IT2654: Systems Administration & Security

Topic 10:
Windows Server Security

Objectives

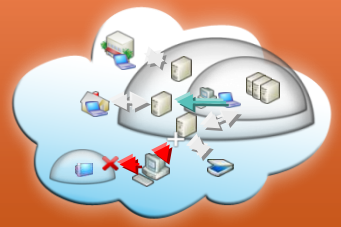
- Identify the various elements and techniques that can be used to secure a Windows Server system
- Use Security Configuration and Analysis tools to configure and review security settings
- Audit access to resources and review Security log settings
- Learn about Application Security through Application Whitelisting using AppLocker
- Protect data using BitLocker tools

Windows Server Security

Fundamentally Secure Platform

- User Account Control
- **Security Templates**
- Manageability and **Auditing**

Securing Anywhere Access



- Network Security
- Network Access Protection
- DirectAccess™

Protect Users & Infrastructure

- **AppLocker™**
- Data Recovery

Protect Data from Unauthorized Viewing

- EFS
- **BitLocker™**

Using Security Configuration Manager Tools

- Tools specifically designed to help configure and manage security settings
- These tools plus Group Policies can be used to set up a Security Policy **template** which is administered centrally
- The Security Configuration and Analysis tool will compare a security template to existing settings
- Consist these components:
  - Security settings in Group Policy objects
  - Security Configuration and Analysis tool
  - SECEDIT command-line tool

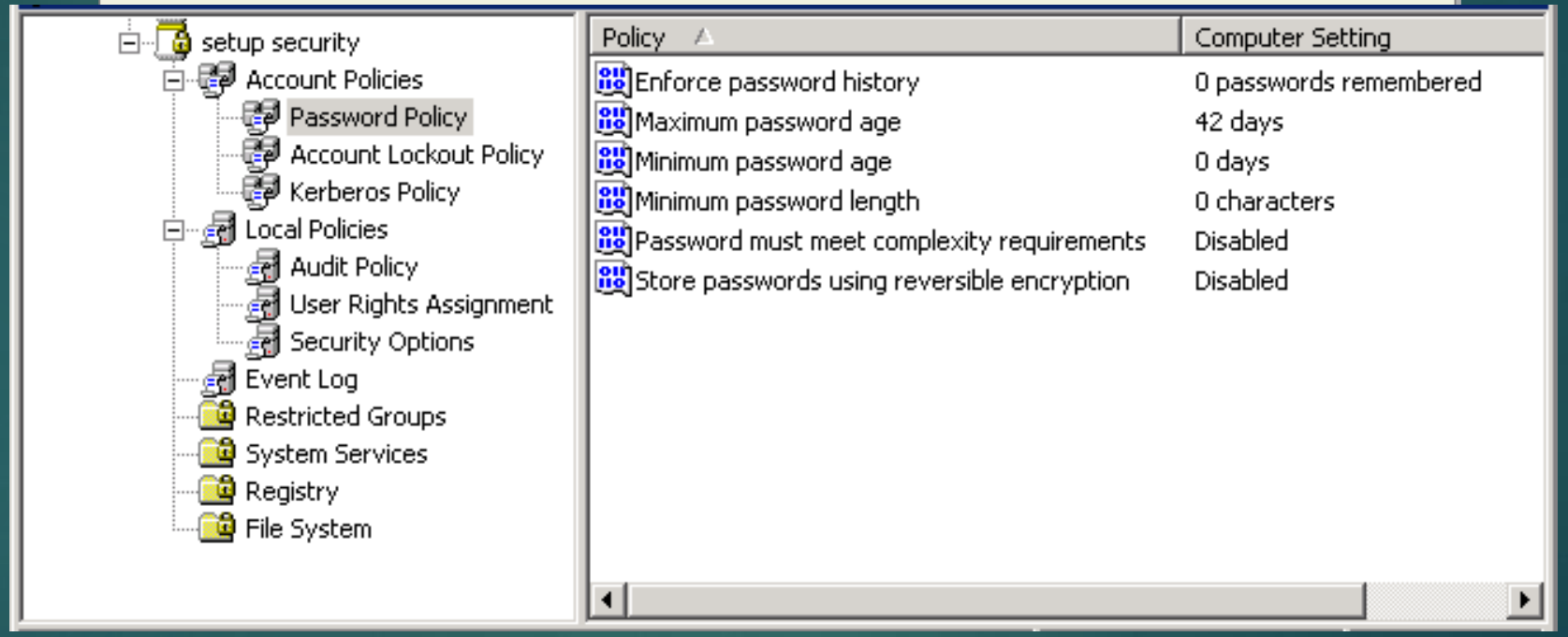
Security Templates

- Templates help ensure consistency and ease maintenance across multiple machines
- Templates are text-based files
  - Should not be edited or changed using a text-based editor

