

## Course Outline

---



### 50093- Deploying and Administering Microsoft Forefront Client Security

**Duration:** 3 days (18 hours)

**Target Audience:**

This course is intended for technical deployment specialists and senior-level administrators who manage a Microsoft Exchange Server or Microsoft SharePoint Products and Technologies infrastructure or security practice.

**Prerequisites:**

Before attending this course, students must have Windows Server certifications or deployment experience and be familiar with the Forefront product line: Client, Server, and Edge.

**Topics Covered:**

- Module 1: Course Overview
  - Forefront Product Overview
  - Forefront Client Security
  - Microsoft Forefront Client Security Components
  - Training Modules

After completing this module, students will be able to:

- Describe the Forefront Client Security components and architecture.
- Module 2: Forefront Client Security Server Roles and Topologies
  - Forefront Client Security Server Roles
  - Collection Server
  - Collection Server Database
  - Reporting Server
  - Reporting Database Server
  - Forefront Client Security Server Setup
  - Role Installation Steps
  - Server Topologies
  - SQL Server Database Sizing
  - Configuration Wizard
  - MOM Concepts
  - Forefront Client Security Server Setup Troubleshooting
    - Lab 1: Installing a Three Server Topology
      - Launch the Virtual Environment
      - Create Forefront Client Security Accounts

- Install the Management, Collection, and Reporting Server
- Install the Reporting Server Database
- Install the Distribution Server Role
- Configure Client Security on a Three Server Topology
- Grant Correct Permissions for Forefront Client Security Service Accounts
- Verify the Installation of Client Security on a Three Server Topology

After completing this module, students will be able to:

- Identify the different server roles within Forefront Client Security.
- Complete the server setup process.
- Identify various server topologies.
- Review basic MOM concepts.
- Discuss Forefront Client Security server setup troubleshooting.

#### ➤ Module 3: Forefront Client Security Client

- General Information
- Antimalware
- MOM Agent
- Client Setup
- Client Deployment Planning
- Forefront Client Security Client Deployment Methods
- Troubleshooting
  - Lab 2: Deploying the Forefront Client Security Client
    - Configure WSUS 3.0 to Deploy the Forefront Client Security Client
    - Create a Forefront Client Security Client Package and Distribute It
    - Distribute the Antimalware and Security Assessment State Definition Updates
    - Malware and Spyware Detection
    - View the Malware and Spyware in the Dashboard

After completing this module, students will:

- Be able to describe Forefront Client Security client component characteristics and information.
- Be able to describe the antimalware agent and engine.
- Understand the MOM agent.
- Understand the client setup process.
- Understand client deployment basics.

#### ➤ Module 4: Forefront Client Security Management

- Administration
- Administration Dashboard
- Forefront Client Security Policy Deployment
- Forefront Client Security Management Console Troubleshooting
  - Lab 3: End-to-End Policy Deployment
    - Deploy a Test Policy
    - Refresh and Verify Policy on the Client
    - View Policy Application via GPRresult
    - View Summary Reports
    - Policy Configuration Effects on Client UI
  - Lab 4: Configuring Forefront Data Retention
    - Examine Data Retention Periods

- Modify Database Retention Settings

After completing this module, students will:

- Be familiar with Forefront Client Security administration.
- Understand Forefront Client Security Administration User roles.
- Understand Forefront Client Security Policy UI settings and policy deployments.
- Be familiar with Forefront Client Security Management Console troubleshooting.

➤ Module 5: Forefront Client Security Reporting and Alerting

- Reporting Services Overview
- Reporting Architecture
- MOM Reporting
- Forefront Client Security Reports
- SQL Server Reporting Services Troubleshooting
- Alerts
  - Lab 5: Viewing Forefront Client Security Reports
    - Explore Forefront Client Security Reports
  - Lab 6: Managing Forefront Client Security Accounts
    - View Reporting Failure
    - Specify SQL Server Reporting Credentials to Forefront Client Security
  - Lab 7: Creating an E-Mail Report Subscription and Setting an E-Mail Notification
    - Configure SQL Server Reporting Services
    - Create an E-Mail Subscription
    - Create an E-Mail Notification
    - Follow the Alert Notification Flow
    - View E-Mail Server Settings

After completing this module, students will:

- Understand the reporting services infrastructure used by Forefront Client Security.
- Be familiar with Forefront Client Security Reports.
- Be familiar with Forefront Client Security Alerting Services.
- Understand Forefront Client Security Reporting troubleshooting procedures.

➤ Module 6: Security State Assessment

- Security State Assessment
- SSA General Information
- SSA Architecture
- SSA Object Processor (OP) and Manifest Updates
- SSA Security Checks
  - Lab 8: Security State Assessment
    - Examine Security State Assessment information in MOM and the Forefront Client Security Management Console
    - Configure WSUS for Security State Assessments
    - Detect Vulnerabilities
    - Update Clients

After completing this module, students will:

- Understand the security state assessment component of Forefront Client Security.
- Be familiar with the architecture of the SSA.
- Be familiar with the object processor and manifest update in SSA.
- Understand the SSA security check messages and results.

➤ Module 7: Submitting Malware to Microsoft for Analysis

- Malware Submission
- Assisting Customers with Malware Submissions

After completing this module, students will be able to:

- Review methods and procedures used to submit malware to Microsoft for analysis.

➤ Module 8: Closing

- Appendix A: Antimalware Client Registry Settings
- Appendix B: Antimalware Errors
- Appendix C: PP Tracing
- Appendix D: Antimalware Events
- Appendix E: SSA Scan Event Log Events
- Appendix F: MOM Command Line Reference