Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Symantec Messaging Gateway 10.6 Administration

CODE:	LENGTH:	PRICE:
SYM_00032312	16 Hours (2 days)	€1,500.00

Description

The Symantec Messaging Gateway 10.6 Administration course is designed to provide you with the fundamental knowledge to configure and administer the Symantec Messaging Gateway. This two-day, instructor-led, hands-on class covers how to install, configure, and administer Messaging Gateway.

Objectives

- By the end of this course, you will be able to configure and use Messaging Gateway 10.6.

Prerequisites

You must have a working knowledge of Windows server operating systems and commands, as well as email infrastructure and security concepts

Programme

Module 1: Introduction to Messaging Gateway 10.6

- Background to Email Scanning
- Introducing Messaging Gateway
- Key Features
- Messaging Gateway Architecture
- Messaging Gateway Deployment

Module 2: Installation and Basic Configuration

- Installation Prerequisites
- Messaging Gateway Virtual Edition
- Installing Messaging Gateway
- Configuring Messaging Gateway
- Overview of Messaging Gateway Control Center
- Address Masquerading
- Aliases
- Domains
- Invalid Recipients

Settings Module 3: Prevent unwanted email with Adaptive Reputation Management

- Reputation tab
- How Global IP Reputation Works
- Configuring Bad Senders Policies
- Configuring Connection Classification
- Configuring Good Senders Policies

- Introducing Fastpass
- Using Reputation Tools
- Hands-On Labs:
  Enable directory harvest attack recognition, enable and configure fastpass, configure connection classification, verify sender group, use IP reputation lookup tool

Module 4: Prevent Spam with Anti-Spam Policies

- Spam Tab
- Email Spam Policy
- Introducing Bounce Attack Prevention
- Modify Spam Quarantine Settings
- Scan Settings
- Configure 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

Module 5: Prevent Malware with Anti-Malware Policies

- Malware Tab
- Email Malware Policy
- Disarm Technology
- LiveUpdate Settings
- Scan Settings
- Suspect Virus Settings
- 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

Module 6: Prevent data leakage with Content Filtering Policies

- Content Tab
- Content Filtering Scanning
- Setting up Content Filtering Scanning
- Creating a Content Filtering Policy
- Using Content Filtering Policies for Structured Data Matching
- Content Filtering Settings
- Introduction to Content Filtering 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

Module 7: Advanced Configuration (Part 1): Managing User and Host Configuration

- Administration Tab
- Managing Users
- Managing Hosts
- Hands-On Labs: Manage users, use utilities, download diagnostics package to desktop

Module 8: Advanced Configuration (Part 2): Managing Control Center Settings

- Configuring Alerts
- Manage Certificates
- Configuring Control Center Settings
- Manage Directory Integration
- Managing 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

Module 9: Introduction to Symantec Network Protect for Email & Content Analysis

- Introducing Symantec Network Prevent for Email
- Network Prevent for Email delivery modes
- Failure behaviour with Network Prevent for Email
- Configure Network Prevent for Email settings in Messaging Gateway Overview of Content Analysis for Email

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.