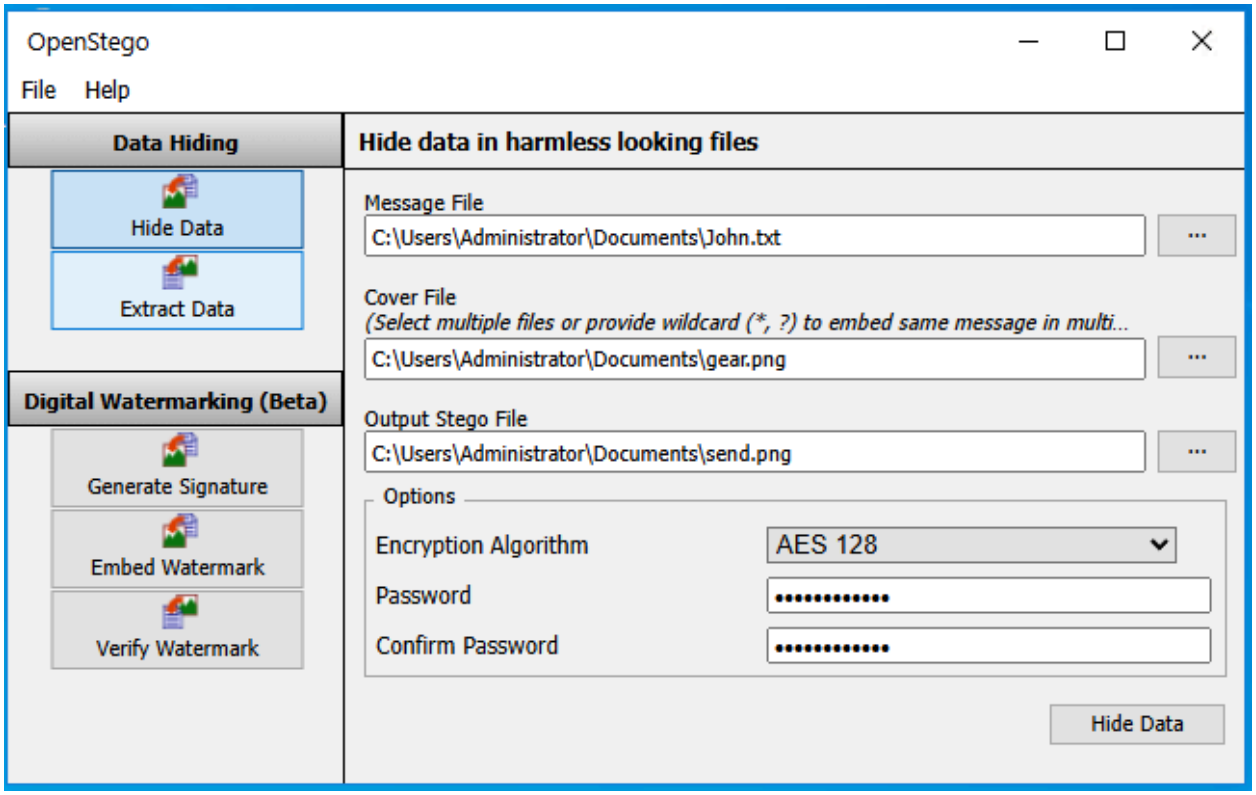
IT Tools/Labs from school

OpenStego:

In this lab, your task is to use OpenStego to hide data in photos as follows:

- Encrypt and password-protect the user data in the file to be shared.
  - Message file: John.txt
  - Cover file: gear.png
  - Output Sego file: send.png (saved in the Documents folder)
  - Password: NoMor3L3@ks!
- Confirm the functionality of the steganography by:
  - Extracting the data to C:\Users\Administrator\Documents\Export.
  - Open the extracted file to confirm that the associated username has been embedded into the file.

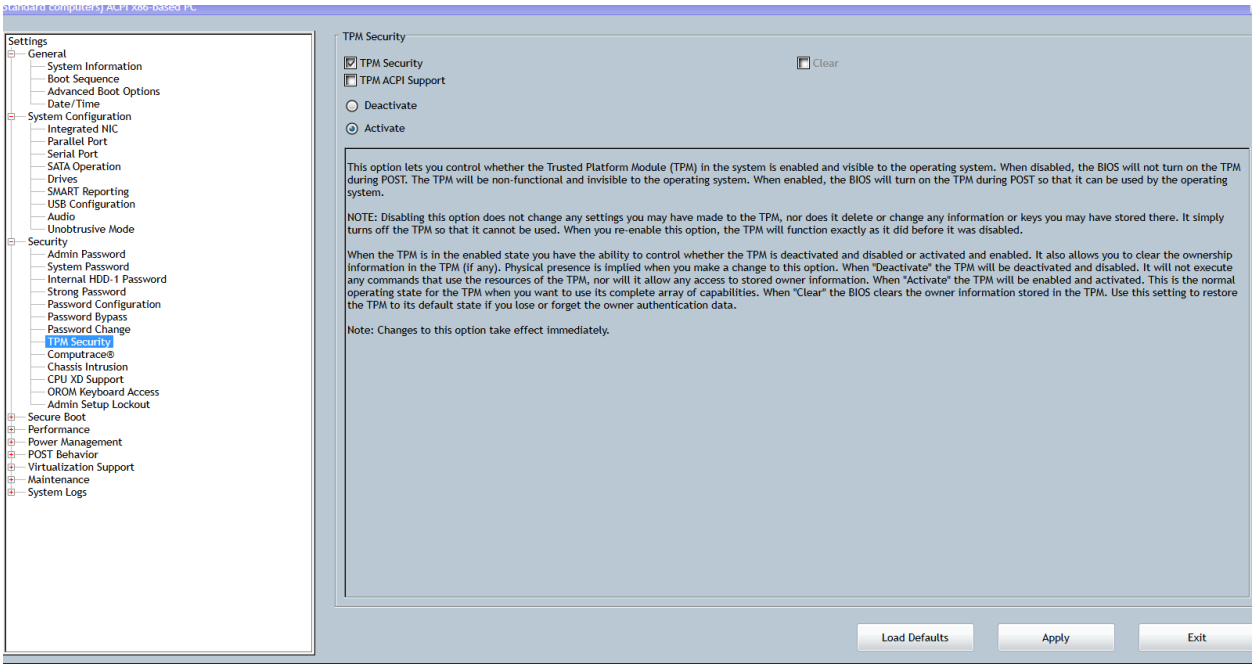


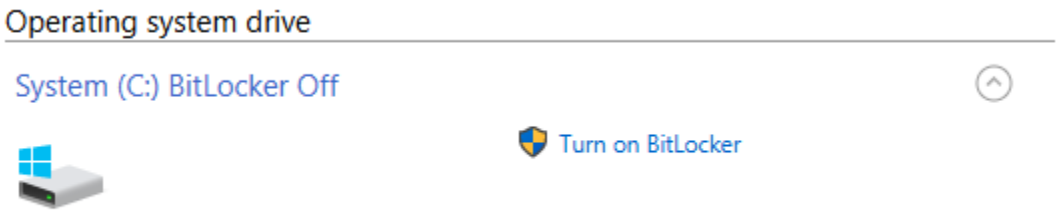
BitLocker

You work as the IT security administrator for a small corporate network. The employee in Office 1 is working on a very sensitive project. Management is concerned that if the hard drive in the computer were stolen, sensitive information could be compromised. As a result, you have been asked to encrypt the entire System volume. The Office 1 computer has a built-in TPM on the motherboard.

In this lab, your task is to configure BitLocker drive encryption as follows:

- From within the computer's BIOS, turn on and activate TPM Security.
- From Windows, turn on BitLocker for the System (C:) drive.
- Back up the recovery key to the **\\CorpServer\BU-Office1** folder.
- Encrypt the entire System (C:) drive.
- Use the new encryption mode.
- Run a BitLocker system check.





BitLocker Drive Encryption (C:)

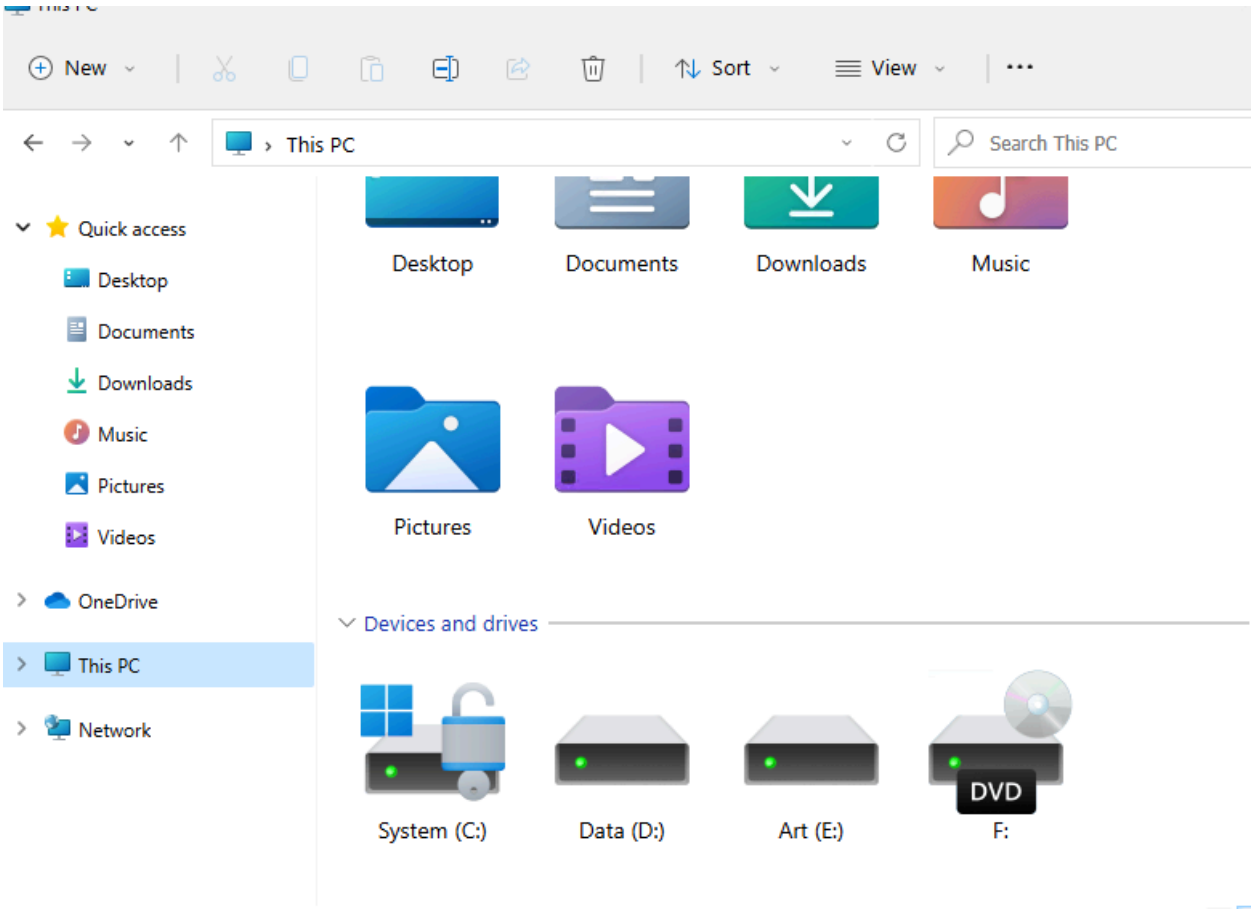
Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

- (●) New encryption mode (best for fixed drives on this device)
- ( ) Compatible mode (best for drives that can be moved from this device)



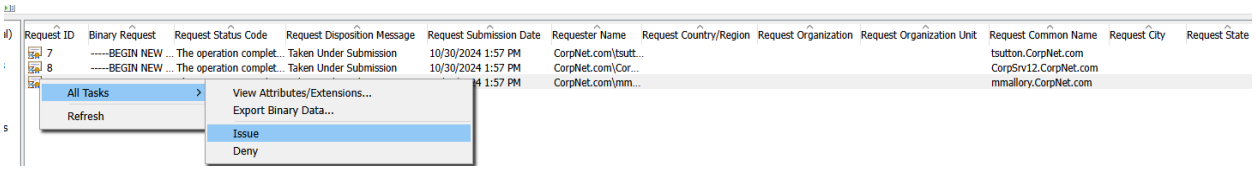
END

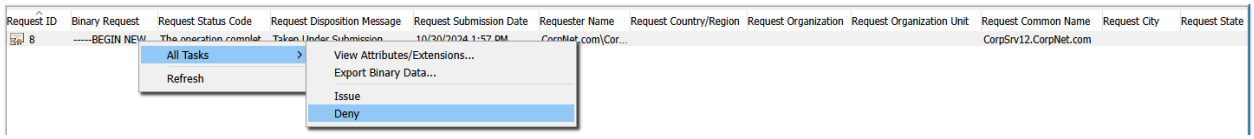
Certificate Authority

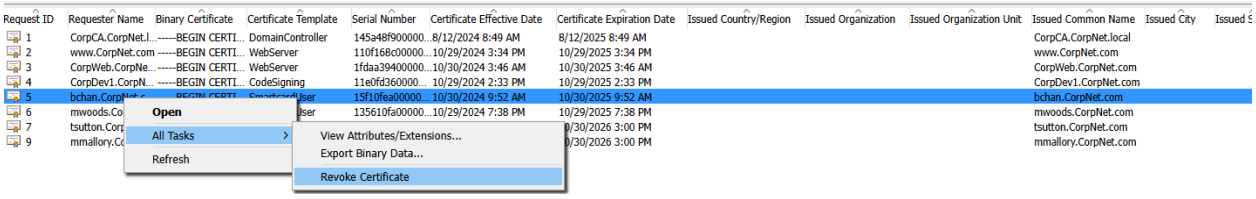
You are the IT administrator for a growing corporate network. You manage the certification authority for your network. As part of your daily routine, you perform several certificate management tasks. CorpCA, the certification authority, is a guest server on CorpServer2.

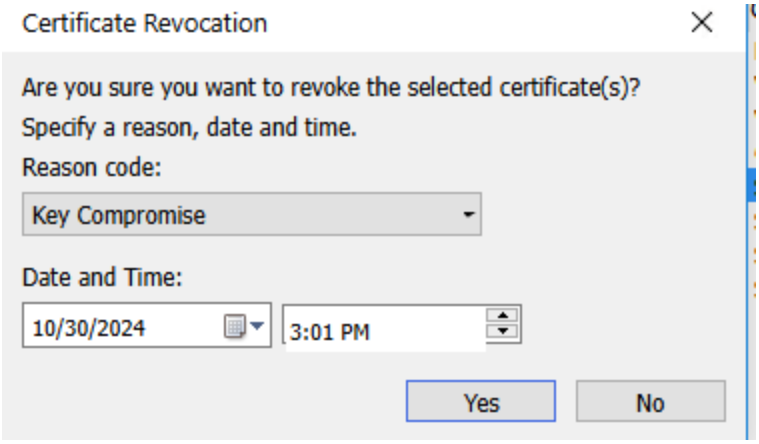
In this lab, your task is to complete the following:

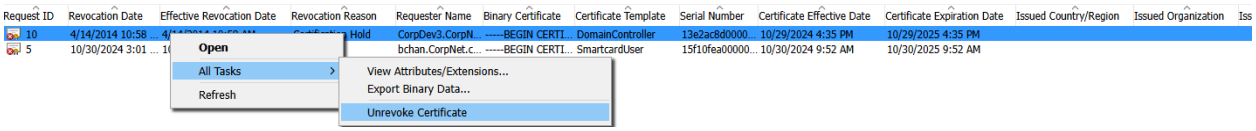
- Your network uses smart cards to control access to sensitive computers. Currently, the approval process dictates that you manually approve smart card certificate requests.
  Approve pending certificate requests for smart card certificates from tsutton and mmallory.
- Deny the pending web server certificate request for CorpSrv12.
- User bchan lost his smartcard. Revoke the certificate assigned to bchan.CorpNet.com using the **Key Compromise** reason code.
- Unrevoke the CorpDev3 certificate











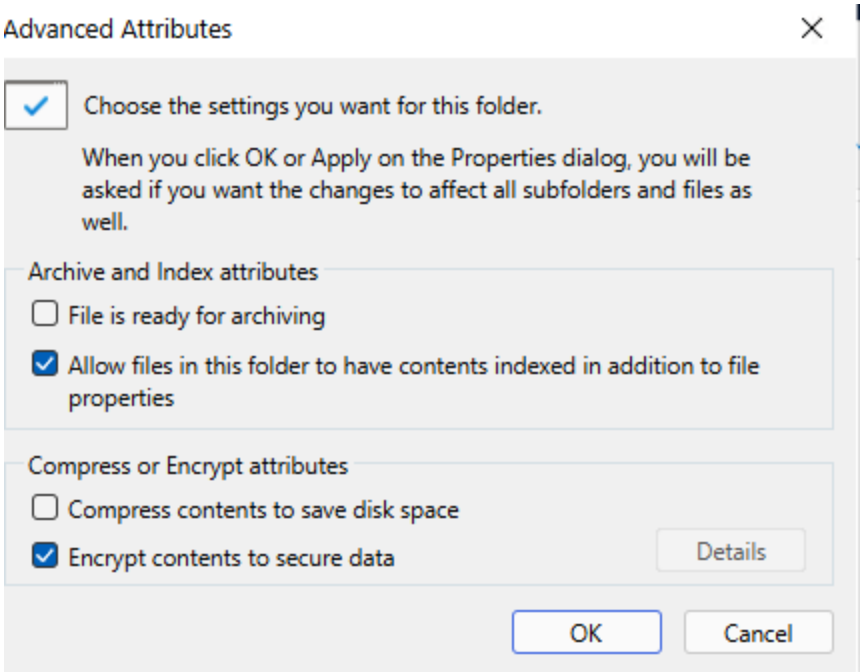
END

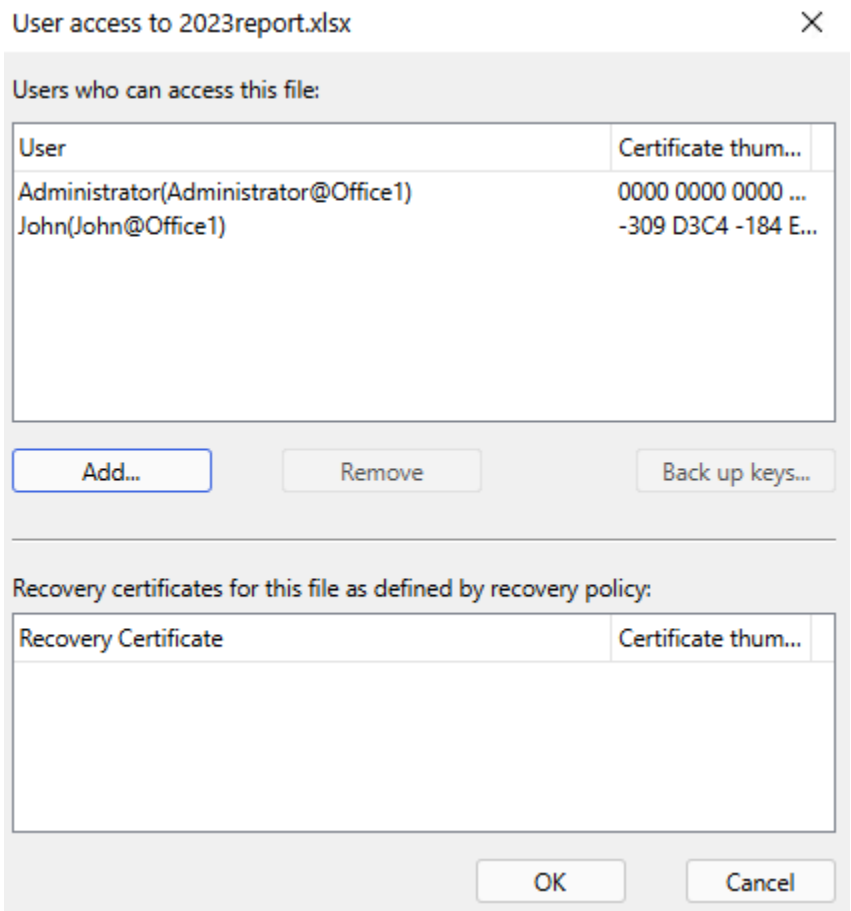
Encrypting File System:

You share a computer with other users at work. You want to secure the contents of the Finances folder so that unauthorized users cannot view its contents.

In this lab, your task is to:

- Encrypt the D:\Finances folder and all of its contents.
- Give John file access to the encrypted D:\Finances\2023report.xls file by adding the encryption certificate.

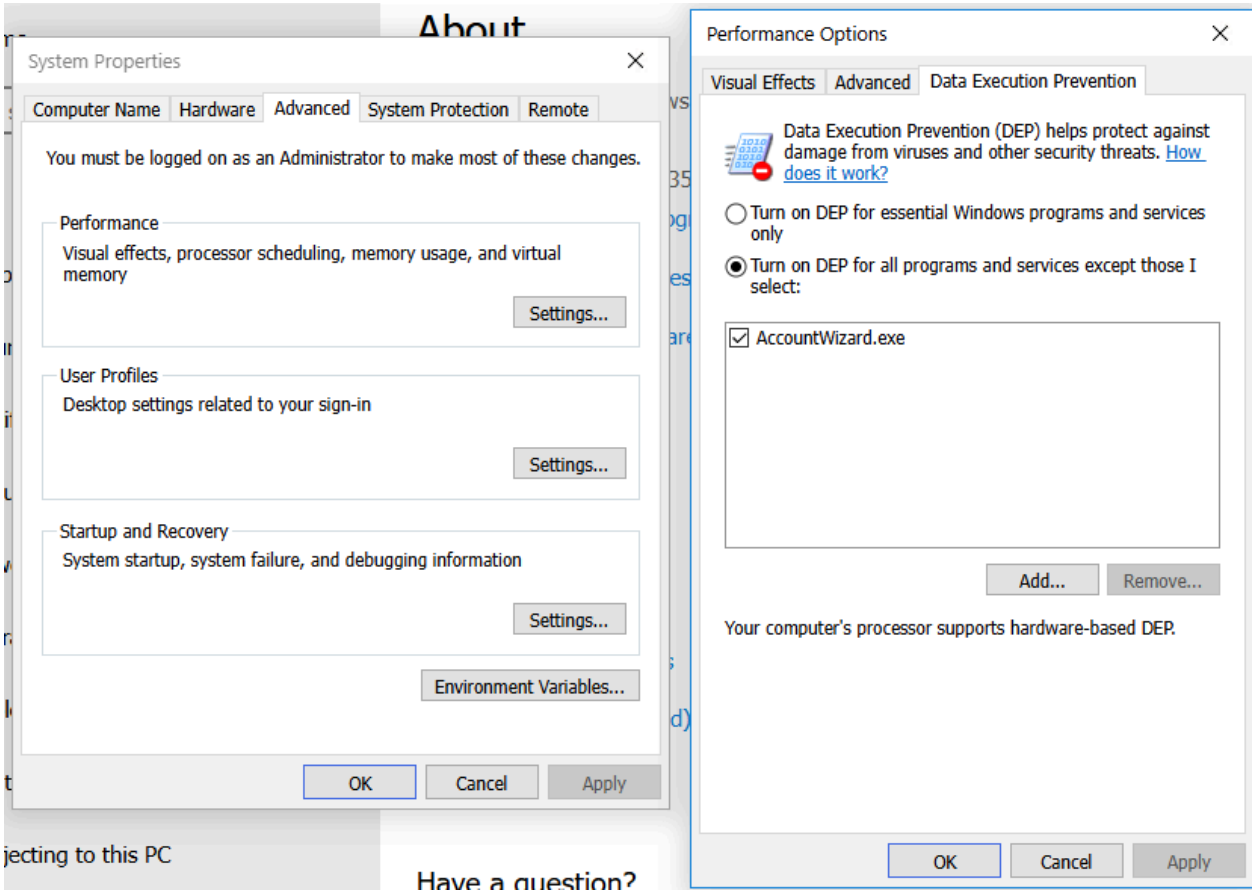

Advanced Attributes
Choose the settings you want for this folder.
When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.
Archive and Index attributes
File is ready for archiving
Allow files in this folder to have contents indexed in addition to file properties
Compress or Encrypt attributes
Compress contents to save disk space
Encrypt contents to secure data
Details
OK
Cancel


User access to 2023report.xlsx
Users who can access this file:
User
Certificate thum...
Administrator(Administrator@Office1)
0000 0000 0000 ...
John(John@Office1)
-309 D3C4 -184 E...
Add...
Remove
Back up keys...
Recovery certificates for this file as defined by recovery policy:
Recovery Certificate
Certificate thum...
OK
Cancel

DEP Data Execution Prevention

In this lab, your task is to configure DEP as follows:

- Enable DEP for all files.
- Disable DEP for **C:\Program Files (x86)\AccountWizard\AccountWizard.exe**.
- Restart the computer to activate DEP.



END

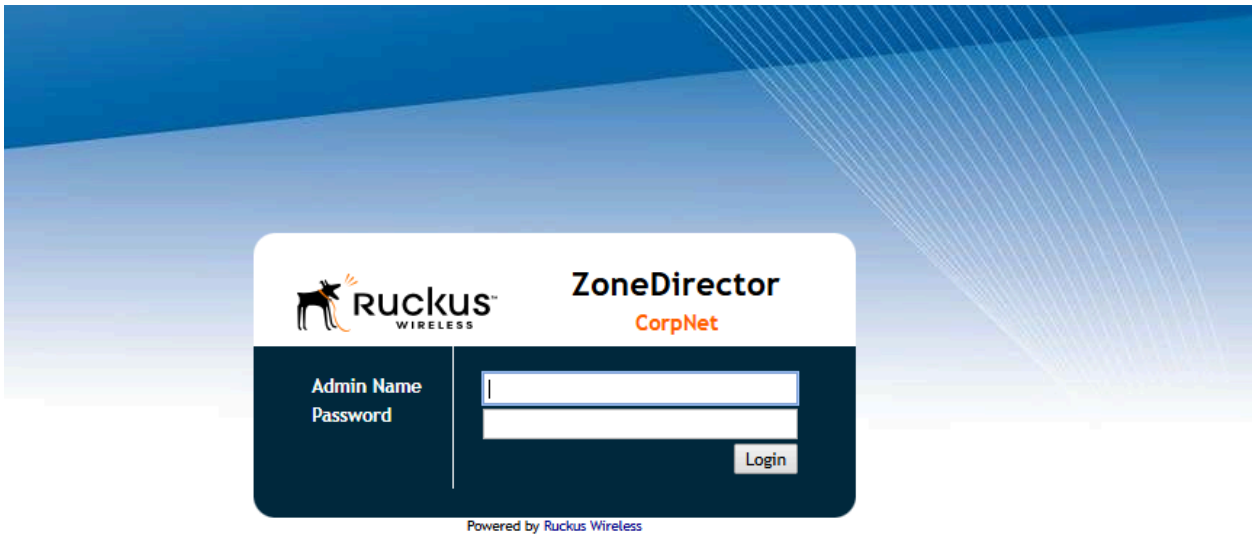
Ruckus wireless

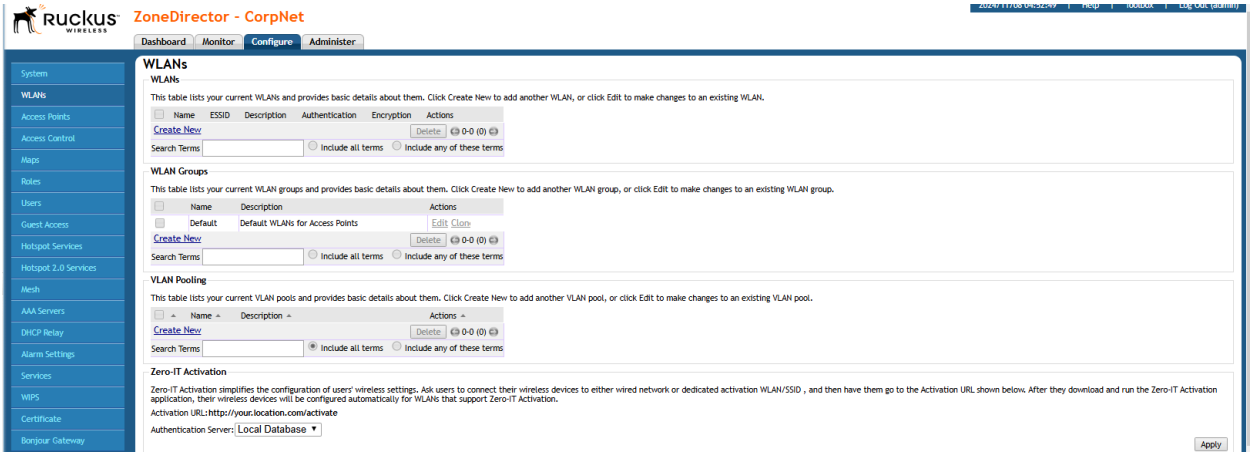
You are a network technician for a small corporate network. You just installed a Ruckus zone controller and wireless access points throughout your office buildings using wired connections. You now need to configure basic wireless network settings.

In this lab, your task is to:

- Create a WLAN using the following settings:

    - Name: **CorpNet Wireless**
    - ESSID: **CorpNet**
    - Type: **Standard Usage**
    - Authentication: **Open**
    - Encryption: **WPA2**
    - Encryption algorithm: **AES**
    - Passphrase: **@CorpNetWeRSecure!**
- Connect the Exec-Laptop in the Executive office to the new wireless network.