Security Template Settings

Security Template: Setup Security

Sample of Settings



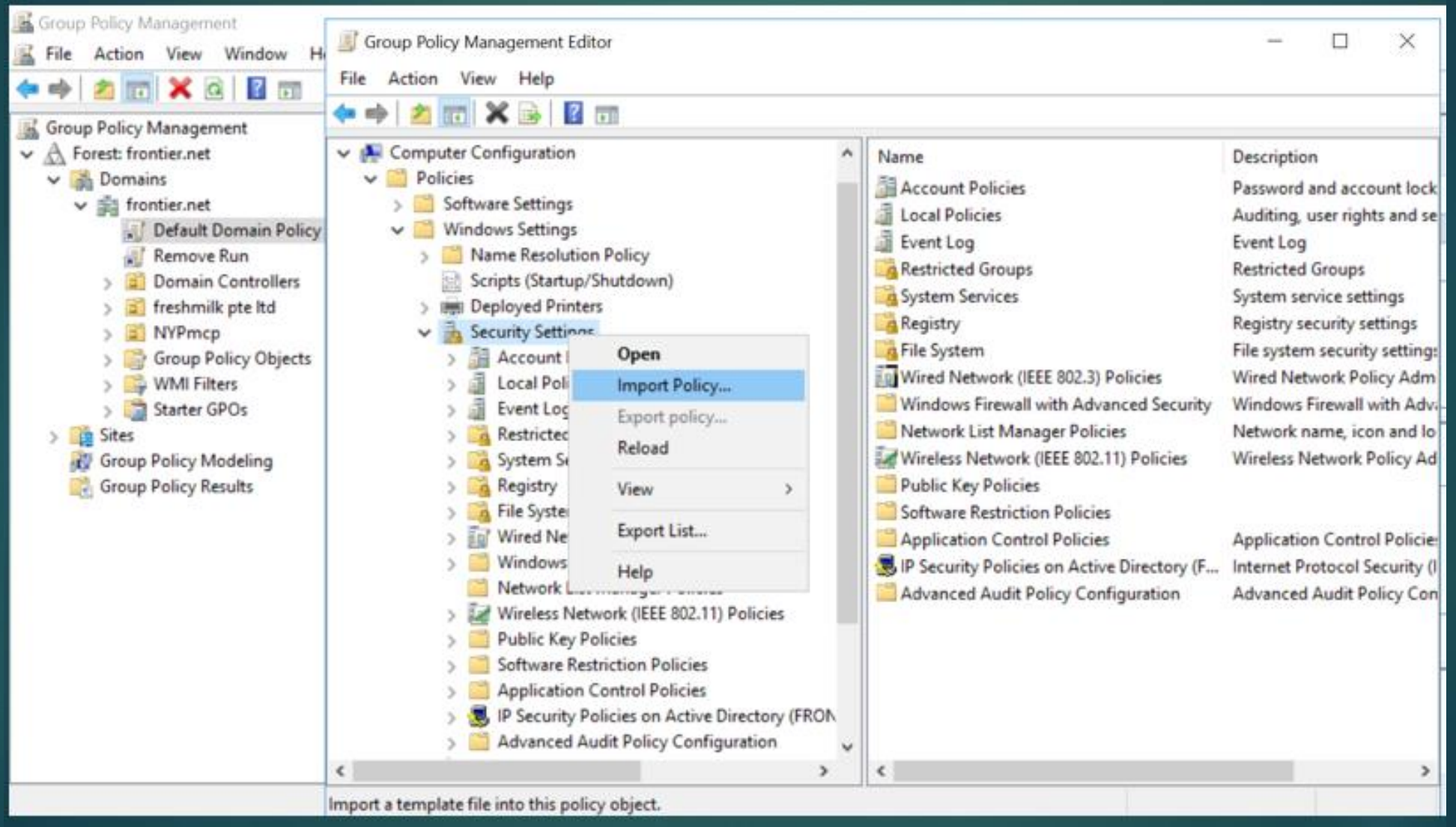
Applying Security Templates

- Security templates can be applied to Local Machine or a Domain
- For Local Machine
  - Open Local Security Setting MMC snap-in and import a policy
- For Domain
  - Use Group Policy Objects
- Security settings from GPOs override local settings

Applying a Security Template

1. Open Active Directory User and Computer, and then navigate to the OU to which you want to apply the security template
2. Create a new GPO and link it to the OU
3. Navigate to Computer Configuration\Windows Settings\Security Settings
4. Right-click Security Settings, and then click Import Policy
5. Select the security template, and then click OK

Importing Security Template via Group Policy



Security Configuration and Analysis Tool

- Compare current system settings to those configured in templates
- Comparison identifies changes and potential weaknesses
- Changes can be made directly within the snap-in by selecting the desired configuration

Security Configuration and Analysis (continued)

