Symantec Messaging Gateway 9.5: Administration

COURSE DESCRIPTION

The *Symantec Messaging Gateway 9.5: Administration* course is designed for the customers, support engineers, SEs, consultants, and partners tasked with installation, configuration and administration of Messaging Gateway. This three-day, virtual academy, hands-on class covers how to install, configure, and administer Messaging Gateway.

Delivery Method
Virtual Academy

Duration
Three days

Course Objectives
By the end of this course, you will be able to:

- Describe some of the e-mail threats that exist today.
- Define Symantec Security Response.
- Describe how Probe Network works.
- Describe Messaging Gateway 9.5.
- List key features of Messaging Gateway 9.5.
- Describe Messaging Gateway 9.5 architecture.
- Describe how Messaging Gateway 9.5 is deployed.
- List installation prerequisites.
- Provide a virtualization overview.
- Install Messaging Gateway 9.5.
- Configure Messaging Gateway 9.5.
- Navigate the Messaging Gateway Control Center.
- Describe the contents of the Reputation tab in the Messaging Gateway 9.5 Control Center.
- Configure bad senders policies.
- Configure connection classes.
- Configure good senders policies.
- Use the Find Sender tool.
- Use the IP Reputation lookup tool.
- Add or modify existing spam policies.
- Modify spam quarantine settings.
- Configure spam scan settings.
- Configure sender authentication.
- View the spam message quarantine.
- Describe the contents of the Virus tab in the Messaging Gateway 9.5 Control Center.
- Add or modify existing virus policies.
- Configure LiveUpdate settings.
- Configure antivirus and exclude scanning lists.
- Configure settings for the virus quarantine.
- View the suspect virus message quarantine.
- Describe the contents of the Content tab in the Messaging Gateway 9.5 Control Center.
- Manage content filtering policies.
- Configure content filtering resources.
- Configure content filtering settings.
- Manage incidences.
- Describe the contents of the Administration tab in the Messaging Gateway 9.5 Control Center.
- Manage users and groups.
- Manage host configuration.
- Back up Messaging Gateway 9.5.
- Configure Messaging Gateway 9.5 settings.
- Manage SSL certificates.
- Enable and configure Bounce Attack Prevention.
- Configure local logging levels.
- Enable and use message audit logs.
- Describe the directory data service.
- Provide an overview of the directory data service architecture.
- Describe new features in the directory data service.
- List default spam and virus policies.

Who Should Attend
Customers, support engineers, SEs, consultants, and partners

Prerequisites
- *E-mail Fundamentals*
- *LDAP Fundamentals*

Hands-On
This course includes practical exercises and demonstrations that enable you to test your new skills and begin to transfer them into your working environment.

COURSE OUTLINE

Introduction to Messaging Gateway 9.5
- E-mail scanning: Background
- Introducing Messaging Gateway 9.5
- Key features
- Messaging Gateway 9.5 architecture
- Messaging Gateway 9.5 deployment

Installation and Configuration
- Installation prerequisites
- Virtualization overview
- Installing Messaging Gateway 9.5
- Configuring Messaging Gateway 9.5
- Overview of Messaging Gateway 9.5 Control Center
- **Hands-On Labs:** Initialize appliance, configure appliance, verify appliance configuration

Adaptive Reputation Management

- The Reputation tab
- How global IP reputation works
- Configuring bad senders policies
- Configuring connection classification
- Configuring good senders policies
- Using the Find Sender tool
- Using the IP Reputation Lookup tool
- **Hands-On Labs:** Enable directory harvest attack recognition, enable and configure fastpass, configure connection classification, verify sender group, use IP reputation lookup tool

Anti-Spam Policies

- The Spam tab
- The Email Spam policy
- Modifying spam quarantine settings
- Spam scan settings
- Configuring sender authentication
- **Hands-On Labs:** Test an inbound spam policy, test an inbound suspected spam policy, enable and configure bounce attack prevention, verify bounce attack prevention configuration, create a spam policy that quarantines spam, enable and test DKIM feature

Anti-Virus Policies

- The Virus tab
- LiveUpdate settings
- The Email Virus policy
- Creating a new virus policy
- Configuring settings for virus quarantine
- Viewing the suspect virus message quarantine
- **Hands-On Labs:** Test an inbound virus policy, test an inbound suspected virus policy, test unscannable virus policy, test encrypted attachment virus policy, configure LiveUpdate, configure virus scan settings

Content Filtering Policy

- The Content tab
- Content filtering scanning
- Setting up content filtering scanning
- Creating a content filtering policy
- Guidelines for multiple content filtering policies
- Using content filtering policies for structured data matching
- Content filtering settings
- Incident management
- **Hands-On Labs:** Setup content filtering policy, create content filtering policy for structured data matching, create an informational incident, create a quarantine incident, run content filtering expunger, test strip matching attachment lists action, test strip matching attachments action

Managing User and Host Configuration

- The Administration tab
- The Users section
- The Hosts section
- **Hands-On Labs:** Manage users, use utilities, download diagnostics package to desktop

Managing Control Center Settings

- Configuring alerts
- Manage certificates
- Configuring Control Center settings
- Manage directory integration
- Manage other Control Center settings
- **Hands-On Labs:** Create a certificate, configure local logging, run a report, add a directory data source, enable and test invalid recipient handling, enable address resolution, edit advanced settings for a directory data source, configure SMTP authentication, configure advanced authentication mail settings

Leveraging Network Prevent for Email

- Introducing Network Prevent for Email
- Configuring Network Prevent for Email
- Failure behavior with Network Prevent for Email
- Resolving delivery queue backups
- Reporting
- **Demonstration:** Configure DLP Connect, Test the Network Prevent for Email configuration