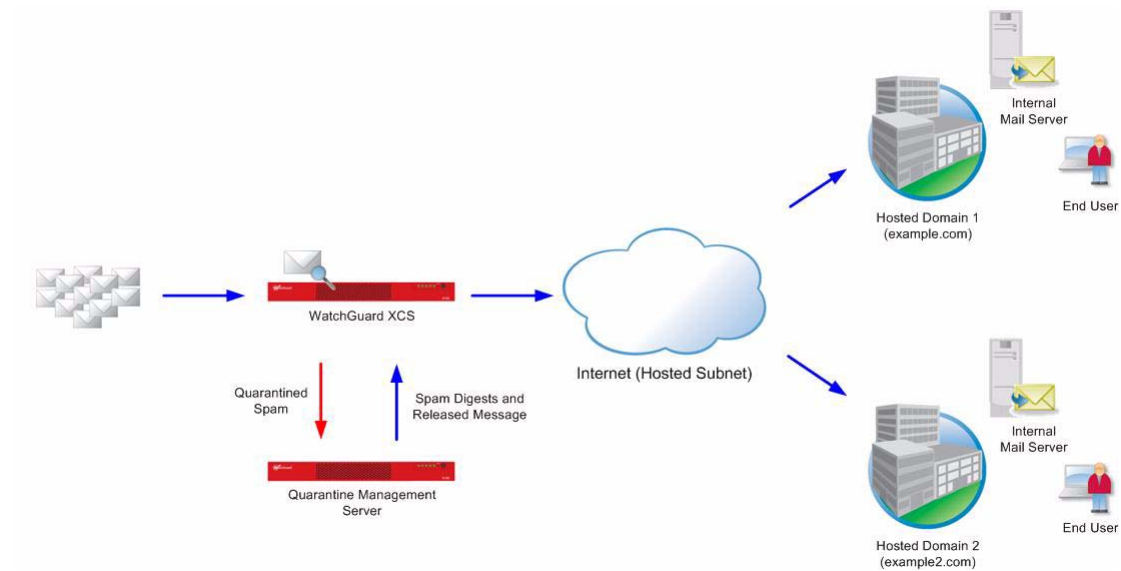
End users can log in to the Quarantine Management Server to manage their specific quarantine settings, select the language template for their spam digest message, and manage their trusted and blocked senders lists.



Hosted deployment

In a hosted service deployment, the Quarantine Management Server is deployed at the same location as the WatchGuard XCS device and can be accessed by external hosted servers and users.

Because all email to the recipient domain email servers is processed and sent by the WatchGuard XCS device, the Quarantine Management Server can support multiple domains.



Network Firewall Configuration

To enable the Quarantine Management Server 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 for sending and receiving of mail) | X | X | X | X | TCP |
| 53 | DNS queries | | X | | X | TCP/UDP |
| 80 | WebMail Access | X | | X | | TCP |
| 123 | Network Time Protocol (NTP) | | X | | X | UDP |
| 389 | LDAP | | | | X | TCP |
| 443 | Software Updates | | X | | | TCP |
| 443 | Secure WebMail Access | X | | X | | TCP |
| 443 | Web UI connections | X | | X | | TCP |
| 514 | Syslog | | | | X | UDP |
| 636 | LDAPS | | | | X | TCP |
| 1812 | RADIUS Server | | | | X | UDP |
| 10101 | Support Access | X | X | | | TCP |

2

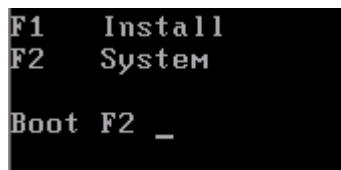
Install the Quarantine Management Server

Use the Console to Install the Server

To use the console to install your Quarantine Server:

1. Unpack the system, cables, and documentation from the shipping carton.
2. Connect the power cable to the server and a power source. We recommend you use a UPS (Uninterruptible Power Supply).
3. Connect a monitor and keyboard to the server.
You can use a USB or PS/2 type keyboard.
4. Connect the first onboard Ethernet network interface at the left of the device (NIC 1) to the network.
For the initial installation, only the internal LAN network interface must be connected to connect to the server with a web browser. You can configure any additional network interfaces after installation.
5. Power on the server.

These options appear when the server starts up:

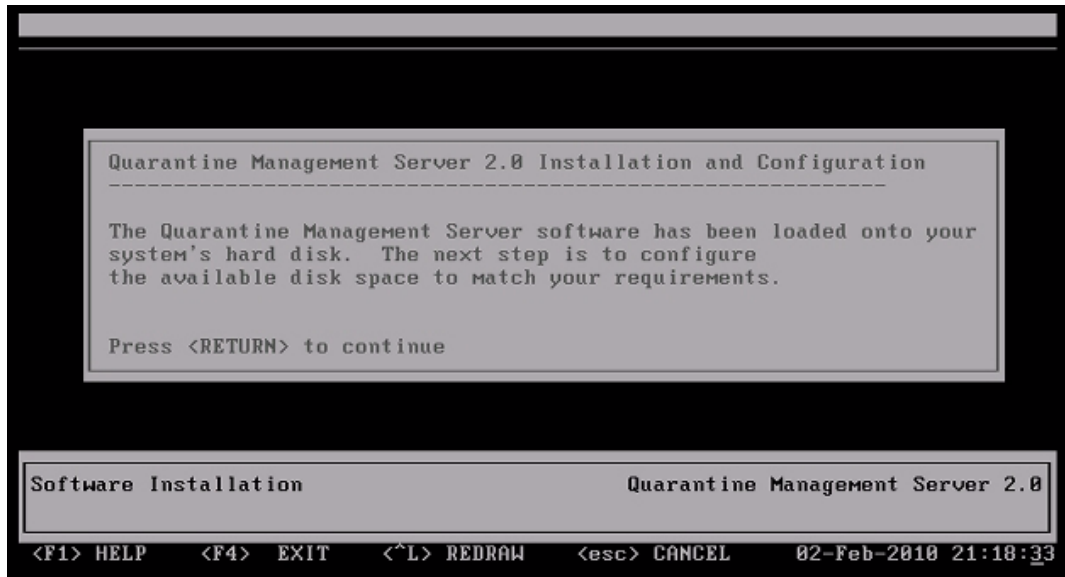


```
F1  Install
F2  System

Boot F2 _
```

- **F1 Install** — Use the **Install** option to reinstall the server software and restore the server to factory default settings.
- **F2 System** — Use the **System** option to load the current installation. This option is chosen by default after a few seconds.

6. Press **F2**.
Or, wait for the **System** option to be selected automatically.



7. Press **Return** or **Enter** to continue the installation.
8. Select the disk installation type.



- **Auto** — This option uses the default values for disk space allocation for log file storage, message storage, backup area, and database area.
- **Custom** — This option enables you to modify the default values for disk space allocation. To increase the size of the backup partition for large backups that include log and report data, select **Custom**.
 - The hard disk is detected and identified. Select **Continue**.
 - To edit the disk layout, select **Edit**.
Use the arrow keys to move to another field.