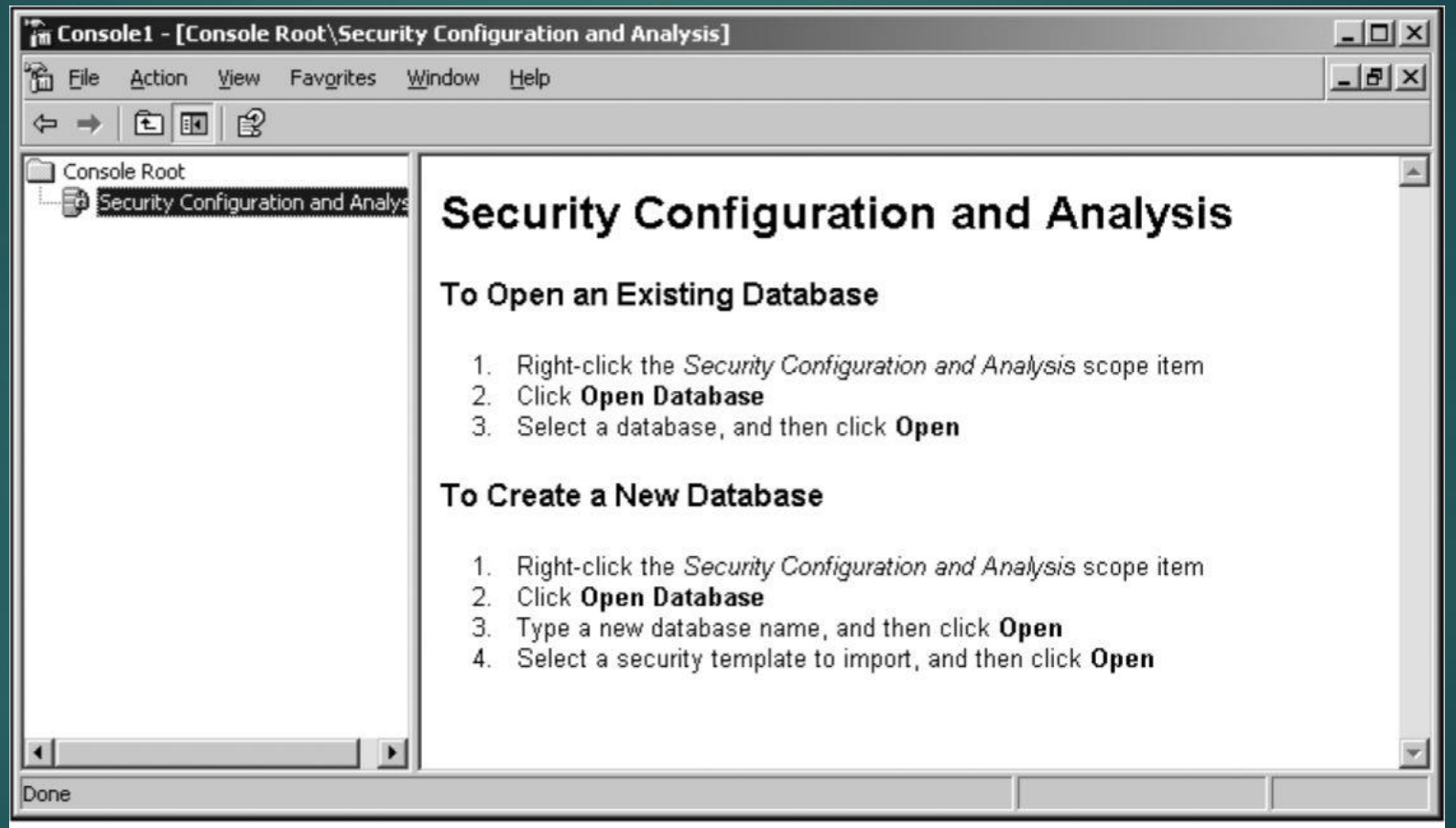
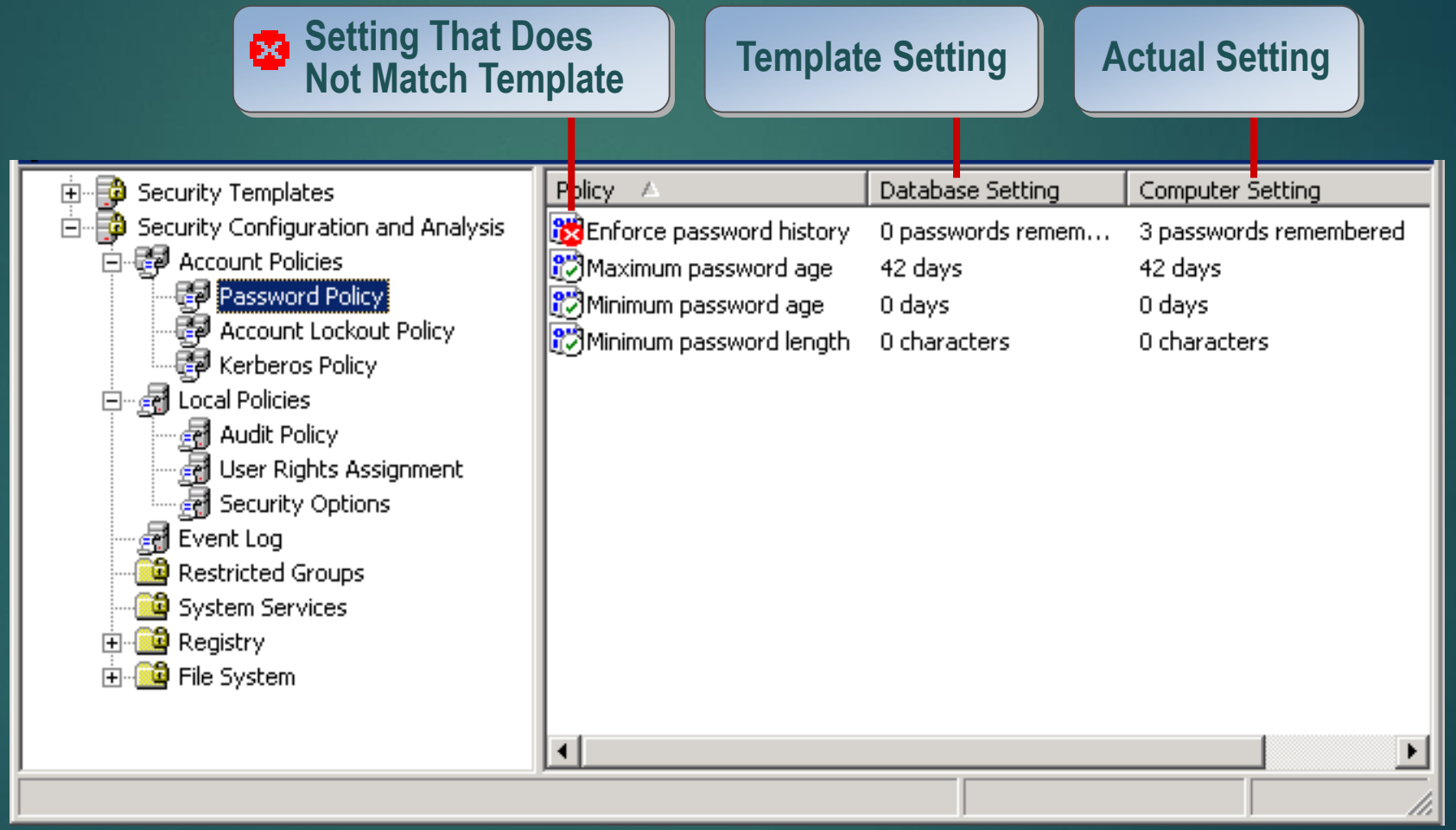


