

Symantec Edge SWG Administration R3

Course Code: 000293

The *Symantec Edge SWG Administration R3* course provides a detailed introduction to the use cases, features, and benefits of Edge SWG.

Delivery Method

Instructor-Led

Duration

2 days

Course Objectives

By the completion of this course, you will be able to:

- Describe the major Edge SWG functions and capabilities
- Write policies to defend enterprise networks against malware attacks and to enforce acceptable Internet browsing behavior
- Understand how the various applications work together to secure enterprise networks

Hands-On

This course includes practical hands-on exercises that enable students to test their understanding of the concepts presented in the lessons.

Prerequisites

- Basic understanding of networking concepts
- Basic understanding of network security concepts
- Basic understanding of the use of proxy servers

Certification exam

The *Exam 250-615: Symantec Edge SWG R3 Technical Specialist* certification exam accompanies this course.

Course Outline

Module 1: Introduction to Symantec Edge SWG

- Symantec Edge SWG overview
- Introduction to the Edge SWG Admin Console
- Key Edge SWG use cases

Module 2: Intercepting traffic and applying policy

- How Edge SWG intercepts traffic
- Writing Edge SWG policy in the Visual Policy Manager
- Informing users when web access is denied or restricted due to policy
- Best practices to avoid troubleshooting issues related to policy

Module 3: Applying security and web usage policy to encrypted traffic

- Introduction to TLS encryption
- Managing HTTPS traffic on Edge SWG
- Offloading HTTPS traffic to the SSL Visibility Appliance to boost performance
- Best practices to avoid troubleshooting issues related to SSL interception

Module 4: Providing security and web usage policies based on role or group

- Authentication basics on Edge SWG
- Using IWA authentication on Edge SWG
- Authentication modes in explicit and transparent proxy deployments
- Connecting to the Windows domain directly using IWA direct
- Connecting to the Windows domain using IWA BCAAA
- Introduction to role-based access control
- Using roles and groups in policy
- Best practices to avoid troubleshooting issues related to authentication

Module 5: Enforcing corporate guidelines for acceptable Internet browsing behavior

- Creating strong corporate guidelines for acceptable Internet use
- Using website categorization to enforce acceptable use guidelines
- Providing Edge SWG with categorization databases to be referenced in policy
- Setting the Request URL Category object in policy to enforce acceptable use guidelines
- Applying policy in order to enforce acceptable use guidelines
- Best practices to avoid troubleshooting issues related to enforcing acceptable use guidelines

Module 6: Protecting the endpoint from malicious activity

- Requirements for a pre-emptive, layered web defense
- WebPulse technical details
- Introduction to Intelligence Services
- Using Intelligence Services data feeds in policy
- Ensuring safe downloads
- Combined policy example
- Best practices to avoid troubleshooting issues related to protecting the endpoint from malicious activity

Module 7: Using built-in diagnostic tools on Edge SWG

- Key sources of information
- Sending service information to Symantec support

Module 8: Edge SWG integrations

- Centrally managing devices with Management Center
- Enhancing security with virus scanning
- Providing security for risky and unknown websites with High Risk Isolation
- Introduction to Cloud SWG
- Reporting on Edge SWG activity

Module 9: Course review

- Symantec Edge SWG Administration R3 course review

Appendix A: Overview of the SSP hardware platform and Integrated Secure Gateway (ISG)

Appendix B: Understanding SGOS architecture and caching on Edge SWG

Appendix C: Introduction to Content Policy Language (CPL)

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.



CRD: 012624