- Press **Enter** to use the current action.
For example, + 100 or + 1000.
The values are in megabytes. Before you increase the value for one file system, you must decrease the value of another file system.
 - When finished, select **Done**, and then **OK** to exit the disk layout screen.
9. Select **Yes** to erase the hard disks.
 10. Click **OK** to configure a network interface.

This is the network interface and IP address you use to connect to the server with a web browser after console installation is complete. We recommend that you configure the internal LAN interface first and use this interface to complete the installation process. Use the first onboard Ethernet connector at the left of the device (NIC 1). When the installation is complete, you can configure additional interfaces on the **Network Settings** screen.



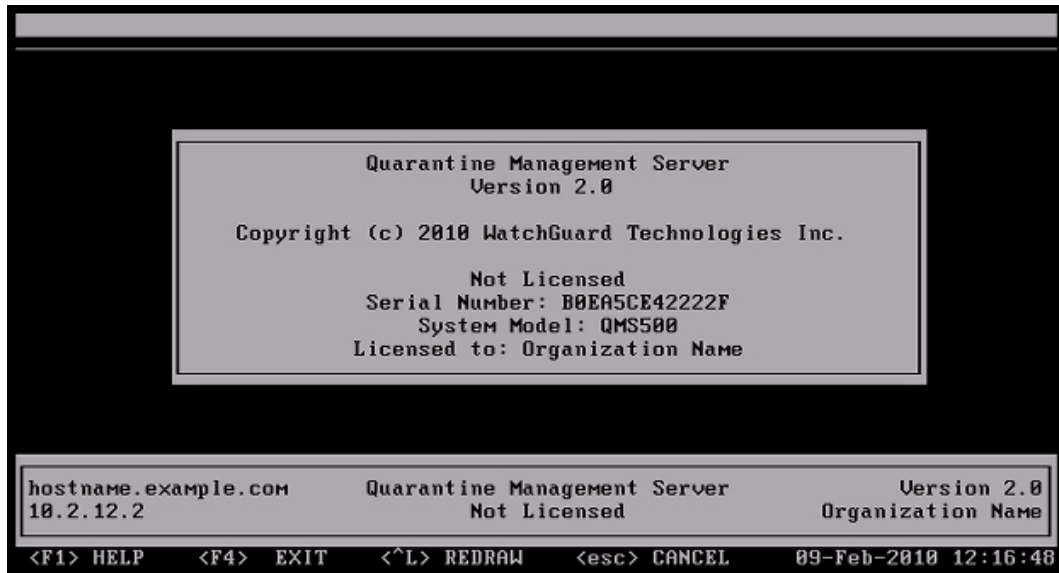
11. Select the **Interface** to configure.
For this example, select **em0**.
This is the first onboard Ethernet connector at the left of the device (NIC 1).
12. Type the **Hostname** for the server.
For example, if your fully qualified domain name is hostname.example.com, type `hostname`.
13. Type your **Domain**.
For this example, type `example.com`.
14. Type the **IP Address** for this interface.
For this example, type `10.0.1.20`.
15. Type the **Subnet mask**.
For this example, type `255.255.0.0`.
16. Type the **Gateway** (typically the router) for your network.
For this example, type `10.0.1.1`.
17. Type the IP address of your DNS **Name Server**.
For this example, type `10.0.2.53`.
18. Select **OK** to continue.

19. Set the region and time zone for your location.



The initial configuration is complete and the system console screen appears.

A warning message that the "Mail System is stopped!" appears because message services have not yet started. You can safely ignore this message.



20. To continue installation, connect to the server with a web browser.

Run the Web UI Setup Wizard

To continue the configuration process and run the Setup Wizard, you must use the Web UI to connect to the server.

Supported web browsers

You can use these web browsers with the Web UI:

- Internet Explorer 6 (Windows XP, Windows 2000, Windows 2003)
- Internet Explorer 7 (Windows XP, Windows 2000, Windows 2003, Windows Vista)
- Firefox 3.0 and newer (Windows, Linux, Mac)

Make sure your screen resolution is at least 1024x768.

Connect to the Web UI

To connect to the Web UI:

1. Open a web browser and go to the IP address of the Quarantine Management Server.

For example, `http://10.0.1.20`

The login page appears.



A security certificate notification appears in the browser because the system uses a self-signed certificate. You can safely ignore the warning (Internet Explorer) or add a certificate exception (Mozilla Firefox).

2. Type the default **Email** account name and **Password**.

When you connect to the server for the first time after installation, the default settings are:

- Email — **admin**
- Password — **admin**

WatchGuard™

• Quarantine Management Server Initialization

Login (hostname.example.com)

Email:

Password:

Login

Install the Quarantine Management Server

3. Type an **Organization Name** and **Server Admin Email** address for this server.
The server admin email address receives all system alerts and notifications.

The screenshot shows the WatchGuard Product Initialization interface. On the left, a sidebar lists three steps: Step 1 (Customer Information), Step 2 (Change Password), and Done! (Ready to go!). Step 1 is currently active. The main content area is titled 'Product Initialization' and contains 'Step 1: Customer Information'. It features two input fields: '*Organization Name:' with the value 'Organization Name' and '*Server Admin Email:' with the value 'admin@example.com'. Both fields have green checkmarks to their right. A 'Complete Step 1' link is located at the bottom right of the Step 1 section. Below this, the 'Step 2: Change Password' section is visible but currently empty.

4. Click **Complete Step 1**.
The Change Password page appears.
5. 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.

The screenshot shows the WatchGuard Product Initialization interface. The sidebar now shows Step 1 as completed with a green checkmark and Step 2 as active. The main content area is titled 'Product Initialization' and contains 'Step 2: Change Password'. It features two input fields: '*New Password:' and '*New Password (again):', both with masked characters and green checkmarks. A green checkmark and the text 'The new passwords match.' are displayed below the second field. A 'Complete Step 2' link is located at the bottom right of the Step 2 section. Below this, the 'Done!' section is visible but currently empty.

6. Click **Complete Step 2**.

The screenshot shows the WatchGuard Product Initialization interface. The sidebar now shows Step 1 and Step 2 as completed with green checkmarks, and the 'Done!' section as active. The main content area is titled 'Product Initialization' and contains the 'Done!' section. It features a green checkmark and the text 'Press 'continue' to complete the initialization.' A 'Continue' button is located at the bottom right of the Done! section.

7. Click **Continue** to complete the installation.

Before you start the messaging system, you must license your server and configure basic mail and network settings. For more information, see the subsequent sections.

3

Licensing and Software Updates

Feature Key

A feature key is a license that enables you to activate your purchased feature set on your Quarantine Management Server. You must register the device serial number on the WatchGuard LiveSecurity® web site and get your feature key before you can add it to the Quarantine Management Server.