Ruckus WIRELESS
ZoneDirector - CorpNet
Dashboard
Monitor
Configure
Administer
System
WLANs
Access Points
Access Control
Maps
Roles
Users
Guest Access
Hotspot Services
Hotspot 2.0 Services
Mesh
AAA Servers
DHCP Relay
Alarm Settings
Services
WIPS
Certificate
Bonjour Gateway
WLANs
WLANs
This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make changes to an existing WLAN.
Name ESSID Description Authentication Encryption Actions
Create New
Delete 0-0 (0)
Search Terms
Include all terms
Include any of these terms
WLAN Groups
This table lists your current WLAN groups and provides basic details about them. Click Create New to add another WLAN group, or click Edit to make changes to an existing WLAN group.
Name Description Actions
Default Default WLANs for Access Points Edit Clon
Create New
Delete 0-0 (0)
Search Terms
Include all terms
Include any of these terms
VLAN Pooling
This table lists your current VLAN pools and provides basic details about them. Click Create New to add another VLAN pool, or click Edit to make changes to an existing VLAN pool.
Name Description Actions
Create New
Delete 0-0 (0)
Search Terms
Include all terms
Include any of these terms
Zero-IT Activation
Zero-IT Activation simplifies the configuration of users' wireless settings. Ask users to connect their wireless devices to either wired network or dedicated activation WLAN/SSID , and then have them go to the Activation URL shown below. After they download and run the Zero-IT Activation application, their wireless devices will be configured automatically for WLANs that support Zero-IT Activation.
Activation URL: http://your.location.com/activate
Authentication Server: Local Database
Apply

WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click Create New to add another WLAN, or click Edit to make ch

Name	ESSID	Description	Authentication	Encryption	Actions

Create New

General Options

Name/ESSID*	CorpNet Wireless ESSID CorpNet
Description	

WLAN Usages

Type	(●) Standard Usage (For most regular wireless network usages.) ( ) Guest Access (Guest access policies and access control will be applied.) ( ) Hotspot Service (WISPr) ( ) Hotspot 2.0 ( ) Autonomous

Authentication Options

Method	(●) Open ( ) 802.1x EAP ( ) MAC Address ( ) 802.1x EAP + MAC Address
Fast BSS Transition	[ ] Enable 802.11r FT Roaming (Recommended to enable 802.11k Neighbor-list Report for assistant.)

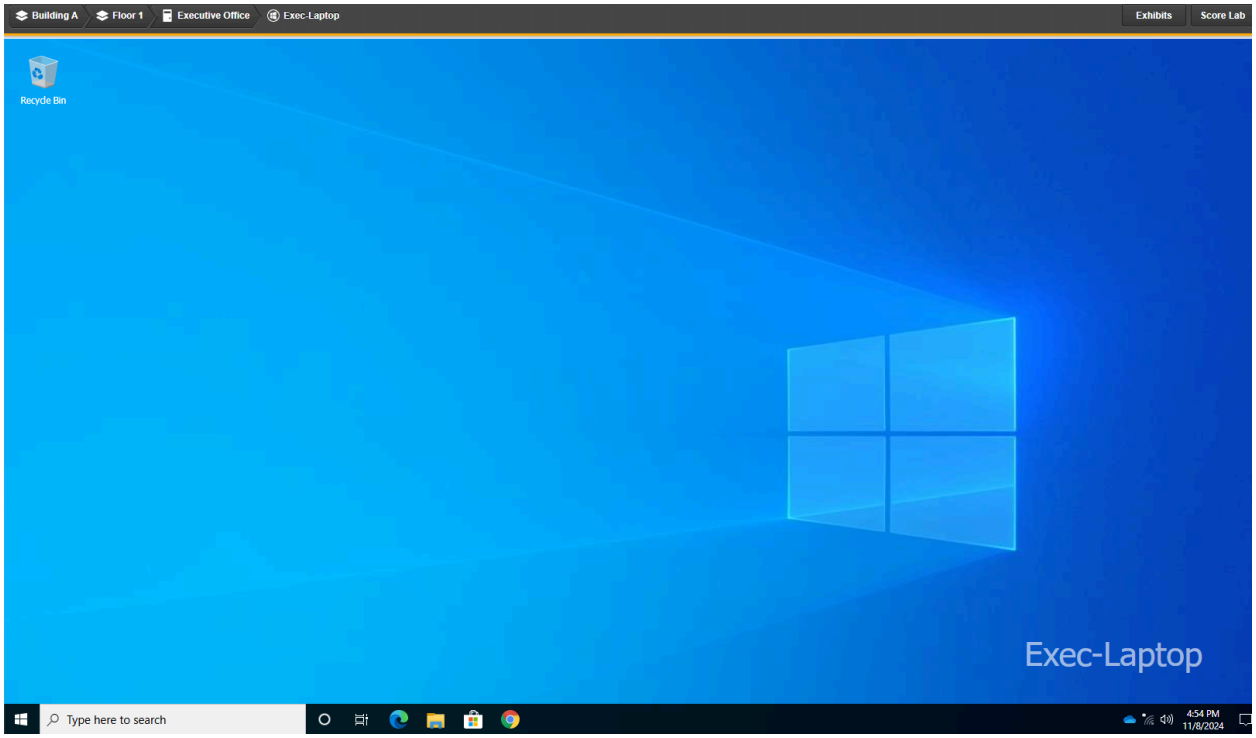
Encryption Options

Method	(●) WPA2 ( ) WPA-Mixed ( ) WEP-64 (40 bit) ( ) WEP-128 (104 bit) ( ) None
Algorithm	(●) AES ( ) Auto (TKIP+AES)
Passphrase*	@CorpNetWeRSecure!

Options

Web Authentication	[ ] Enable captive portal/Web authentication (Users will be redirected to a Web portal for authentication before they can access the WLAN.)
Authentication Server	Local Database ▼
Wireless Client Isolation	[ ] Isolate wireless client traffic from other clients on the same AP. [ ] Isolate wireless client traffic from all hosts on the same VLAN/subnet. No WhiteList ▼ (Requires whitelist for gateway and other allowed hosts.)
Zero-IT Activation	[ ] Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.)
Priority	( ) High (●) Low

⊞ Advanced Options



Lab Report

Time Spent: 05:00

Score: 2/2 (100%)

TASK SUMMARY

Required Actions

- ✓ Create the CorpNet WLAN Show Details
- ✓ Connect Exec-Laptop to the CorpNet Wireless network

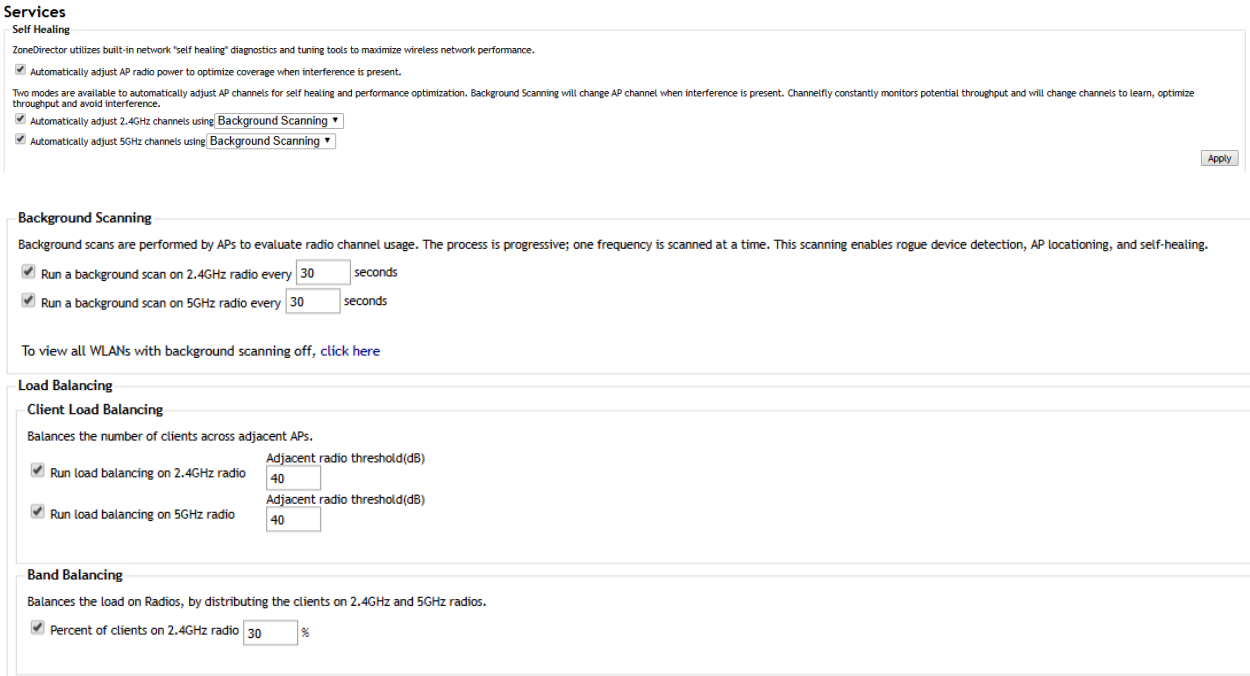
END Lab

Ruckus Wireless lab Configure Rogue Host Protection

You are a network technician for a small corporate network. You want to take advantage of the self-healing features provided by the small enterprise wireless solution you've implemented. You're already logged in as WxAdmin on the Wireless Controller console from ITAdmin.

In this lab, your task is to:

- Configure self-healing on the wireless network.
    - Automatically adjust AP radio power to optimize coverage when interference is present.
    - Set 2.4 GHz and 5 GHz radio channels to use the **Background Scanning** method to adjust for interference.
- Configure the background scanning needed for rogue device detection, AP locationing, and self-healing. Background scans should be performed on all radios every **30 seconds**.
- Configure load balancing for all radios by adjusting the threshold to **40 dB**.
- Configure band balancing to allow no more than **30%** of clients to use the 2.4 GHz radios.
- Reduce the power levels to **-3 dB** for three access points in Building A to reduce RF emanations. Use the wireless survey results in the exhibit to identify the access points.



Radio B/G/N(2.4G)	
Channelization	☐ Override Group Config Auto ▼
Channel	☐ Override Group Config Auto ▼
TX Power	☑ Override Group Config -3dB(1/2) ▼
WLAN Group	☐ Override Group Config Default ▼
Call Admission Control	☐ Override Group Config OFF ▼
SpectraLink Compatibility	☐ Override Group Config Disable ▼
WLAN Service	☑ Enable WLAN service for this radio.
Radio A/N/AC(5G)	
Channelization	☐ Override Group Config Auto ▼
Channel	☐ Override Group Config Auto ▼
TX Power	☑ Override Group Config -3dB(1/2) ▼
WLAN Group	☐ Override Group Config Default ▼
Call Admission Control	☐ Override Group Config OFF ▼
SpectraLink Compatibility	☐ Override Group Config Disable ▼
WLAN Service	☑ Enable WLAN service for this radio.

Lab Report

Time Spent: 08:19

Score: 5/5 (100%)

END Lab

Ruckus wireless Harden a wireless network

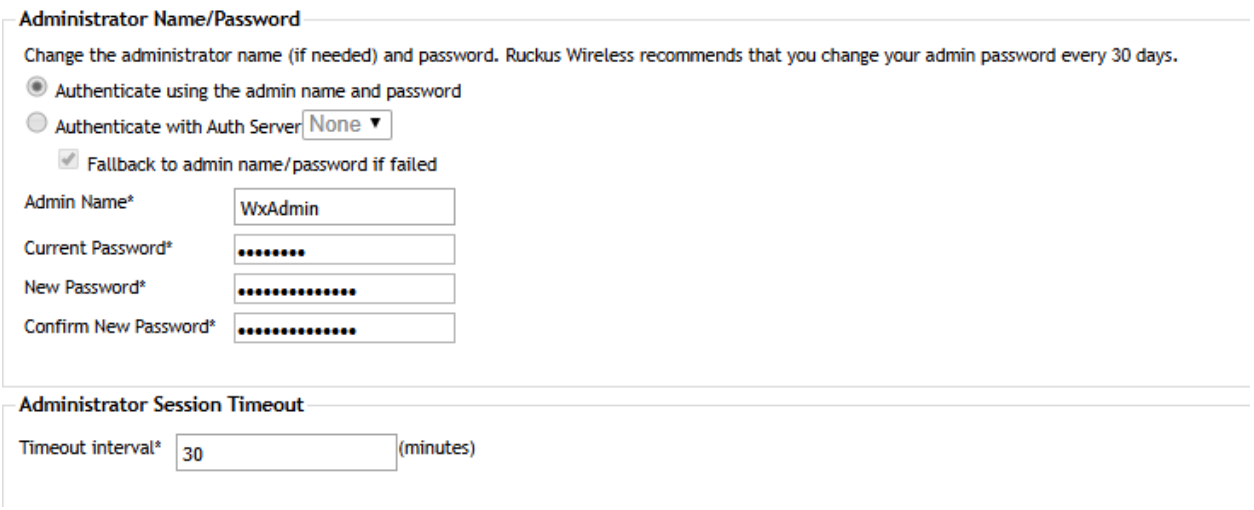
You are a network technician for a small corporate network. You need to increase the security of your wireless network. Your new wireless controller provides several security features that you want to implement.

In this lab, your task is to:

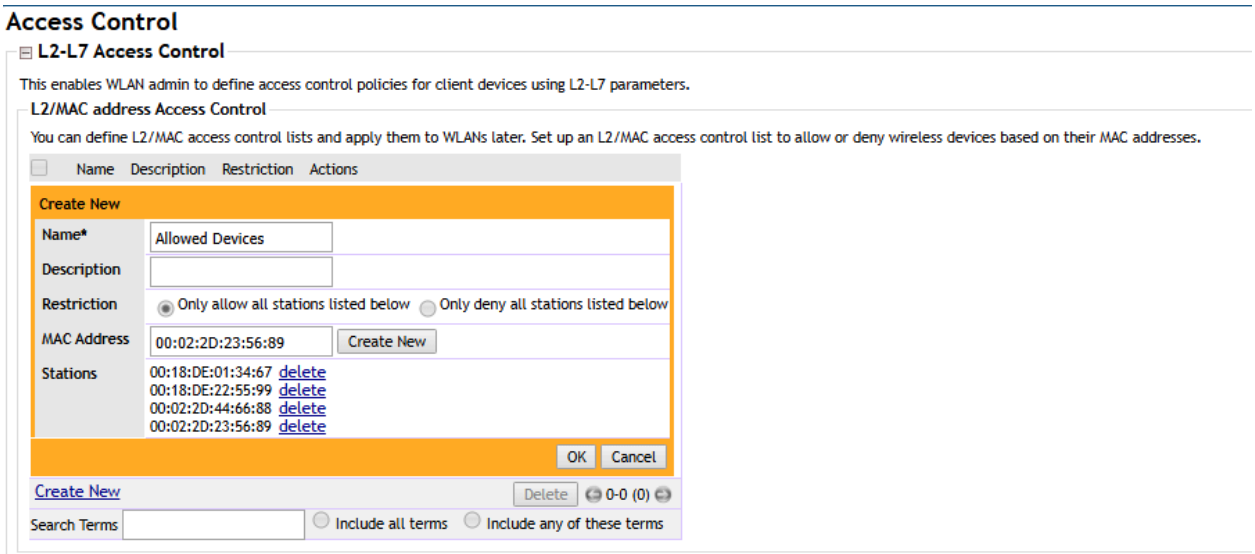
- Change the admin username and password for the Zone Director controller to the following:
    - Admin Name: **WxAdmin**
    - Password: **ZDAdminsOnly!$** (O is the capital letter O)

- Set up MAC address filtering (L2 Access Control) to create an allow list called **Allowed Devices** that includes the following wireless devices:
    - **00:18:DE:01:34:67**
    - **00:18:DE:22:55:99**
    - **00:02:2D:23:56:89**
    - **00:02:2D:44:66:88**
- Implement a device access policy called **NoGames** that blocks gaming consoles from the wireless network.

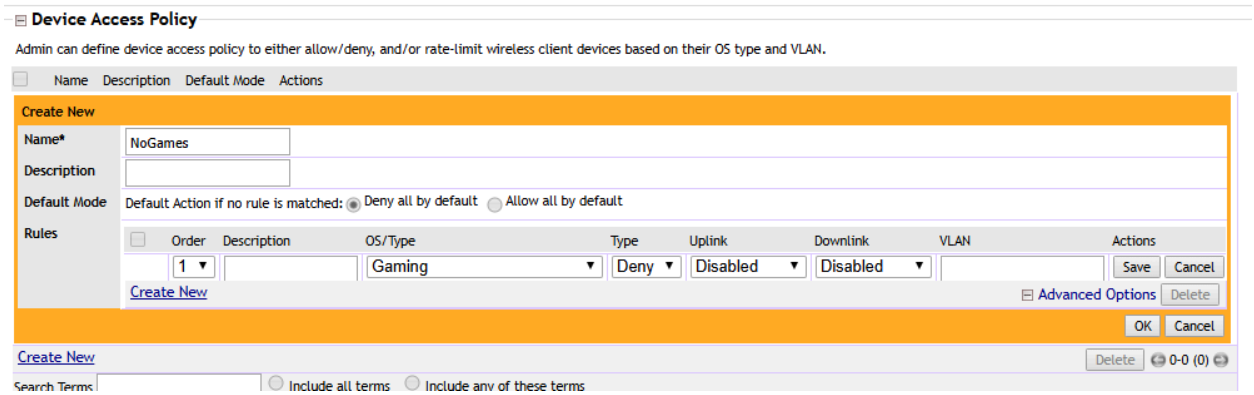
Changing administrative name and password



Creating access control list based on MAC addresses.



Create a device access policy called NoGames to block gaming on the wireless network.



END Lab

Ruckus Wireless Configure WIPS

You are a network technician for a small corporate network. You would like to enable Wireless Intrusion Prevention on the wireless controller. You are already logged in as WxAdmin.

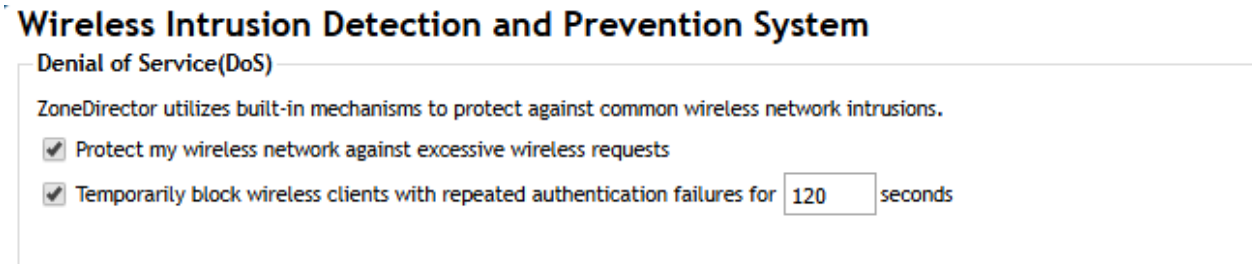
In this lab, your task is to:

- Configure the wireless controller to protect against denial-of-service (DOS) attacks as follows:
    - Protect against excessive wireless requests.
    - Block clients with repeated authentication failures for two minutes (120 seconds).
- Configure Intrusion Detection and Prevention as follows:
    - Report all rogue devices regardless of type.

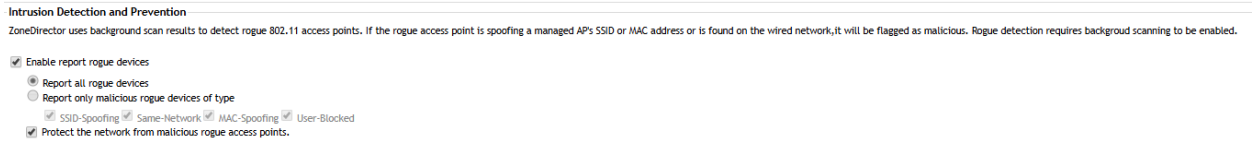
    - Protect the network from rogue access points.

- Enable **Rogue DHCP Server Detection**.

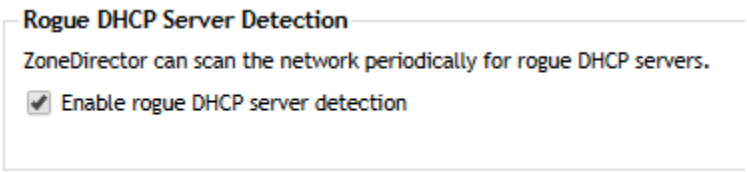
Protect against DOS attacks



Configure Intrusion Detection and Prevention



Enable Rogue DHCP server detection



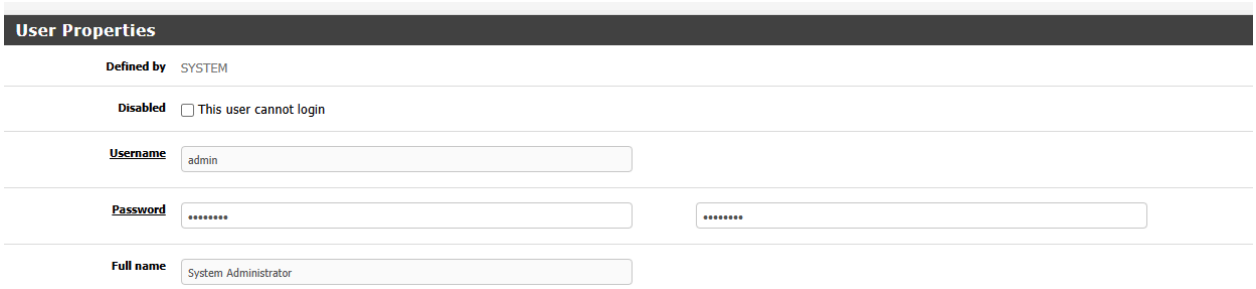
LAB Secure access to pfSense Appliance

You work as the IT security administrator for a small corporate network. You need to secure access to your pfSense appliance, which is still configured with the default user settings.

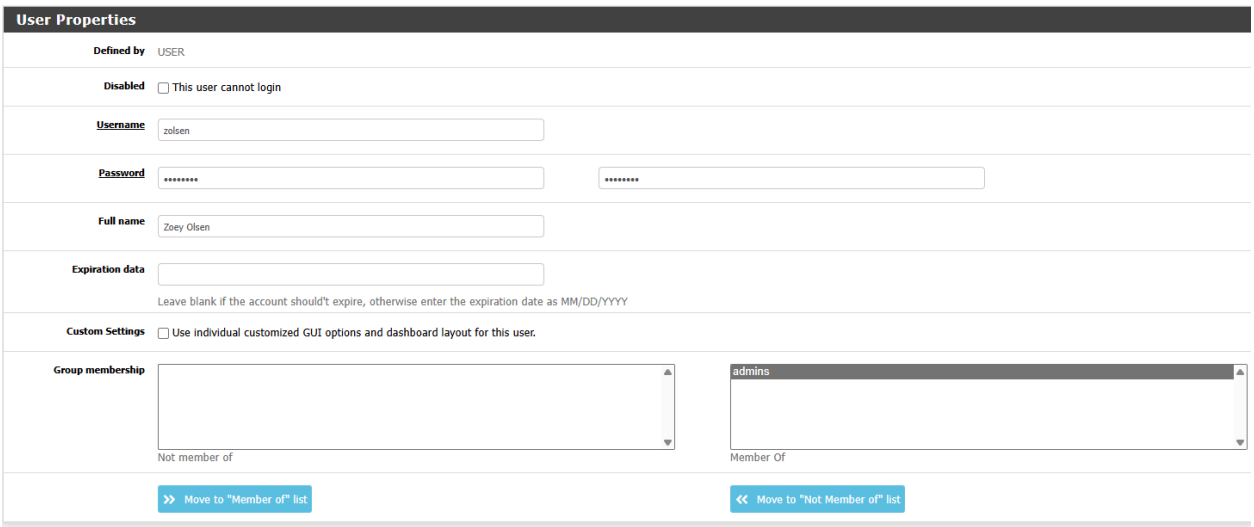
In this lab, your task is to:

- Change the password for the default pfSense account from P@ssw0rd to **1w0rm4b8.**
- Create a new administrative user with the following parameters:
    - Username: **zolsen**
    - Password: **St@yout!**
    - Full Name: **Zoey Olsen**
    - Group Membership: **admins**
- Set a session timeout of **15** minutes for pfSense.
- Disable the webConfigurator anti-lockout rule for HTTP.

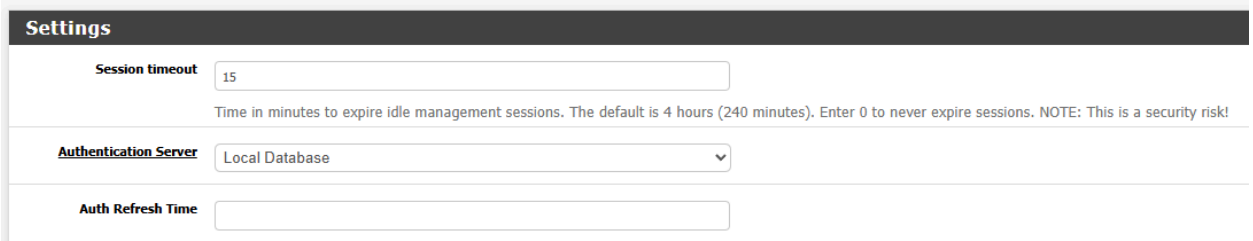
Changing admin password:



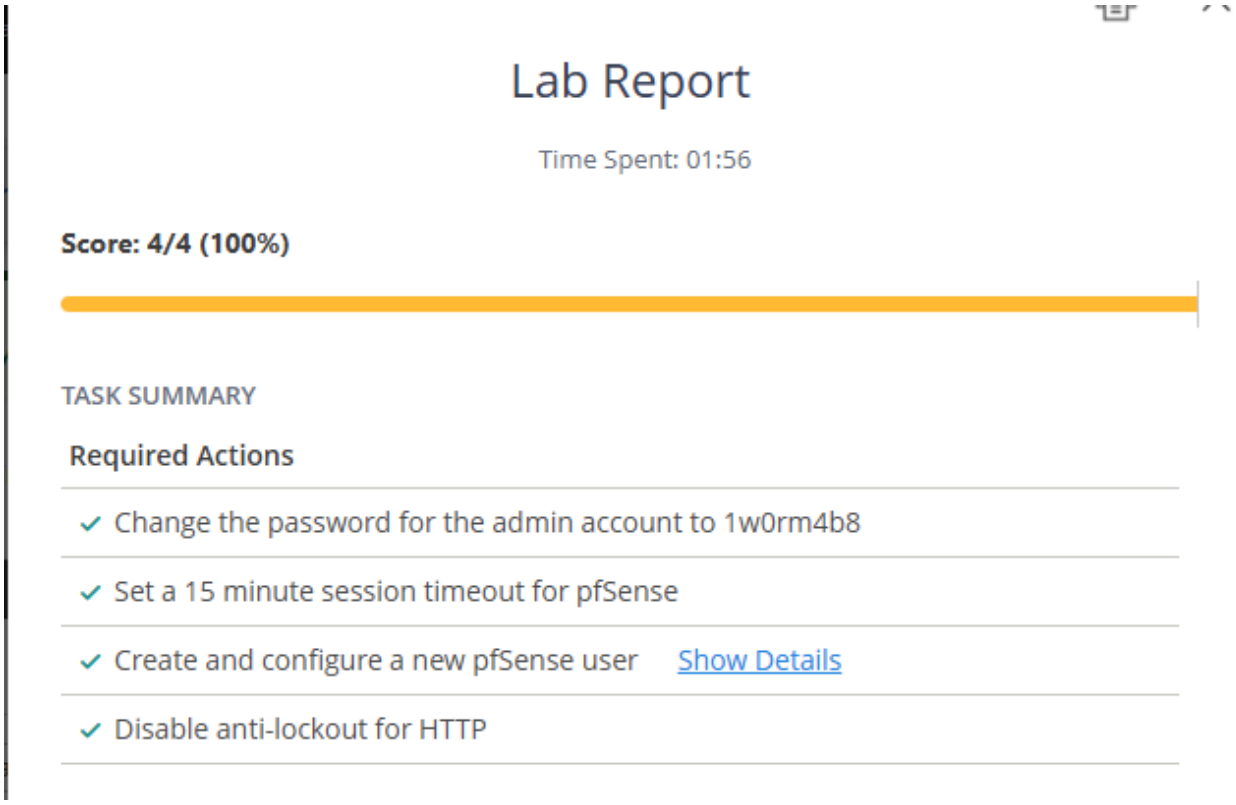
Creating a new user with the provided parameters:



Set session timeout for 15 minutes:



Disable webConfigurator anti-lockout rule for HTTP:



END LAB

LAB Configure a screened subnet

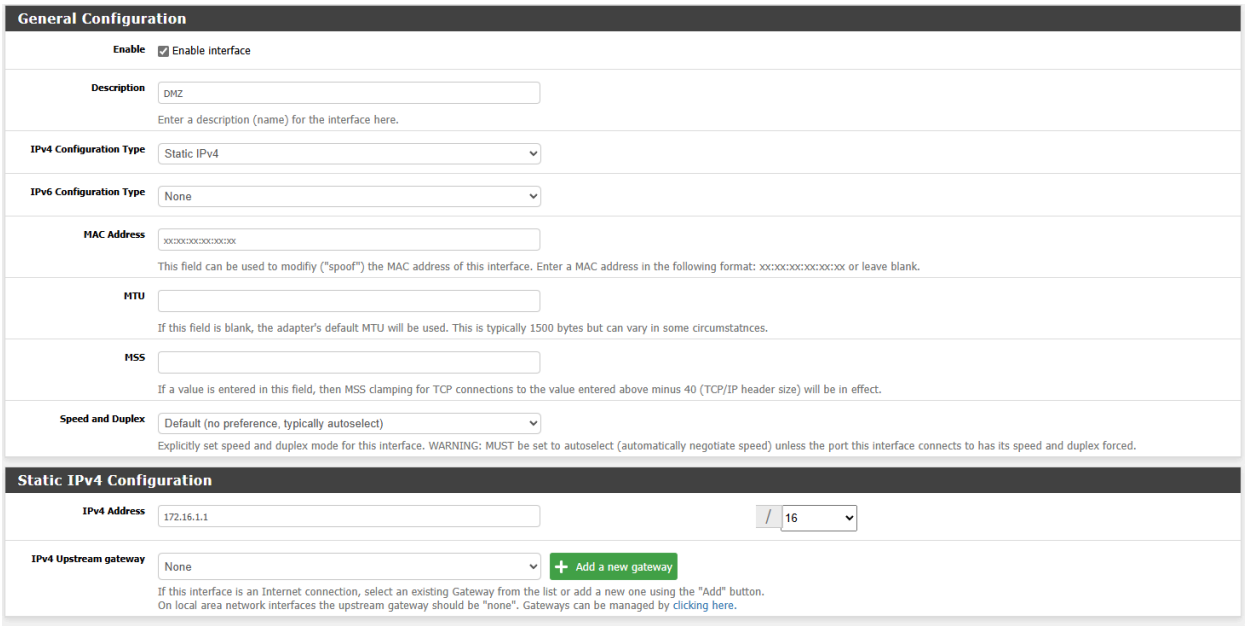
You are the IT administrator for a small corporate network. You want to make a web server that runs services accessible from the internet. To help protect your company, you want to place this server and other devices in a demilitarized zone (DMZ). This

DMZ and server need to be protected by the pfSense Security Gateway Appliance (pfSense). Since a few of the other devices in the DMZ require an IP address, you have also decided to enable DHCP on the DMZ network.