Figure 14-5 The Security Configuration and Analysis snap-in

Security Configuration and Analysis Tool



SECEDIT Command-Line Tool

- SECEDIT - command-line tool used to create and apply security templates and analyze settings
- Six main switches
  1) Analyze
  2) Configure
  3) Export
  4) Import
  5) Validate
  6) GenerateRollback

Auditing

- Auditing tracks user and operating system activities and records selected events in security logs

What occurred? | Who did it? | When?

What was the result?

- Enable auditing to:
  - –Create a baseline
  - –Detect threats and attacks
  - –Determine damages
  - –Prevent further damage
- Audit access to objects, management of accounts, and users logging on and logging off

Audit Policy

- Determines the security events that will be reported to the network administrator
- Set up an audit policy to:
  - Track success or failure of events
  - Minimize unauthorized use of resources
  - Maintain a record of activity
- Security events are stored in security logs

Configuring Auditing

- Member servers or workstations
  - Audit policies are implemented using GPOs assigned to the domain or OUs
- Domain Controllers
  - Audit policies are implemented via the Default Domain Controllers Policy applied to Domain Controllers OU
- Standalone workstations and servers
  - Audit policies defined using Local Security Policy tool

Configuring an Audit Policy

Figure 14-12 Configuring audit policy settings

Auditing Object Access

- Files and folders reside on an NTFS volume - can monitor attempted and successful accesses of these objects
- Caution – this can result in a large number of events being logged
- Object auditing - configured through the Advanced Security Settings on the resource

Best Practices

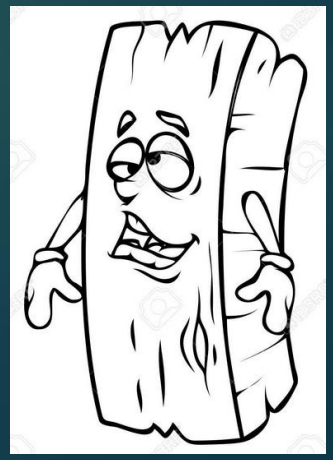
- Plan carefully before implementing an audit policy
- General guidelines:
  - Only audit events that provide truly useful information
  - Review entries in the security log regularly
  - Audit sensitive and confidential information
  - Audit the Everyone group – it includes unauthenticated users
  - Audit the assignment of user rights
  - Audit the Administrators group

What Are Log Files?

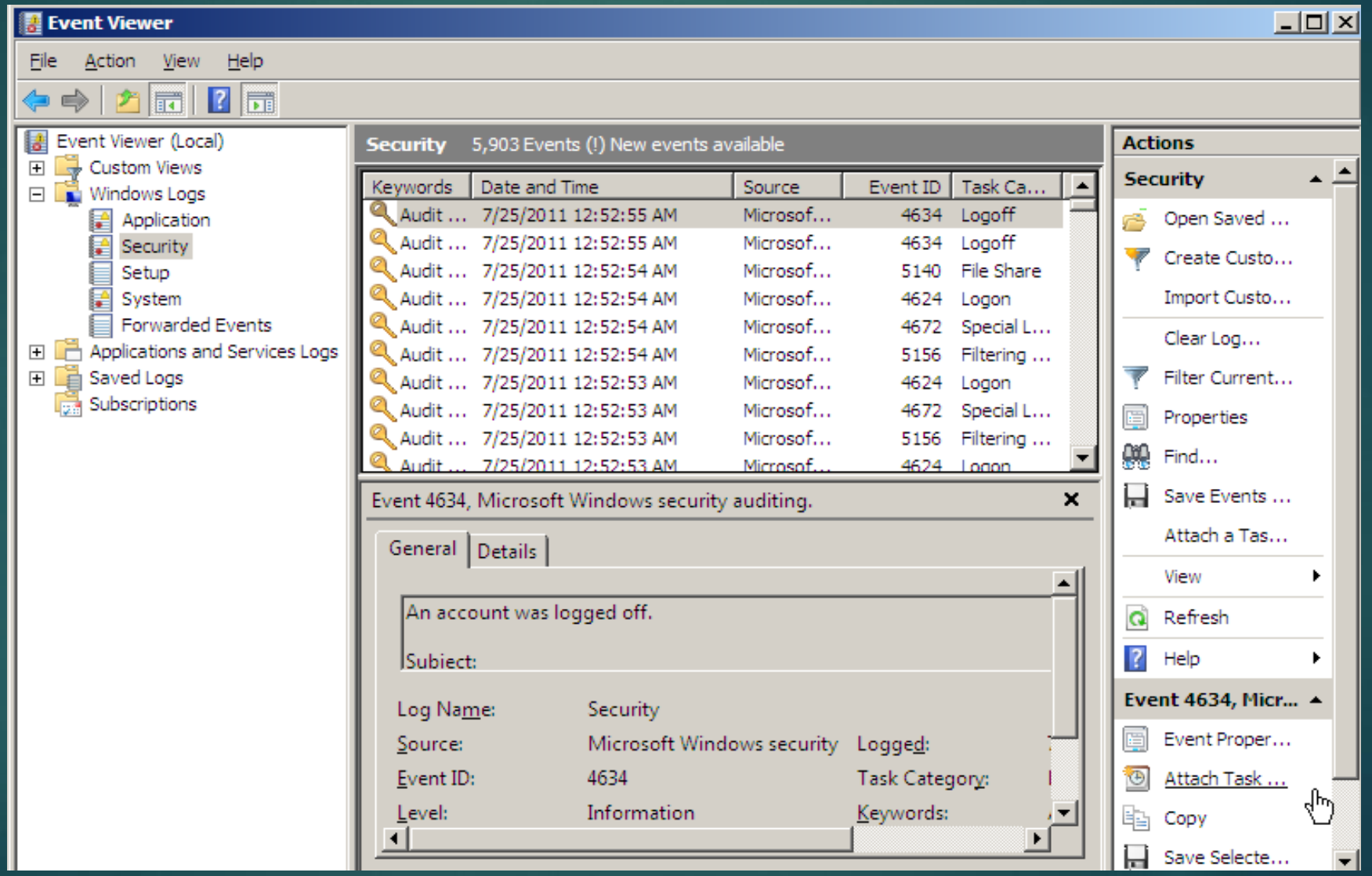
- Records of events occurred in computer.
- Following logs available in Event Viewer:
  - Application
  - Security
  - System
  - Directory service
  - File Replication service

