The McAfee® Web Gateway Administration course from Education Services provides an in-depth introduction to the tasks crucial to setting up and administering McAfee Web Gateway effectively. The course combines lectures and practical lab exercises, with significant time allocated for hands-on interaction with the McAfee Web Gateway user interface. It provides detailed instructions for the integration of this product.

**Course Goals**
- Identify the purpose of the solution, as well as its key features.
- Plan the deployment.
- Install and configure solution components.
- Configure rules, rule sets, lists, and related component to meet customer security, performance, and usage requirements.
- Implement controls for administrator access.
- Monitor solution's operation and performance.
- Gather information about the solution and generate reports for more detailed analysis.

**Agenda At A Glance**

**Day 1**
- Welcome
- Solution Overview
- Planning
- Installation
- System Configuration
- Policy Overview
- Rule, Rule Sets, and List Configuration

**Day 2**
- McAfee Global Threat Intelligence and URL Filtering
- Media Type Filtering
- Malware Filtering
- Authentication and Account Management
- Secure Socket Layer (SSL) Scanning

**Audience**
This course is intended for system and network administrators, security personnel, auditors, and/or consultants.
Course Description

Agenda At A Glance (continued)

Day 3
- Quota Management and Coaching
- Web Caching, Next Hop Proxies, Progress Pages, and Block Pages
- Cloud Storage Encryption and Decryption (no lab)
- Logging
- Dashboards and Monitoring
- Content Reporting System

Day 4
- Advanced Management
- Basic Troubleshooting
- Web Hybrid Solution (no lab)
- McAfee Advanced Threat Defense Overview and Integration

Recommended Pre-Work
It is recommended that students have a working knowledge of Microsoft Windows administration, system administration concepts, a basic understanding of computer security concepts, and a general understanding of internet services.

Course Outline

Module 1—Welcome
- About the Course
- Acronyms and Terms
- About You
- Intel Security Community

Module 2—Solution Overview
- Challenges of Effective Web Security
- Solution Overview
- Key Features
- New/Enhanced Features for This Release
- Flexible and Scalable Deployments
- Access Controls
- Management Interface
- Central Management
- Integration

Module 3—Planning
- Planning Overview
- Business Requirements
- Appliance Types
- Physical Appliance Requirements
- McAfee Web Gateway Operating System
- Supported Peripheral Component Interconnect (PCI) Cards
- Virtual Appliance Requirements
- McAfee Blade Server System Requirements
- Client Requirements
- Supported Browsers
- Open Port Requirements
- Web Security Licenses
- Proxy Design
- Explicit/Transparent Proxies: Overview
- Explicit/Transparent Proxies: Comparison
- Proxy High Availability (HA)
- Reverse HTTPS Proxy
- Comparing ICAP and Reverse HTTPS Proxy
- Deployment Plan
- Change Control

Module 4—Installation
- Installation Overview
- Requirements
- Downloading Appliance Software
- Using Online Tools
- Installing Software on Physical Appliances
- Installing Software on Virtual Appliances
- Setting up Virtual Appliance with Hyper-V
- Initial Configuration Settings
- Implementing Default Settings
- Implementing Custom Settings: DHCP Not Used
Course Description

- Implementing Custom Settings: DHCP Used
- Downloading McAfee Web Gateway UI Webstart
- Completing the Setup
- Logging into the User Interface
- Verifying User Interface Is Accessible
- Navigating McAfee Web Gateway Interface

Module 5—System Configuration
- Configuration Overview
- McAfee Web Gateway License Administration
- Obtaining McAfee Web Gateway Updates
- Downloading Update Package Manually
- Uploading Update Package Manually
- Configuring Automatic Updates
- Triggering Automatic Updates
- Reviewing Update Information on Dashboard
- Reviewing Update Logs
- Network Settings Overview
- Review: Gateway Versus Proxy Service
- Review: Transparent Gateway
- Review: Proxy Server
- Viewing Proxy Configuration
- Supported Network Modes
- Supported Data Transfer Technologies
- Proxy (optional WCCP)
- HTTP Proxy Settings
- Web Cache Settings
- Domain Name System (DNS) Settings
- Other Proxy Settings
- Configuring Network Interfaces
- Configuring Domain Name Service
- Configuring Network Protection
- Configuring Static Routes
- Configuring Port Forwarding
- Configuring Date and Time
- Log File Manager Overview
- Enabling and Configuring Audit Log Settings

Module 6—Policy Overview
- Review: Web Page Components
- Review: Hypertext Transfer Protocol (HTTP)
- Policy Overview
- Policy Page Overview
- Policy Page Overview: Rule Sets Tab Views
- Policy Page Overview: Lists Tab
- Policy Page Overview: Settings Tab
- Policy Page Overview: Templates Tab
- How Rules and Rule Sets Work
- Inside a Rule Set
- Rule Elements: Criteria
- Operators
- Rule Elements: Actions
- Rule Elements: Event
- Rule Cycles
- Rule Processing
- Nested Rule Sets
- How Lists and Rules Interwork
- Permissions
- Best Practices