In this lab, your task is to perform the following:

- Access the pfSense management console:
  - Username: **admin**
  - Password: **P@ssw0rd** (zero)
- Add a new pfSense interface that can be used for the DMZ.
  - Name the interface **DMZ**.
  - Use a static IPv4 address of **172.16.1.1/16**.
- Add a firewall rule for the DMZ interface that allows all traffic from the DMZ.
  - Use a description of **Allow DMZ to any rule**.
- Configure and enable the DHCP server for the DMZ interface.
  - Use a range of **172.16.1.100** to **172.16.1.200**.

Add a new pfSense interface to be used for the DMZ



Add a firewall rule for the DMZ interface:

Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface DMZ

Choose the interface from which packets must come to match this rule

Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol Any

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match DMZ net Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match any Destination Address /

Extra Options

Log

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description Allow DMZ to any rule

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Configure and enable the DHCP server for the DMZ interface:

General Options

Enable ☑ Enable DHCP server on DMZ interface

BOOTP ☐ Ignore BOOTP queries

Deny unknown clients ☐ Only the clients defined below will get DHCP leases from this server.

Ignore denied clients ☐ Denied clients will be ignored rather than rejected.

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers ☐ If a client includes a unique identifier of its DHCP request, that UID will not be recorded in its lease.

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 172.16.0.0

Subnet Mask 255.255.0.0

Available range 172.16.1.1 - 172.16.1.254

Range 172.16.1.100 (From) 172.16.1.200 (To)

Lab Report

Time Spent: 18:56

Score: 3/3 (100%)

TASK SUMMARY

Required Actions

- ✓ Configure an interface for the DMZ Show Details
- ✓ Add a firewall rule to the DMZ interface
- ✓ Configure pfSense's DHCP server for the DMZ interface Show Details

END LAB

LAB Configuring a perimeter firewall

LAN network to the DMZ network.

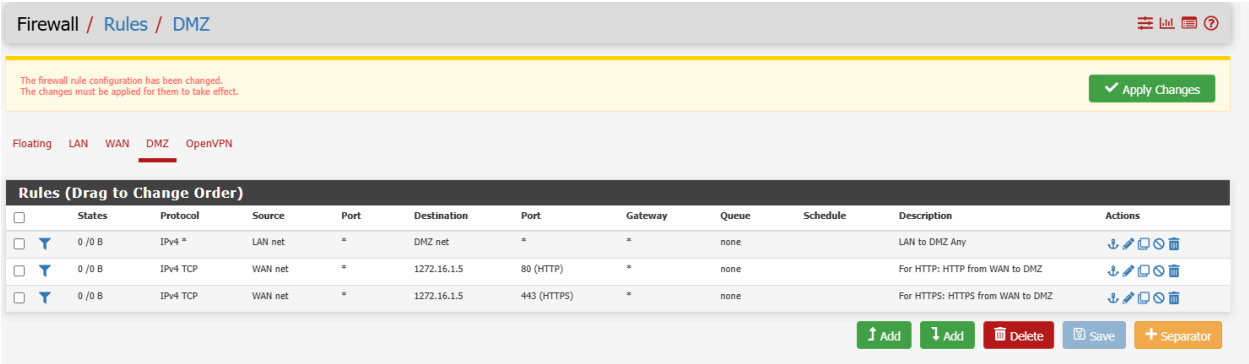
In this lab, your task is to:

- Access the pfSense management console:
  - Username: **admin**
  - Password: **P@ssw0rd** (zero)
- Create and configure a firewall rule to pass HTTP traffic from the WAN to the Web server in the DMZ.
- Create and configure a firewall rule to pass HTTPS traffic from the WAN to the Web server in the DMZ.
  - Use the following table when creating the HTTP and HTTPS firewall rules:

Parameter	Setting
Source	WAN network

Destination port/service	HTTP (80), HTTPS (443)
Destination	A single host
IP address for host	172.16.1.5
Descriptions	For HTTP: HTTP from WAN to DMZ For HTTPS: HTTPS from WAN to DMZ

- Create and configure a firewall rule to pass all traffic from the LAN network to the DMZ network. Use the description *LAN to DMZ Any*.



Lab Report

Time Spent: 02:52

Score: 3/3 (100%)

TASK SUMMARY

Required Actions

✓ Create and configure a firewall rule to pass HTTP traffic from the internet to the Web server Show Details

✓ Create and configure a firewall rule to pass HTTPS traffic from the internet to the Web server Show Details

✓ Create and configure a firewall rule to pass all traffic from the LAN network to the DMZ network Show Details

END Lab

LAB Configure a remote access VPN

You work as the IT security administrator for a small corporate network. Occasionally, you and your co-administrators need to access internal resources when you are away from the office. You would like to set up a Remote Access VPN using pfSense to allow secure access.

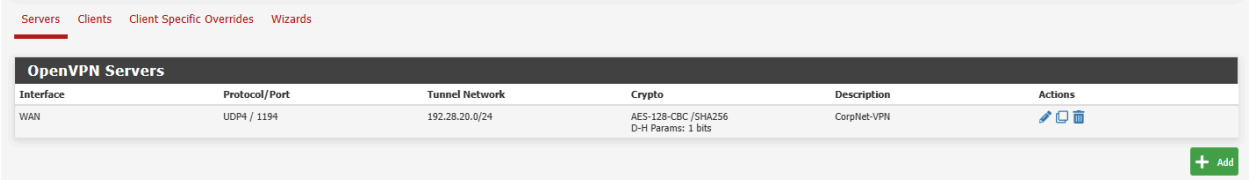
In this lab, your task is to use the pfSense wizard to create and configure an OpenVPN Remote Access server using the following guidelines:

- Sign in to pfSense using:
  - Username: admin
  - Password: P@ssw0rd (zero)
- Create a new certificate authority certificate using the following settings:
  - Name: **CorpNet-CA**
  - Country Code: **GB**
  - State: **Cambridgeshire**

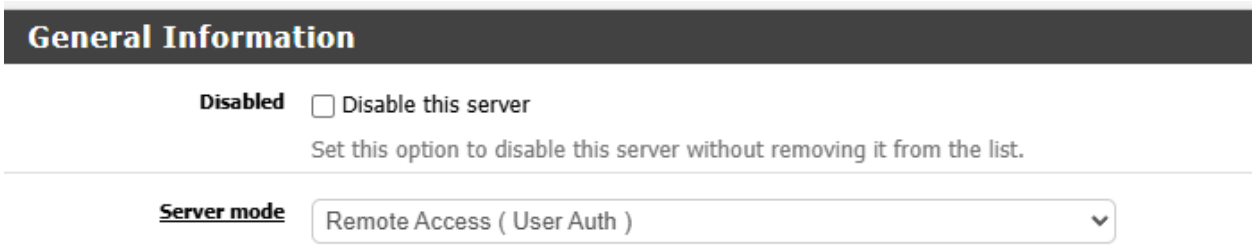
    - City: **Woodwalton**
    - Organization: **CorpNet**
- Create a new server certificate using the following settings:
    - Name: **CorpNet**
    - Country Code: **GB**
    - State: **Cambridgeshire**
    - City: **Woodwalton**
- Configure the VPN server using the following settings:
    - Interface: **WAN**
    - Protocol: **UDP on IPv4 only**
    - Description: **CorpNet-VPN**
    - Tunnel network IP: **198.28.20.0/24**
    - Local network IP: **198.28.56.18/24**
    - Concurrent Connections: **4**
    - DNS Server 1: **198.28.56.1**
- Configure the following:
    - A firewall rule
    - An OpenVPN rule
- Set the OpenVPN server just created to **Remote Access (User Auth)**.
- Create and configure the following standard remote VPN users:
-

Username	Password	Full Name
blindley	L3tM31nNow	Brian Lindley
jphillips	L3tM31nToo	Jacob Phillips

Create the certificate authority certificate, create a new server certificate, and configure the VPN server:



Set the OpenVPN server to Remote Access (User auth):



Create standard remote VPN users:

Lab Report

Time Spent: 02:40

Score: 6/6 (100%)

TASK SUMMARY

Required Actions

- ✓ Create a new certificate authority certificate Show Details
- ✓ Create a new server certificate named CorpNet
- ✓ Configure the VPN server Show Details
- ✓ Configure the firewall rules Show Details
- ✓ Set the OpenVPN server to Remote Access (User Auth)
- ✓ Configure the following standard VPN users Show Details

End LAB

LAB Configure a VPN connection on an Ipad

You work as the IT security administrator for a small corporate network. You recently set up the Remote Access VPN feature on your network security appliance to provide you and your fellow administrators with secure access to your network. You are currently at home and would like to connect your iPad to the VPN. Your iPad is connected to your home wireless network.

In this lab, your task is to:

- Add an IPSec VPN connection using the following values:

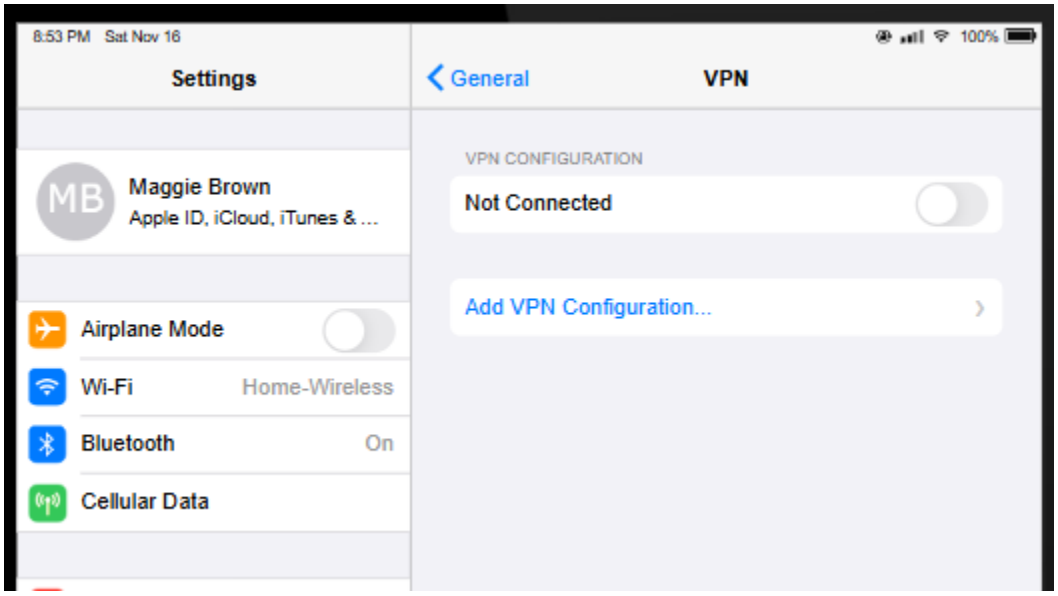
This can be added by selecting **Settings** > **General** > **VPN**.

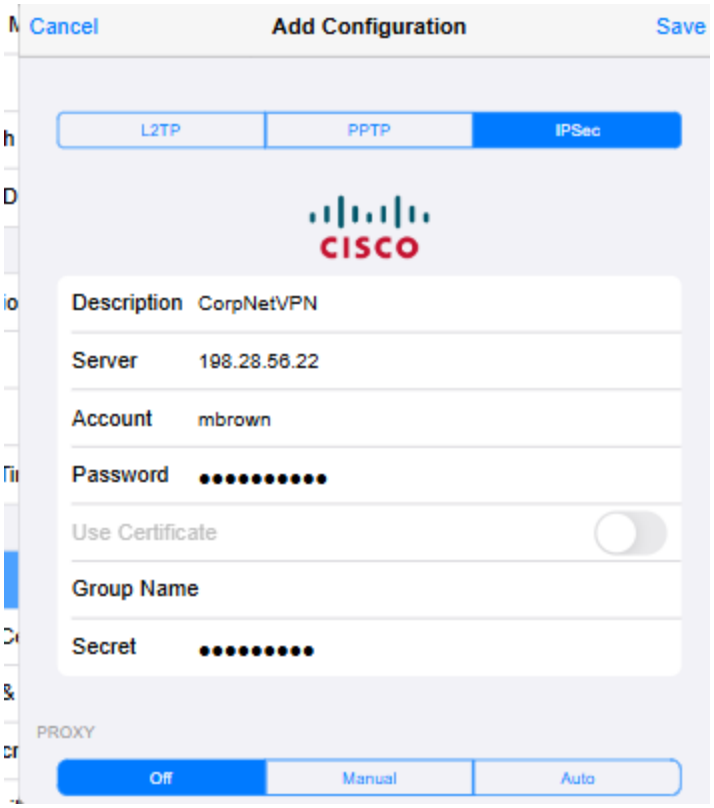
Parameter	Value

Description	**CorpNetVPN**
Server	**198.28.56.22**
Account	**mbrown**
Secret	**asdf1234$**

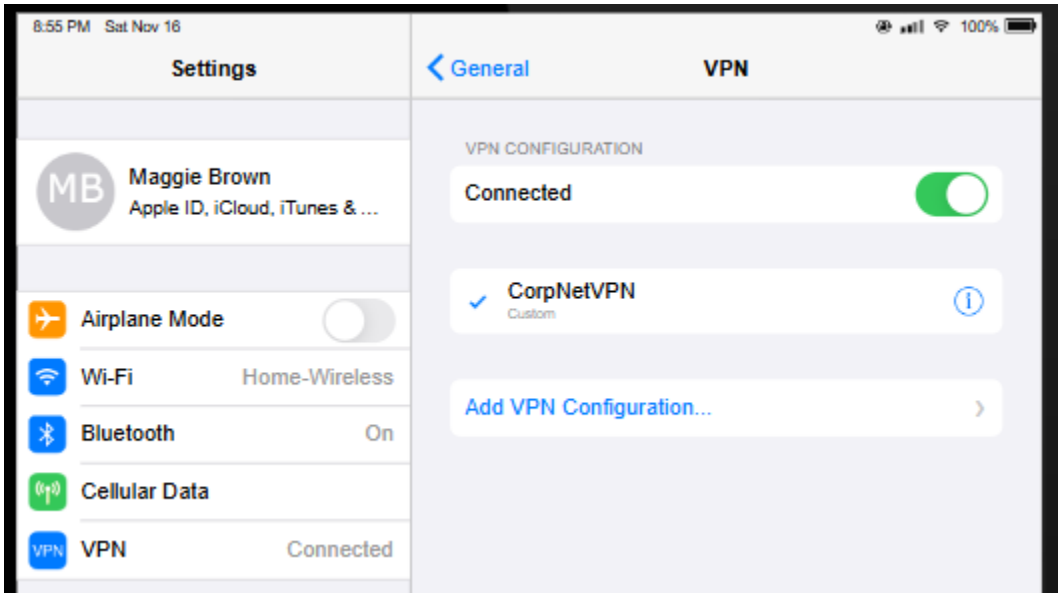
- Turn on the VPN.
- Verify that a connection is established. The password for mbrown is **L3tM31nN0w** (0 = zero).

Add IPSec VPN connection:




Cancel
Add Configuration
Save
L2TP
PPTP
IPSec
CISCO
Description CorpNetVPN
Server 198.28.56.22
Account mbrown
Password ●●●●●●●●●●
Use Certificate
Group Name
Secret ●●●●●●●●●
PROXY
Off
Manual
Auto

Success!


8:55 PM Sat Nov 16
100%
Settings
General
VPN
MB
Maggie Brown
Apple ID, iCloud, iTunes & ...
Airplane Mode
Wi-Fi Home-Wireless
Bluetooth On
Cellular Data
VPN Connected
VPN CONFIGURATION
Connected
CorpNetVPN
Custom
Add VPN Configuration...

Lab Report

Time Spent: 02:50

Score: 2/2 (100%)

TASK SUMMARY

Required Actions

✓ Add an IPSec VPN connection Show Details

✓ Turn on VPN and connect

END LAB

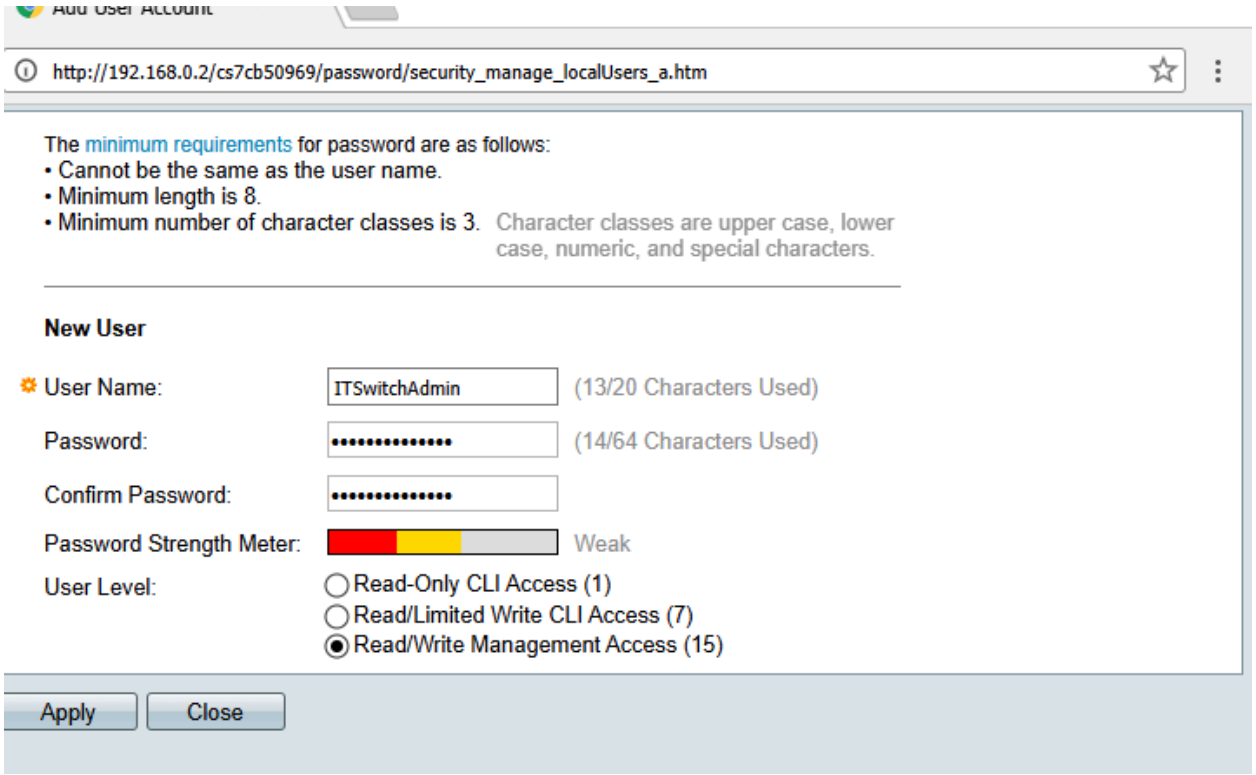
LAB Secure a switch

You are the IT security administrator for a small corporate network. You need to secure access to your switch, which is still configured with the default settings.

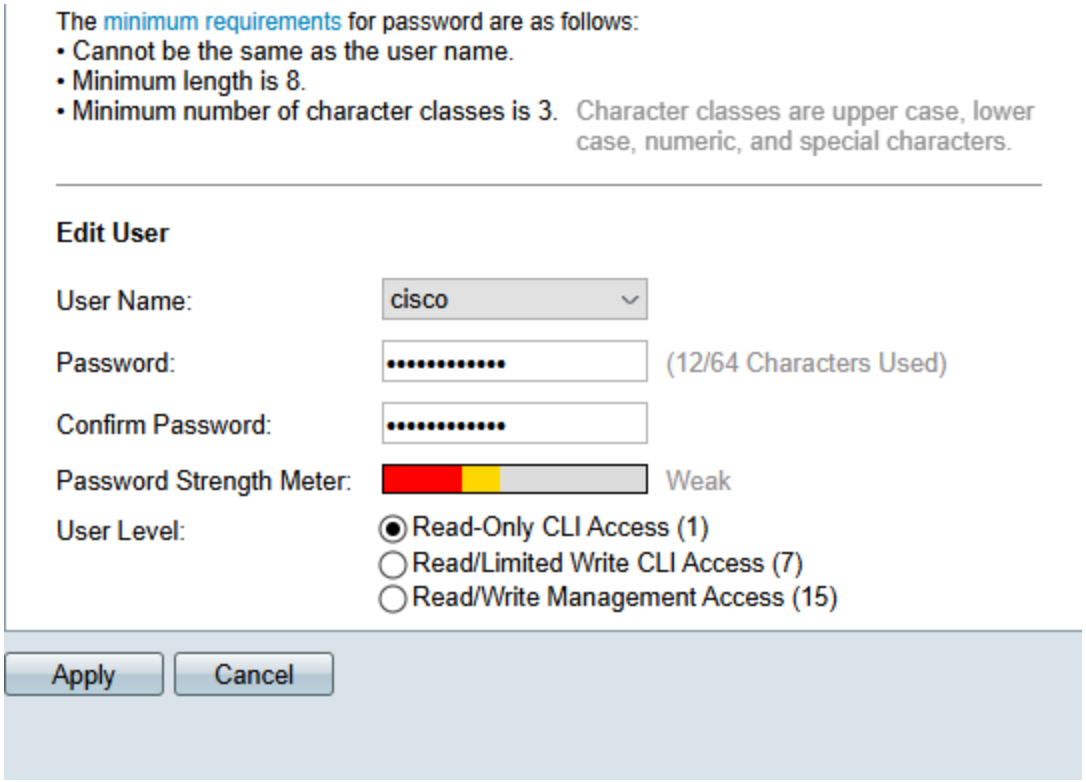
Access the switch management console through Chrome on **http://192.168.0.2** with the username **cisco** and password **cisco**.

In this lab, your task is to:

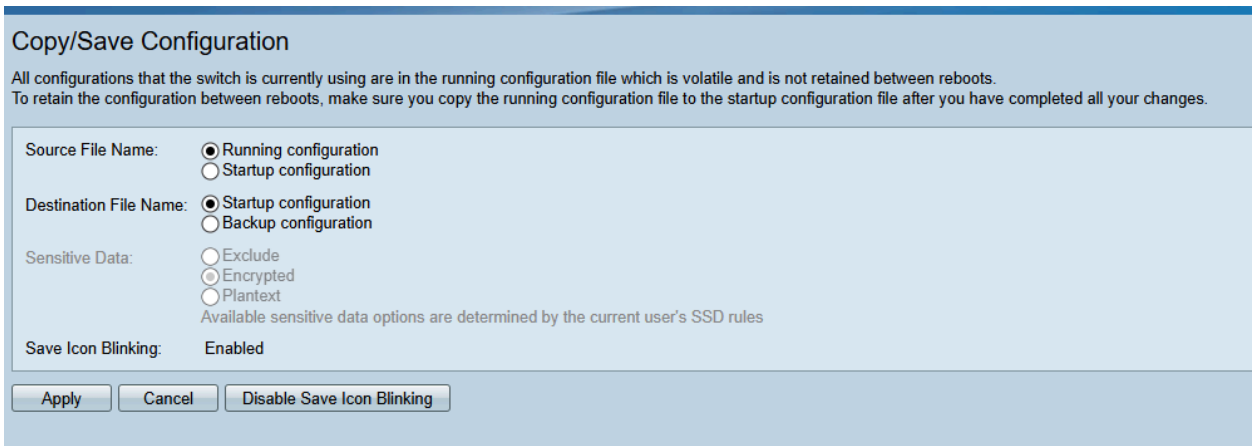
- Create a new user account with the following settings:
  - Username: **ITSwitchAdmin**
  - Password: **Admin$only1844**
  - User Level: **Read/Write Management Access (15)**
- Edit the default user account as follows:
  - Username: **cisco**
  - Password: **CLI$only1958**
  - User Level: **Read-Only CLI Access (1)**
- Save the changes to the switch's startup configuration file.



Edit the default user account:



Save configuration:



Lab Report

Time Spent: 03:12

Score: 3/3 (100%)

TASK SUMMARY

Required Actions

- ✓ Create a new user account Show Details
- ✓ Edit the default user account Show Details
- ✓ Save the changes to the switch's startup configuration file

END LAB

LAB Harden a switch

You are the IT security administrator for a small corporate network. You need to increase the security on the switch in the networking closet.