Analyzing Security Logs

- For each event defined in an audit policy, an entry is written in the Security log if that event occurs
- Use Event Viewer to examine the Security log
- The log provides a summary of the date and time of each event, and the user performing the action
- More details by double-clicking the entry
- Event Viewer provides find and filter options to assist in managing the Security log

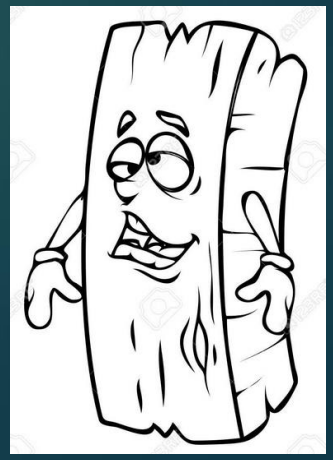


Analyzing Security Logs (continued)



Configuring Event Viewer

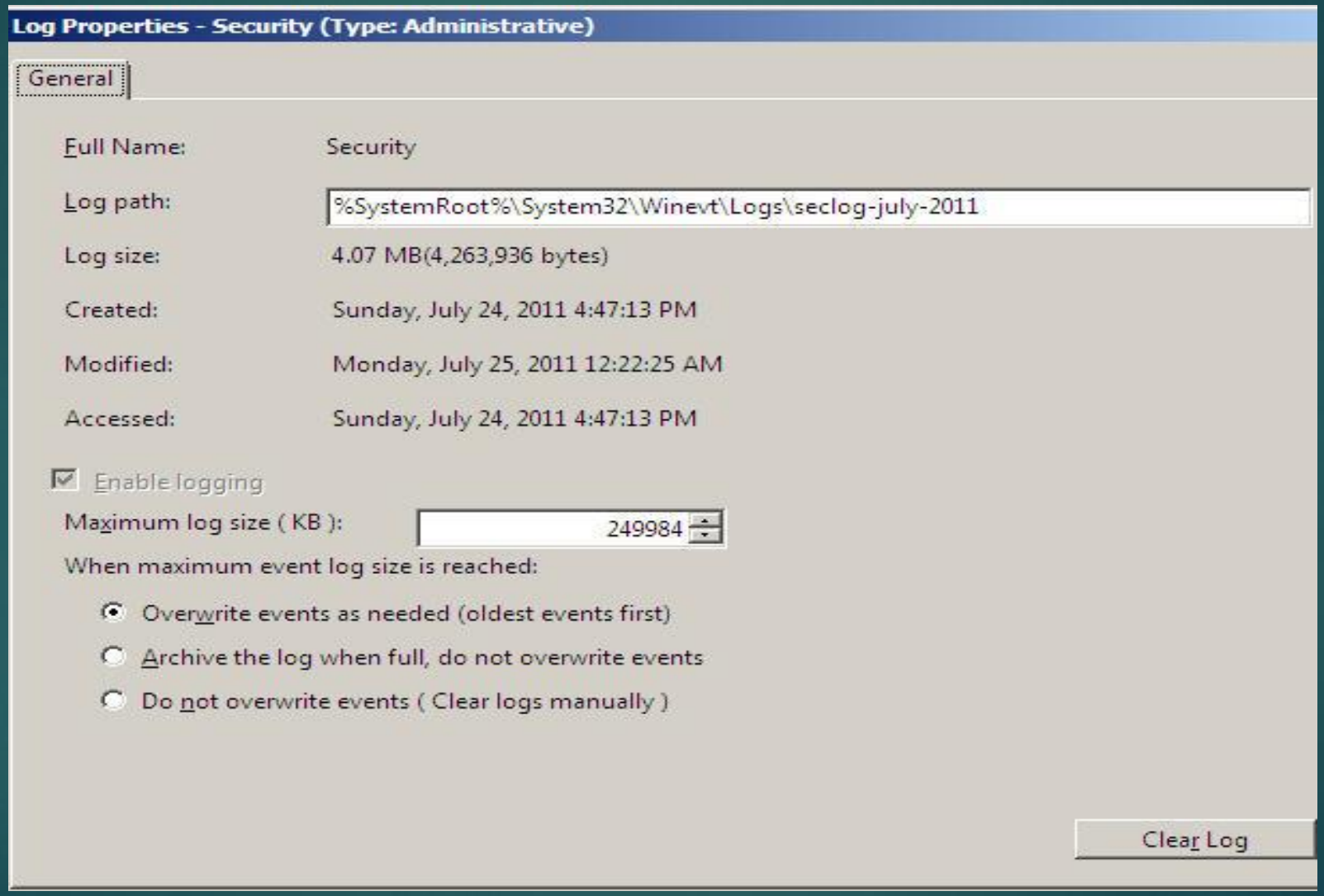
- There are a number of configurable settings that determine the size, number of entries, and overwrite policy in a security log
- Default initial security log size is 16 MB in Windows Server (up from 512 KB in 2000)
- Settings are configured from the Properties of the Security log in Event Viewer



