Microsoft® Official Course

Module11

Implementing Security Software

Microsoft®

Module Overview

- Client Software Protection Features
- Email Protection
- Server Protection

Lesson 1: Client Software Protection Features

- What Are Software Restriction Policies?
- What Is AppLocker?
- SRP vs. AppLocker
- Demonstration: Create and Enforce a AppLocker Rule

What Are Software Restriction Policies?

- SRPs allow administrators to identify which applications are allowed to run on client computers
- SRPs can be based on the following:
  - Hash
  - Certificate
  - Path
  - Zone
- SRPs are applied through Group Policy and include a Default Security Level
- By default, SRPs are not enabled

What Is AppLocker?

- Allows for creation of rules based on a wide variety of variables, which can be assigned to users or groups
- Rule Behaviour
  - Allow or Deny
- Enforcement Modes:
  - Not Configured
  - Enforce
  - Audit Only
- Configured and Managed by:
  - Group Policy
  - Windows PowerShell

SRP vs. AppLocker

- AppLocker provides more flexibility and granular control

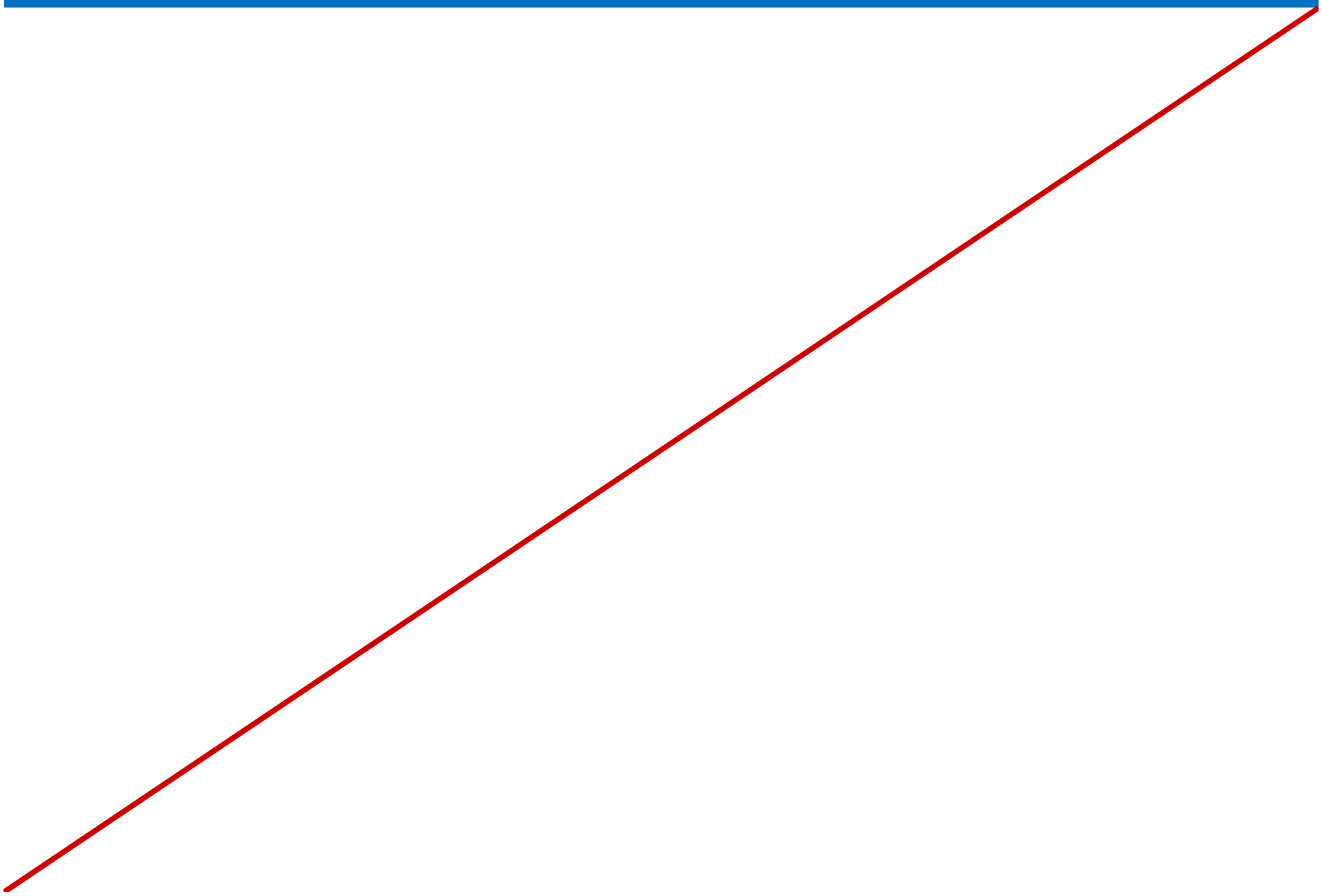
Feature	SRP	AppLocker
Rule scope	All users	Specific users or groups (per rule)
Rule conditions provided	File hash, path, certificate, registry path, Internet zone	File hash, path, publisher
Rule types provided	Allow and Deny	Allow and Deny
Default rule action	Allow and Deny	Implicit Deny
Windows PowerShell Support	No	Yes
Audit Only Mode	No	Yes
Customized Error Messages	No	Yes