The following table lists the used and unused ports:

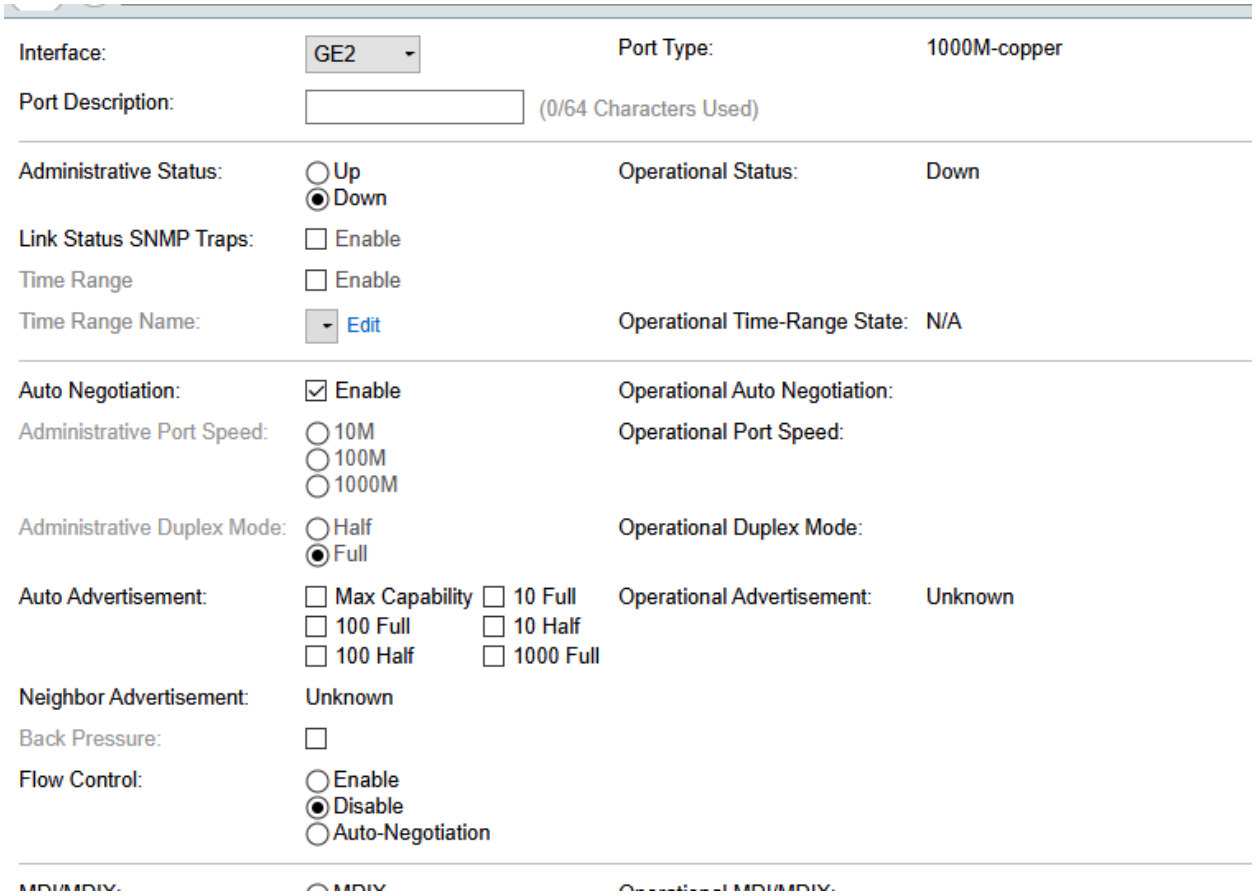
Unused Ports	Used Ports
GE2 GE7 GE9-GE20 GE25 GE27-GE28	GE1 GE3-GE6 GE8 GE21-GE24 GE26

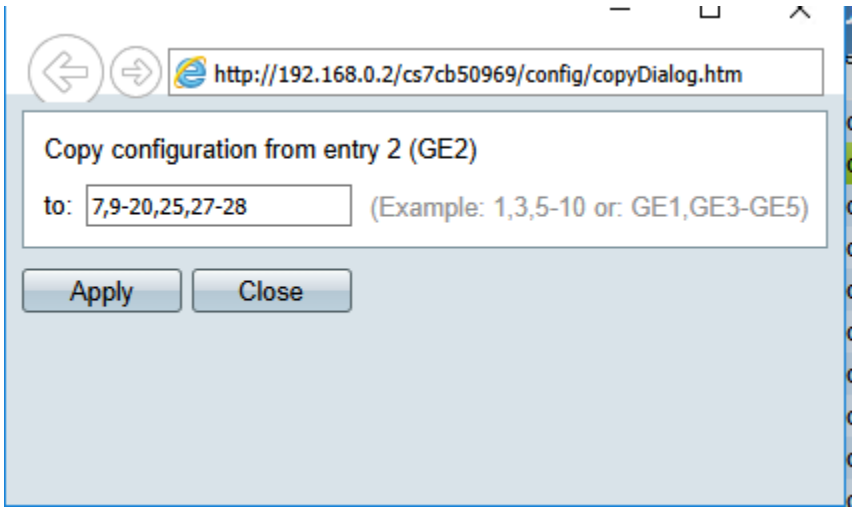
In this lab, your task is to:

- Shut down the unused ports.
- Configure the following Port Security settings for the used ports:

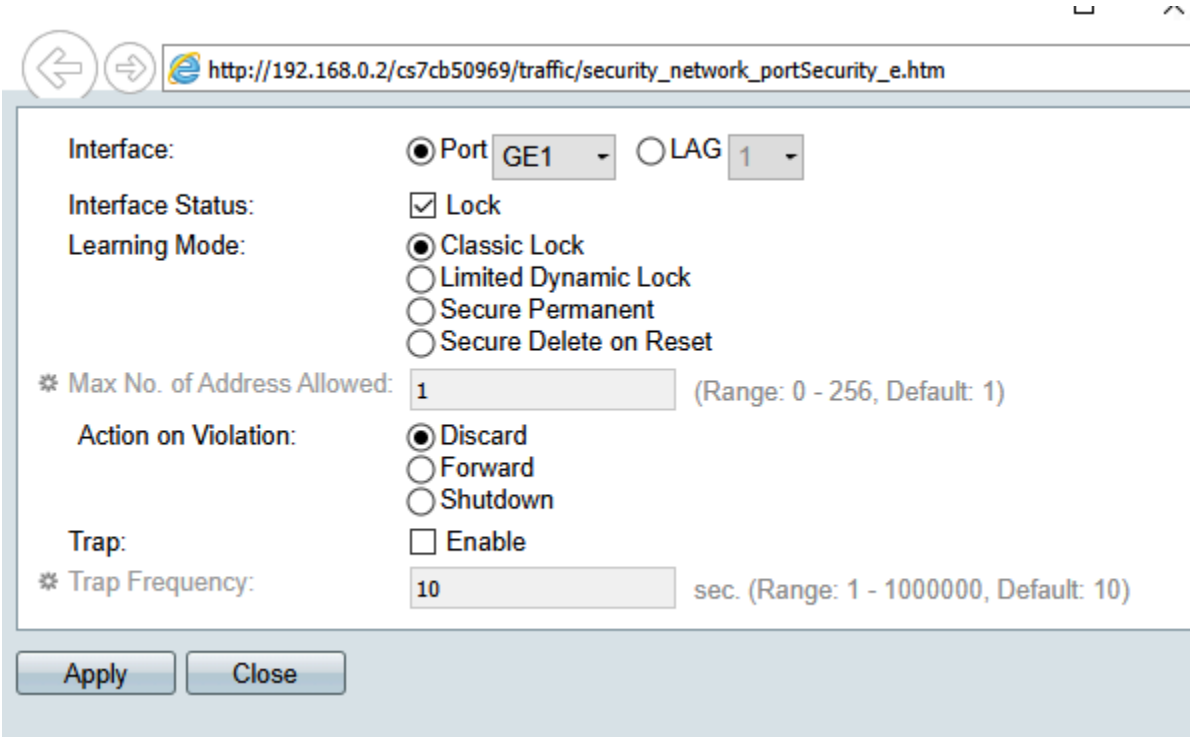
- Interface Status: **Lock**
- Learning Mode: **Classic Lock**
- Action on Violation: **Discard**

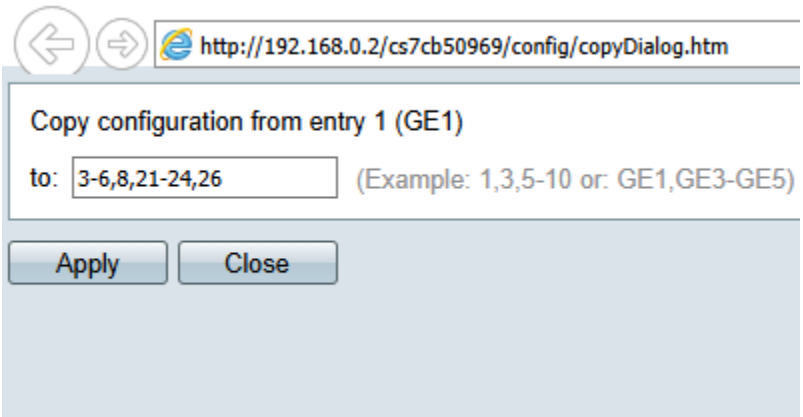
Shut down unused ports:





Configure Port Security for the used ports:





Lab Report

Time Spent: 05:08

Score: 2/2 (100%)

TASK SUMMARY

Required Actions

✓ Disable the unused ports Show Details

✓ Configure Port Security settings for the used ports Show Details

END LAB

LAB Secure access to a switch

You are the IT security administrator for a small corporate network. You need to increase the security on the switch in the Networking Closet by restricting access management.

In this lab, your task is to:

- Create an access profile named *MgtAccess* and configure it with the following settings:

Setting	Value
Access Profile Name	MgtAccess
Rule Priority	1
Management Method	All
Action	Deny
Applies to Interface	All

Applies to Source IP address	All

- Add a profile rule to the *MgtAccess* profile with the following settings:

Setting	**Value**
Rule Priority	2
Management Method	HTTP
Action	Permit
Applies to interface	All
Applies to Source IP address	User defined IP Version: Version 4 IP Address: 192.168.0.10 Network Mask: 255.255.255.0

- Set the *MgtAccess* profile as the active access profile.
- Save the changes to the switch's startup configuration file using the default settings.

Create an Access Profile named MgtAccess:

Access Profile Name: MgtAccess (9/32 Characters Used)

Rule Priority: 1 (Range: 1 - 65535)

Management Method:
- (●) All
- ( ) Telnet
- ( ) Secure Telnet (SSH)
- ( ) HTTP
- ( ) Secure HTTP (HTTPS)
- ( ) SNMP

Action:
- ( ) Permit
- (●) Deny

Applies to Interface: (●) All ( ) User Defined

Interface: (●) Port GE1 ( ) LAG 1 ( ) VLAN 1

Applies to Source IP Address: (●) All ( ) User Defined

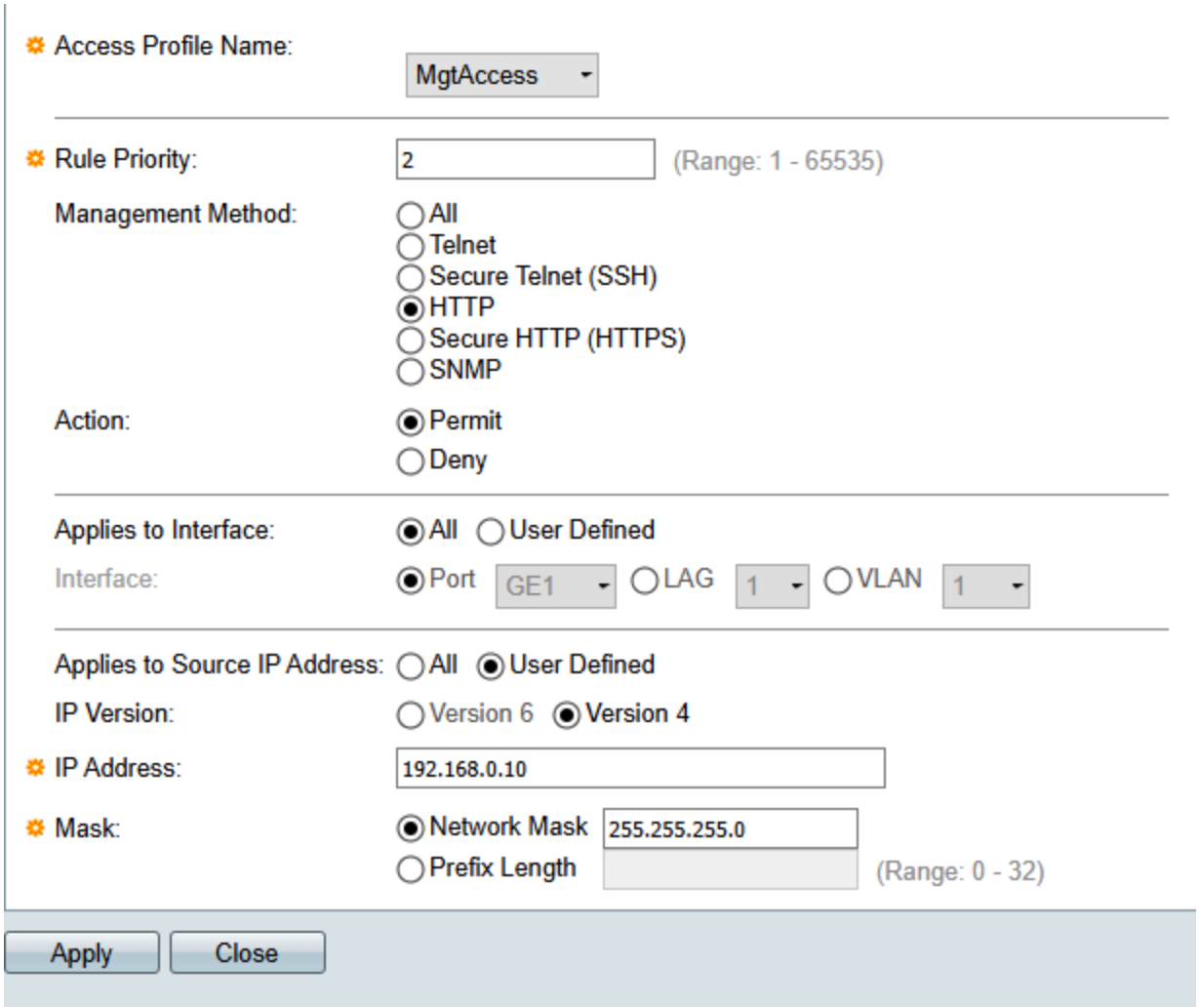
IP Version: ( ) Version 6 (●) Version 4

IP Address:

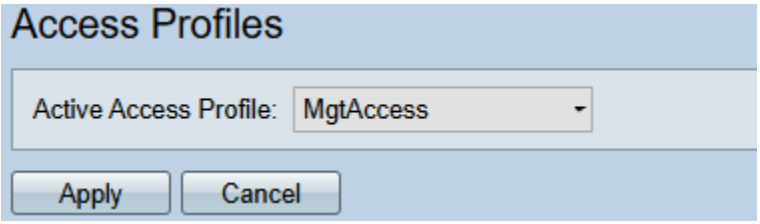
Mask:
- (●) Network Mask
- ( ) Prefix Length (Range: 0 - 32)

Apply Close

Add a profile rule to the MgtAccess profile:



Set the MgtAccess profile as the active access profile:



Lab Report

Time Spent: 04:36

Score: 4/4 (100%)

TASK SUMMARY

Required Actions

- ✓ Create an access profile to restrict management access Show Details
- ✓ Add a profile rule
- ✓ Set the active access profile
- ✓ Save changes to the startup configuration

END LAB

LAB Secure access to a switch 2

You are the IT security administrator for a small corporate network. You need to increase the security on the switch in the Networking Closet by creating an access control list. You have been asked to prevent video game consoles from connecting to the switch.

In this lab, your task is to:

- Create a MAC-based ACL named **GameConsoles**.
- Configure the **GameConsoles** MAC-based access control entry (ACE) settings as follows:

Priority	Action	Destination MAC Address	Source MAC Address
1	Deny	Any	Value: **00041F111111** Mask: **000000111111**

2	Deny	Any	Value: **005042111111** Mask: **000000111111**
3	Deny	Any	Value: **000D3A111111** Mask: **000000111111**
4	Deny	Any	Value: **001315111111** Mask: **000000111111**
5	Deny	Any	Value: **0009BF111111** Mask: **000000111111**
6	Deny	Any	Value: **00125A111111** Mask: **000000111111**

- Bind the **GameConsoles** ACL to all of the **GE1-GE30** interfaces.

Use **Copy Settings** to apply the binding to multiple interfaces.

Configure access control entries:

ACL Name:	GameConsoles	
Priority:	1	(Range: 1 - 2147483647)
Action:	◯ Permit ◉ Deny ◯ Shutdown	
Logging	☐ Enable	
Time Range	☐ Enable	
Time Range Name:	Edit	
Destination MAC Address:	◉ Any ◯ User Defined	
Destination MAC Address Value:		
Destination MAC Address Mask:		(0s for matching, 1s for no matching)
Source MAC Address:	◯ Any ◉ User Defined	
Source MAC Address Value:	00041F111111	
Source MAC Address Mask:	000000111111	(0s for matching, 1s for no matching)
VLAN ID:		(Range: 1 - 4094)
802.1p:	☐ Include	
802.1p Value:		(Range: 1 - 7)
802.1p Mask:		(Range: 1 - 7)

MAC-Based ACE Table

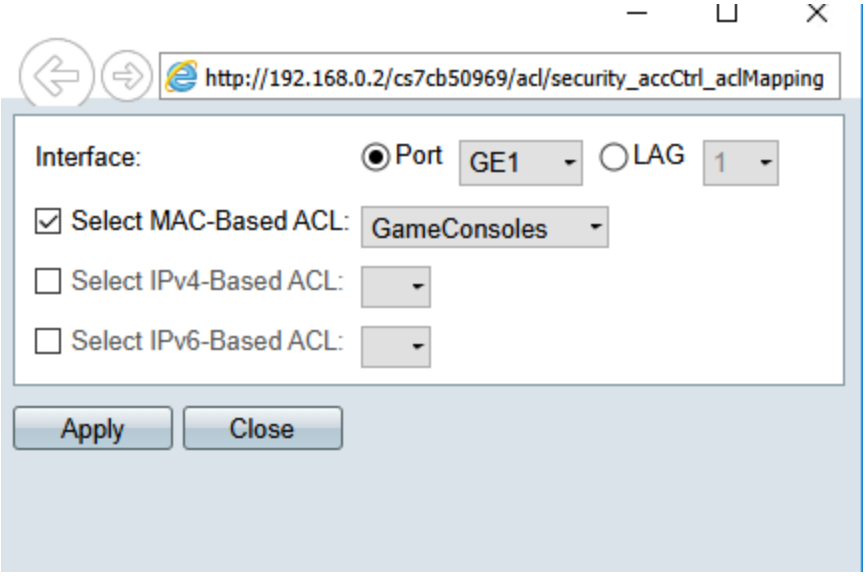
Filter: *ACL Name equals to* GameConsoles Go

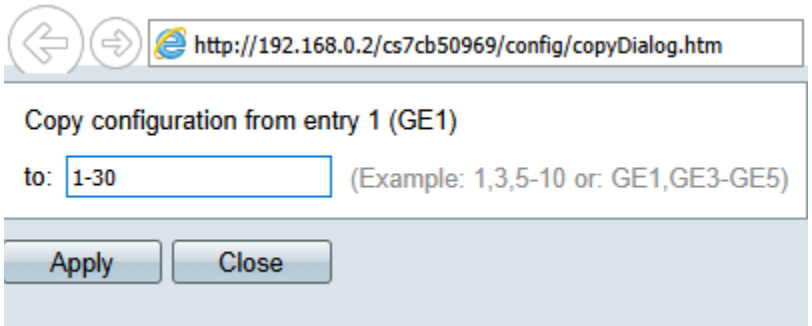
	Priority	Action	Logging	Time Range		Destination		Source		VLAN ID	802.1p	802.1p Mask	Ethertype
				Name	State	MAC Address	Wildcard Mask	MAC Address	Wildcard Mask				
☐	1	Deny				Any	Any	00:04:1f:11:11:11	00:00:00:11:11:11				
☐	2	Deny				00:50:42:11:11:11	00:00:00:11:11:11	Any	Any				
☐	3	Deny				00:0d:3a:11:11:11	00:00:00:11:11:11	Any	Any				
☐	4	Deny				00:13:15:11:11:11	00:00:00:11:11:11	Any	Any				
☐	5	Deny				00:09:bf:11:11:11	00:00:00:11:11:11	Any	Any				
☐	6	Deny				00:12:5a:11:11:11	00:00:00:11:11:11	Any	Any				

Add... Edit... Delete

MAC-Based ACL Table

Bind the GamerConsoles ACL to all GE Interfaces:


http://192.168.0.2/cs7cb50969/acl/security_accCtrl_aclMapping
Interface:
Port
GE1
LAG
1
Select MAC-Based ACL:
GameConsoles
Select IPv4-Based ACL:
Select IPv6-Based ACL:
Apply
Close


http://192.168.0.2/cs7cb50969/config/copyDialog.htm
Copy configuration from entry 1 (GE1)
to:
1-30
(Example: 1,3,5-10 or: GE1,GE3-GE5)
Apply
Close

Lab Report

Time Spent: 03:44

Score: 4/4 (100%)

TASK SUMMARY

Required Actions

- ✓ Create the GameConsoles ACL
- ✓ Create a MAC-based access control Show Details
- ✓ Bind the GameConsoles ACL to all of the interfaces Show Details
- ✓ Save the configuration

LAB Restrict Telnet and SSH access

You are in the process of configuring a new router. The router interfaces connect to the following networks:

Interface	Network
FastEthernet0/0	192.168.1.0/24
FastEthernet0/1	192.168.2.0/24
FastEthernet0/1/0	192.168.3.0/24

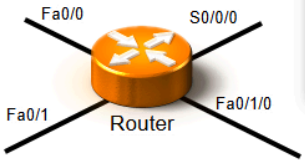
Only Telnet and SSH access from these three networks should be allowed.

In this lab, your task is to:

- Use the **access-list** command to create a standard numbered access list using number 5.

- Add a **permit** statement for each network to the access list.
- Use the **access-class** command to apply the access list to VTY lines 0–4. Use the **in** direction to filter incoming traffic.
- Save your changes in the **startup-config** file.

Create a standard numbered access list:




```
Press RETURN to get started.

Router>en
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list-5 permit 192.168.1.0 0.0.0.255
                                ^
% Invalid input detected at '^' marker.

Router(config)#access-list 5 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 5 permit 192.168.2.0 0.0.0.255
Router(config)#access-list 5 permit 192.168.3.0 0.0.0.255
Router(config)#line vty 0 4
Router(config-line)#access-class 5 in
Router(config-line)#^Z
*Nov 16 21:48:04.950: %SYS-5-CONFIG_I: Configured from console by admin on con 0

Router#copy run start
Destination filename [startup-config]
Building configuration...
[OK]

Router#_
```

Lab Report

Time Spent: 03:34

Score: 6/6 (100%)

TASK SUMMARY

Required Actions

- ✓ Create Standard Access List 5
- ✓ Permit Network 192.168.1.0 0.0.0.255
- ✓ Permit Network 192.168.2.0 0.0.0.255
- ✓ Permit Network 192.168.3.0 0.0.0.255
- ✓ Apply Access List 5 to VTY lines 0-4 Show Details
- ✓ Save your changes in the startup-config file Show Details

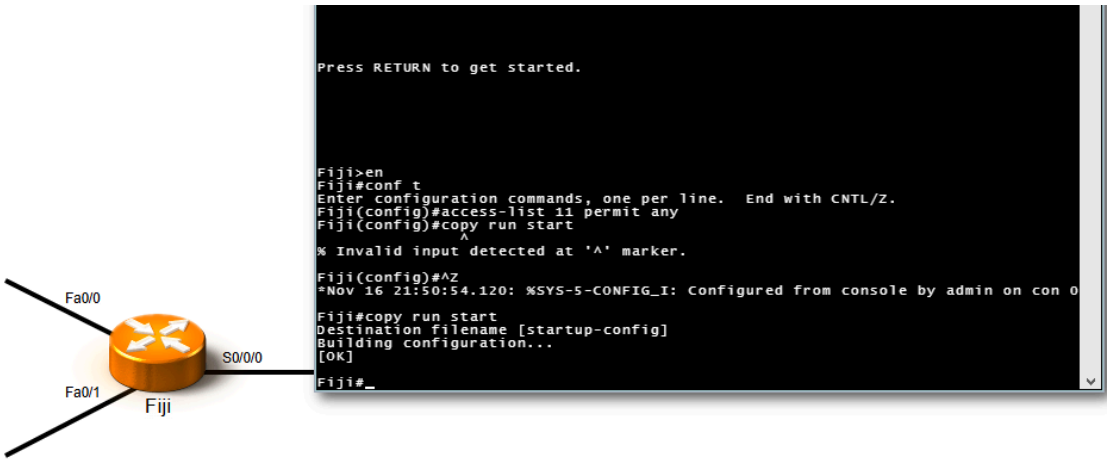
END LAB

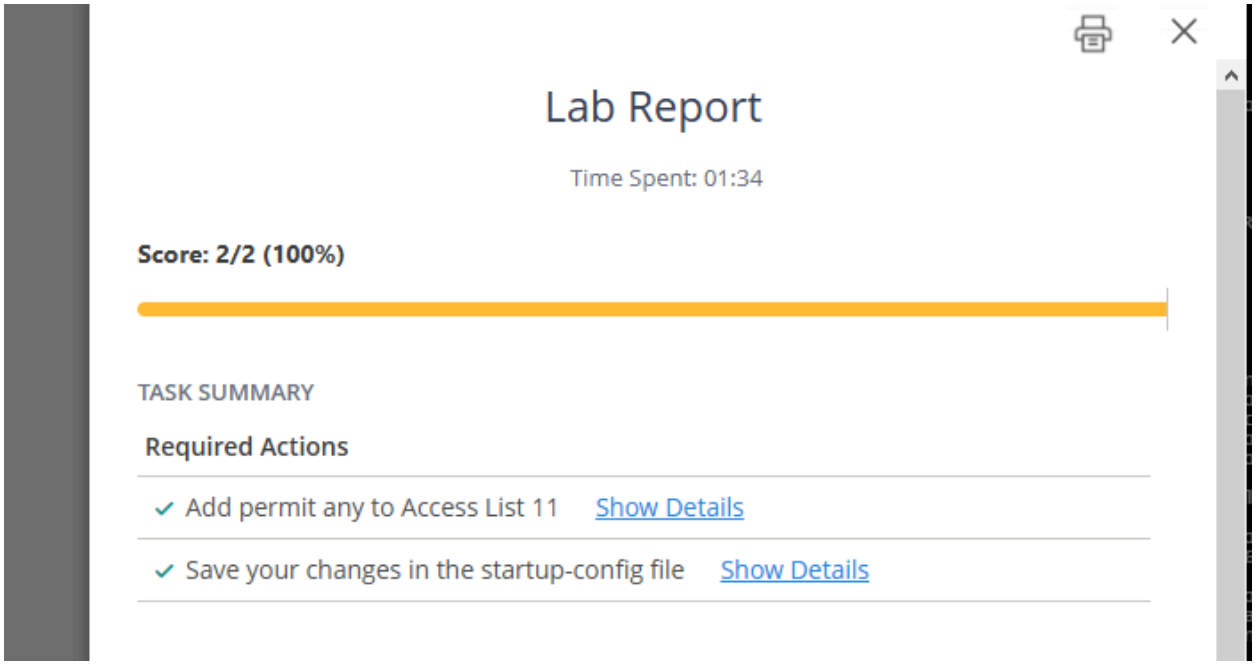
LAB Permit Traffic

The Fiji router has been configured with Standard IP Access List 11. The access list is applied to the *Fa0/0 interface*. The access list must allow all traffic except traffic coming from hosts 192.168.1.10 and 192.168.1.12. However, you've noticed that it's preventing all traffic from being sent on Fa0/0. You remember that access lists contain an implied **deny any** statement. This means that any traffic not permitted by the list is denied. For this reason, access lists should contain at least one permit statement, or all traffic is blocked.

In this lab, your task is to:

- Add a **permit any** statement to Access List 11 to allow all traffic other than the restricted traffic.
- Save your changes in the **startup-config** file.





LAB Scan for Cleartext Vulnerabilities

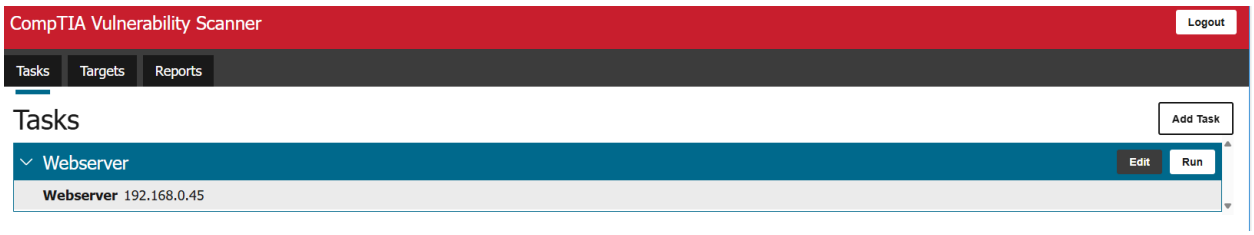
One of the content developers on the Engineering team uses an Embedthis GoAhead webserver for several devices that are maintained by their team.

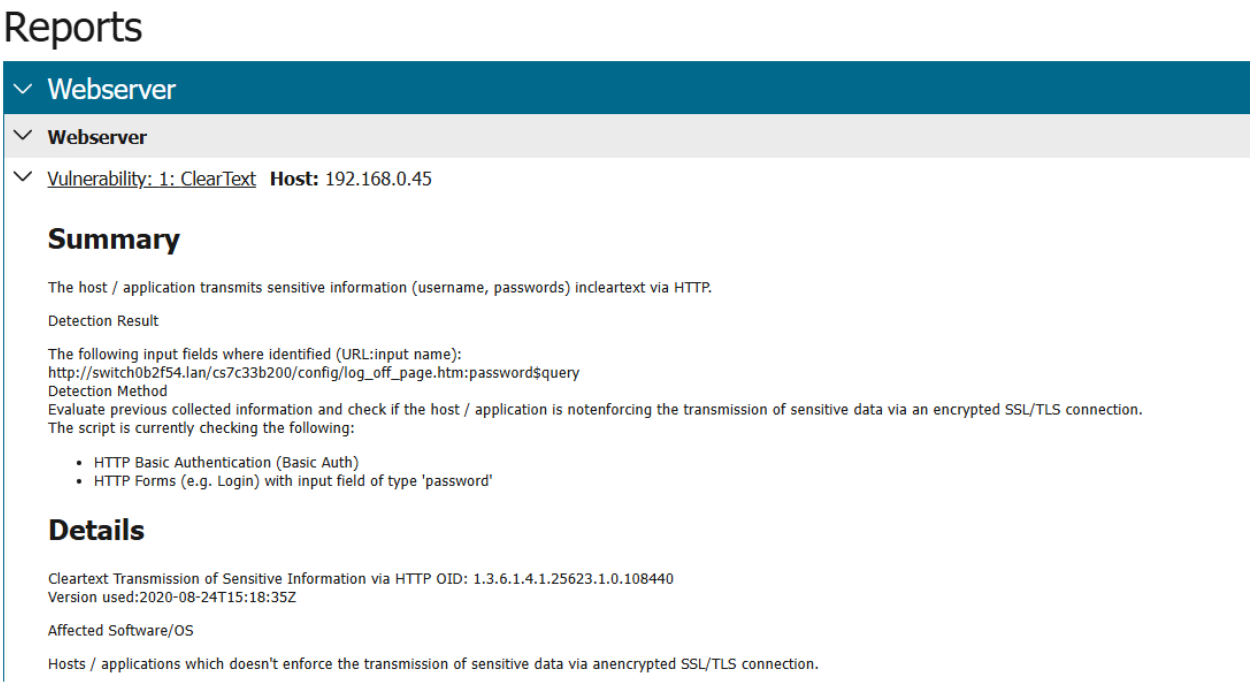
In this lab, you need to scan the test machine where the Engineering team prepares deployments and complete the following tasks:

- Login to the CompTIA Vulnerability Scanner in Chrome.
    - URL: **http://192.168.0.52**
    - Username: **securityadmin**

- Password: **P@ssw0rd**

- Use the CompTIA Vulnerability Scanner to scan the test machine found at 192.168.0.45.
- Answer the questions about any vulnerabilities found.