Configuring Event Viewer (continued)

Option	Description
Log name	Changes the name and location of the log
Maximum log size	Specifies the size of the log file; the default is 128 MB
Overwrite events as needed	All new events overwrite the oldest events when the log file becomes full; if you plan to use this option, check the log file at regular intervals
Overwrite events older than X days	Sets the number of days before a log is overwritten (between 1 and 365)
Do not overwrite events (clear log manually)	Events in the log are not overwritten and when the log becomes full new events are discarded until the log is manually cleared
Using a low-speed connection	Specifies whether the log is located on another computer and whether you are connected using a low-speed device (such as a modem)

Log File Properties



Application Control

- **Application control** is a security practice that blocks or restricts unauthorized **applications** from executing in ways that put data at risk

Application Control

- Prevent all other, unauthorized applications from executing – they may be malicious, untrusted, or simply unwanted
- Eliminate unknown and unwanted applications in your network to reduce IT complexity and application risk
- Reduce the risks and costs associated with malware
- Improve your overall network stability
- Identify all applications running within the endpoint environment
- Protect against exploits of unpatched OS and third-party application vulnerabilities

Application Control in Windows

Situation Today

- Users can install and run non-standard applications
- Even standard users can install some types of software
- Unauthorized applications may:
  - Introduce malware
  - Increase helpdesk calls
  - Reduce user productivity
  - Undermine compliance efforts

Application Control

Windows Solution

AppLocker

- Eliminate unwanted/unknown applications in your network
- Enforce application standardization within your organization
- Easily create and manage flexible rules using Group Policy

AppLocker

Technical Details

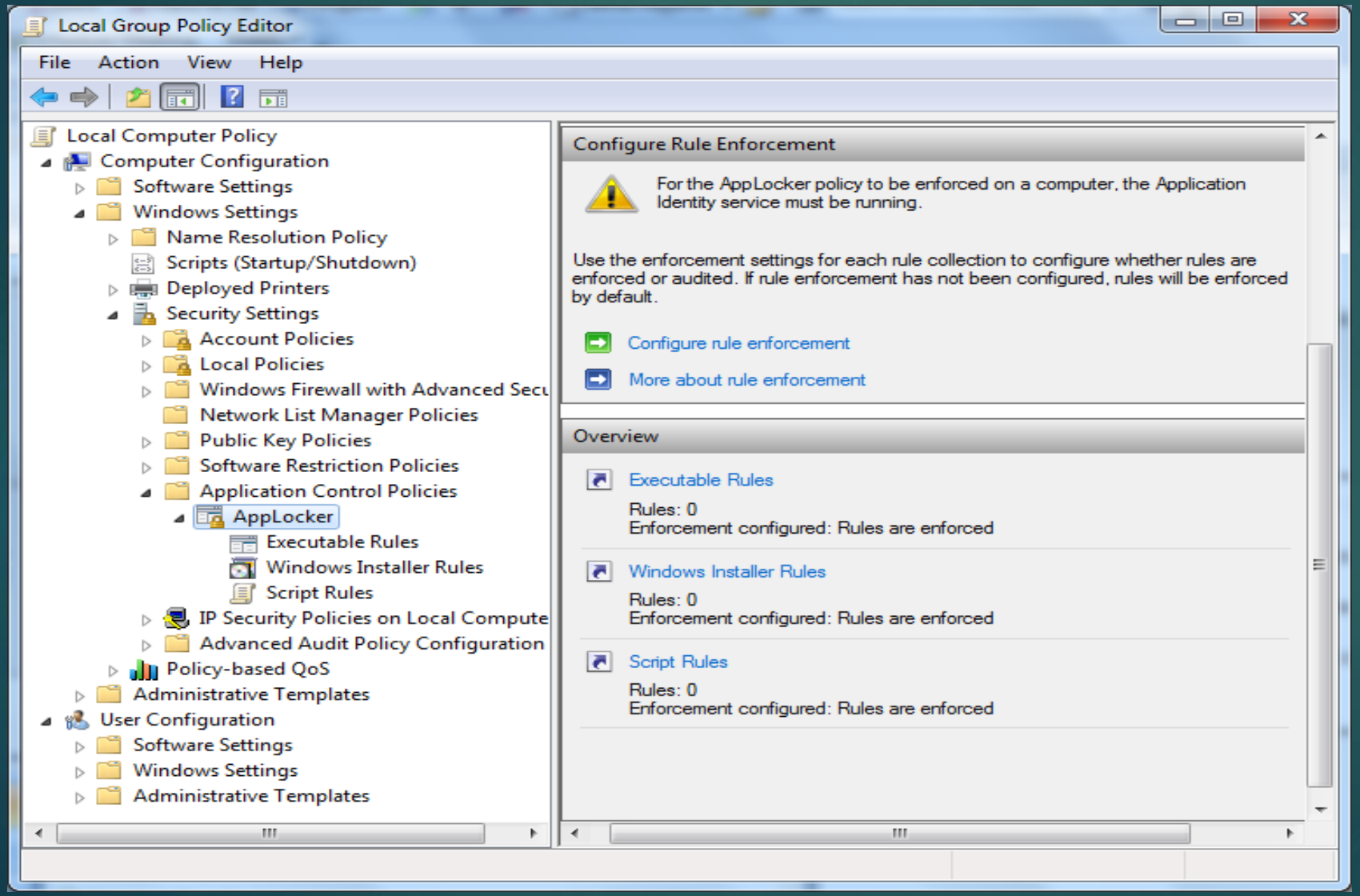
- Simple Rule Structure: Allow, Exception & Deny
- Publisher Rules
  - Product Publisher, Name, Filename & Version
- Multiple Policies
  - Executables, installers, scripts & DLLs
- Rule creation tools & wizard
  - Including PowerShell cmdlets
- Audit only mode