Demonstration: Create and Enforce a AppLocker Rule

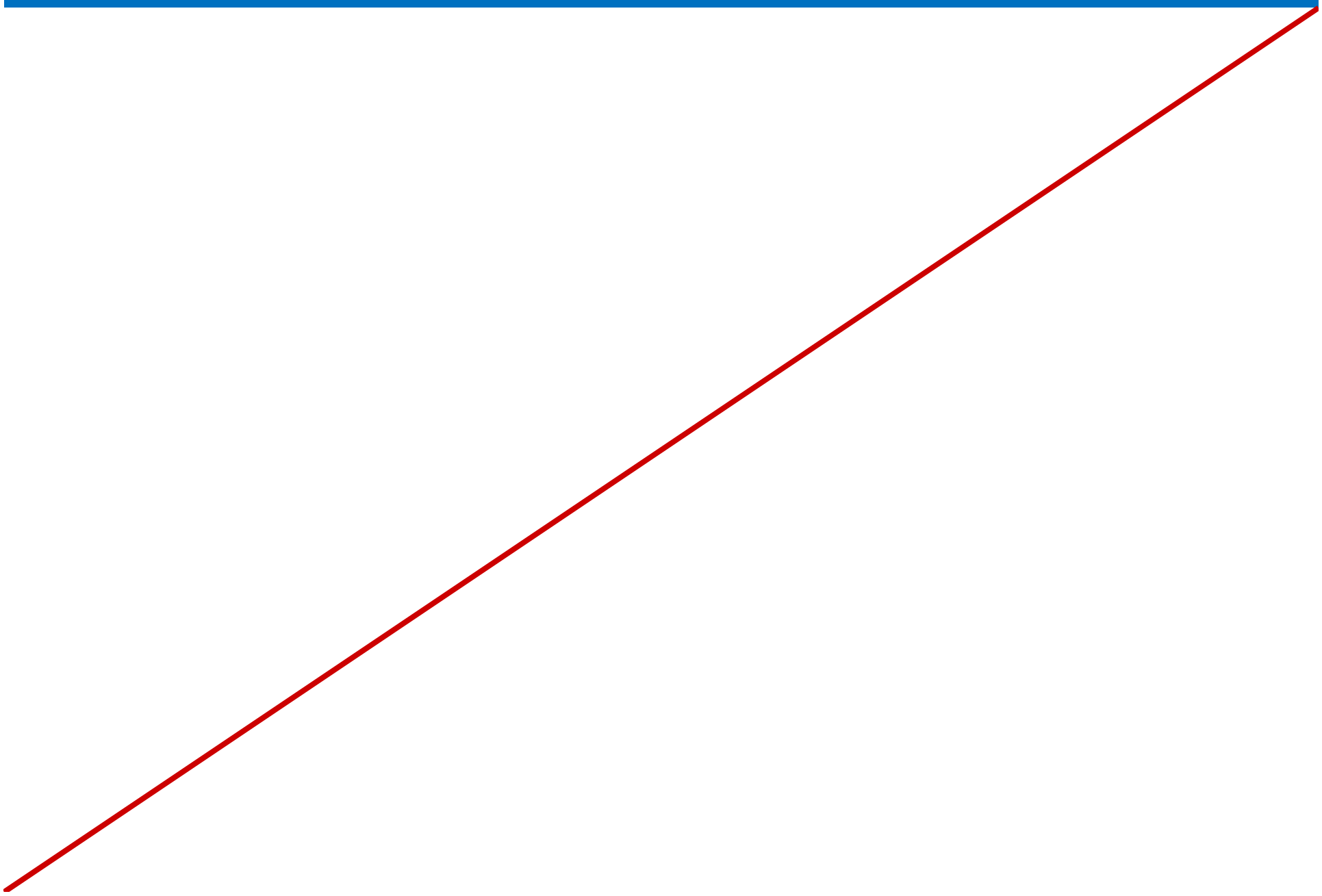
In this demonstration, you will see how to:

- Create a new AppLocker executable rule
- Use GPO to enforce the new AppLocker rule
- Confirm AppLocker rule enforcement

Notes Page Over-flow Slide. Do Not Print Slide.



Notes Page Over-flow Slide. Do Not Print Slide.



Lesson 2: Email Protection

- Common Email Security Threats
- Server-Side Solutions
- Client-Side Solutions

Common Email Security Threats

- The identification of and protection from email-based security threats is a critical part of protecting your infrastructure
- Common email security threats:
  - Spam
  - Phishing
  - Spoofing
  - Viruses

Server-Side Solutions

- Server-side email management methods:
  - Content Filtering
  - Sender and Recipient Filtering
  - IP Block/Allow Lists
  - DNS Reverse Lookup
- Cloud-based email management tools:
  - Microsoft Forefront Online Protection for Exchange (FOPE)
  - Microsoft Exchange Online Protection

Client-Side Solutions

- Client-side solutions offer an additional level of protection from email based attacks
- Client-side security features include:
  - Junk mail filters
  - Safe/Blocked sender lists
  - Junk mail security protection levels
  - Top-level domain lists
  - Antivirus programs

Lesson 3: Server Protection

- Maintaining Server Security
- What Is the Security Configuration Wizard?
- What Is the Best Practices Analyzer?
- What Is the Security Compliance Manager?
- Demonstration: How to Use the Best Practices Analyzer

Maintaining Server Security

- Server maintenance is critical to the continued security of your network environment

- Areas where server maintenance affects server security:
  - Operating system and software updates
  - User account maintenance and policies
  - Unused services and features
  - Unused or unwanted application installations
  - Windows Firewall configuration

What Is the Security Configuration Wizard?

- The Security Configuration Wizard (SCW) reduces the surface attack area of a server by customizing the server settings of server roles
- The SCW contains possible modifications to:
  - Services
  - Network security, including firewall rules
  - Registry values
  - Audit policy
- SCW policies can be created, modified, and redeployed to other servers within your infrastructure