For more information about how to get a feature key, see “Get a WatchGuard device feature key” on page 2.

Add a feature key to the Quarantine Management Server

To add a new feature key:

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

The screenshot shows the 'Feature Key' page. It has a title bar 'Feature Key' and a 'Summary' section. The summary includes 'Appliance Model: QMS500', 'Appliance Serial: B0EA5CE42222F', and a note 'To download your feature key through LiveSecurity'. There are three buttons: 'Update', 'Remove', and 'Get Feature Key'. Below the summary is a 'Features' section with a table header: 'Features', 'Expiration', and 'Time Left'. The table body contains the text 'No licensed features available.' and a 'Help' button is located at the bottom left of the page.

2. Click **Update**.

The Update Feature Key page appears.

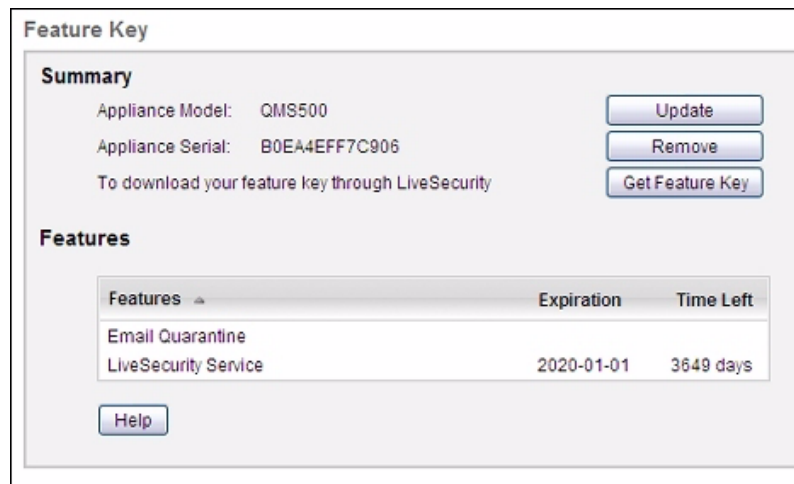


The image shows a dialog box titled "Update Feature Key". It contains a text input field with the placeholder text "Please enter your feature key:". Below the input field are two buttons: "Update Key" and "Cancel".

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 image shows the "Feature Key" page. It has a "Summary" section with the following information:

- Appliance Model: QMS500
- Appliance Serial: B0EA4EFF7C906
- To download your feature key through LiveSecurity

There are three buttons in the Summary section: "Update", "Remove", and "Get Feature Key".

Below the Summary section is a "Features" section with a table:

| Features | Expiration | Time Left |
|----------------------|------------|-----------|
| Email Quarantine | | |
| LiveSecurity Service | 2020-01-01 | 3649 days |

There is a "Help" button at the bottom of the page.

Enable Security Connection

The Security Connection is a service that polls your WatchGuard support servers for new updates. You can configure your server to send a notification to the administrator when new updates are received.

To make sure you automatically receive notifications for the latest software updates, we recommend that you enable Security Connection immediately after the initial product installation.



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

To enable and connect to Security Connection:

1. Select **Administration > Software Updates > Security Connection**.
The Security Connection page appears.

Security Connection

Security Connection

Enabled:

Frequency:

Auto Download:

Display Alerts:

Send Email:

Send Emails To:

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.

Install Software Updates

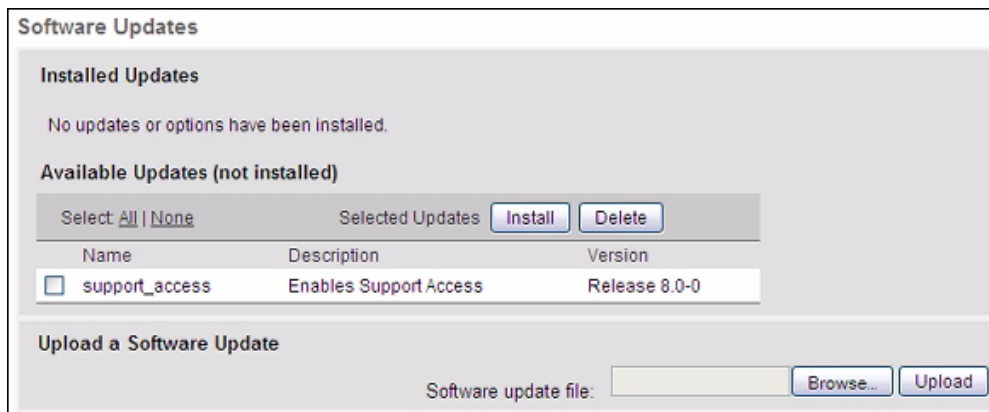
To make sure your system software is up to date with the latest patches and upgrades, you must install any updates released for your version of software. If you enable Security Connection, any available software updates are downloaded automatically and appear on the **Software Updates** page.

Updates appear in two sections: *Available Updates* (on the server, 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.



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 server.

4

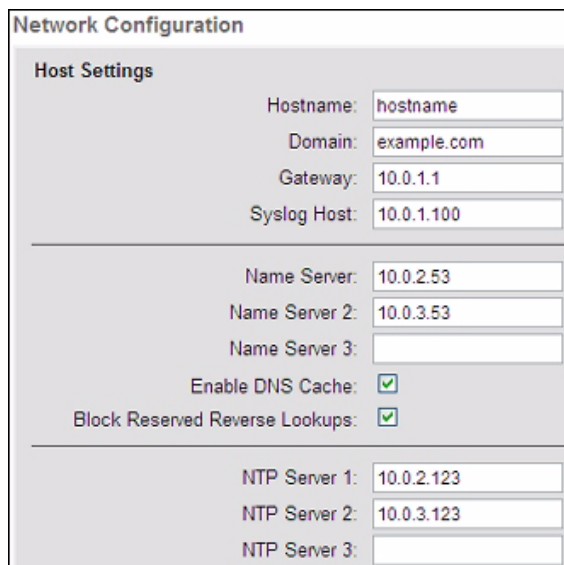
Quarantine Server Configuration

Network Configuration

When you complete the initial installation process for your Quarantine Server, you configure the basic network information for your server. From the **Network Configuration** page, you can configure other network interfaces and advanced network settings. These settings include options for the DNS and NTP servers for your network.

To configure your network settings:

1. Select **Configuration > Network > Interfaces**.
The Network Configuration page appears.



The screenshot shows a web interface titled "Network Configuration". It is divided into three sections:

- Host Settings:** Contains four text input fields: "Hostname" (value: hostname), "Domain" (value: example.com), "Gateway" (value: 10.0.1.1), and "Syslog Host" (value: 10.0.1.100).
- Name Servers:** Contains three text input fields: "Name Server" (value: 10.0.2.53), "Name Server 2" (value: 10.0.3.53), and "Name Server 3" (empty). Below these are two checkboxes: "Enable DNS Cache" (checked) and "Block Reserved Reverse Lookups" (checked).
- NTP Servers:** Contains three text input fields: "NTP Server 1" (value: 10.0.2.123), "NTP Server 2" (value: 10.0.3.123), and "NTP Server 3" (empty).