AppLocker Rule Collection

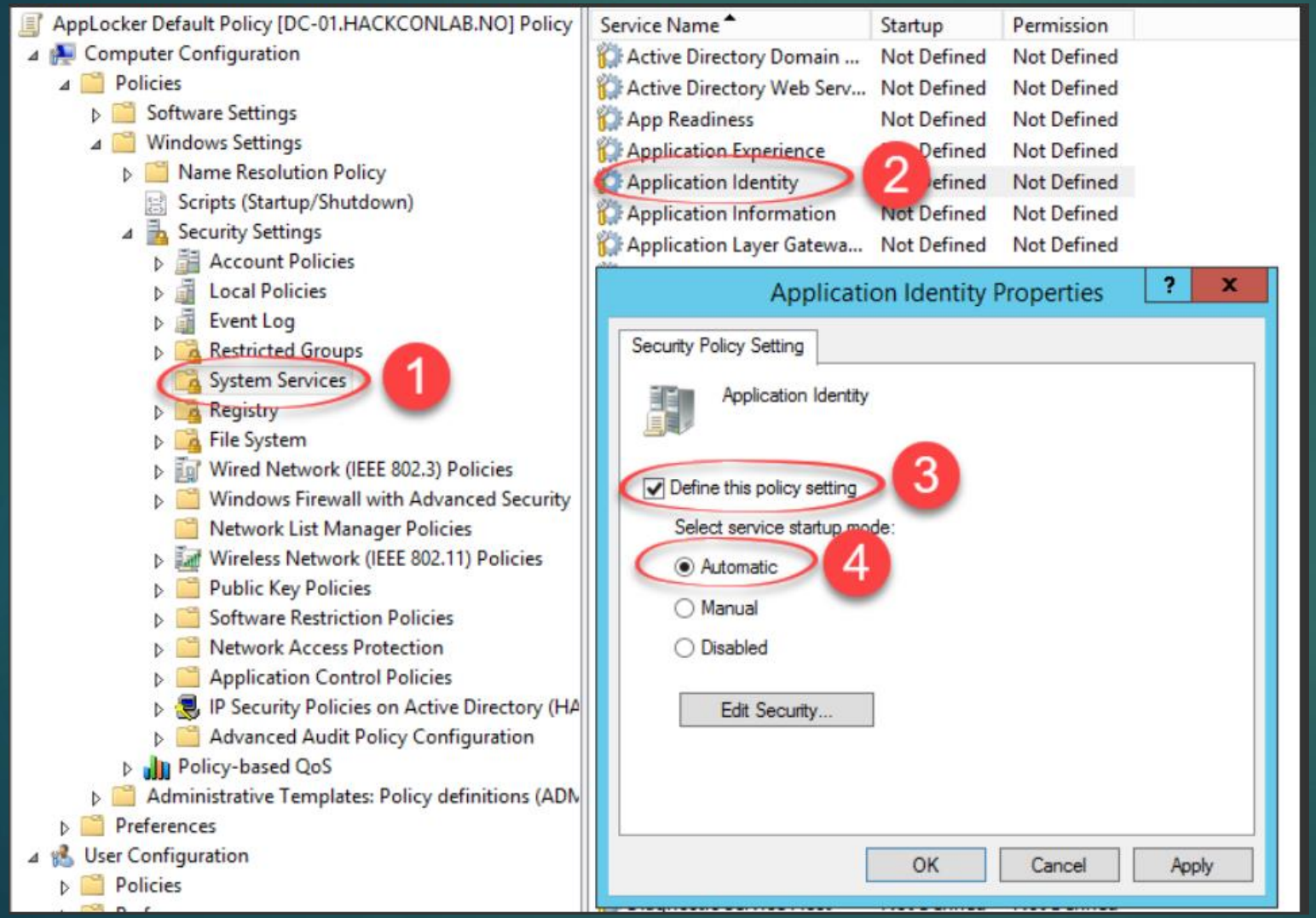
Rule collection	Associated file formats
Executable files	.exe .com
Windows Installer files	.msi .msp .mst
Scripts	.ps1 .bat .cmd .vbs .js
Packaged apps and packaged app installers	.appx
DLL files	.dll .ocx

- The AppLocker console is ordered into rule collections, which include executable files, scripts, Windows Installer files, packaged apps, and packaged app installers, and DLL files.
- These collections allow you to easily distinguish rules for different types of applications.
- The table lists the file formats included in each rule collection.