Lab Report

Time Spent: 00:58

Score: 3/3 (100%)

TASK SUMMARY

Required Actions & Questions

✓ Scan the host at IP address 192.168.0.45.

✓ *Q1*: Which CVE was reported for the discovered vulnerability?

Your answer: CVE-2019-16645

Correct answer: CVE-2019-16645

✓ *Q2*: Which of the following are possible solutions to remediate the vulnerability?

Your answer: Upgrade to a newer release, Replace the product with another one, Remove the product

Correct answer: Upgrade to a newer release, Remove the product, Replace the product with another one

END LAB

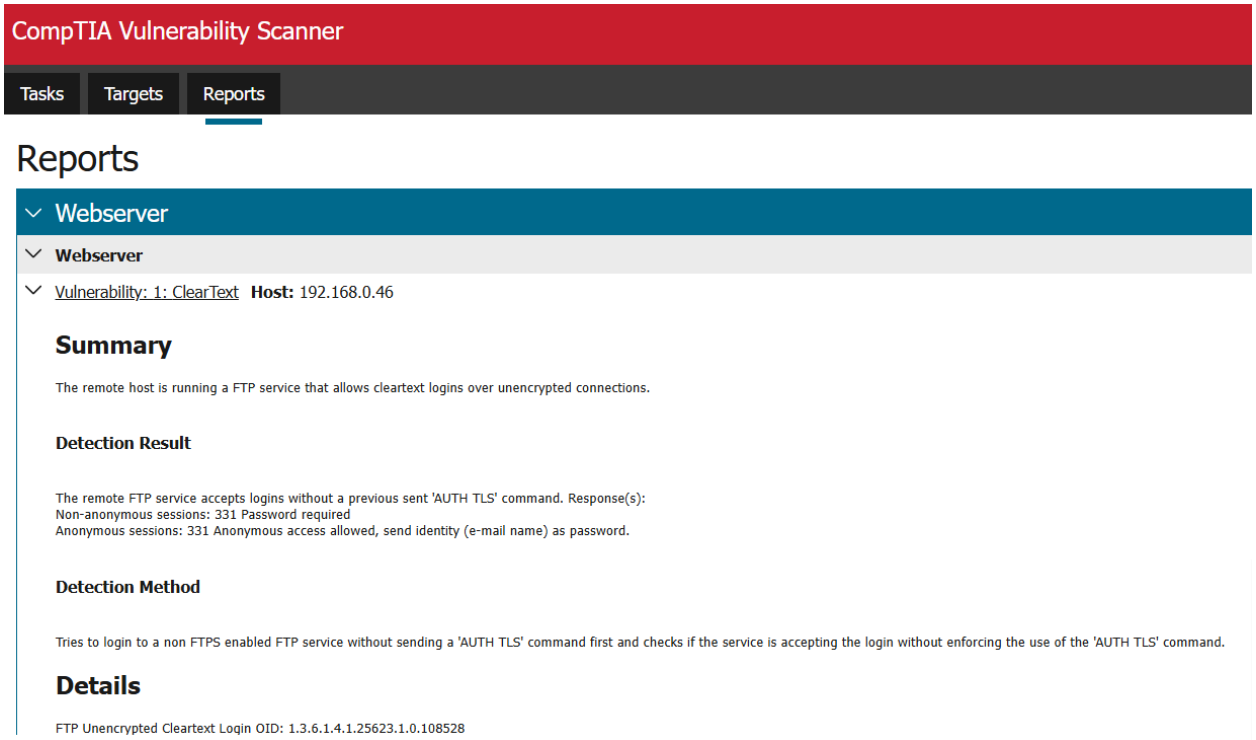
LAB Scan for FTP Vulnerabilities

A server is used to transfer company financial data to remote branches using the FTP protocol. Since the data is sensitive to the company, you have been asked to scan the host for vulnerabilities.

In this lab, your task is to complete the following:

- Login to the CompTIA Vulnerability Scanner in Chrome.
    - URL: **http://192.168.0.52**
    - Username: **securityadmin**
    - Password: **P@ssw0rd**

- Using the CompTIA Vulnerability Scanner, scan the server found at 192.168.0.46.
- Answer the questions presented about what the Vulnerability Scanner finds.



Lab Report

Time Spent: 05:24

Score: 3/3 (100%)

TASK SUMMARY

Required Actions & Questions

✓ Scan the host found at 192.168.0.46.

✓ *Q1*: How many vulnerabilities were found on the FTP server?

Your answer: 2

Correct answer: 2

✓ *Q2*: Which of the services or networking functions were shown as being vulnerable?

Your answer: ICMP packet responses, The FTP service

Correct answer: The FTP service, ICMP packet responses

END LAB

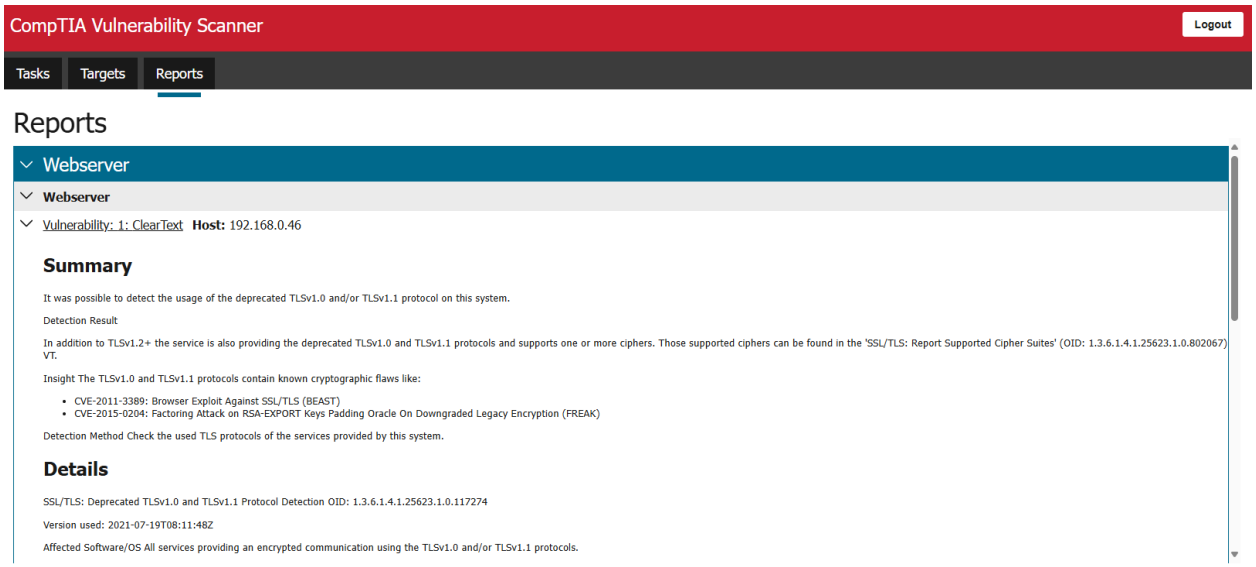
LAB Scan for TLS Vulnerabilities

An older server has been providing file sharing for Windows, Linux, and MacOS clients to the Sales team.

In this lab, you need to scan the file server to ensure it is secure by completing the following tasks:

- Login to the CompTIA Vulnerability Scanner in Chrome.
    - URL: **http://192.168.0.52**
    - Username: **securityadmin**
    - Password: **P@ssw0rd**

- Use the CompTIA Vulnerability Scanner to scan the test machine found at 192.168.0.46.
- Answer the questions about any vulnerabilities found.



Lab Report

Time Spent: 01:31

Score: 3/3 (100%)

TASK SUMMARY

Required Actions & Questions

✓ Scan the host at IP address 192.168.0.46.

✓ *Q1*: Which CVEs were reported for the discovered vulnerability?

Your answer: CVE-2011-3389, CVE-2015-0204

Correct answer: CVE-2011-3389, CVE-2015-0204

✓ *Q2*: Which of the following are suggested possible solutions to remediate the vulnerability?

Your answer: Disable TLSv1.0 and TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

Correct answer: Disable TLSv1.0 and TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

END LAB

LAB Scan for Windows Vulnerabilities

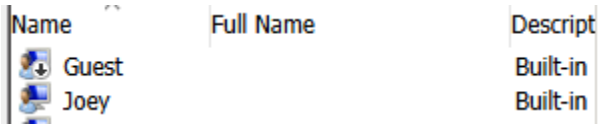
You are the IT security administrator for a small corporate network. You are performing vulnerability scans on your network. Mary is the primary administrator for the network and the only person authorized to perform local administrative actions. The company's network security policy requires complex passwords for all users that are at least 12 characters long. It is also required that Windows Firewall is enabled on all workstations. Sharing personal files is not allowed.

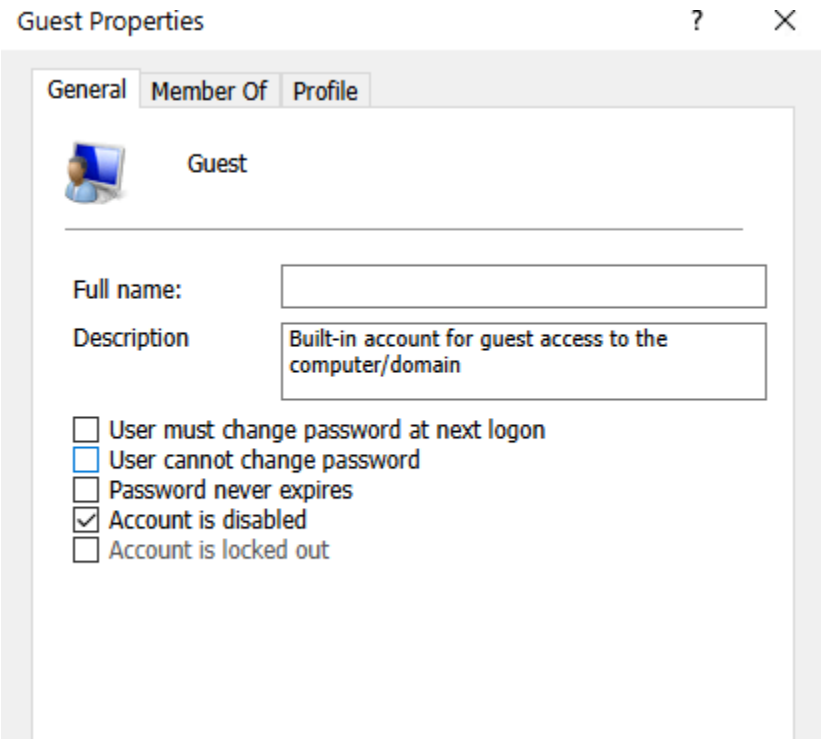
In this lab, your task is to:

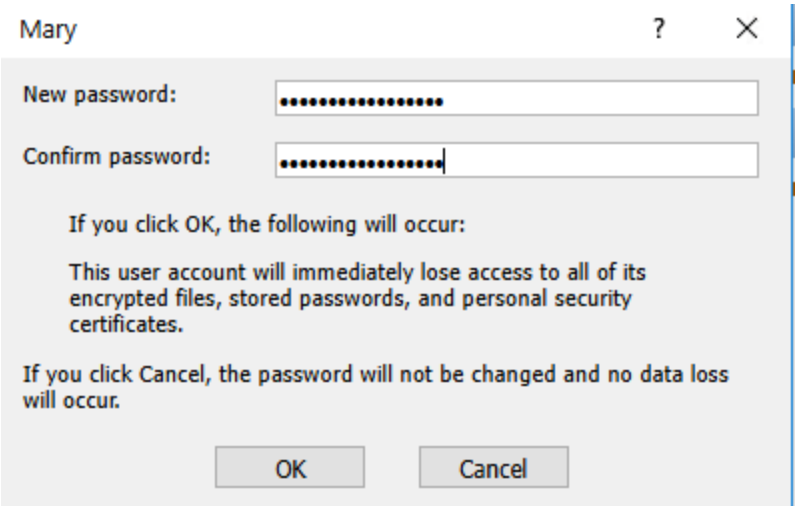
- Login to the CompTIA Vulnerability Scanner in Chrome.
    - URL: http://192.168.0.52
    - Username: securityadmin

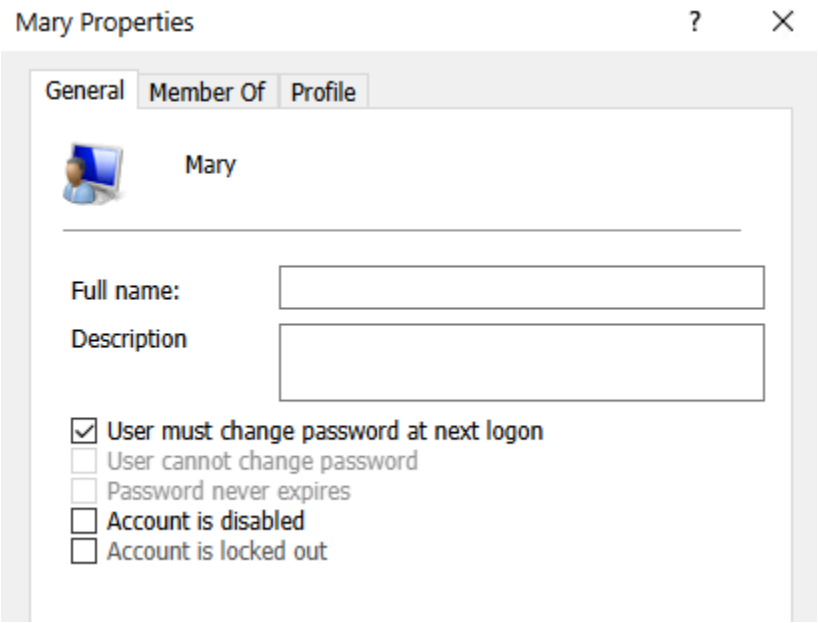
    - Password: P@ssw0rd
    - Select **Sign In**
- Create a target for the Office2 workstation (192.168.0.34).
- Create a task and run a vulnerability scan for the Office2 workstation.
- View the report for the scan task you created.
- Remediate the vulnerabilities found in the report for Office2. Use Computer Management, Settings, and File Explorer to make needed changes.
- Re-run a vulnerability scan to make sure all of the issues are resolved.

Renamed Admin to Joey

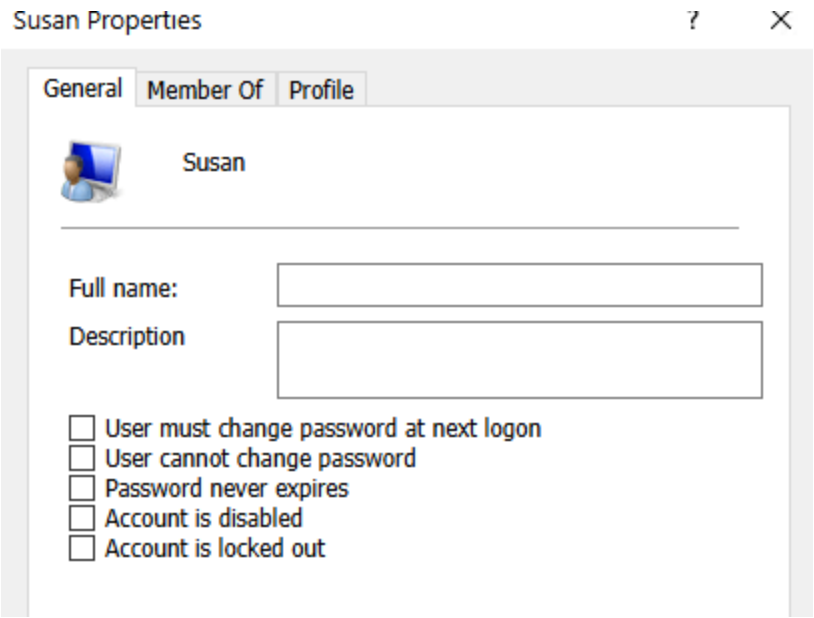


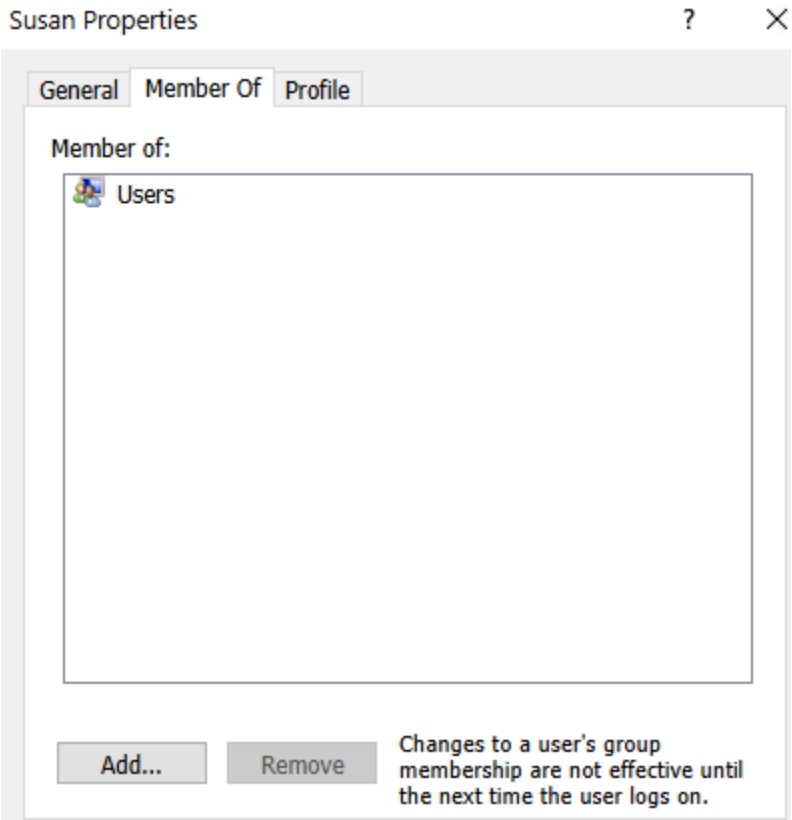




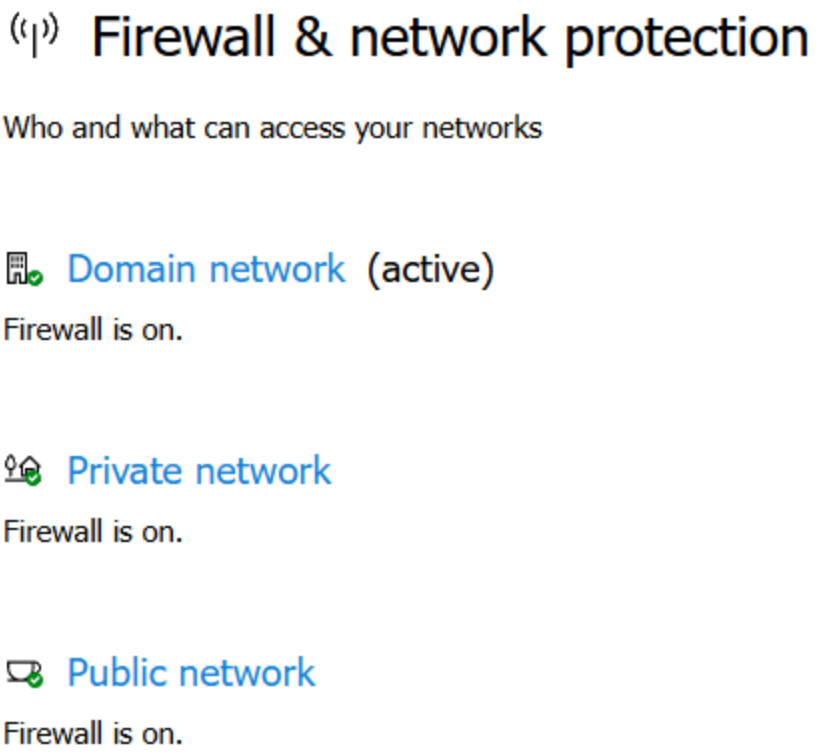


Unlock Susan’s account and remove her from the admin group

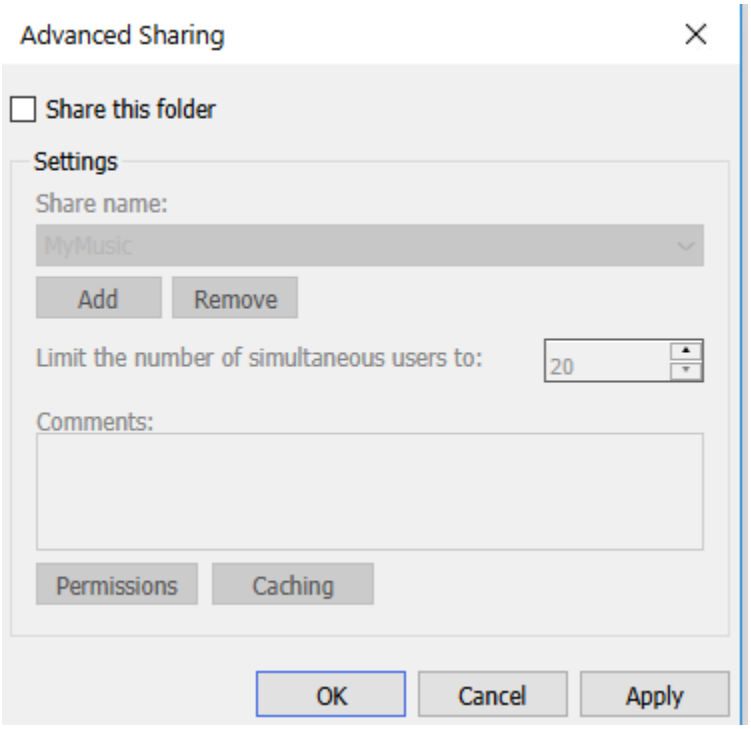




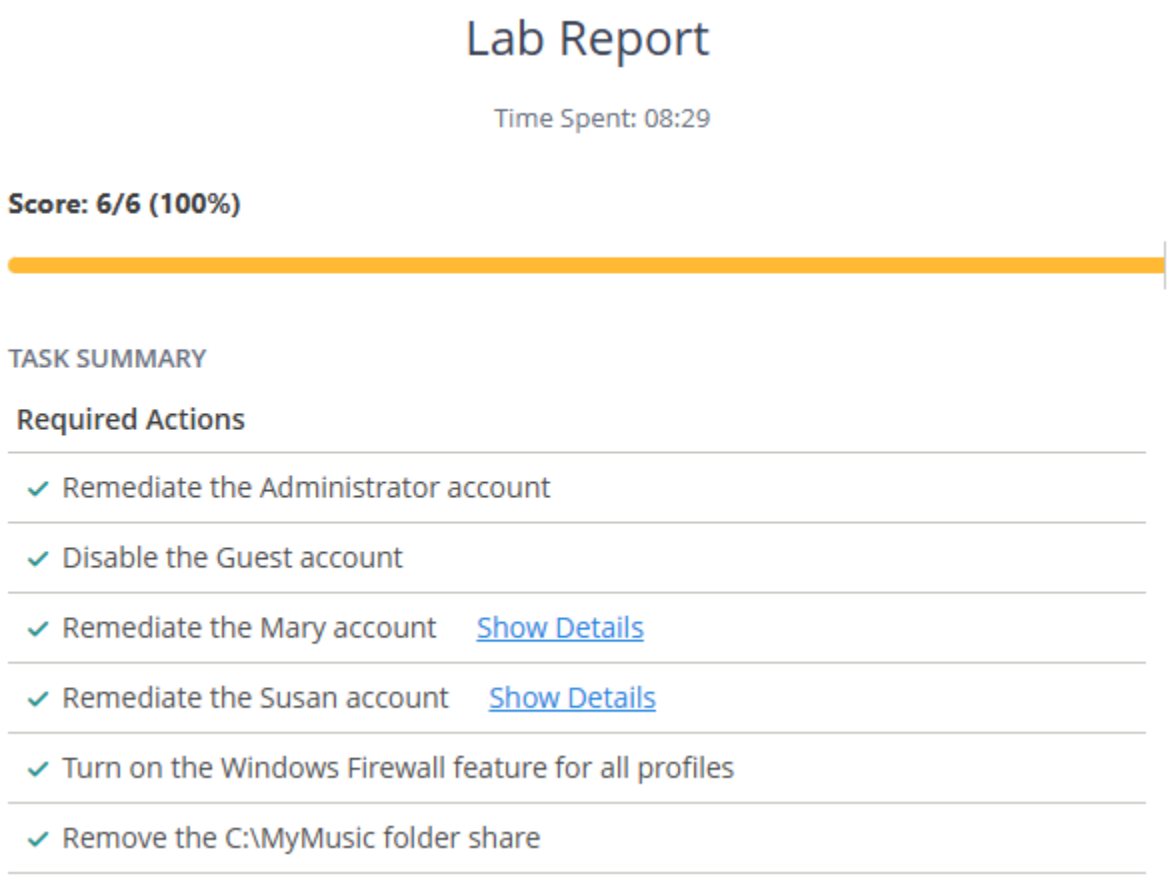
Turning firewall on for all profiles



Remove the file share in MyMusic



Rerun vulnerability scanner to confirm issues have been addressed



END LAB

LAB Scan for Linux Vulnerabilities

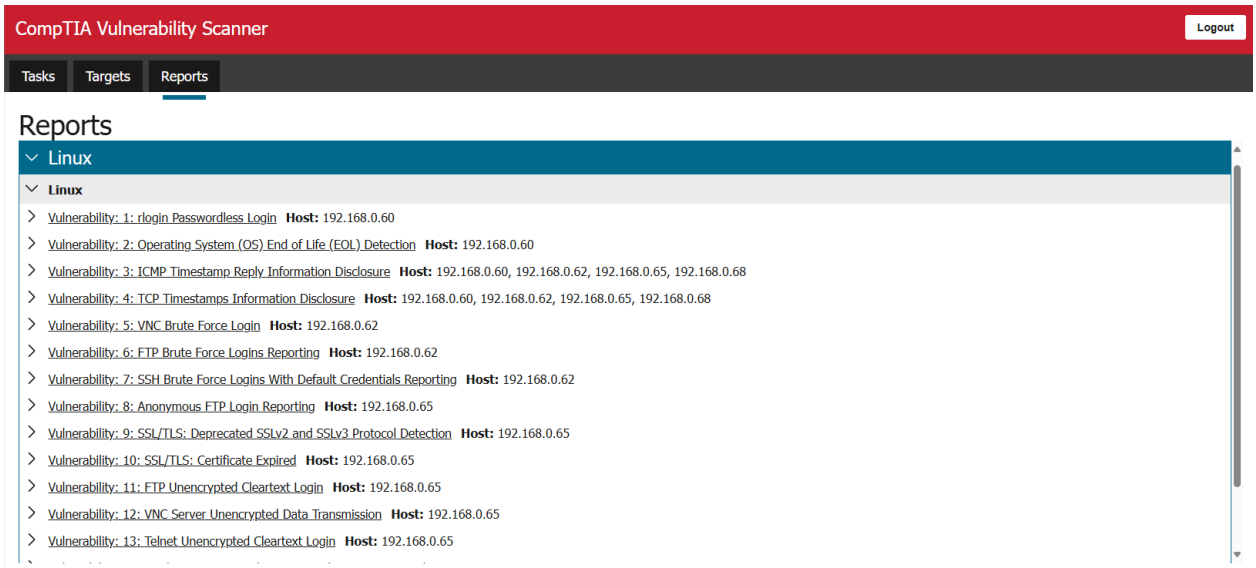
You are the IT security administrator for a small corporate network. You need to use a vulnerability scanner to check for security issues on your Linux computers.

In this lab, your task is to:

- Login to the CompTIA Vulnerability Scanner in Chrome.
    - URL: **http://192.168.0.52**

    - Username: **securityadmin**
    - Password: **P@ssw0rd**
- Create a target for the Linux computers on IP range **192.168.0.60 - 192.168.0.69**
- Answer the first question
- Create a task and run a vulnerability scan for the Linux range.
- View the report for the scan task you created.
- Answer the remaining questions.

Vulnerability Scan



Lab Report

Time Spent: 03:12

Score: 6/6 (100%)

TASK SUMMARY

Required Actions & Questions

✓ *Q1*: Which Linux computers were discovered on the IP range 192.168.0.60 - 192.168.0.69?

Your answer: 192.168.0.60, 192.168.0.62, 192.168.0.65, 192.168.0.68

Correct answer: 192.168.0.60, 192.168.0.62, 192.168.0.65, 192.168.0.68

✓ Scan the IP Address range 192.168.0.60 - 192.168.0.69.

✓ *Q2*: Which vulnerabilities are present on all the computers in the range?

Your answer: ICMP Timestamp Reply Information Disclosure, TCP Timestamps Information Disclosure

Correct answer: ICMP Timestamp Reply Information Disclosure, TCP Timestamps Information Disclosure

✓ *Q3*: For the Linux computer with the 192.168.0.60 IP address, which vulnerabilities should be remediated immediately?