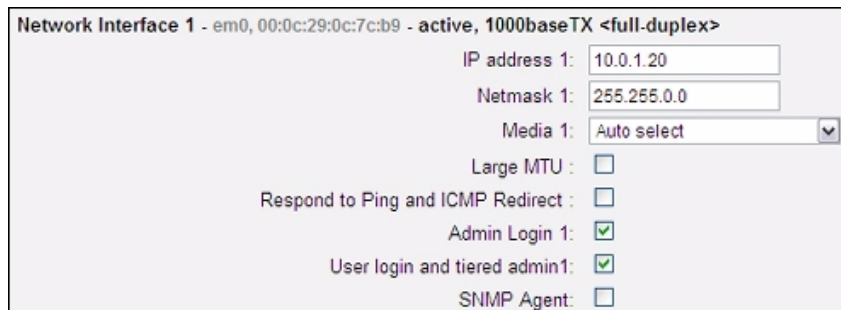
2. In the **Hostname** text box, type the hostname (not the Fully Qualified Domain Name) of this server. For example, if your Fully Qualified Domain Name is hostname.example.com, type `hostname`.
3. In the **Domain** text box, type the domain name for your server. For this example, type `example.com`.

- In the **Gateway** text box, type the IP address of the default route for this server.
This is usually your local router.
- If you use a syslog host on your network, in the **Syslog Host** text box, type the name of your syslog host.
A syslog host collects and stores log files from many sources.
- In the **Name Servers** text boxes, type the name of your primary and secondary DNS servers.
At least one DNS (Domain Name Service) name server must be configured for hostname resolution. We recommend that you specify at least one secondary DNS server to use when the primary DNS server is unavailable.
- To enable DNS caching, select the **Enable DNS Cache** check box.
This option is enabled by default and provides the best performance in most cases. When this option is enabled, the system determines which of the configured DNS servers sends the fastest response, and caches the result.
Clear the **Enable DNS Cache** check box to:
 - Use the configured DNS servers in the order they appear
 - Use your ISP DNS servers as failover servers
 - Use external proxy servers for system updates (for example, Anti-Virus)
- To make sure private reserved IP addresses are not used in a reverse lookup to a DNS server, select the **Block Reserved Reverse Lookups** check box.
This option is enabled by default.
Clear the **Block Reserved Reverse Lookups** check box if reverse lookups for reserved addresses are required in your network environment.
- In the **NTP Server** text boxes, type the IP addresses for your primary and any secondary time servers.
We recommend that you specify secondary NTP servers to use if the primary NTP server is unavailable.

Network interface configuration

For each network interface, you can set these options:

- Type an **IP Address** for this interface.
For example, 10.0.1.20.



Network Interface 1 - em0, 00:0c:29:0c:7c:b9 - active, 1000baseTX <full-duplex>

IP address 1: 10.0.1.20

Netmask 1: 255.255.0.0

Media 1: Auto select

Large MTU:

Respond to Ping and ICMP Redirect:

Admin Login 1:

User login and tiered admin1:

SNMP Agent:

- Type the **Netmask** for this interface.
For example, 255.255.0.0.
- Select the **Media** type for the network card.
For automatic configuration, select **Auto select**.

4. Enable these additional network interface options as appropriate for your network.
Some options only appear if you enabled the related feature.

Large MTU

Sets the MTU (Maximum Transfer Unit) to 1500 bytes. This can improve the connection performance for servers on the local network.

The default MTU setting is 576 bytes. For most organizations, the default setting is sufficient. We recommend you do not change this setting unless instructed to do so by Technical Support.

Respond to Ping and ICMP Redirect

Enables ICMP ping requests to this interface. When you select this option, you can complete network connectivity tests for this interface, however, this interface is then more susceptible to denial of service ping attacks.

User Login and tiered admin

Enables access to this interface for administrative purposes, which includes tiered admin users and end user logins for spam quarantine.

SNMP Agent

Enables access to the SNMP (Simple Network Management Protocol) agent through this interface.

5. Click **Apply** to save your network settings.
You must reboot the system for your network settings to take effect.

Default Mail Relay

To integrate the WatchGuard XCS device with the Quarantine Server, you must configure the **Default Mail Relay** for the Quarantine Server with the address of the WatchGuard XCS device.

To configure the mail delivery settings:

1. Select **Configuration > Mail > Delivery**.
The Delivery Settings page appears.
2. In the **Relay to** text box, type the full host name or IP address of the WatchGuard XCS device.

Delivery Settings

Delivery Settings

Maximum time in mail queue: 5

Maximum time in queue for bounces: 5

Maximum original message text in bounces: 5000

Time before delay warning: 4

Time to retain undeliverable notice mail:

Mail Relay

Relay To: 10.0.1.10

SMTP Port: 25

Ignore MX record:

Enable client authentication:

User ID:

Password:

Confirm Password:

3. Click **Apply**.

Quarantine Configuration

The Quarantine Management Server allows spam messages from the WatchGuard XCS device to be redirected to the local quarantine storage area. You can configure global settings for spam expiration times, disk space quotas, quota and disk full actions, and spam digest summary messages. You can also customize policies to configure quarantine settings for specific domains and users.

To configure the global settings for the Quarantine Management Server:

1. Select **Configuration > Mail > User Quarantine**.

The *User Spam Quarantine* page appears.

User Spam Quarantine

User Spam Quarantine Configuration

Enable User Spam Quarantine:

Expiry Time (days):

Per user spam quota:

Reserved disk space:

Quota exceeded action:

Disk full action:

Unknown user action:

User Digest Settings

Enable digest email:

New messages only:

Maximum messages per digest:

Digest source email address:

Generate digests:

at:

Default template:

Alternate template #1:

Alternate template #2:

Alternate template #3:

2. Select the **Enable User Spam Quarantine** check box.

If you do not enable this option:

- Spam digest notifications are not sent and users cannot log in to the Quarantine Server.
- Spam messages are still accepted and quarantined.

3. In the **Expiry Time** text box, type the expiration time for mail in each quarantine folder.
Any mail quarantined for longer than the specified time is deleted. We recommend that you set the time difference between the expiry time and spam digest time to a value that enables each process to complete before the next process is run. The expiry process runs nightly at 12:10 AM.
4. To limit the amount of quarantined mail that is stored for each user, in the **Per User Spam Quota** drop-down list, select a value in megabytes.
5. In the **Reserved Disk Space** text box, type a value (in KB).
The default value is 1000000 KB.
If the free disk space is less than the value you select, the **Disk Full Action** you specify is performed.
If you do not want to check the available disk space, type 0.

