Windows Defender Application Control (WDAC)

3 Days (8 Hours/Day)

Day 1 – WDAC Architecture, Policy Creation & Rule Design

Module 1 – Windows Application Control Fundamentals (1 Hour)

- Evolution from AppLocker to WDAC
- Windows Defender Application Control architecture
- Code Integrity (CI)
- UMCI vs KMCI
- Secure Boot relationship
- HVCI / Memory Integrity
- Smart App Control vs WDAC
- Enterprise use cases
- WDAC limitations

Lab

- Verify Device Guard readiness
- Inspect Code Integrity status
- Explore Event Viewer logs

Module 2 – WDAC Components (1 Hour)

- Policy structure
- Base Policies
- Supplemental Policies
- Multiple Policy Format
- Rule options
- Signing requirements
- Policy lifecycle

Lab

- Explore existing Microsoft policies
- Examine XML policy format

Module 3 – Rule Design Methodology (2 Hours)

- Publisher Rules
- File Publisher Rules
- File Name Rules
- File Path Rules
- File Hash Rules
- Managed Installer
- Intelligent Security Graph
- Allow vs Deny rules
- Trusted Signing
- Selecting proper rule levels

Best Practices

- Minimize hash rules
- Handle software updates
- Vendor certificate trust
- Rule precedence

Lab

- Create publisher-based policies
- Compare publisher vs hash rules
- Create path-based rules
- Validate XML

Module 4 – Creating WDAC Policies (2 Hours)

PowerShell cmdlets

- New-CIPolicy
- Merge-CIPolicy
- ConvertFrom-CIPolicy
- ConvertTo-CIPolicy
- Set-RuleOption
- Remove-RuleOption
- Add-SignerRule

- New-CIPolicyRule

Policy generation methods

- Golden image scanning
- Reference workstation
- Production machine inventory

Lab

- Generate policy from reference machine
- Merge multiple policies
- Export Binary Policy
- Validate policy syntax

Module 5 – Audit Mode (2 Hours)

Audit Mode

- Why start in Audit
- Event IDs
- Policy simulation
- Collecting telemetry
- Identifying missing rules

Using

- Event Viewer
- PowerShell
- Microsoft Defender logs

Lab

- Deploy audit policy
- Execute blocked applications
- Analyze audit logs
- Add missing rules

Day 2 – Deployment, Administration & Enterprise Operations

Module 1 – WDAC Deployment Methods (2 Hours)

Deployment options

- Local deployment
- Group Policy
- Intune
- Microsoft Configuration Manager
- Microsoft Defender for Endpoint
- Offline deployment
- Imaging integration

Policy distribution strategy

Lab

- Deploy policy locally
- Deploy through GPO
- Validate deployment

Module 2 – Policy Administration (2 Hours)

Managing production policies

- Updating policies
- Supplemental policies
- Policy versioning
- Rollback strategy
- Policy signing
- Certificate management

Lab

- Create supplemental policy
- Update production policy
- Rollback failed policy

Module 3 – Operational Support (2 Hours)

Daily administration

- Application onboarding
- Exception handling
- Software updates
- New vendor approval
- Emergency allow process
- Policy documentation
- Governance

Lab

- Approve new application
- Handle software update
- Add vendor certificate

Module 4 – Monitoring & Reporting (2 Hours)

Monitoring

- Event IDs
- Code Integrity logs
- Windows Event Forwarding
- Defender for Endpoint integration
- SIEM integration

Reporting

- Policy compliance
- Audit reports
- Unauthorized execution attempts

Lab

- Generate operational reports
- Forward WDAC events
- Review blocked execution attempts

Day 3 – Troubleshooting, Advanced Administration & Best Practices

Module 1 – WDAC Troubleshooting (2 Hours)

Common issues

- Applications blocked unexpectedly
- Driver loading failures
- Missing signer
- Certificate expiration
- Software updates breaking rules
- Boot failures
- Recovery procedures

Tools

- Event Viewer
- CI Logs
- PowerShell
- Windows Security Logs

Lab

- Diagnose blocked applications
- Repair policy
- Recover failed deployment

Module 2 – Advanced Policy Engineering (2 Hours)

Advanced topics

- Managed Installer
- ISG integration
- Policy inheritance
- Supplemental policy hierarchy
- Multiple policy strategy
- Enterprise segmentation
- Developer workstations
- Server-specific policies

Lab

- Multi-policy deployment
- Create server policy
- Create developer workstation policy

Module 3 – Enterprise Design Workshop (2 Hours)

Designing WDAC for

- Workstations
- Servers
- VDI
- Domain Controllers
- Developer systems
- Kiosk devices

Migration

- AppLocker to WDAC
- Pilot rollout
- Phased deployment
- Change management

Lab

- Design enterprise rollout
- Policy planning exercise

Module 4 – Final Enterprise Practical (2 Hours)

Scenario

A company with:

- 500 Windows endpoints
- Microsoft Office
- Adobe
- Chrome
- Internal applications
- PowerShell administration
- Visual Studio developers

- Legacy software

Tasks

- Design policy
- Build reference machine
- Generate policy
- Deploy in Audit
- Review logs
- Update policy
- Switch to Enforced Mode
- Handle software updates
- Troubleshoot blocked application
- Perform rollback

Complete Lab Environment

VM 1 – Active Directory

Windows Server 2022

- Domain Controller
- DNS
- Group Policy
- Certificate Services (optional)

Specs:

- 2 vCPU
- 4 GB RAM
- 60 GB Disk

VM 2 – Windows 11 Reference Machine

Purpose:

- Golden image
- Policy generation

Installed software:

- Microsoft Office
- Google Chrome
- 7-Zip
- Notepad++
- Adobe Acrobat Reader
- Visual Studio Code
- Sysinternals Suite
- PowerShell 7
- Microsoft Edge

Specs:

- 2 vCPU
- 6 GB RAM
- 80 GB Disk

VM 3 – Windows 11 Managed Endpoint

Purpose:

- Receive WDAC policies
- Testing
- Troubleshooting

Software:

- Same as reference machine
- Plus intentionally installed unknown applications

Specs:

- 2 vCPU
- 6 GB RAM
- 80 GB Disk

VM 4 – Windows 11 Developer Workstation

Purpose:

- Visual Studio
- Git
- Python
- Node.js
- Docker Desktop (optional)
- Windows SDK

Used to demonstrate policy exceptions.

Specs:

- 4 vCPU
- 8 GB RAM
- 120 GB Disk