Your answer: rlogin Passwordless Login, Operating System (OS) End of Life (EOL) Detection

Correct answer: rlogin Passwordless Login, Operating System (OS) End of Life (EOL) Detection

END LAB

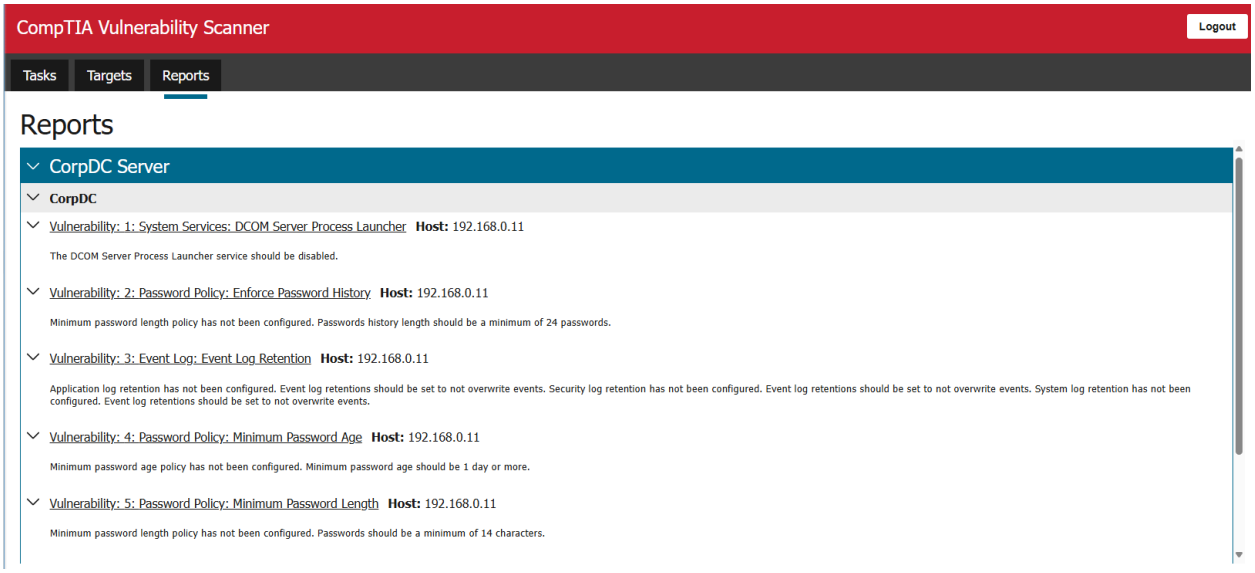
LAB Scan for Domain Controller Vulnerabilities

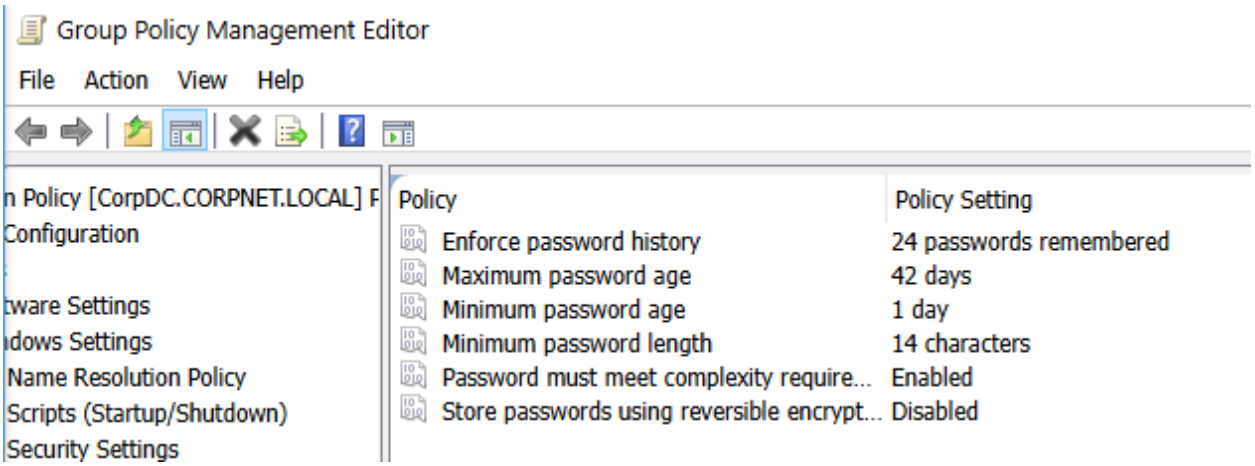
You are the IT security administrator for a small corporate network. You are performing vulnerability scans on your network. Use the CompTIA Vulnerability Scanner tool to run a vulnerability scan on the CorpDC domain controller.

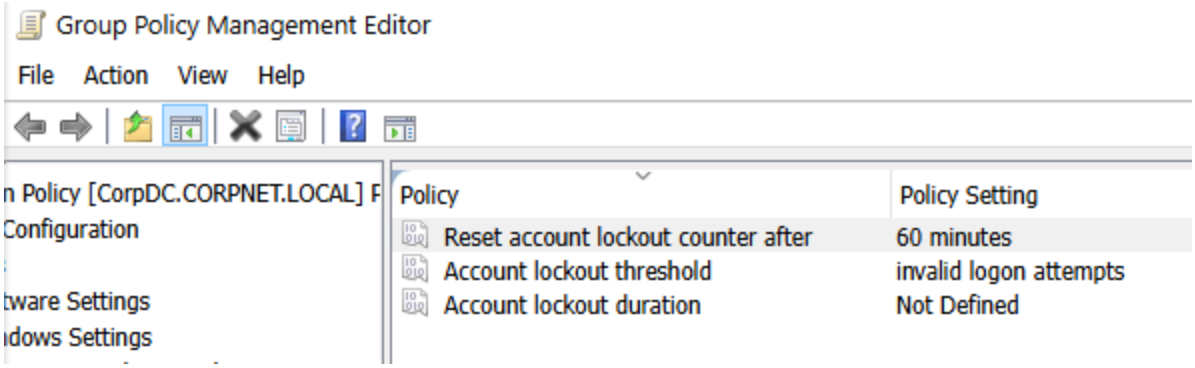
In this lab, your task is to:

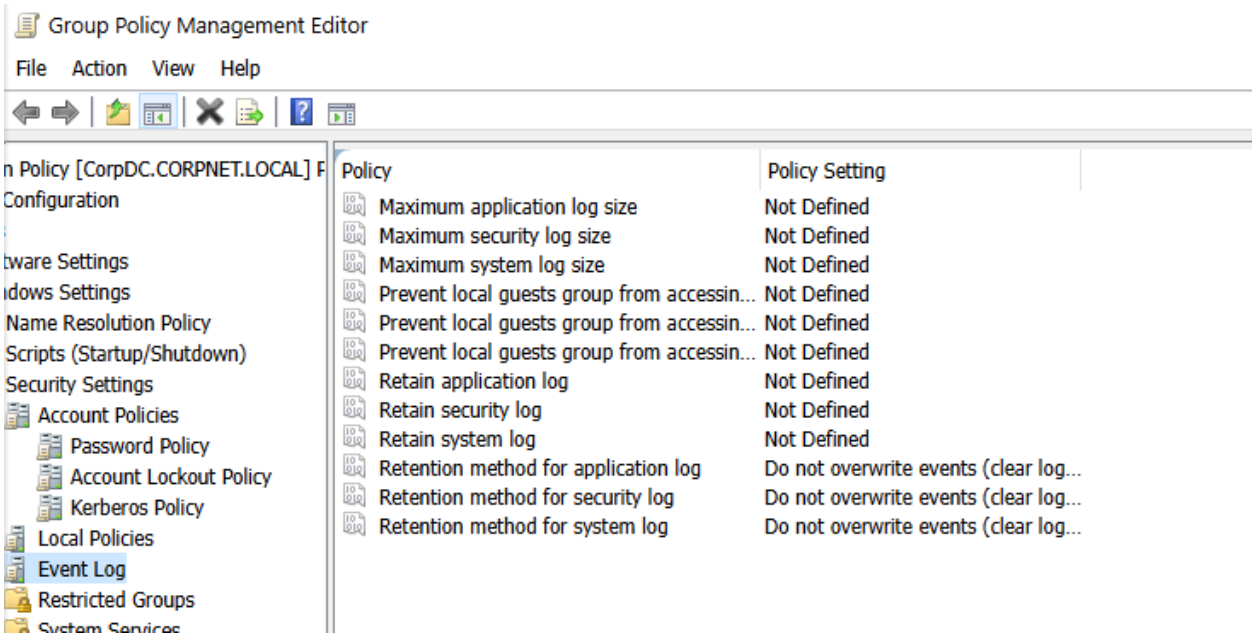
- Login to the CompTIA Vulnerability Scanner in Chrome.

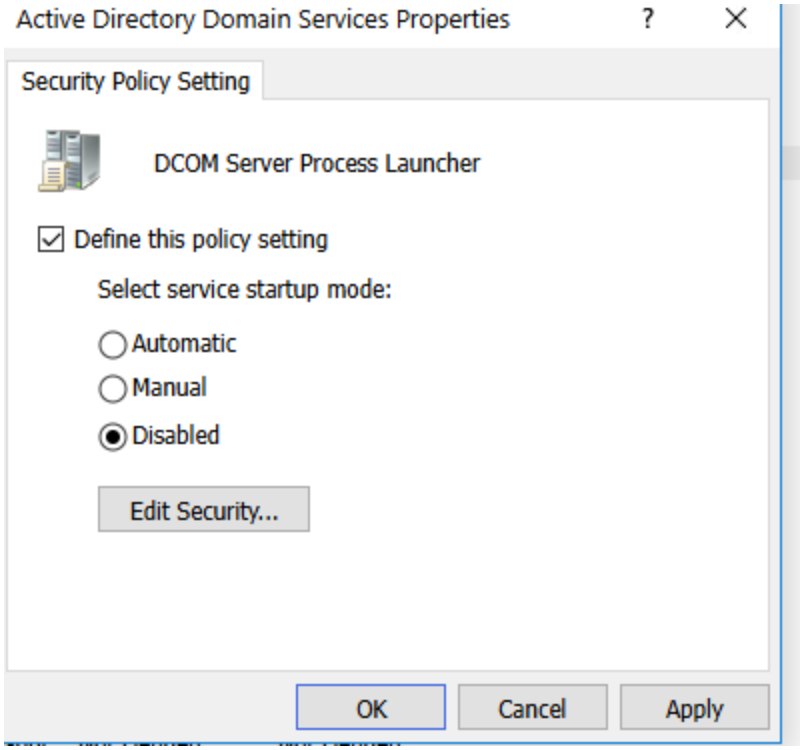
    - URL: http://192.168.0.52
    - Username: securityadmin
    - Password: P@ssw0rd
- Create a target for the CorpDC server (192.168.0.11).
- Create a task and run a vulnerability scan for the CorpDC server.
- View the report for the scan task you created.
- Remediate the vulnerabilities in the Default Domain Policy using Group Policy Management on CorpDC.
- Re-run a vulnerability scan to make sure all of the issues are resolved.

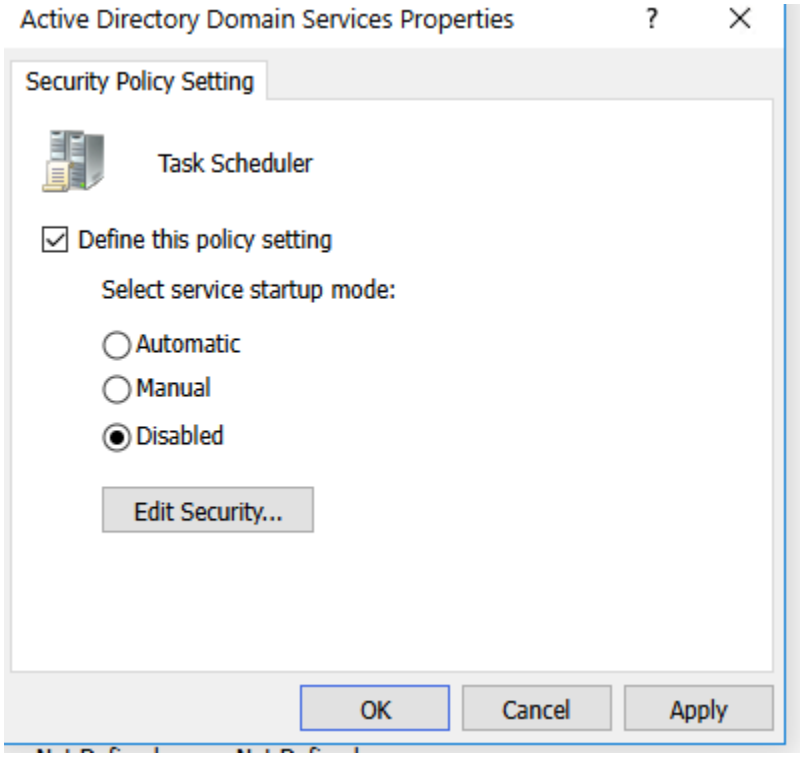




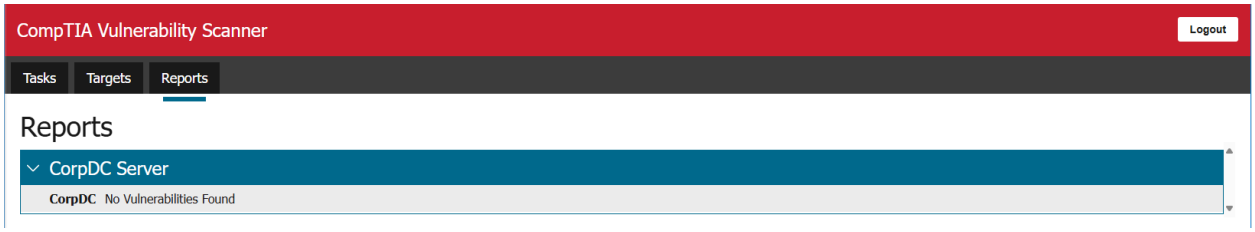

Group Policy Management Editor
File Action View Help
n Policy [CorpDC.CORPNET.LOCAL] F
Configuration
tware Settings
ndows Settings
Policy
Policy Setting
Reset account lockout counter after
60 minutes
Account lockout threshold
invalid logon attempts
Account lockout duration
Not Defined


Group Policy Management Editor
File Action View Help
n Policy [CorpDC.CORPNET.LOCAL] F
Configuration
tware Settings
ndows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
Policy
Policy Setting
Maximum application log size
Not Defined
Maximum security log size
Not Defined
Maximum system log size
Not Defined
Prevent local guests group from accessin...
Not Defined
Prevent local guests group from accessin...
Not Defined
Prevent local guests group from accessin...
Not Defined
Retain application log
Not Defined
Retain security log
Not Defined
Retain system log
Not Defined
Retention method for application log
Do not overwrite events (clear log...
Retention method for security log
Do not overwrite events (clear log...
Retention method for system log
Do not overwrite events (clear log...





Rerun vulnerability scan to ensure all issues are resolved



Lab Report

Time Spent: 08:22

Score: 7/7 (100%)

TASK SUMMARY

Required Actions

- ✓ Reset account lockout counter after 60 minutes
- ✓ Use a minimum password length of 14 characters
- ✓ Use a minimum password age of one day
- ✓ Enforce password history for 24 passwords
- ✓ Event log retention set not to overwrite events Show Details
- ✓ DCOM Server Process Launcher service disabled
- ✓ Task Scheduler service disabled

END LAB

LAB Configure Advanced Audit Policy

You work as the IT security administrator for a small corporate network. As part of an ongoing program to improve security, you want to implement an audit policy for all workstations. You plan to audit user logon attempts and other critical events.

In this lab, your task is to configure the following audit policy settings in WorkstationGPO:

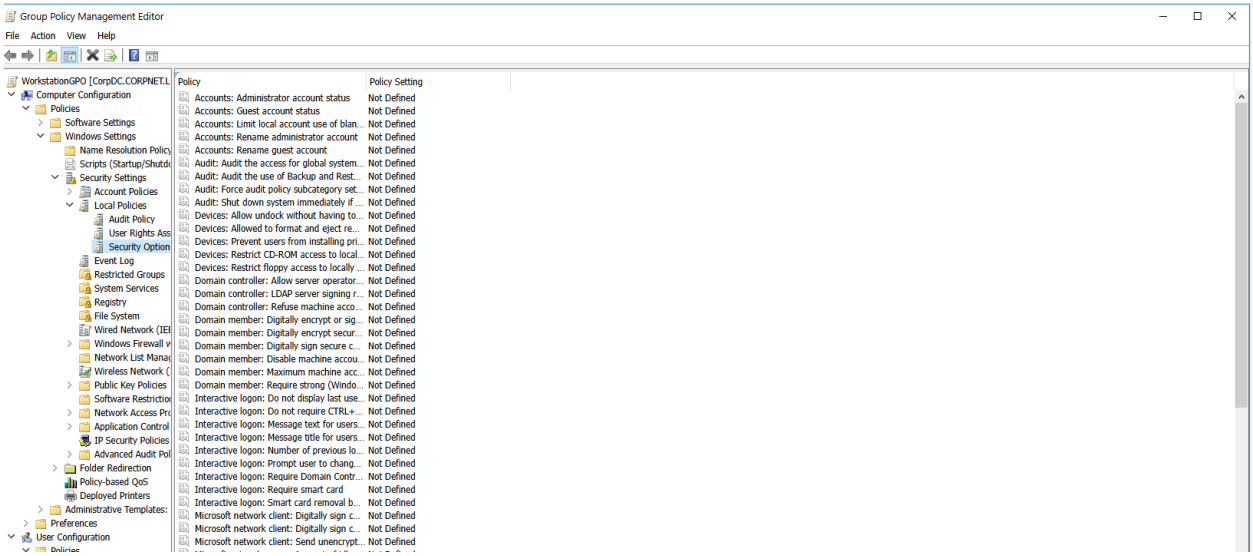
Local Policies	Setting
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	**Enabled**
Audit: Shut down system immediately if unable to log security audits	**Enabled**

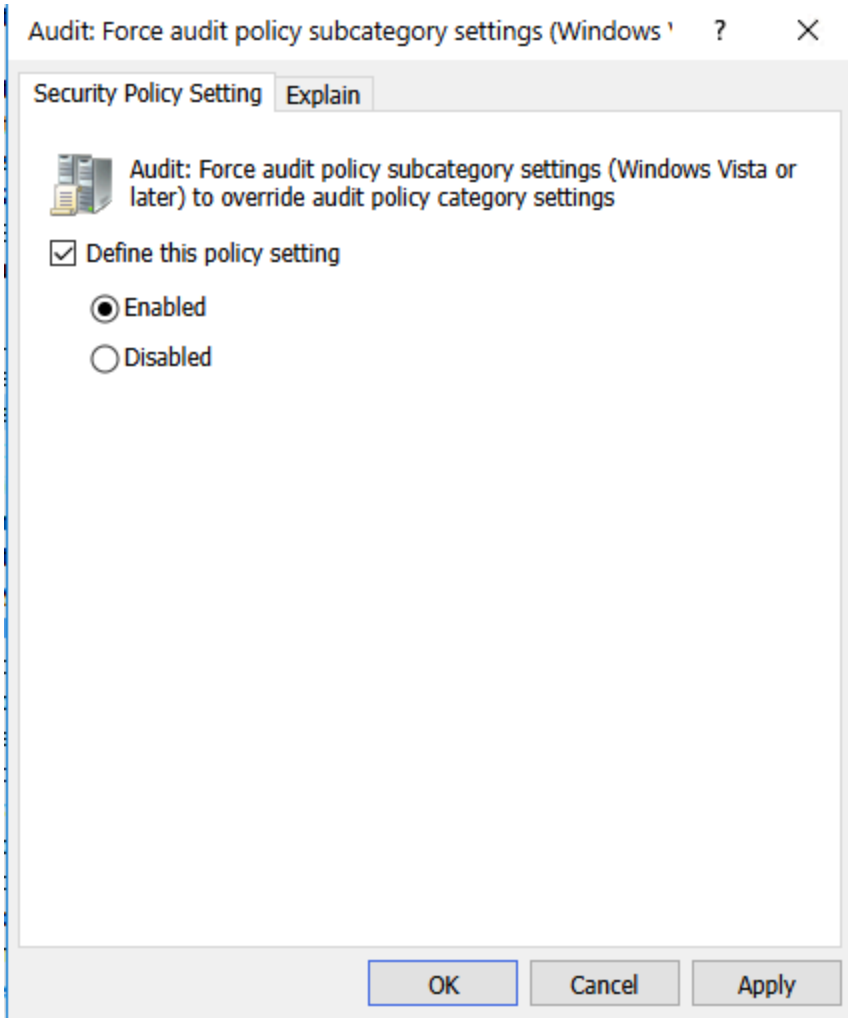
Event Log	Setting
Retention method for security log	***Define: Do not overwrite events (clear log manually)***

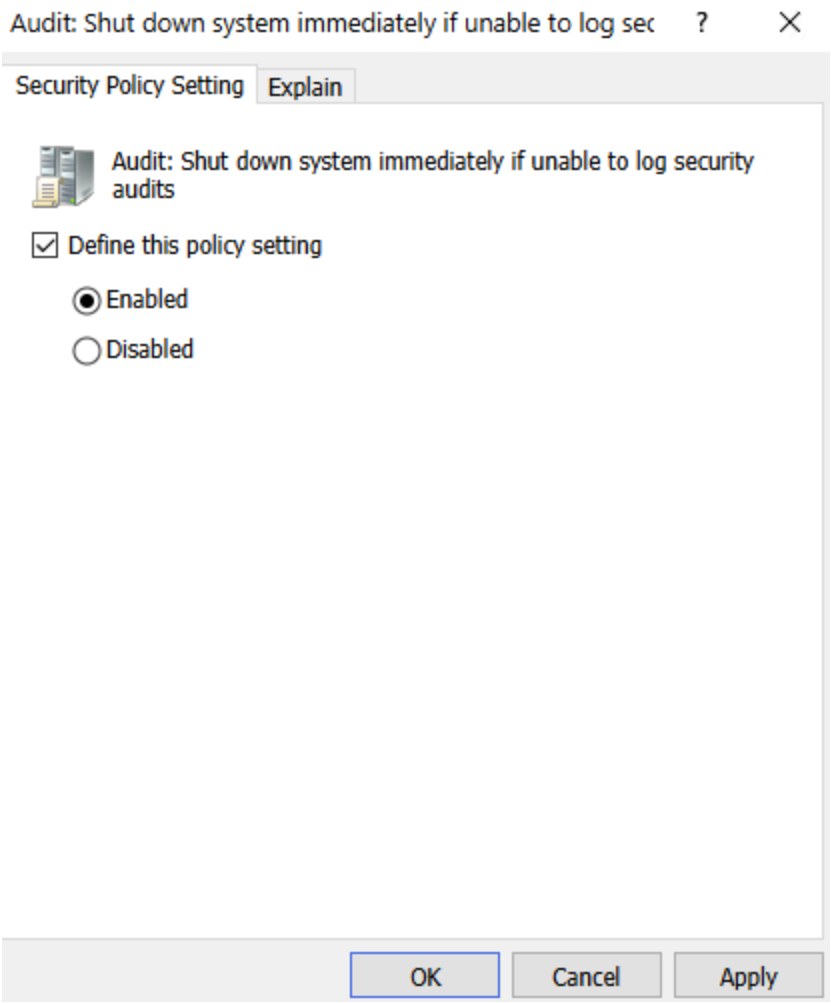
Advanced Audit Policy Configuration	Setting
Account Logon: Audit Credential Validation	**Success and Failure**
Account Management: Audit User Account Management	**Success and Failure**
Account Management: Audit Security Group Management	**Success and Failure**
Account Management: Audit Other Account Management Events	**Success and Failure**
Account Management: Audit Computer Account Management	**Success**
Detailed Tracking: Audit Process Creation	**Success**
Logon/Logoff: Audit Logon	**Success and Failure**
Logon/Logoff: Audit Logoff	**Success**

Policy Change: Audit Authentication Policy Change	**Success**
Policy Change: Audit Audit Policy Change	**Success and Failure**
Privilege Use: Audit Sensitive Privilege Use	**Success and Failure**
System: Audit System Integrity	**Success and Failure**
System: Audit Security System Extension	**Success and Failure**
System: Audit Security State Change	**Success and Failure**
System: Audit IPsec Driver	**Success and Failure**

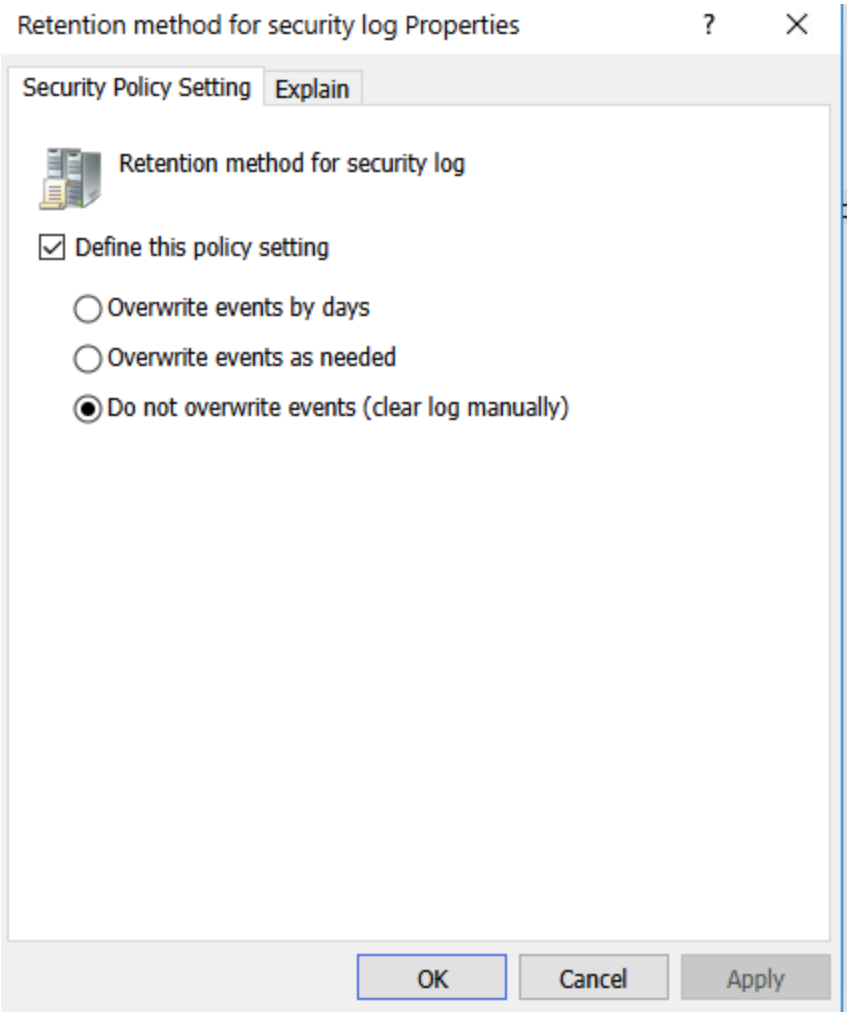
Starting WorkstationGPO and editing it’s local security policies



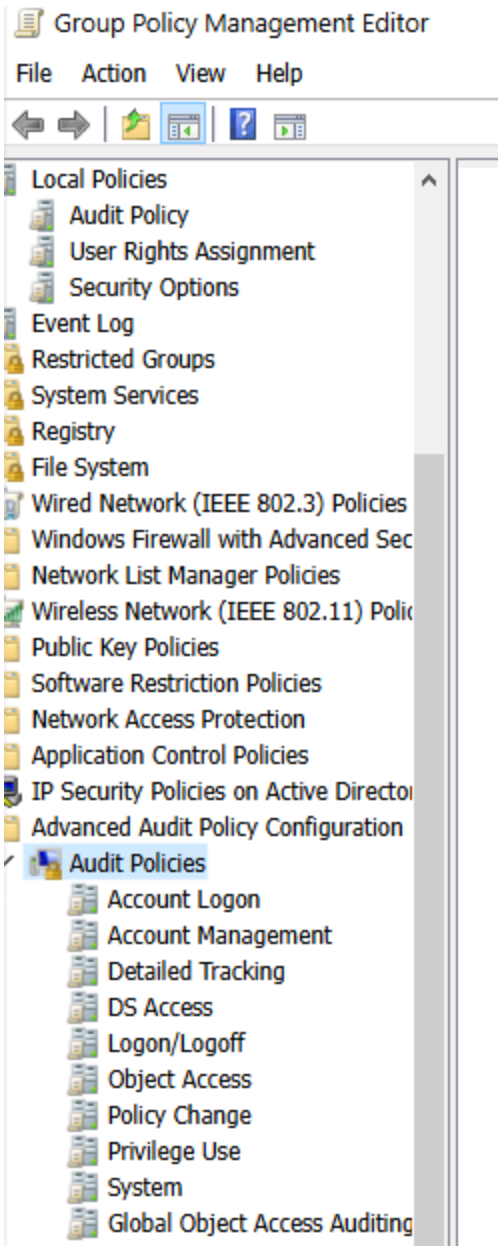

Audit: Force audit policy subcategory settings (Windows '
?
Security Policy Setting
Explain
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings
Define this policy setting
Enabled
Disabled
OK
Cancel
Apply