6. In the **Quota Exceeded Action** drop-down list, select the action to perform if the disk space quota for a specific user is exceeded.
 - **Discard** — The message is discarded and a notification is not sent to the sender or recipient.
 - **Release to User** — The message is not quarantined and is immediately released to the mailbox of the end user.
 - **Queue** — The message is placed in the queue for delivery when disk space is recovered.
7. In the **Disk Full Action** drop-down list, select the action to perform if the disk is full, or the **Reserved Disk Space** value is reached.
 - **Discard** — The message is discarded and a notification is not sent to the sender or recipient
 - **Release to User** — The message delivery is deferred, and is placed in the user's quarantine area when there is available disk space.
 - **Temporarily Reject** — Sends an error message to the sending server and does not accept the message. The mail delivery can be attempted again after a period of time.
8. In the **Unknown User Action** drop-down list, select the action to perform if the recipient for a quarantined message is for a user who does not exist as a local or mirror account.
 - **Create new account** — A user account is automatically created on the Quarantine Management Server. Before this user can log in, the administrator must configure a password for the user.
 - **Discard message** — The message is discarded and a notification is not sent to the sender or recipient.
 - **Bounce message** — The message is rejected and sent back to the sender.



*If a message is bounced back to the sender, the WatchGuard XCS device may train this message as legitimate. We recommend that you select the **Discard** message option instead of **Bounce**.*

9. To send a spam digest notification message to users when messages are in their quarantine folders, select the **Enable Digest Email** check box.
These summary messages are based on the configured spam digest template.
10. To send only the most recent spam summary email, select the **New Messages Only** check box.
If you do not select this option, the digest message users receive includes both the new messages that have arrived since the last digest, and the older messages. The spam digest is only sent if there are new messages in the quarantine folder.
11. In the **Maximum Messages Per Digest** text box, type the maximum number of message headers to send in the notification message.
The default setting is 200 message headers. Select a value from 0 to 100000. To send all message headers, set the value to 0.
12. In the **Digest source email address** text box, type the email address from which to send the spam quarantine digest messages.
For example, `quarantine@hostname.example.com`.
13. In the **Generate Digests** text box, select the specific days and time of day to send the spam digest message.



The Spam Digest processing begins at the time you select, but the summary notifications are not delivered until processing (which can take several hours, depending on the number of users) is complete.

14. In the **Default Template** drop-down list, select the template to use as the spam digest template for all users.

15. In the **Alternate Template** drop-down list, select the template to make available to a user.
End users can log in to the Quarantine Management Server to modify the template they use to receive the spam digest. For example, a user can specify an alternate language template to use for the spam digest.
16. To add a link in the spam summary message that end users can click to modify their Quarantine Server passwords, select the **Allow Changing Password** check box.

The screenshot shows a configuration window with the following sections and options:

- Web user interface**
 - Allow changing password:
 - Require SSL encryption:
- New Users**
 - Enable new user notification:
 - Length of generated password:
- New user notification email**
 - To: New User <%RECIPIENT%>
 - From: System Administrator <%FROM%>
 - Subject: New Spam Quarantine Account Created
 - A new account was created for you to hold your quarantined spam messages.
 - You may login by accessing: %WEBMAIL_URL%

At the bottom of the window are four buttons: **Apply**, **Purge Expired Spam**, **Notify All Users**, and **Help**.

17. To make sure web links in the spam digest use HTTPS links for SSL encryption, select the **Allow SSL Encryption** check box.
This protects communications between the end user client and the Quarantine Server when spam quarantine actions are performed directly from the spam digest notification.
18. To send an email to new users with their account details, select the **Enable new user notification** check box.
This notification is sent to users when automatic account creation is enabled for new users.
19. In the **Length of generated password** text box, type the number of characters the password for an automatically created new user account must use.
The default setting is 9.
20. Click **Apply**.

Start Mail System

When the Quarantine Server configuration is completed, you can start the mail system.

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



The Quarantine Server is now ready to accept mail for quarantine from the WatchGuard XCS device. For detailed information on how to create user accounts, and configure your WatchGuard XCS device to send quarantined mail to the Quarantine Server, see the subsequent sections.

5

User Accounts

Create User Accounts

The Quarantine Management Server requires an account for each user to store their quarantined spam messages from the WatchGuard XCS device.

There are three ways to add accounts to the Quarantine Server:

- **Manual creation of Local Accounts** — Administrators must manually add each local user account. This method is recommended only for small deployments with a manageable number of users.
- **Automatic creation of Local Accounts** — If the Quarantine Server receives a message to be quarantined and that user account does not already exist, the Quarantine Server can automatically create a local account based on the recipient email address. This method is recommended for organizations that do not use LDAP directory services, but do support multiple independent domains.



The user will not be able to log in to this account until the administrator assigns a password for the account or sets the system to automatically generate a password for the user.

- **LDAP Import of User Accounts** — User account information can be imported from an LDAP directory, and the accounts mirrored locally on the Quarantine Server. If you enable remote authentication, users who log in to the Quarantine Server are automatically authenticated to the LDAP directory server.

Local User Accounts

To create local user accounts for the Quarantine Server:

1. Select **Administration > Accounts > Local Accounts**.
2. Click **Add**.

3. In the **User ID** text box, type the user name for the new user.
For example, if the email address for the user is user@example.com, type `user`.
4. In the **Domain for user** text box, type the domain name for this user.
For example, `example.com`.
5. To forward messages for this user to another email address, in the **Forward email to** text box, type another email address.
6. In the **Set Password** text box, type the password for the user.
7. In the **Confirm Password** text box, type the password again.
We recommend that users change their passwords the first time they log in. If a user account was automatically created by the Quarantine Server, the administrator must set a password before the user can log in.
8. Select a **Strong Authentication** method, if required.
9. In the **Disk Space Quota** text box, type the maximum disk space size (in MB) to allocate to this user in the quarantine area.
The **Disk Space Quota** value you select cannot exceed the default global value that you set on the **User Spam Quarantine** page (**Per user spam quota** option).
To use the default global value, type `0`, or do not set a value.
10. Select any additional **Administrator Privileges**.
11. Click **Create**.

Upload and download user accounts

You can upload lists of users in comma or tab separated text files. You can specify the login ID, password, email address, and disk quota in megabytes. Use this format:

```
[login],[password],[email address],[quota]
```

For example:

```
user1,ajg7rY,user1@example.com,0
```

```
user2,gh39ds,user2@example.com,100
```


You must use a text editor to create the file (user.csv) in csv format.

To create the user list text file:

1. To download the user list from the Quarantine Server, click **File Download**.
2. Open the file and update the user list.
3. Click **File Upload** and upload the edited file to the Quarantine Server.

