



Fireware Wireless Exam Guide

The Fireware Wireless Exam tests your knowledge of how to configure and manage wireless access points from a Firebox that runs Fireware OS. This exam is appropriate for network administrators who have experience configuring and managing Fireboxes that run the most current version of Fireware OS.

Exam Overview

Key Concepts

To successfully complete the Fireware Wireless Exam, you must understand these key concepts:

General Wireless Knowledge

- Wireless radio bands and channels
- 802.11 wireless modes
- Wireless security modes and encryption protocols
- Wireless authentication methods
- SSIDs

Fireware Knowledge

- Wireless Firebox configuration and monitoring (T Series wireless models)
- WatchGuard AP device configuration and monitoring from the Gateway Wireless Controller on a Firebox
- VLAN configuration for a WatchGuard AP device
- Wireless guest network configuration
- Wireless Hotspot configuration

Exam Description

Content

40 multiple choice (select one option), multiple selection (select more than one option), and true/false questions

Passing score

75% correct

Time limit

Two hours

Reference material

You cannot reference printed or online materials during the exam

Test environment

This is a proctored exam, with two location testing options:

- Kryterion testing center
- Online, with virtual proctoring through an approved webcam

Prerequisites

None

Prepare for the Exam

WatchGuard provides reference materials to help you prepare for the Fireware Wireless Exam. In addition to the reference materials described in the subsequent sections, we strongly recommend that you use a Firebox with Fireware OS v12.x to set up one or more WatchGuard wireless devices before you begin the exam.

Self-Study Materials

WatchGuard offers courseware that you can use for self-study. We recommend that you review all available courseware before you take the exam. Courseware is available on the Technical Training tab in the WatchGuard Portal (login required).

Fireware Wireless

The *Fireware Wireless* courseware (PowerPoint) is available online for self-study.

To get the most from this self study course, we recommend that you set up at least one Firebox wireless device, and one AP device to gain experience with the settings described in the training. If you do not have a WatchGuard wireless device, you can still use Policy Manager to create a configuration file to learn about many of the wireless configuration settings described in the training.

Other Resources

Online Help

For the knowledge categories included in the [Assessment Objectives](#) section, we recommend that you review the help sections about wireless device management in the Fireware Help system. The help sections and topics that contain the most relevant information to help you prepare for this exam are:

Fireware Help:

- Section: **Firebox Wireless Device Setup** — all topics in this section
First topic: [Wireless Firebox Configuration](#)
- Section: **WatchGuard AP Device Setup** — all topics in this section
First topic: [WatchGuard AP Configuration](#)
- Section: **Monitor Your Device**
Topic: [Monitor AP Status](#)
- Section: **Authentication > Hotspot** — all topics in this section
First topic: [Configure a Hotspot](#)

Assessment Objectives

The Fireware Wireless Exam evaluates your knowledge of the categories in the subsequent list. For each knowledge category assessed in this exam, the *Weight* column includes the approximate percentage of exam questions from that knowledge category. Because some exam questions require skills or knowledge from more than one category, the weights do not exactly correspond to the percentage of exam questions.

Category	Skills / Knowledge	Weight
General wireless knowledge	Radio bands for wireless access points	20%
	802.11 wireless modes	
	Wireless security modes	
	Wireless encryption and authentication protocols	
	MAC access control	
Firebox wireless device configuration	Configure a wireless Firebox as a wireless client	25%
	Configure access points on a wireless Firebox	
	Configure interface settings for a wireless access point	
	Configure a wireless guest network	
	Monitor access point and wireless client status in Firebox System Manager and Fireware Web UI	
WatchGuard AP device configuration	Configure and pair a WatchGuard AP device	25%
	Configure an SSID used by multiple AP devices for wireless roaming	
	Configure an AP device on a custom interface	

Category	Skills / Knowledge	Weight
	Configure station isolation	
WatchGuard AP devices and VLANs	Configure VLANs for AP device VLAN tagging	10%
	Enable VLAN tagging in an SSID	
	Understand the impact of enabling management VLAN tagging	
Gateway Wireless Controller	Use Firebox System Manager to monitor AP devices and wireless clients	10%
	Use the Gateway Wireless Controller Dashboard to monitor AP devices and wireless clients	
	Use the Gateway Wireless Controller maps to assess wireless coverage and identify radio channel conflicts	
Wireless Hotspot	Configure a wireless hotspot for a wireless Firebox	10%
	Configure a wireless hotspot for an AP device	
	Manage hotspot guest user accounts	
	Configure a hotspot for wired and wireless guests	

Example Exam Questions

The exam includes multiple choice, multiple selection, and true/false questions. The subsequent examples show the types of questions to expect on the exam. Answers to each question appear on the last page.

Questions

1. Which of these wireless modes are supported on the 5 GHz radio band? (Select two.)
 - a. 802.11a
 - b. 802.11b
 - c. 802.11g
 - d. 802.11n
2. When two AP devices paired to the same Firebox use the same SSID, what controls wireless roaming behavior for wireless clients? (Select one.)
 - a. The Gateway Wireless Controller on the Firebox
 - b. The two AP devices
 - c. The wireless clients
3. If you enable VLAN tagging in an SSID, you must also enable management VLAN tagging in the Gateway Wireless Controller settings.
 - a. True
 - b. False
4. Which tool can you use on the Gateway Wireless Controller to check for channel conflicts on your wireless network? (Select one.)
 - a. Access points tab on the Dashboard
 - b. Auto-deployment configuration
 - c. Rogue AP detection
 - d. Wireless maps
5. Which of these options can you configure in the hotspot connection settings? (Select three.)
 - a. Allow hotspot users to connect without credentials.
 - b. Allow hotspot users to connect without accepting Terms and Conditions.
 - c. Require hotspot users to authenticate with a user name and passphrase.
 - d. Require hotspot users to authenticate with only a passphrase.
 - e. Require users to authenticate with a VPN client.

Answers

1. a, d. The 5 GHz radio band supports 802.11a and 802.11n wireless modes.
2. c. Roaming behavior is controlled by the wireless clients, not the AP devices or the Gateway Wireless Controller.
3. b. (False) You can optionally enable management VLAN tagging, but it is not required.
4. d. You can use the Wireless Maps feature to view channel conflicts on your network.
5. a, c, d. There are no options to skip the Terms and Conditions or require a VPN client.

Register for the Exam

To schedule an exam, you must create a Kryterion user account.

1. Log in to the WatchGuard website with your WatchGuard account credentials.
2. Select the **Technical Training** tab.
3. At the right side of the page, click **Register for an exam**.
This opens a WatchGuard-branded Kryterion web page.
4. At the top-right corner of the page, click the link to create a new Kryterion user account, or log in with an existing Kryterion user account for WatchGuard exams.
5. Click **Schedule an Exam**.

For more information about the certification process, see this [FAQ](#).

Copyright, Trademark, and Patent Information

Copyright © 1998–2018 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 at <http://www.watchguard.com/help/documentation/>.