Module 7—Rule, Rule Set, and List Configuration
- Review: Filtering Traffic
- Review: Transactions (Request-Response)
- Review: Cycles
- Review: How Rules Work
- Default Rule Sets with Preconfigured Rules
- Rule Design Overview
- Example Rule Construction
- Deleting Default Policies
- Adding Top Level Rule Set
- Adding IP Blacklist Rule
- Adding IP Whitelist Rule
- Adding Block All Rule
- Review: Lists
Course Description

- Example: List Management
- Editing IP Blacklist
- Editing IP Whitelist Tag Catalog

Module 8—McAfee Global Threat Intelligence (McAfee GTI) and URL Filtering
- URL Filtering Overview
- McAfee GTI Overview
- Some Ways McAfee Web Gateway Uses McAfee GTI
- Gateway Anti-Malware Engine Overview
- Configuring Gateway Anti-Malware Engine
- URL Filter Engine Overview
- Configuring Default URL Filter Engine
- Configuring Dynamic Content Classifier (DCC)
- Rule Construction
- Default URL Filter Rule Sets and Rules
- Default URL Filtering by Category Rule Set
- Default Web Category Filtering Rules
- Default Geolocation Rule Set
- Default Dynamic Content Classification (DCC) Rules
- Use Cases

Module 9: Media Type Filtering
- Media Type Filtering Overview
- Some Ways McAfee Web Gateway Controls Media Access
- Rule Construction
- Rule Construction: Media Type Criteria
- Rule Construction: Media Type Lists
- Default Enable Opener Rule
- Default Media Type Filtering Rule Set
- McAfee Data Loss Prevention (McAfee DLP) Overview
- Adding McAfee DLP Classifications
- Adding McAfee DLP Dictionary Entries
- Default McAfee DLP Rule Sets and Rules
- Use Cases

Module 10—Malware Filtering
- Malware Filtering Overview
- Anti-Malware Scanning Engines and Behavior
- Configuring Mobile Code Behavior
- Configuring Advanced Settings
- Configuring Gateway Anti-Malware Settings
- Configuring Advanced Settings for Avira
- Configuring Custom Gateway Anti-Malware Engine
- Rule Construction Overview
- Default URL Filter Rule Sets and Rules
- Default Gateway Anti-Malware Rules
- McAfee Advanced Threat Defense—Handle Offline Scan Rules
- McAfee Advanced Threat Defense—Initial Offline Scan Rules
- McAfee Advanced Threat Defense Rules
- Use Cases

Module 11: Authentication and Account Management
- Authentication Overview
- Authentication Types
- Authentication Engines
- Configuring Authentication Method
- Joining Appliance to Windows Domain
- Rule Construction
- Default Authentication Rule Sets
- Transparent Authentication with Cookies
- Default Authentication Rule Sets
- Administrator Management Overview
- Default Administrator Roles
- Adding a Role
- Adding an Administrator Account
- Configuring External Account Management
- Use Cases

Module 12: Secure Socket Layer Scanning
- SSL Overview
- SSL Scanning Engines
- Viewing Default Certificate Authority
- Generating Certificate
- Exporting Certificate
- Importing Certificate: Internet Explorer
- Importing Certificate: Firefox
Course Description

- Configuring Default Certificate Verification
- Configuring SSL Inspection
- Configuring SSL Client Certificate Handling
- Configuring SSL Client Context without CA
- Rule Construction
- Default SSL Scanner Rule Sets
- Default Restrict CONNECT Rule Sets
- Configuring SSL Scanner Rule Set
- Configuring Handle CONNECT Call Rule Set
- Configuring Certificate Verification Rule Set
- Configuring Verify Common Name (Proxy Setup) Rule Set
- Configuring Content Inspection Rule Set
- Use Cases

Module 13—Quota Management and Coaching
- Quota Management Overview
- Coaching Overview
- Configuring Quota System Settings
- Configuring Coaching Engine Settings
- Configuring Time Quota Engine Settings
- Configuring Volume Quota Engine Settings
- Configuring Authorized Override Engine Settings
- Configuring Blocking Session Engine Settings
- Rule Construction
- Importing Coaching Rule Sets
- Default Coaching/Quota Rule Sets
- Other Default Rule Sets
- Configuring Coaching Rule Set
- Defining Coaching Criteria: Redirection
- Defining Coaching Criteria: Block
- Adding URLs to Coaching Rule Set
- Configuring Time Quota Rule Set
- Configuring Volume Quota Rule Set
- Other Rule Set Types
- Authorized Override Rule Set
- Blocking Sessions Rule Set
- Welcome Page Rule Sets
- Use Cases

Module 14—Web Caching, Next Hop Proxies, Progress Pages, and Block Pages
- Web Caching Overview
- Enabling Cache Option
- Web Cache Rule Construction
- Configuring Read from Cache Rule Set
- Default Write to Cache Rule Set
- Next Hop Proxies Overview
- Next Hop Proxy Rule Construction
- Progress Indication Overview
- Default Progress Indication Rule Sets
- Default Enable Progress Page Rule
- Default Enable Data Trickling Rule
- Block Pages Overview
- Basic Components
- Creating a Custom Block Page
- Modifying Custom Block Page
- Creating Block Action
- Configuring Action in Rule
- Exporting Templates to Archive
- Importing Template Archive