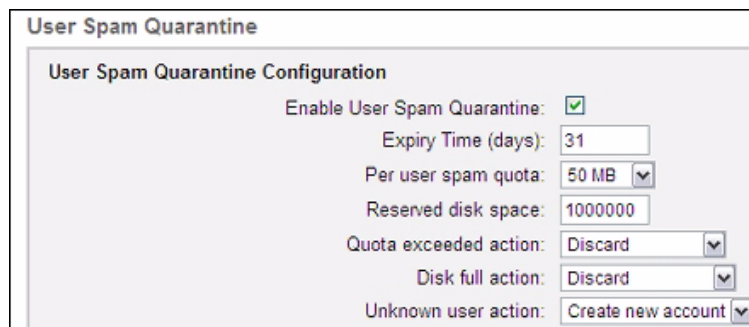
Automatic User Account Creation

If the Quarantine Server receives a message to be quarantined for a user account that does not already exist, the Quarantine Server can automatically create a local account based on the recipient email address. Before the user can log in to this account, the administrator must either manually create a password for the account, or configure the account to automatically generate a password.

 *Accounts will not be automatically created for user names with the following punctuation symbols: |, ' , ` , ! , \$, % , ~ . Any quarantined messages for these users are discarded.*

To enable automatic user account creation:

1. Select **Configuration > Quarantine > User Spam Quarantine**.



User Spam Quarantine Configuration

Enable User Spam Quarantine:

Expiry Time (days): 31

Per user spam quota: 50 MB

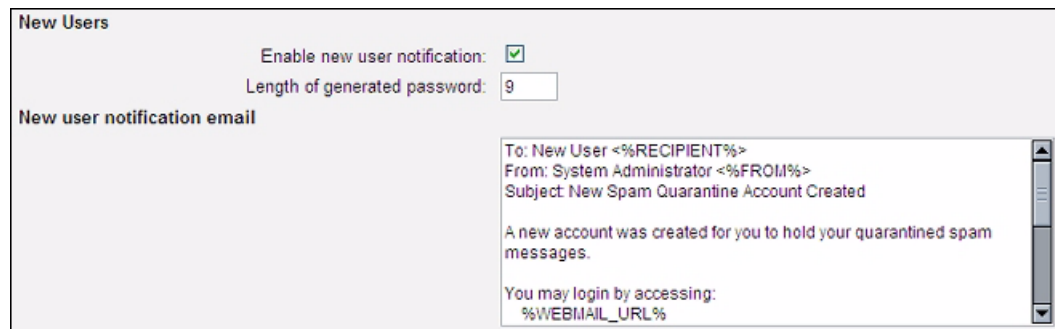
Reserved disk space: 1000000

Quota exceeded action: Discard

Disk full action: Discard

Unknown user action: Create new account

2. From the **Unknown User Action** drop-down list, select **Create new account**.
3. To enable the server to send a new user notification message with the account name and password to new users, select the **Enable new user notification** check box.
4. In the **Length of generated password** text box, type the number of characters that can be used in a generated password. The default setting is 9. Or, the administrator can assign a password on the **Local Accounts** page.
5. In the **New user notification email** text box, type or paste the text to include in the notification message that is sent to users.



New Users

Enable new user notification:

Length of generated password: 9

New user notification email

To: New User <%RECIPIENT%>
 From: System Administrator <%FROM%>
 Subject: New Spam Quarantine Account Created

A new account was created for you to hold your quarantined spam messages.

You may login by accessing:
 %WEBMAIL_URL%

LDAP User Accounts

You can import account information for your users from an LDAP directory. Imported accounts are mirrored locally on the Quarantine Server.

To import user accounts from an LDAP server, you must:

1. **Define Directory Servers** — Add directory servers to the Quarantine Server configuration.
2. **Import Directory Users** — After the directory servers are configured, you must import the user accounts from the directory server to the Quarantine Server. To mirror the user accounts from the LDAP server on the Quarantine Server, make sure to enable account mirroring. You can schedule the import and mirror process to occur at regular intervals. This helps to make sure the local account data is always the same as the directory server.

Define directory servers

The Quarantine Server uses the directory servers you specify for all LDAP functions. This includes user and group membership confirmation, authentication, and alias resolution.

1. Select **Administration > Directory Servers > Servers**.
2. To configure a new directory server, click **Add**.

To modify an existing server, click **Edit**.

The screenshot shows the 'Directory Server' configuration window. The 'Edit Server' section includes the following fields and values:

- Server URI: ldap://10.0.2.120
- Label: LDAP
- Type: Active Directory
- Bind:
- Bind DN: cn=Admin,cn=users,dc=example,dc=com
- Bind Password: [masked]
- Search Base: dc=example,dc=com
- Timeout: 5
- Dereference Aliases: Never
- Paged:
- Page Size: 1000

Buttons at the bottom: Test, Delete, Apply, Cancel.

3. In the **Server URI** text box, type the URI (Uniform Resource Identifier) address for the server. For example, `ldap://10.0.2.120`. If you use SSL with the with the LDAP server directory, type `ldaps` instead of `ldap`. To query an Active Directory global catalog, add the port number 3268 to the server URI. For example, `ldap://10.0.2.120:3268`.
4. In the **Label** text box, type a name or alias for the LDAP server.
5. From the **Type** drop-down list, select the type of LDAP server you specified. If you use an OpenLDAP or iPlanet server, select **Others**.
6. Select the **Bind** check box.

7. In the **Bind DN** text box, type the DN (Distinguished Name) for your directory server.
For example, for Active Directory, type: `cn=Administrator, cn=users, dc=example, dc=com`
Older Windows login names such as `DOMAIN/Administrator` are also supported. Make sure that you select a bind DN specific to your environment.

In Active Directory, if you use an account other than Administrator to bind to the LDAP server, the name must be specified as the full name, not the account name. For example, use "John Smith" instead of "jsmith".
8. In the **Bind Password** text box, type the password to use for the LDAP server.
9. In the **Search Base** text box, type the default search base for account lookups.
For example, `dc=example, dc=com`.
10. In the **Timeout** text box, type the maximum amount of time, in seconds, to wait for the search to complete.
You can set the timeout value to between 1 and 100 seconds.
11. In the **Dereference Aliases** drop-down list, select the method to use for alias dereferencing in a directory search:
 - **Never** — Aliases are never dereferenced.
 - **Searching** — Aliases are dereferenced in subordinates of the base object, but not when the base object of the search is found.
 - **Finding** — Aliases are only dereferenced the base object of the search is found.
 - **Always** — Aliases are dereferenced when the base object of the search is searched for and found.
12. To enable paging support for an Active Directory server, select the **Paged** check box.
When a query is sent to an LDAP server, the amount of information returned may contain thousands of entries and sub-entries. Paging enables the information from the LDAP server to be retrieved in more manageable sections to control the rate of data return.
13. In the **Page Size** text box, type the maximum number of entries to be returned in a query to the Active Directory server.
The default setting is 1000.
If you do not type a new setting, the default value of 1000 is used. The setting you select must match the size configured in the LDAP query policy for the Active Directory server.
14. Click **Test**.
A test query is sent to the LDAP server to test your LDAP settings.
15. Click **Apply**.