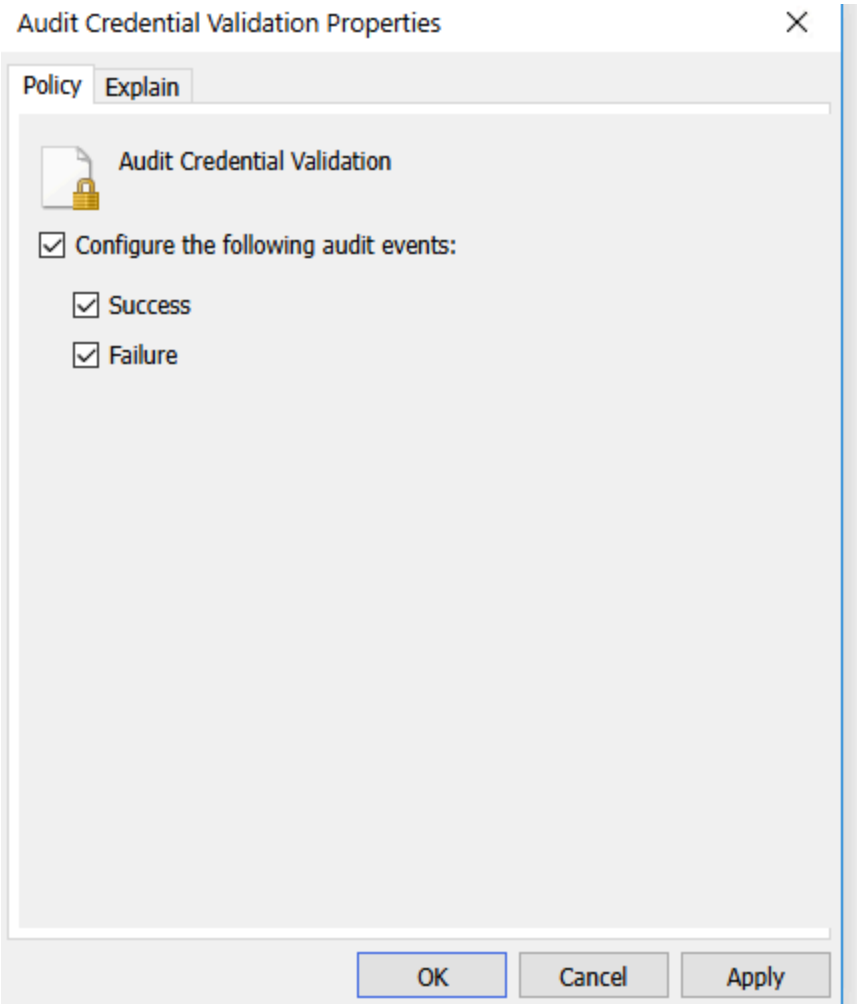


Edit the event log:



Edit advanced audit policy configuration:


Group Policy Management Editor
File
Action
View
Help
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Sec
Network List Manager Policies
Wireless Network (IEEE 802.11) Polic
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directo
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing



Subcategory	Audit Events
Audit User Account Management	Success, Failure
Audit Security Group Management	Success, Failure
Audit Other Account Management Events	Success, Failure
Audit Distribution Group Management	Not Defined
Audit Computer Account Management	Success
Audit Application Group Management	Not Defined

Subcategory	Audit Events
Audit RPC Events	Not Defined
Audit Process Termination	Not Defined
Audit Process Creation	Success
Audit DPAPI Activity	Not Defined

Subcategory	Audit Events
Audit Special Logon	Not Defined
Audit Other Logon/Logoff Events	Not Defined
Audit Network Policy Server	Not Defined
Audit Logon	Success, Failure
Audit Logoff	Success
Audit IPsec Quick Mode	Not Defined
Audit IPsec Main Mode	Not Defined
Audit IPsec Extended Mode	Not Defined
Audit Account Lockout	Not Defined

Subcategory	Audit Events
Audit Other Policy Change Events	Not Defined
Audit MPSSVC Rule-Level Policy Change	Not Defined
Audit Filtering Platform Policy Change	Not Defined
Audit Authorization Policy Change	Not Defined
Audit Authentication Policy Change	Success
Audit Audit Policy Change	Success, Failure

Subcategory	Audit Events
Audit Sensitive Privilege Use	Success, Failure
Audit Other Privilege Use Events	Not Defined
Audit Non Sensitive Privilege Use	Not Defined

Subcategory	Audit Events
Audit System Integrity	Success, Failure
Audit Security System Extension	Success, Failure
Audit Security State Change	Success, Failure
Audit Other System Events	Not Defined
Audit IPsec Driver	Success, Failure

Lab Report

Time Spent: 06:58

Score: 9/9 (100%)

TASK SUMMARY

Required Actions

- ✓ Enable Audit Policies Show Details
- ✓ Enable Event Log Policy
- ✓ Enable Account Logon Audit Policy
- ✓ Enable Account Management Audit Policies Show Details
- ✓ Enable Detailed Tracking Audit Policy
- ✓ Enable Logon-Logoff Audit Policies Show Details
- ✓ Enable Policy Change Audit Policies Show Details
- ✓ Enable Privelege Use Audit Policy
- ✓ Enable System Audit Policies Show Details

END LAB

LAB Enable Device Logs

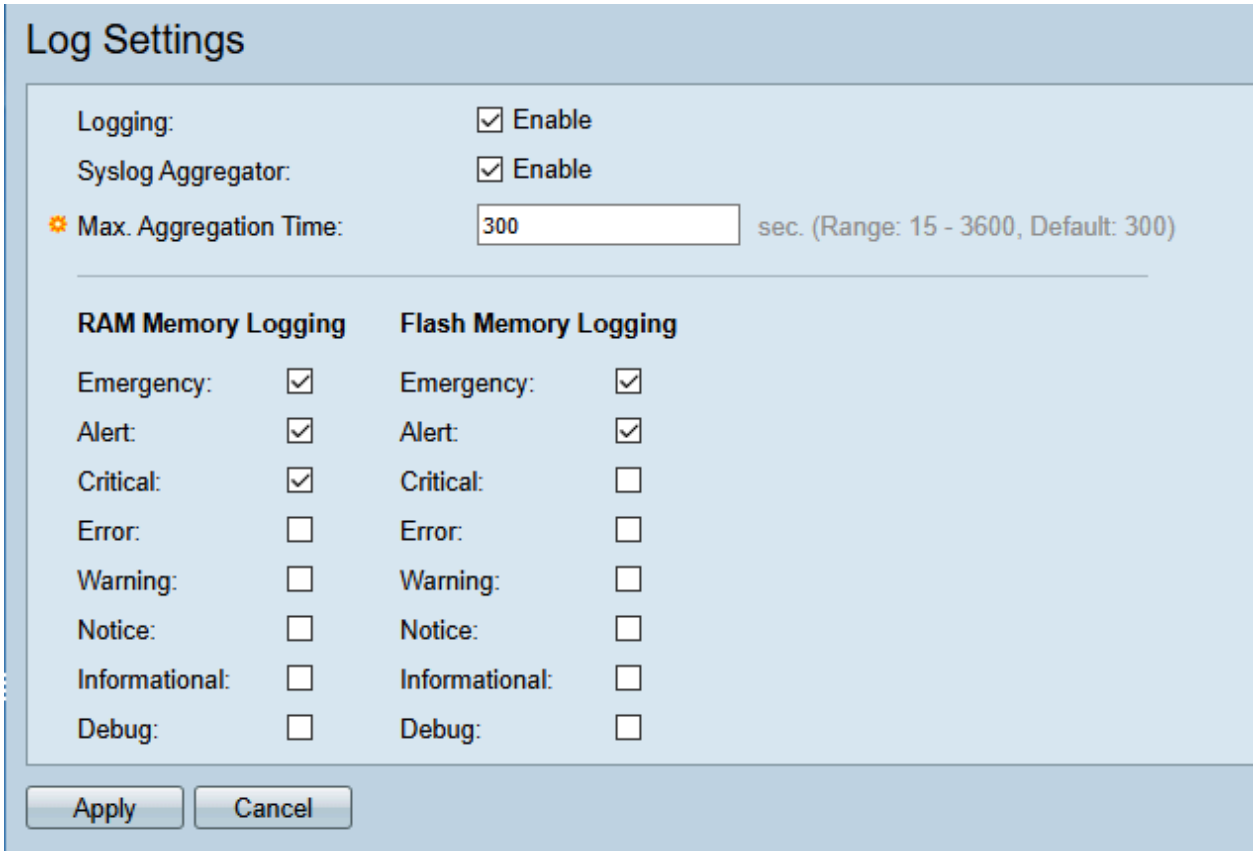
You are the IT security administrator for a small corporate network. You need to enable logging on the switch in the networking closet.

In this lab, your task is to:

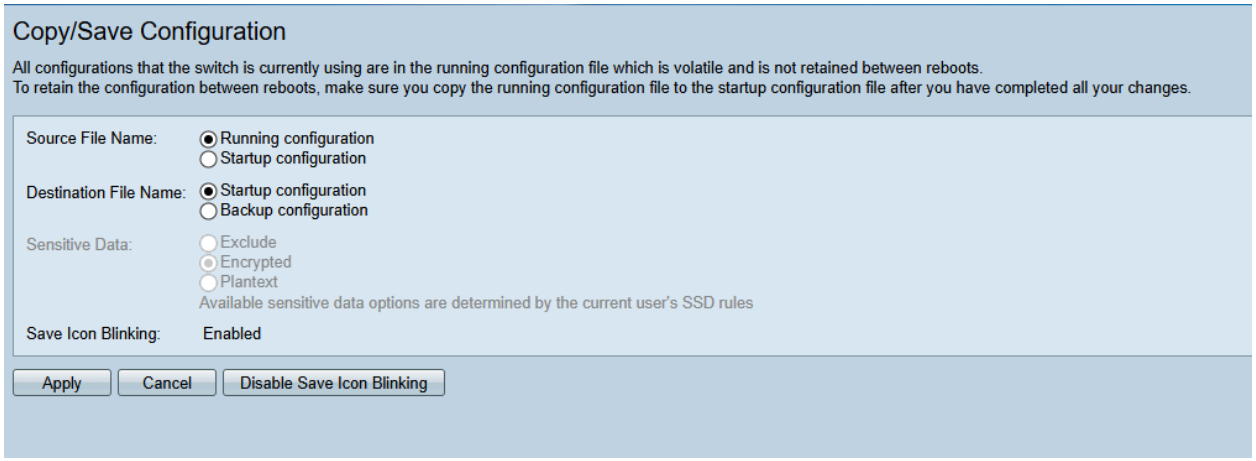
- Enable logging and the Syslog Aggregator.
- Configure RAM Memory Logging as follows:
    - Emergency, Alert, and Critical: **Enable**
    - Error, Warning, Notice, Informational, and Debug: **Disable**

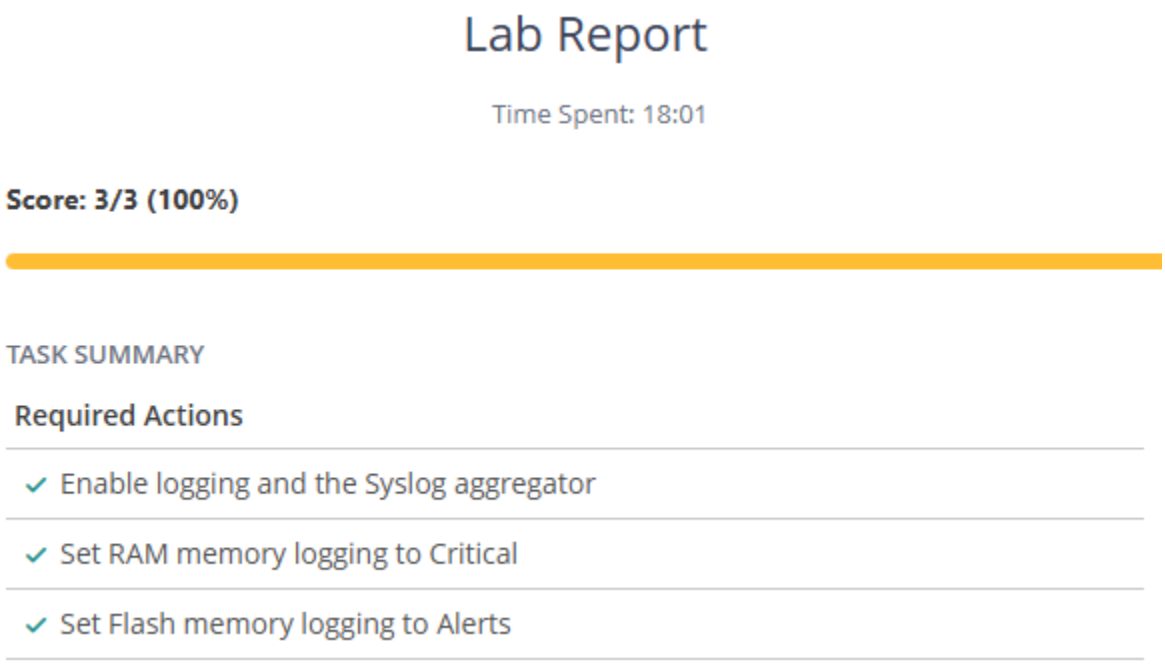
- Configure Flash Memory Logging as follows:
    - Emergency and Alert: **Enable**
    - Critical, Error, Warning, Notice, Informational, and Debug: **Disable**
- Copy the running configuration file to the startup configuration file using the following settings:
    - Source File Name: **Running configuration**
    - Destination File Name: **Startup configuration**

Enable logging and Syslog Aggregator, configure RAM memory logging and Flash memory logging:



Copy the running config file to the startup config file using the settings provided:





END LAB

LAB Create Virtual Machines

You have installed Hyper-V on ITAdmin. You're experimenting with creating virtual machines.

In this lab, your task is to create two virtual machines named VM1 and VM2. Use the following settings as specified for each machine:

VM1:

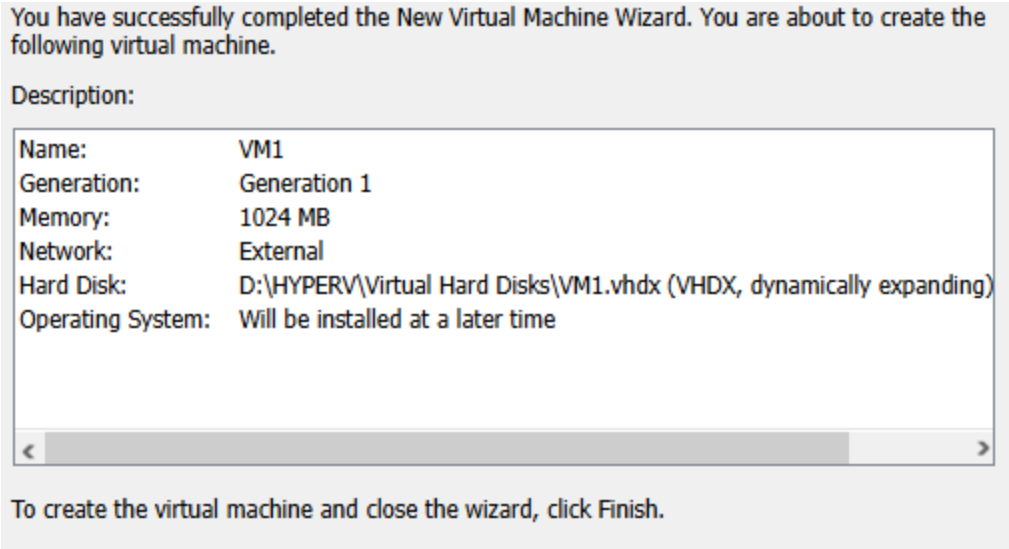
- Virtual machine name: **VM1**

- Virtual machine location: **D:\HYPERV**
- Generation: **Generation 1**
- Startup memory: **1024 MB** (do not use dynamic memory)
- Networking connection: **External**
- Virtual hard disk name: **VM1.vhdx**
- Virtual hard disk location: **D:\HYPERV\Virtual Hard Disks**
- Virtual hard disk size: **50 GB**
- Operating system will be installed later

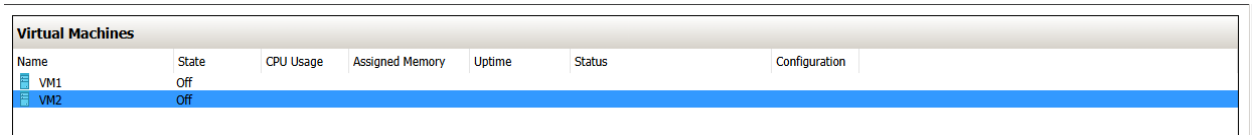
VM2:

- Virtual machine name: **VM2**
- Virtual machine location: **D:\HYPERV**
- Generation: **Generation 1**
- Startup memory: **2048 MB** (use dynamic memory)
- Networking connection: **Internal**
- Virtual hard disk name: **VM2.vhdx**
- Virtual hard disk location: **D:\HYPERV\Virtual Hard Disks**
- Virtual hard disk size: **250 GB**
- Operating system will be installed later
- Minimum RAM: **512 MB**
- Maximum RAM: **4096 MB**

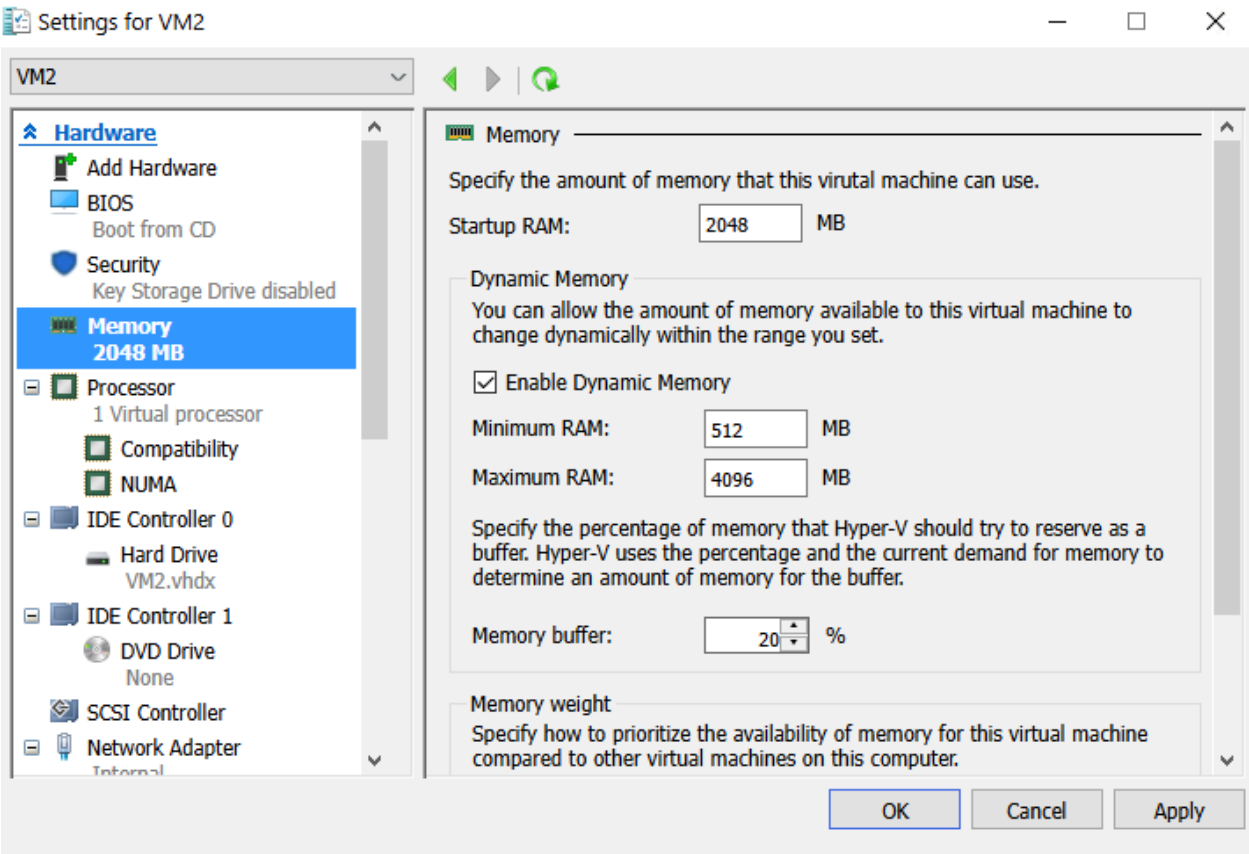
Creating VM1:

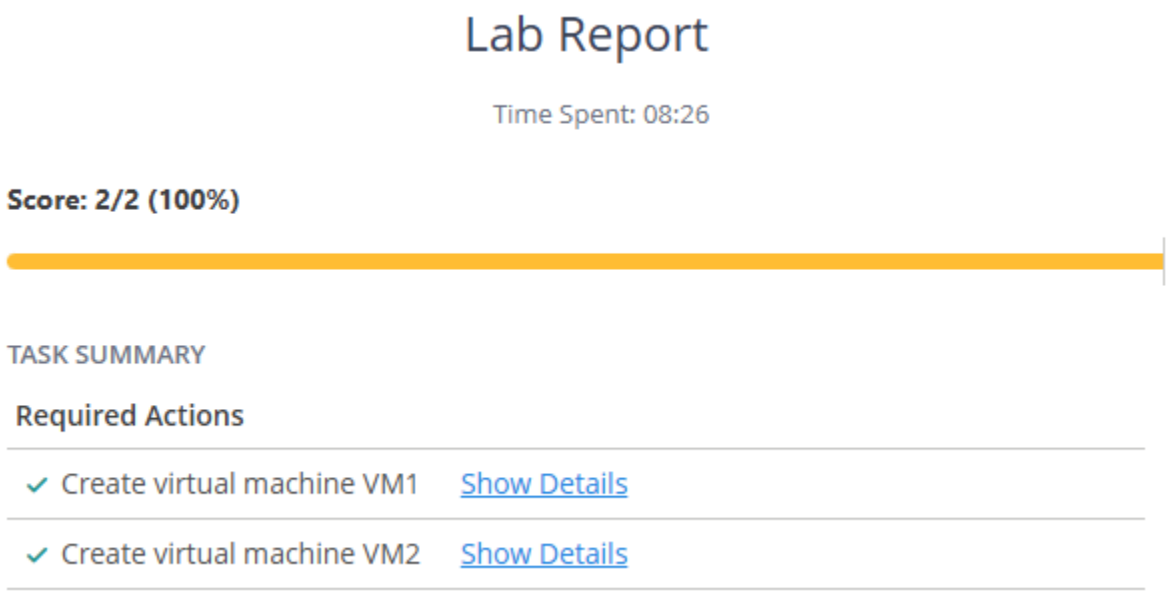


Creating VM2:



Setting min and max RAM for VM2:





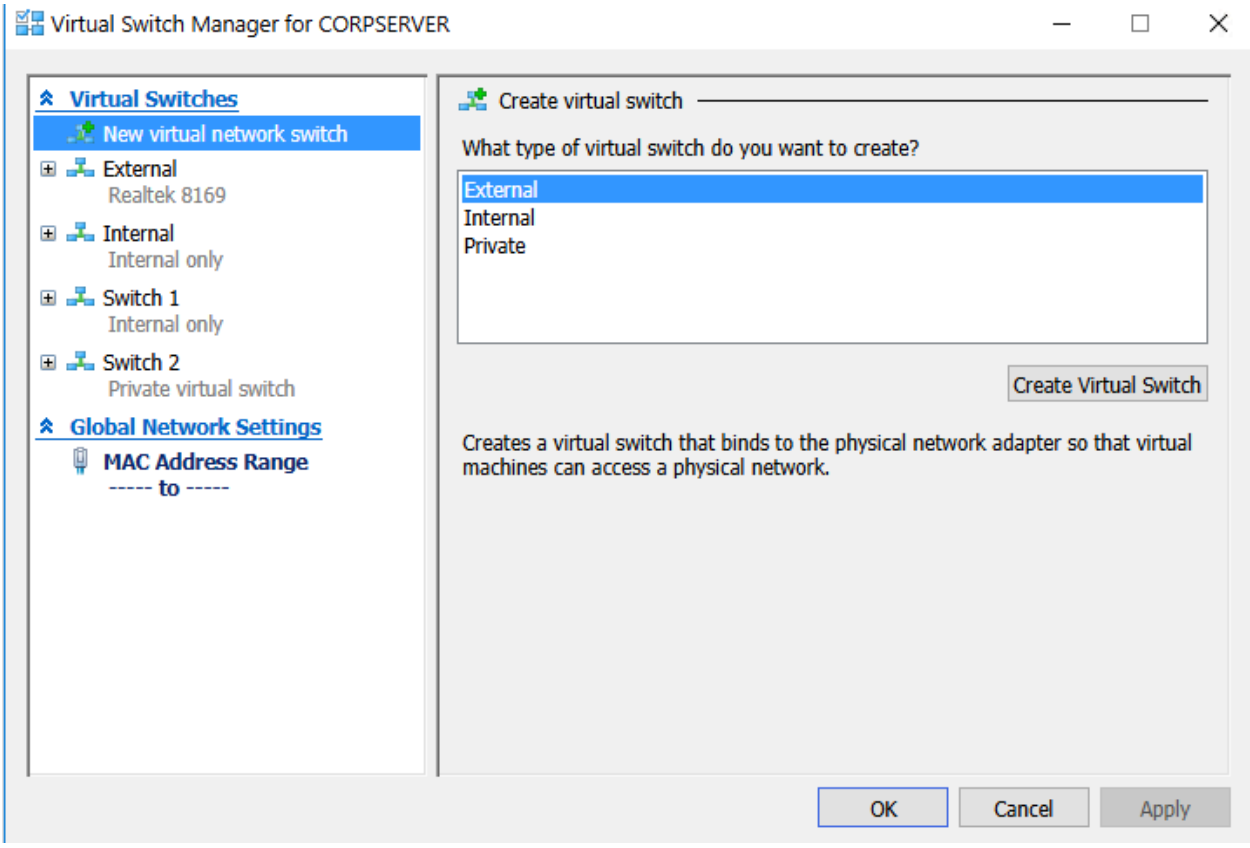
END LAB

LAB Create Virtual Switches

You have installed Hyper-V on the CorpServer server. You want to use the server to create virtual machines. Prior to creating the virtual machines, you are experimenting with virtual switches.

In this lab, your task is to:

- Create an internal virtual switch named *Switch 1.*
- Create a private virtual switch named *Switch 2.*



Lab Report

Time Spent: 02:06

Score: 2/2 (100%)

TASK SUMMARY

Required Actions

✓ Create the Switch 1 virtual switch	Show Details
✓ Create the Switch 2 virtual switch	Show Details

END LAB

LAB Secure an iPad

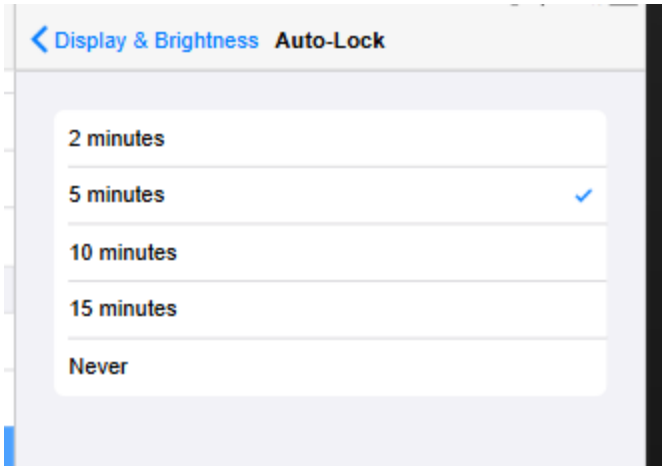
You work as the IT security administrator for a small corporate network. The receptionist uses an iPad to manage employees' schedules and messages. You need to help her secure the iPad because it contains all of the employees' personal information.

In this lab, your task is to:

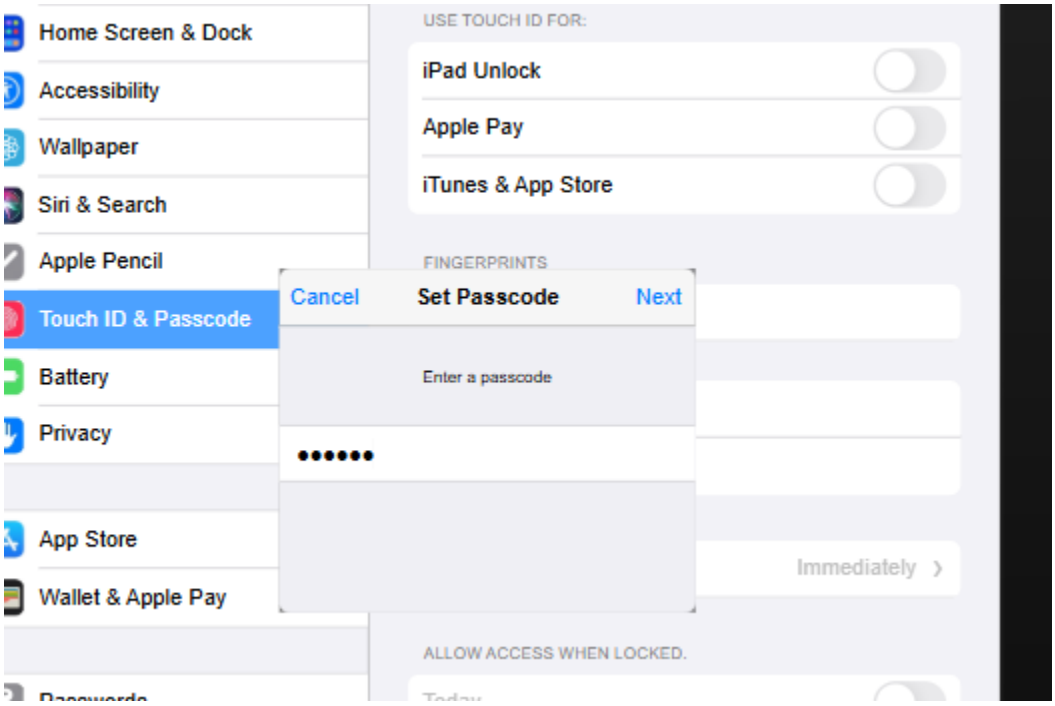
- View the current iOS version and then answer the applicable question.
- Apply the latest software update and then answer the applicable question.
- Configure Auto-Lock with a five-minute delay.
- Configure Passcode Lock using a passcode of **C@sp3r**
- Require the passcode after five minutes.
- Configure Data Erase to wipe all data after 10 failed passcode attempts.
- Require unknown networks to be added manually.
- Turn off Bluetooth.