Accessing AppLocker



AppLocker Pre-requisite



Must turn on Application Identity service in order for AppLocker to work.

Data Protection - Encryption

- Encryption is the process of converting data into a format that cannot be read by another user.
- Once a user has encrypted a file, it automatically remains encrypted when the file is stored on disk.
- Decryption is the process of converting data from encrypted format back to its original format.
- A key, which can be thought of as a password, is applied mathematical to plain text to provide cipher or encrypted text.

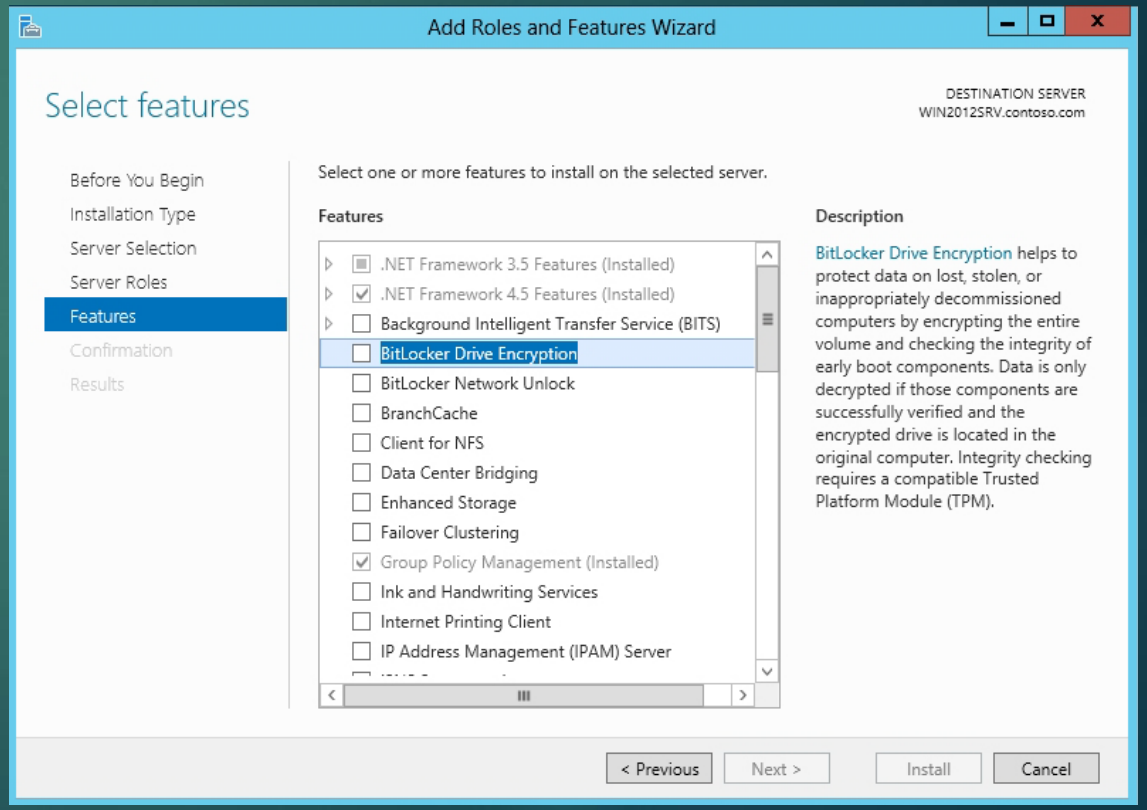
Encrypting Files (Volume) with BitLocker

When you use BitLocker on fixed and removable data drives that are not the OS volume, you can use one of these:

- Password
- Smart card
- Automatic Unlock

Configuring BitLocker Encryption

- Before you can use BitLocker on a server running Windows Server 2016, you must first install BitLocker using Server Manager.
- You can then determine whether you have TPM and turn on BitLocker.
- Install BitLocker as a Feature



BitLocker™ Drive Encryption

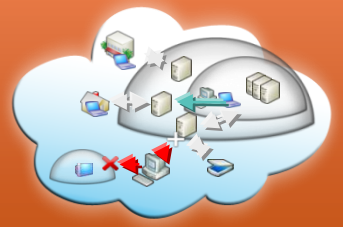
- BitLocker™ Drive Encryption gives you improved data protection on your Windows
  - Notebooks – Often stolen, easily lost in transit
  - Desktops – Often stolen, difficult to safely decommission
  - Servers – High value targets, often kept in insecure locations
  - All three can contain very sensitive IP and customer data
- Designed to provide a **transparent user experience** that requires little to no interaction on a protected system
- Prevents thieves from using another OS or software hacking tool to break OS file and system protections
  - Prevents offline viewing of user data and OS files
  - Provides enhanced data protection and boot validation through use of a Trusted Platform Module (TPM)

Summary

Fundamentally Secure Platform

- User Account Control
- **Security Templates**
- Manageability and **Auditing**

Securing Anywhere Access



- Network Security
- Network Access Protection
- DirectAccess™

Protect Users & Infrastructure

- **AppLocker™**
- Data Recovery

Protect Data from Unauthorized Viewing

- EFS
- **BitLocker™**