Import directory users

Use the *Directory Users* feature to import the user account and group membership information that you specify from your LDAP server to your Quarantine Server.

To import directory users:

1. Select **Administration > Directory Servers > Users**.
2. Click **Add**.

3. In the **Directory Server** drop-down list, select the directory server from which you want to import accounts.
4. In the **Search Base** text box, type the location in the directory structure from which to start the search. For example, `dc=example,dc=com`.
5. In the **Scope** drop-down list, select the level in the directory structure to include in the search.
 - **Base** — Searches the base object only.
 - **One Level** — Searches objects below the base object, but excludes the base object.
 - **Subtree** — Searches the entire subtree, of which the base distinguished name is the topmost object, and includes the base object.
6. In the **Query Filter** text box, type a search query for the server you selected. For example, for Active Directory type: `(!(objectCategory=group)(objectCategory=person))`
7. In the **Timeout** text box, type the maximum amount of time, in seconds, to wait for the search to complete. *You can set the timeout value to between 1 and 100 seconds.*
8. In the **Email attribute** text box, type an attribute to identify the user email address. If you use an Active Directory, iPlanet, or OpenLDAP server, type `mail`.
9. If the user account includes an alternate email address, in the **Email alias attribute** text box, type an attribute for the alternate email addresses. For Active Directory, type `proxyAddresses`. For iPlanet, type `Email`. For OpenLDAP, leave this setting blank.

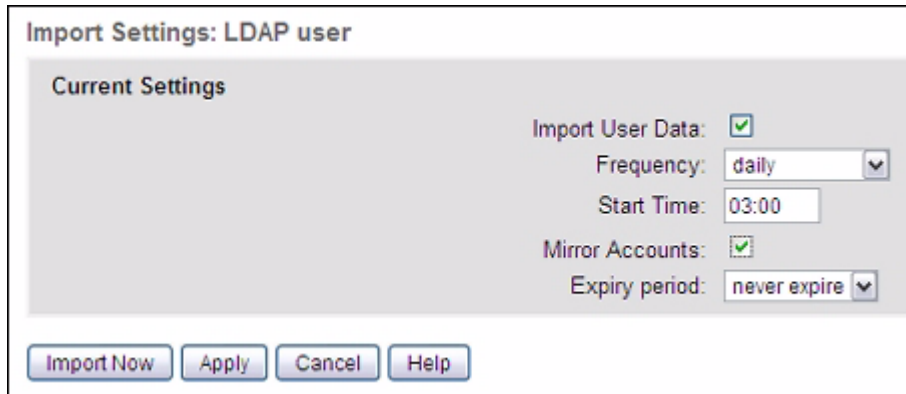
10. In the **Member of attribute** text box, type the attribute that identifies the groups to which the user belongs.
This information is used for Policy controls.
For Active Directory, type `memberOf`.
For iPlanet, type `Member`.
For OpenLDAP, leave this setting blank.
11. In the **Account Name Attribute** text box, type the login attribute for the user account name.
For Active Directory, type `sAMAccountName`.
For iPlanet, type `uid`.
For OpenLDAP, type `cn`.
12. Click **Test**.
The server tests your LDAP settings.
13. Click **Apply**.

Import Settings

To make sure the user data on your Quarantine Server is current with the data on your LDAP server, you can configure your Quarantine Server to automatically import LDAP user data at a scheduled time.

To import LDAP users and groups:

1. Select **Administration > Directory Servers > Users**.
2. Click **Import Settings**.



3. Select the **Import User Data** check box.
4. From the **Frequency** drop-down list, select how often user data is imported from the LDAP server.
 - **Hourly**
 - **Every 3 Hours**
 - **Daily**
 - **Weekly**
 - **Monthly**
5. In the **Start Time** text box, type the time for the import to begin (format hh:mm).
For example, to schedule an import at midnight type `00:00`.
6. Click **Apply**.
7. To immediately import user data, click **Import Now**.
8. To see the progress of the import, select **Activity > Logs > System**.

Mirror LDAP accounts as local users

To provide local account access to the Quarantine Server, you can mirror the user accounts that are on your LDAP server. This creates a local account on the Quarantine Server for each user account you import. This is a simple method that enables directory-based users to view and manage quarantined messages.

1. On the **Import Settings** page, select the **Mirror accounts** check box.
2. From the **Expiry period** drop-down list, select a time for the mirrored accounts to expire.
If the user no longer exists in the LDAP directory for the specified period of time, the local mirrored account is deleted.
3. Click **Apply**.
4. Click **Import Now**.
The import begins immediately and mirrored accounts are created.
5. To see the progress of your LDAP imports, select **Activity > Logs > System**.
6. To see all mirrored accounts, select **Administration > Accounts > Mirrored Accounts**.

Remote Authentication

Another option for user authentication is *Remote Authentication*. With this method, you can enable your users to authenticate without a local Quarantine Server account. When a user without a local account logs in to the Quarantine Server, the server sends the user credentials to the configured directory server. If the credentials match those for a user account on the directory server, the user is authenticated. The user is logged in to the Quarantine Server and can manage account settings and the trusted/blocked sender lists.

Configuring LDAP Remote Authentication

To use LDAP for remote authentication:

1. Select **Administration > Accounts > Remote Authentication**.
2. To select an LDAP server, in the **LDAP Sources** section, click **New**.

The screenshot shows the 'LDAP Authentication Source' configuration window. It contains the following fields and controls:

- Directory server:** A dropdown menu with 'AD' selected.
- Search Base:** A text box containing 'cn=users,dc=example.com,dc=com'.
- Scope:** A dropdown menu with 'Subtree' selected.
- Query Filter:** A text box containing '(ObjectClass=user)'.
- Timeout:** A text box containing '5'.
- Result Attributes:** A section containing 'Account name attribute:' with a text box containing 'sAMAccountName'.
- At the bottom, there are four buttons: 'Test', 'Apply', 'Delete', and 'Cancel'.

3. From the **Directory Server** drop-down list, select a configured LDAP directory server.
4. In the **Search Base** text box, type the location in the directory structure from which to start the search. For example, `dc=example,dc=com`.

5. From the **Scope** drop-down list, select the scope of the search.
 - **Base** — Searches the base object only.
 - **One Level** — Searches objects one level below the base object, but excludes the base object.
 - **Subtree** — Searches the entire subtree, of which the base distinguished name is the topmost object, and includes the base object.
6. In the **Query Filter** text box, type a specific query filter to use to search for a user in your LDAP directory.
For Active Directory, type `(ObjectClass=user)`.
7. In the **Timeout** text box, type the maximum amount of time, in seconds, to wait for the search to complete.
The default setting is 5. You can set the timeout value to between 1 and 100 seconds.
8. In the **Account name attribute** text box, type the account name result attribute for the user login or account name.
For example, for Active Directory, type `sAMAccountName`.
If you use another LDAP server, for example OpenLDAP or iPlanet, you must select the correct query filter and account name attribute for your server.