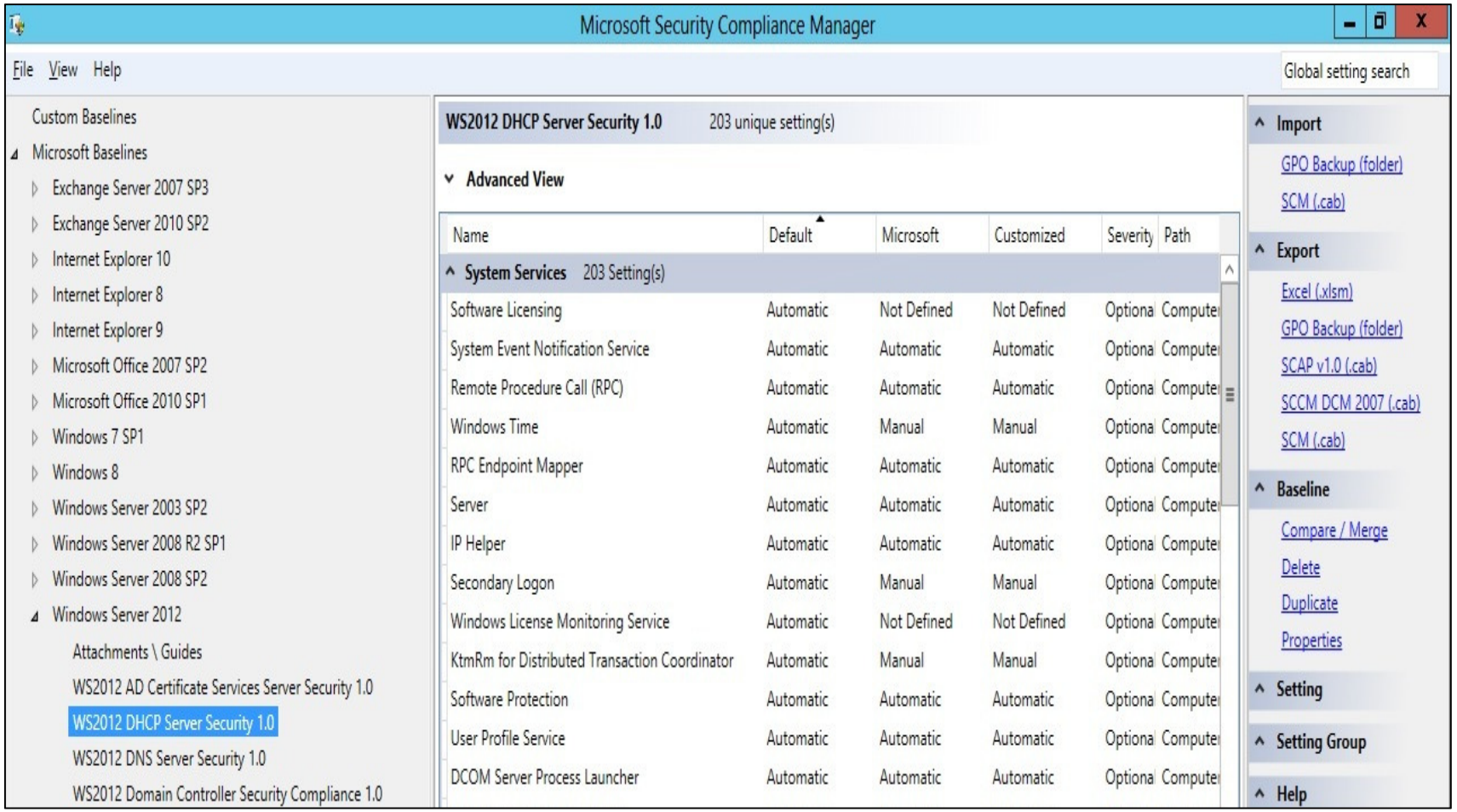
What Is the Best Practices Analyzer?

- The Best Practices Analyzer scans server roles against predefined rules
- Measures a role's compliance in effectiveness, trustworthiness, and reliability
- Reports best practice analysis results as noncompliant (error), compliant, and warnings

- Can be Run and Managed through
  - Server Manager
  - Windows PowerShell

What Is the Security Compliance Manager?

- The Security Compliance Manager is a Solution Accelerator tool for centralized management of security baselines



Demonstration: How to Use the Best Practices Analyzer

- In this demonstration, you will see how to use the Best Practices Analyzer

Lab: Implementing Security Software

- Exercise 1: Create and Enforce an AppLocker Rule
- Exercise 2: Use the Security Configuration Wizard
- Exercise 3: Use the Best Practices Analyzer

Logon Information
Virtual Machines: 10967A-LON-DC1, 10967A-LON-CL1
User Name: ADATUM\Administrator and ADATUM\Allie on 10967A-LON-CL1
Password: Pa$$w0rd

Estimated Time: 60 minutes

Lab Scenario

A. Datum has recently experienced several security breaches and is taking steps to tighten server security. You have been asked to prevent the installation of a particular Windows Installer .msi file which has caused some performance issues and raised some security issues for the organization. You are also asked to use the Security Configuration Wizard to configure security settings on a domain controller. And, to use the Best Practices Analyzer to scan the Active Directory Domain Services (AD DS) server role to ensure it is operating efficiently and as per best practices.

Lab Review

- What is the benefit of exporting a SCW security policy to a GPO?
- When would you use the Security Policy XML format?

Module Review and Takeaways

- Review Questions
- Tools

Notes Page Over-flow Slide. Do Not Print Slide.