Module 15—Cloud Storage Encryption and Decryption
- Solution Overview
- Importing Cloud Storage Encryption Rule Set
- Configuring Cloud Storage Encryption Engines
- Ensuring Secure Communications
- Manually Decrypting Data
- Encrypting Data Multiple Times

Module 16: Logging
- Logging Overview
- System Log Files
- Viewing System Log Files
- User-Defined Log Files
- Log File Settings
- Log File Manager Settings: System Log Files
Course Description

- File System Logging Settings: User-Defined Log Files
- Rule-Based Logging Overview
- Rule Construction
- Configuring File System Logging Settings
- Adding Custom Log Handler (Optional)
- Defining User-Defined Properties
- Using the File Editor
- Use Cases

Module 17—Dashboards and Monitoring
- McAfee Web Gateway Dashboard Overview
- Alerts and Charts and Tables Tabs
- McAfee ePolicy Orchestrator® (McAfee ePO™) Software Solution Overview
- Integration Workflow: McAfee Web Gateway Activities
- Configuring McAfee ePO in McAfee Web Gateway
- Configuring Common Catalog Role
- Configuring Administrator Account for McAfee ePO
- Enabling REST-Interfaces
- Adding Bypass Rule Set and Rule
- Integration Workflow: McAfee ePO Activities
- Installing McAfee Web Gateway Extension
- Registering McAfee Web Gateway with McAfee ePO
- McAfee Web Gateway Queries and Reports
- Working with Dashboards and Monitors
- Queries Overview
- McAfee Web Gateway Queries
- Creating Custom Queries and Reports
- Using the Common Catalog

Module 18—McAfee Content Security Reporter
- McAfee Content Security Reporter Overview
- Planning: Platform
- Planning: Database
- Planning: McAfee ePO
- Deployment Overview
- Downloading McAfee Content Security Reporter Software
- Installing McAfee Content Security Reporter Software
- Installing McAfee Content Security Reporter Extension in McAfee ePO
- Registering Report Server in McAfee ePO
- Adding Log Source in McAfee ePO
- Configuring Log Settings in McAfee Web Gateway
- Rotating and Pushing Log in McAfee Web Gateway
- Verifying Log Push in McAfee ePO
- Post Installation Activities
- Working with McAfee Content Security Reporter Dashboards in McAfee ePO
- Working with McAfee Content Security Reporter Queries and Reports in McAfee ePO
- Managing McAfee Content Security Reporter Permission Sets
- Maintaining McAfee Content Security Reporter

Module 19—Advanced Management
- Central Management Overview
- How It Works
- Configuring Central Management
- Working with Policies
- Configuring Updates
- Using Different Central Management Groups
- Single Network Group (Default)
- Multiple Network Groups
- Runtime Groups
- Update Groups
Course Description

- Proxy High Availability Overview
- Configuring Proxy High Availability
- REST Interface Overview
- Types of Scripts
- Preparing Use of REST Interface
- Enabling Use of REST Interface
- Adding Custom Role and Account for REST Access

Module 20—Basic Troubleshooting
- Troubleshooting Overview
- Common Problem Areas
- Performing a Backup and Restore
- McAfee Web Gateway Troubleshooting Tools
- Creating a Feedback File
- Reviewing Log Files
- Running a Packet Tracing
- Using Rule Tracing Central
- Connection Tracing Overview
- Working with Rule Tracing Files
- Working with Core Files
- System and Network Tools Overview
- Using System Tools
- Using Network Tools
- Command Line Interface (CLI)

Module 21—Web Hybrid Solution
- Hybrid Solution Overview
- Configuring Web Hybrid Solution
- Web Hybrid Legacy Configuration
- Hybrid Lists
- Web Hybrid Policy Lists
- Web Hybrid Rules
- Authentication Considerations
- McAfee Client Proxy Solution Overview
- Deploying with McAfee ePO
- Deploying Outside of McAfee ePO
- McAfee Client Proxy Policies Overview
- Configuring Proxy Server List
- Defining Client Configuration
- Configuring Bypass List
- Configuring Block List
- Configuring Permission Sets

Module 22—McAfee Advanced Threat Defense Overview and Integration
- Malware Challenges
- McAfee Advanced Threat Defense Solution Overview
- Multilayer Defense
- Local Blacklist and Whitelist
- Static Code Unpacking
- Embedded Anti-Malware Engines
- McAfee GTI Integration
- Dynamic Analysis (Sandboxing)
- Integrated Advanced Threat Detection
- McAfee Advanced Threat Defense Basic Solution Components
- Physical Appliance Specifications
- Virtual Machine Requirements
- Supported File Types for Analysis
- Client Requirements
- Standalone Deployment
- Integrated Deployment
- McAfee Web Gateway Integration Overview
- Integration Workflow
- Configuring McAfee Web Gateway User Account in McAfee Advanced Threat Defense
- Configuring Settings for McAfee Advanced Threat Defense
- Configuring Rule Sets