6

WatchGuard XCS Configuration

Add Mail Routes to the Quarantine Server

You must create a mail route on the WatchGuard XCS device to use to send spam messages to the Quarantine Server.

To configure the mail route on the WatchGuard XCS device:

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

| Sub. Domain | Route-to... | Port | MX | KeepOpen | | |
|--------------------------|---------------------|-----------|----|--------------------------|--------------------------|-----|
| <input type="checkbox"/> | .quarantine_reroute | 10.0.1.20 | 25 | <input type="checkbox"/> | <input type="checkbox"/> | Add |

LDAP Routing Upload File Download File Help

2. In the **Domain** text box, type a name for the mail route. At the start of the name, type ".".
For example, type .quarantine_reroute
This is the route name you select for the domain when you configure an Intercept Anti-Spam redirect action (without the "." character).
3. In the **Route-to** text box, type the IP address of the Quarantine Server.
For example, type 10.0.1.20
4. In the **Port** text box, type the port number.
For example, type 25 which is the default SMTP port.
5. Click **Add**.

Redirect Spam Messages to the Quarantine Management Server

To redirect spam messages from the WatchGuard XCS device to the Quarantine Management Server, you must set the Intercept Anti-Spam action on the WatchGuard XCS device to redirect the spam messages to the address of the Quarantine Server. Intercept Anti-Spam actions include three categories: *Certainly Spam*, *Probably Spam*, and *Maybe Spam*. You can set the **Action** to take for each category. We recommend that you do not change the **Threshold** setting.

- **Certainly Spam** messages have a high spam threshold setting, are usually spam, and can be safely rejected.
- **Probably Spam** messages can have false positives. We recommend that you select to quarantine these messages. Users can then review the spam messages before they are discarded.
- **Maybe Spam** messages can be sent to users. Users can decide if the messages are spam or legitimate mail, and add the sender to the trusted or blocked senders list as required. You can select the **Modify Subject Header** action and to add an indicator to the message that the message might be spam.

Though you can choose to redirect messages from any of these categories to the Quarantine Server, we recommend that you send the messages in the **Probably Spam** category.

To configure the redirect Anti-Spam action on your WatchGuard XCS device:

1. Select **Security > Anti-Spam > Anti-Spam**.

The Intercept Anti-Spam page appears.

The screenshot shows the 'Intercept™ Anti-Spam' configuration page. It is divided into three sections: 'Certainly Spam', 'Probably Spam', and 'Maybe Spam'. Each section has a 'Threshold' field, an 'Email Action' dropdown menu, and an 'Email Action data' text box. For 'Certainly Spam', the threshold is 99 and the action is 'Reject mail'. For 'Probably Spam', the threshold is 90 and the action is 'Redirect to...' with 'quarantine_reroute' entered in the data field. For 'Maybe Spam', the threshold is 60 and the action is 'Just log'.

2. In the **Probably Spam** section, from the **Action** drop-down list, select **Redirect to**.
3. In the **Action data** text box, type the route name for the Quarantine Server that you specified in the mail routing configuration.

For example, `quarantine_reroute`

You must have a mail route to the IP address of the Quarantine Server on the WatchGuard XCS device. This mail route must include a "." at the start of the route.

For example, `.quarantine_reroute`.

For more information about how to add a mail route, see "Add Mail Routes to the Quarantine Server" on page 37.

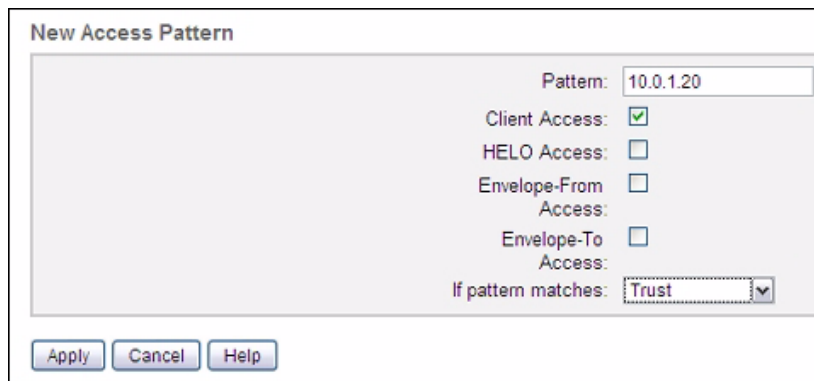
4. Click **Apply**.

Trust Mail from the Quarantine Server

To enable the WatchGuard XCS device to trust the Quarantine Server, you must configure a Specific Access Pattern on the WatchGuard XCS device. This pattern is used to make sure that mail from the Quarantine Server, such as spam digest notifications and released quarantined messages, are not scanned for spam or content issues.

To configure a Specific Access Pattern on your WatchGuard XCS device:

1. Select **Configuration > Mail > Mail Access**.
2. Click **Add Pattern**.
3. In the **Pattern** text box, type the hostname or IP address of the Quarantine Server.
4. Select the **Client Access** check box.
5. From the **If pattern matches** drop-down list, select **Trust**.



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

- Pattern:** 10.0.1.20
- Client Access:**
- HELO Access:**
- Envelope-From Access:**
- Envelope-To Access:**
- If pattern matches:** Trust (selected in a drop-down menu)

At the bottom of the dialog are three buttons: **Apply**, **Cancel**, and **Help**.

6. Click **Apply**.

Prevent Spam Digest Training

You can configure your WatchGuard XCS device to make sure the Intercept Anti-Spam feature does not train spam digest notification messages from the Quarantine Server. The spam quarantine notification message contains the subject headers from the actual spam messages in quarantine. If these quarantined messages are trusted, it can cause errors in the training database configuration.

To trust spam digest notifications:

1. Select **Security > Content Control > Pattern Filters**.
2. Click **Add**.

Pattern Based Message Filtering

Enable PBMF:

| Apply To | Message Part | Pattern | Priority | Action |
|----------|--------------|---------------------------------------|----------|---------------|
| All Mail | Subject | Contains Quarantined Email Summary | Medium | Do Not Train* |

Apply Remove BTI Default PBMFs Cancel Preferences Upload File Download File Help

3. Select the **Enable PBMF** check box.
4. In the **Apply To** drop-down list, select **All Mail**.
5. In the **Message Part** drop-down list, select **Subject**.
6. In the **Pattern** drop-down list, select **Contains**.
7. In the **Pattern** text box, type the text pattern for which to search.
For example, type `Quarantined Email Summary`. You can also type the subject line you configured for the spam quarantine notification messages on the Quarantine Server.
8. In the **Priority** drop-down list, select **Medium**.
9. In the **Action** drop-down list, select **Do Not Train**.
10. Click **Apply**.