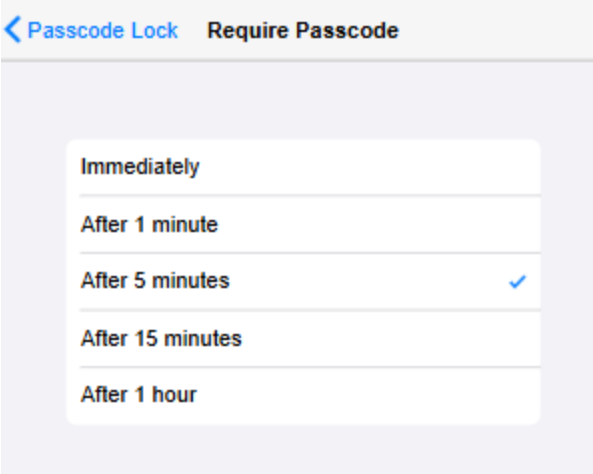
Since an update is easy to perform, I skipped documenting the process.

Configure auto-lock:

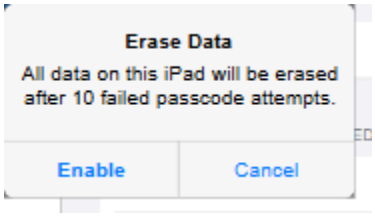


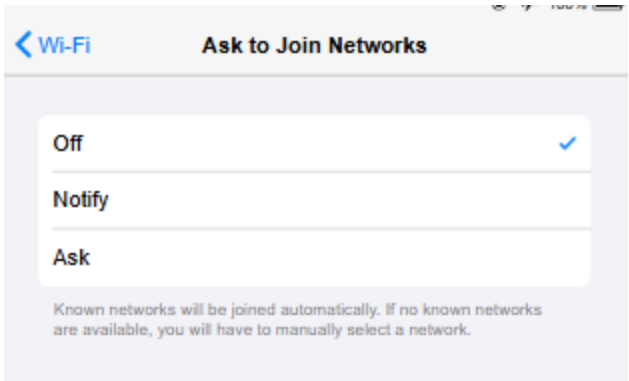
Configure passcode lock:

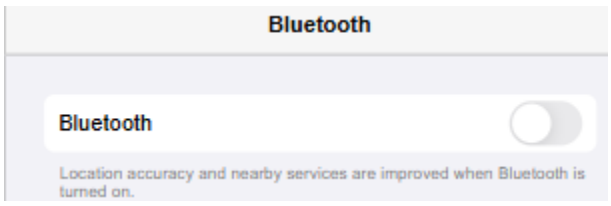




Enable erase data:







Lab Report

Time Spent: 09:45

Score: 8/8 (100%)

TASK SUMMARY

Required Actions & Questions

- ✓ *Q1*: Which version of iOS is currently running?
  - Your answer: 15.2
  - Correct answer: 15.2
- ✓ Apply the latest IOS update
- ✓ *Q2*: Which version of iOS is installed after the update?
  - Your answer: 15.2.1
  - Correct answer: 15.2.1
- ✓ Set Auto-Lock to 5 minutes
- ✓ Enable a passcode Show Details
- ✓ Enable data erase
- ✓ Turn off Ask to Join Networks
- ✓ Turn off Bluetooth

END LAB

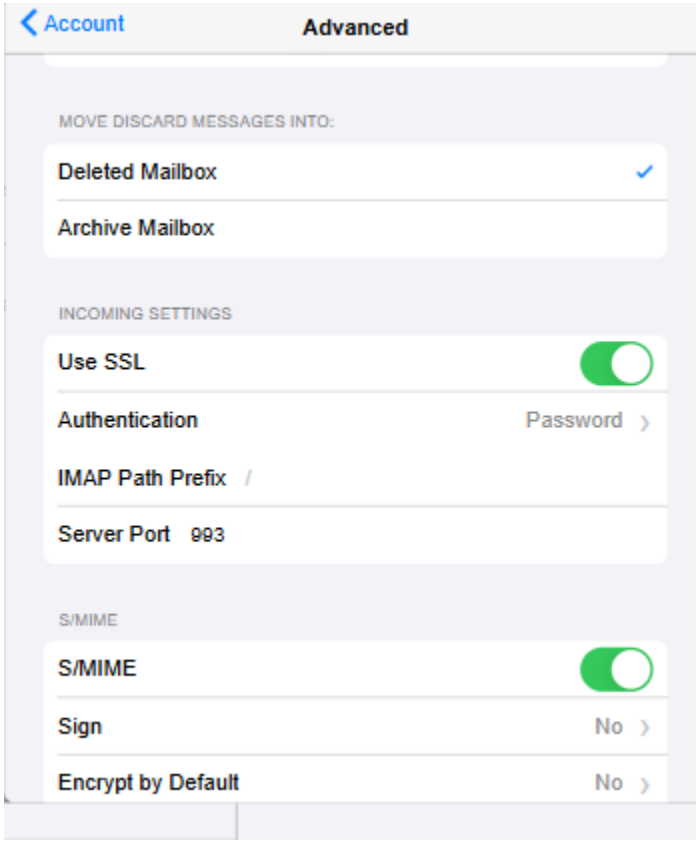
LAB Secure Email on Ipad

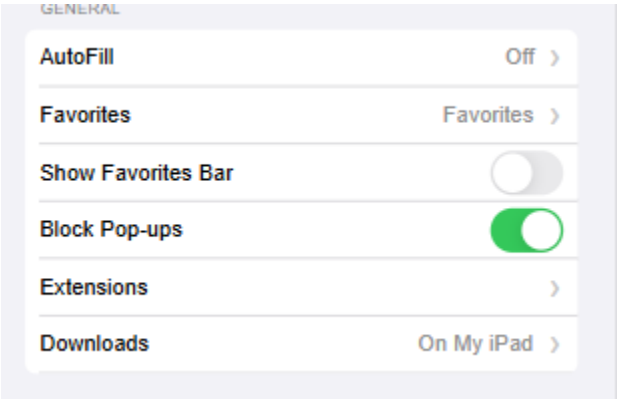
You work as the IT security administrator for a small corporate network. The receptionist, Maggie Brown, uses an iPad to manage employee schedules and messages. You need to help her secure her email and browser on her iPad.

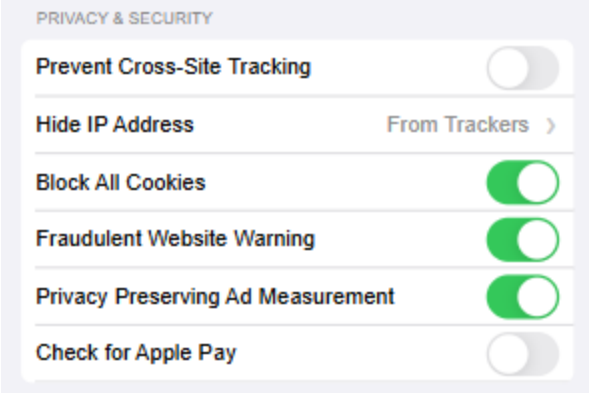
In this lab, your task is to complete the following:

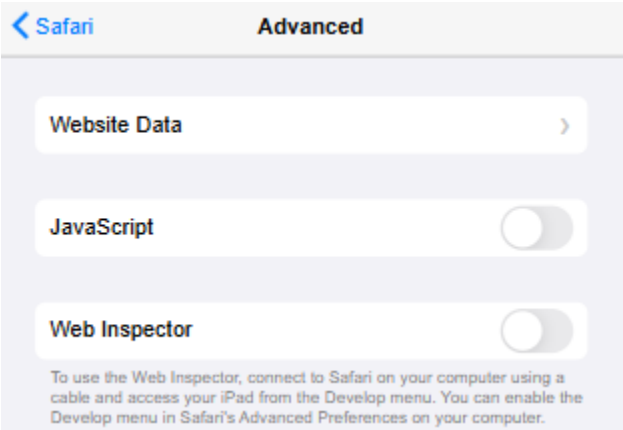
- Configure Maggie's email account to use SSL for incoming mail.

- Secure the internet browser as follows:
    - Turn off AutoFill
    - Turn on Block Pop-ups
    - Block all cookies
    - Turn on Fraudulent Website Warning
    - Turn off JavaScript









Lab Report

Time Spent: 07:46

Score: 5/5 (100%)

TASK SUMMARY

Required Actions

- ✓ Configure the Maggie Brown email account for SSL
- ✓ Turn off AutoFill on Safari Show Details
- ✓ Turn on Fraud Warning
- ✓ Turn off JavaScript
- ✓ Turn on Block Pop-ups

END LAB

LAB BACKUP FILES WITH FILE HISTORY

You have recently installed a new Windows 10 computer. To protect valuable data, you need to implement file history backups on this computer.

In this lab, your task is to configure automatic backups for the Exec computer as follows:

- Save the backup to the **Backup (E:)** volume.
- Back up files **daily**.
- Keep backup files for **six months**.
- Back up the entire **Data (D:)** volume.
- Make a backup now.

Settings

Backup options

Overview

Size of backup: 5.68 MB

Total space on Backup (E:): 549 GB

Last backup: 12/02/2024 08:54 PM

Back up now

Back up my files

Daily

Keep my backups

6 months

Back up these folders

Add a folder

Data (D:)
D:\

Exclude these folders

Add a folder

Lab Report

Time Spent: 00:58

Score: 5/5 (100%)

TASK SUMMARY

Required Actions

- ✓ Save the backup to the Backup (E:) Volume
- ✓ Back up files daily
- ✓ Keep backup files for six months
- ✓ Back up the entire Data (D:) volume
- ✓ Make a backup now

END LAB

LAB Recover a File from File History

Susan produces your organization's monthly magazine. While working on an upcoming issue, Susan accidentally deleted significant portions of the layout image. She also made extensive changes to the cover artwork but has now been asked to discard the changes and use the original artwork.

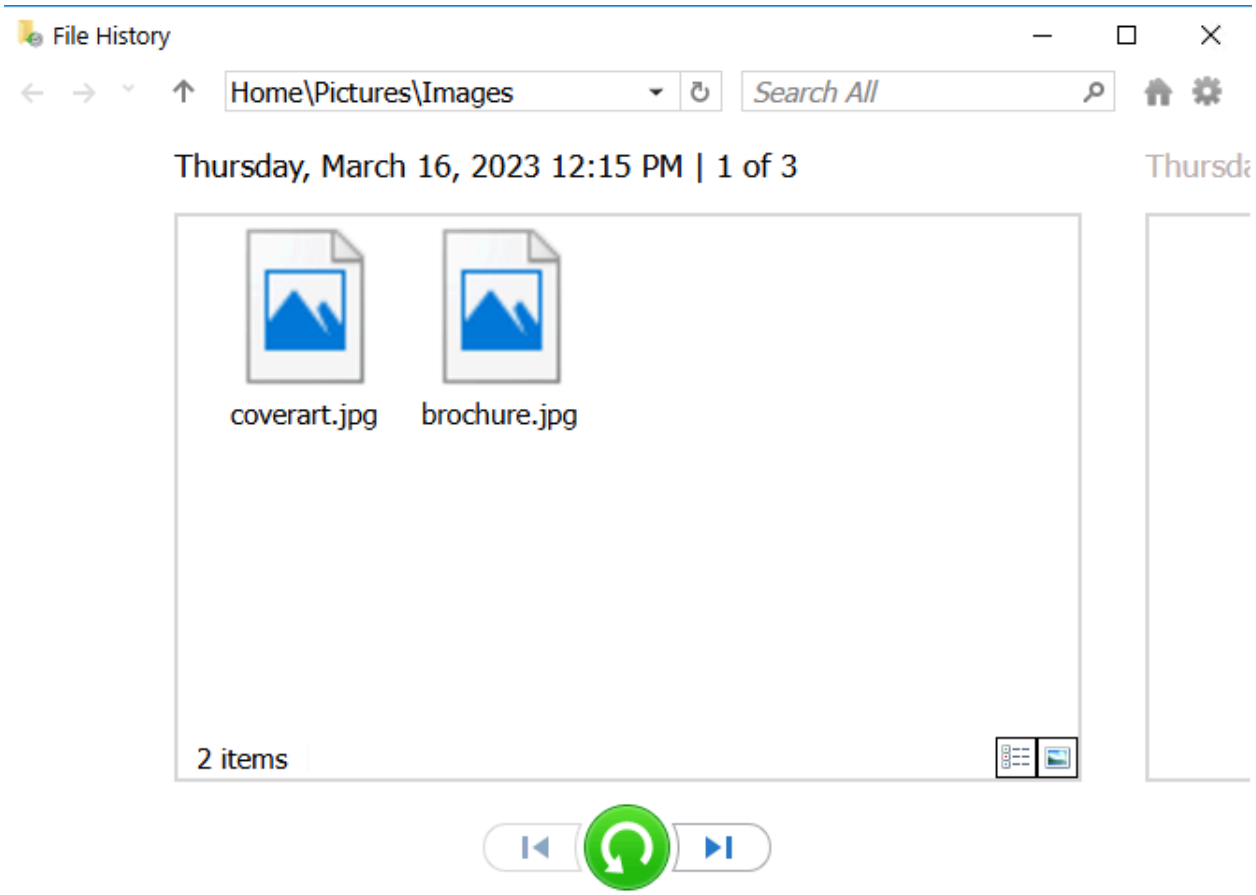
Susan has asked you to help her recover older versions of her files in the Pictures library so she can still meet her publishing deadline.

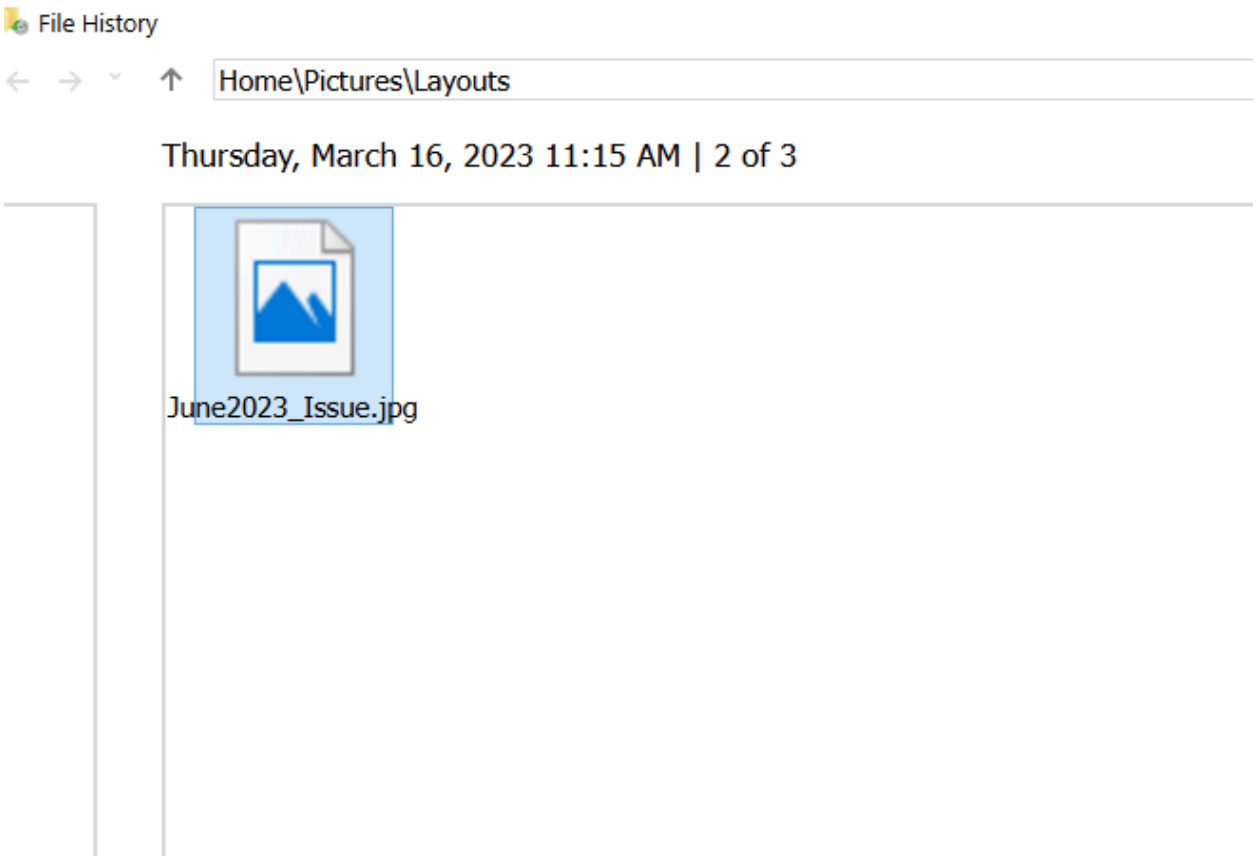
In this lab, your task is to complete the following:

- Using the Settings app, access the program needed to restore files from a current backup.
- From the File History dialog, restore the following files:

File	File Version to Restore

Pictures\Layouts\June2023_Issue.jpg	Thursday, March 16, 2023 11:15 AM
Pictures\Images\coverart.jpg	Thursday, March 16, 2023 12:15 PM





Lab Report

Time Spent: 02:09

Score: 2/2 (100%)

TASK SUMMARY

Required Actions

- ✓ Restore the March 16th at 11:15 AM version of June2023_Issue.jpg
- ✓ Restore the March 16th at 12:15 PM version of coverart.jpg

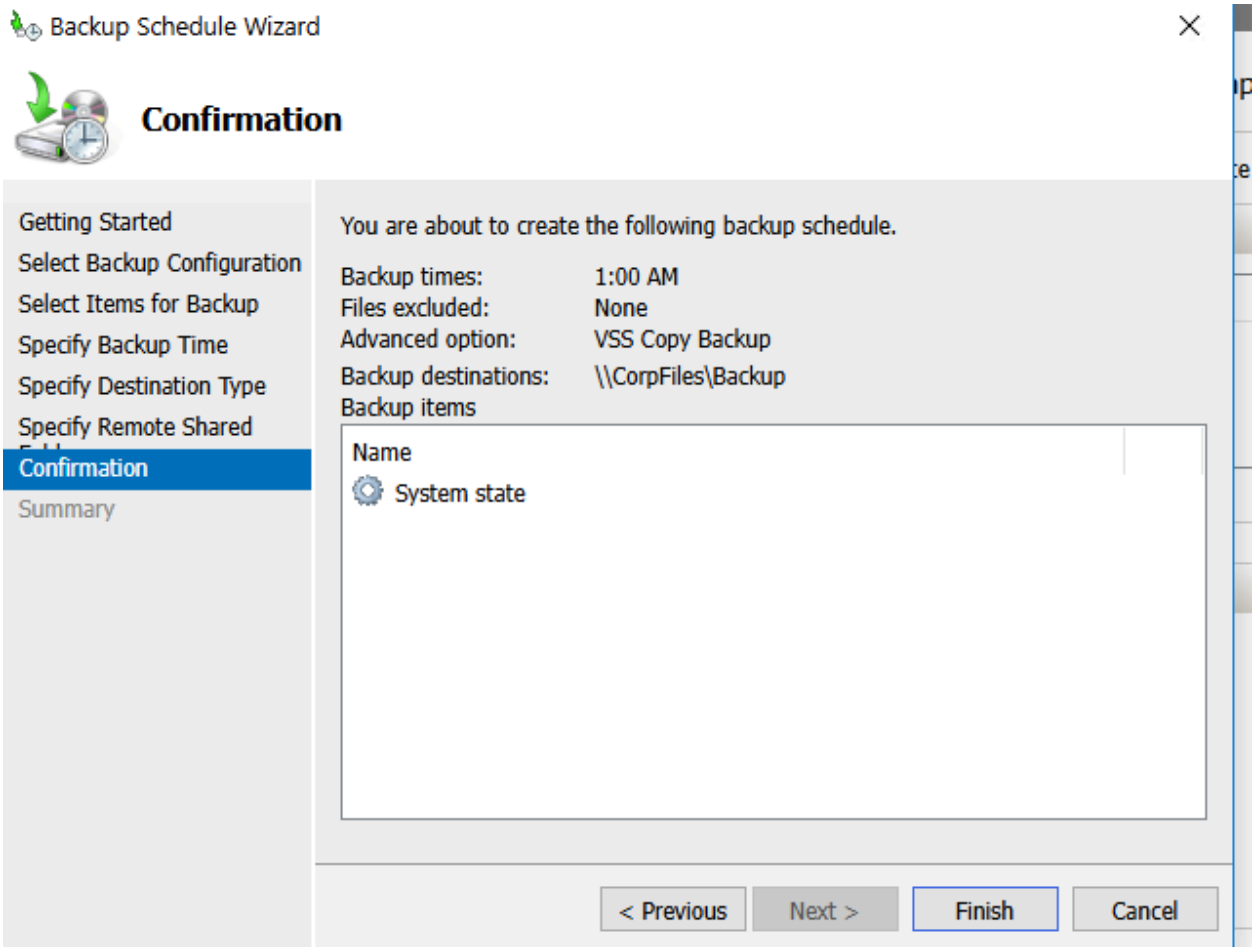
END LAB

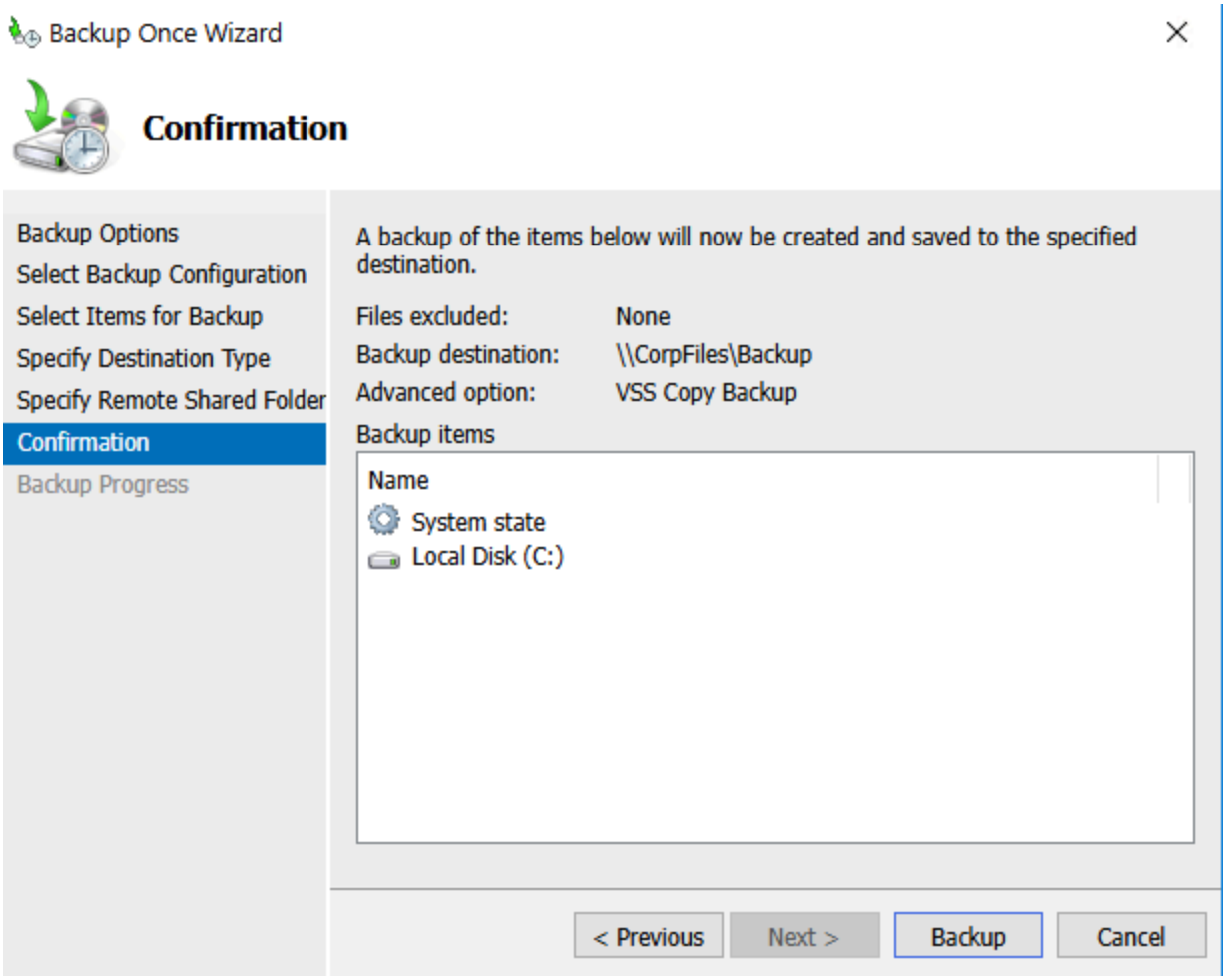
LAB Backup a Domain Controller

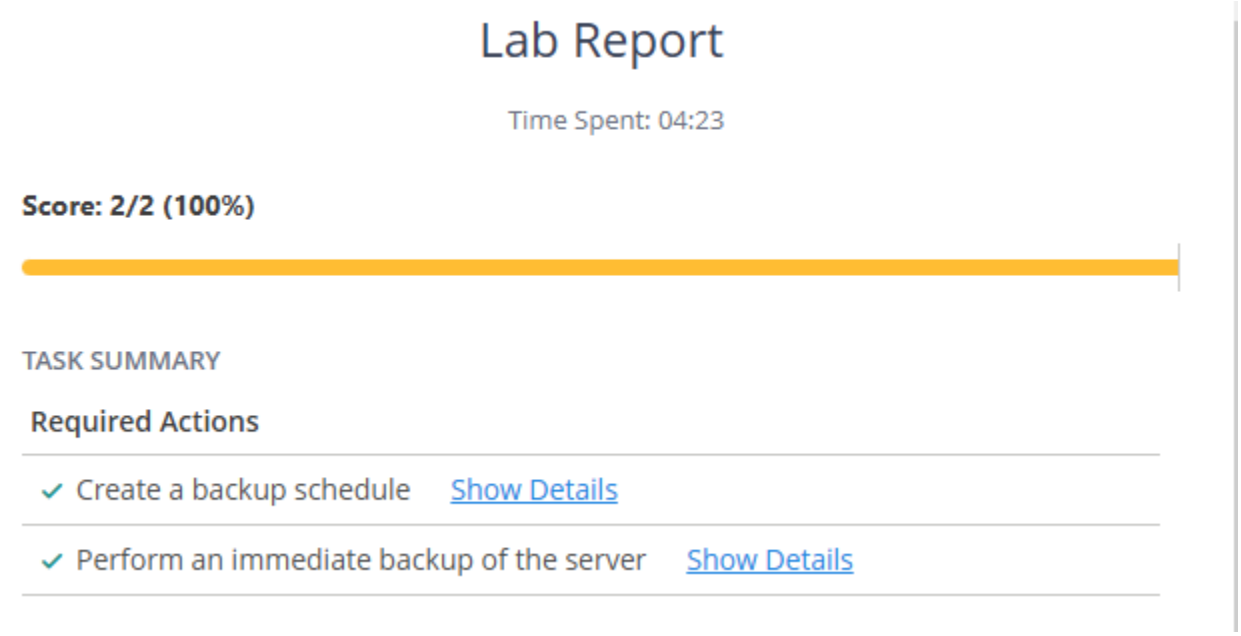
You are the IT administrator for a small corporate network. You need to back up the system state of your domain controllers so that, in the event of a disaster, Active Directory is backed up. You want to configure regular backups on CorpDC4.

In this lab, your task is to perform the following using Windows Server Backup on CorpDC4:

- Create a regular backup schedule for the CorpDC4 server using the following settings:
    - Backup items: **System State**
    - Backup schedule: **once per day at 1:00 a.m.**
    - Backup location: **\\CorpFiles\Backup**
- Take an immediate backup using the following settings:
    - Backup items: **System State and C: drive**
    - Backup location: **\\CorpFiles\Backup**




Backup Once Wizard
Confirmation
Backup Options
Select Backup Configuration
Select Items for Backup
Specify Destination Type
Specify Remote Shared Folder
Confirmation
Backup Progress
A backup of the items below will now be created and saved to the specified destination.
Files excluded: None
Backup destination: \\CorpFiles\Backup
Advanced option: VSS Copy Backup
Backup items
Name
System state
Local Disk (C:)
< Previous
Next >
Backup
Cancel


Lab Report
Time Spent: 04:23
Score: 2/2 (100%)
TASK SUMMARY
Required Actions
Create a backup schedule
Show Details
Perform an immediate backup of the server
Show Details

END LAB