ADAM GATHERER
MAGIC MEMORIES
SECURITY UPGRADE
2: DEVELOPMENT
JANUARY 2021 - MAY 2021

CONTENTS

2.0 - BACKGROUND

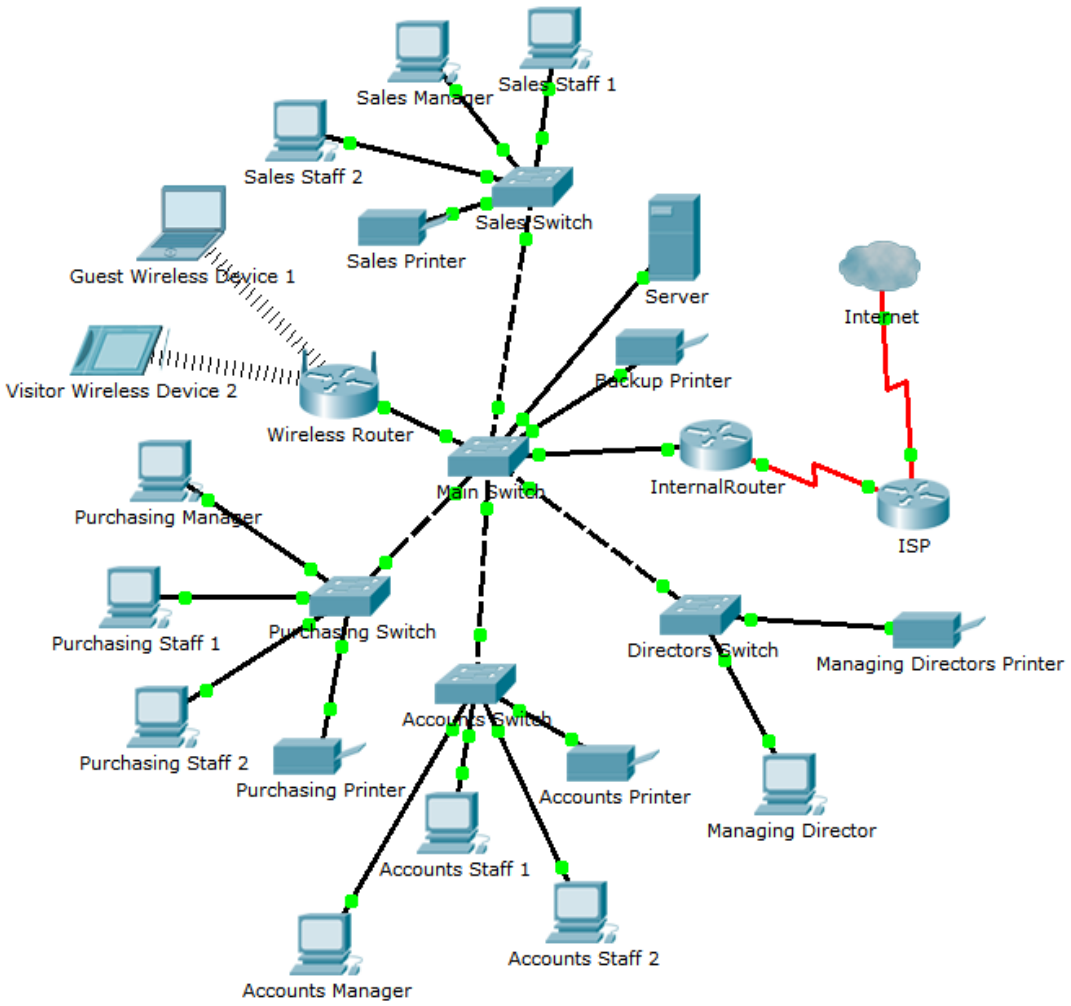
Continuing from the previous section, the planning stage, this section will cover the implementation of the security recommendations laid out in section 1.1.9. A copy of this table is included below as *fig i*.

NETWORK SECURITY	**RECOMMENDED**	**IMPLEMENTED**
Subnet the network		X
Implement VLANs per department		X
Set management passwords on the routers/switches		X
Purchase a hardware firewall		X
Implement ACLs		X
Restrict open network interfaces		X
Implement NAT on the ISP router		X
Harden wireless network		X
Use WPA2-AES		X
Limit DHCP lease time		X
Move antennae	X	
COMPLIANCE AND OPERATIONAL SECURITY	**RECOMMENDED**	**IMPLEMENTED**
Create a privacy policy	X	
Forbid use of personal devices	X	
Forbid use of social media on company network	X	
Implement a disaster plan	X	
Weekly local backups		X
Configure RAID for important data storage	X	
Monthly off-site backup for recovery	X	
Implement a clear desk policy	X	
Ensure Fire suppression system is in place if needed	X	
Install security cameras in server room & entryway	X	
Use cables with EMI shielding		X
THREATS AND VULNERABILITIES	**RECOMMENDED**	**IMPLEMENTED**
Purchase anti-malware software		X
Develop DDoS response plan	X	
List of assets to implement	X	
Response team	X	
Notification procedures	X	
List of on-site and off-site contacts	X	
Foster staff awareness of social attacks	X	
Configure switchport security		X
MAC filtering		X
Disable unused switchports		X
Implement policy of staff having ID badges visible at all times	X	
Require off-site visitors to display ID badges	X	
Keep access, events, and security logs		X
Purchase privacy filters for staff in open areas		X
Purchase shredder for secure disposal of documents	X	
Only permit use of company wireless network when on-site	X	
Implement physical security changes	X	
Harden doors (locking hinges, rotate handles)	X	
Install window restrictors	X	
Install smart card entry system	X	

APPLICATION, DATA AND HOST SECURITY	RECOMMENDED	IMPLEMENTED
Purchase and install anti-malware software		X
Lock network cabinets	X	
Encrypt hard disks		X
Implement screen locking policy when employees away from desk		X
Purchase and install cable locks for computers	X	
ACCESS CONTROL AND IDENTITY MANAGEMENT		
Harden authentication means for sensitive areas		
Biometric authentication for server room	X	
Implement password policy changes		X
Lockout after incorrect guesses		X
Passphrases rather than passwords		X
Remove mandatory password changes	X	

Fig i, the security recommendations table.

The items marked in this table with a X under “IMPLEMENTED” will be the changes made to the network.



The current network topology

2.1 - INTRODUCTION

In this section of the report we will be looking at the development of the prototype network. Here, the security recommendations outlined in the previous section will be implemented and tested. The implementation will be documented.

To begin, I will provide a summary of the previous section. The computer network at Magic Memories is lacking in five areas of security. Network security, compliance and operational security, threats and vulnerabilities, application, data and host security, and access control and identity management. The recommendations to fix these areas are as follows:

Network Security

Subnet the network, implement VLANs as per the department structure, configuring management passwords on the routers and switches, implementing a hardware firewall, setting up ACLs, restricting open ports, configuring NAT on the ISP router, hardening the wireless network with WPA2-AES and limiting the DHCP lease time.

Compliance and Operational Security

The majority of recommendations in this area are just that, recommendations. The only changes being implemented by myself here are the configuring of weekly backups and the use of cables with EMI shielding. If there is enough time some of the recommendations may be implemented (RAID configuration, creation of a privacy policy etc.)

Threats and Vulnerabilities

Purchasing and installing anti-malware software, configuring switchport security, setting up MAC filtering, disabling unused switchports, keeping access, events and security logs, and purchasing privacy filters for computers in open areas.

Application, Data and Host Security

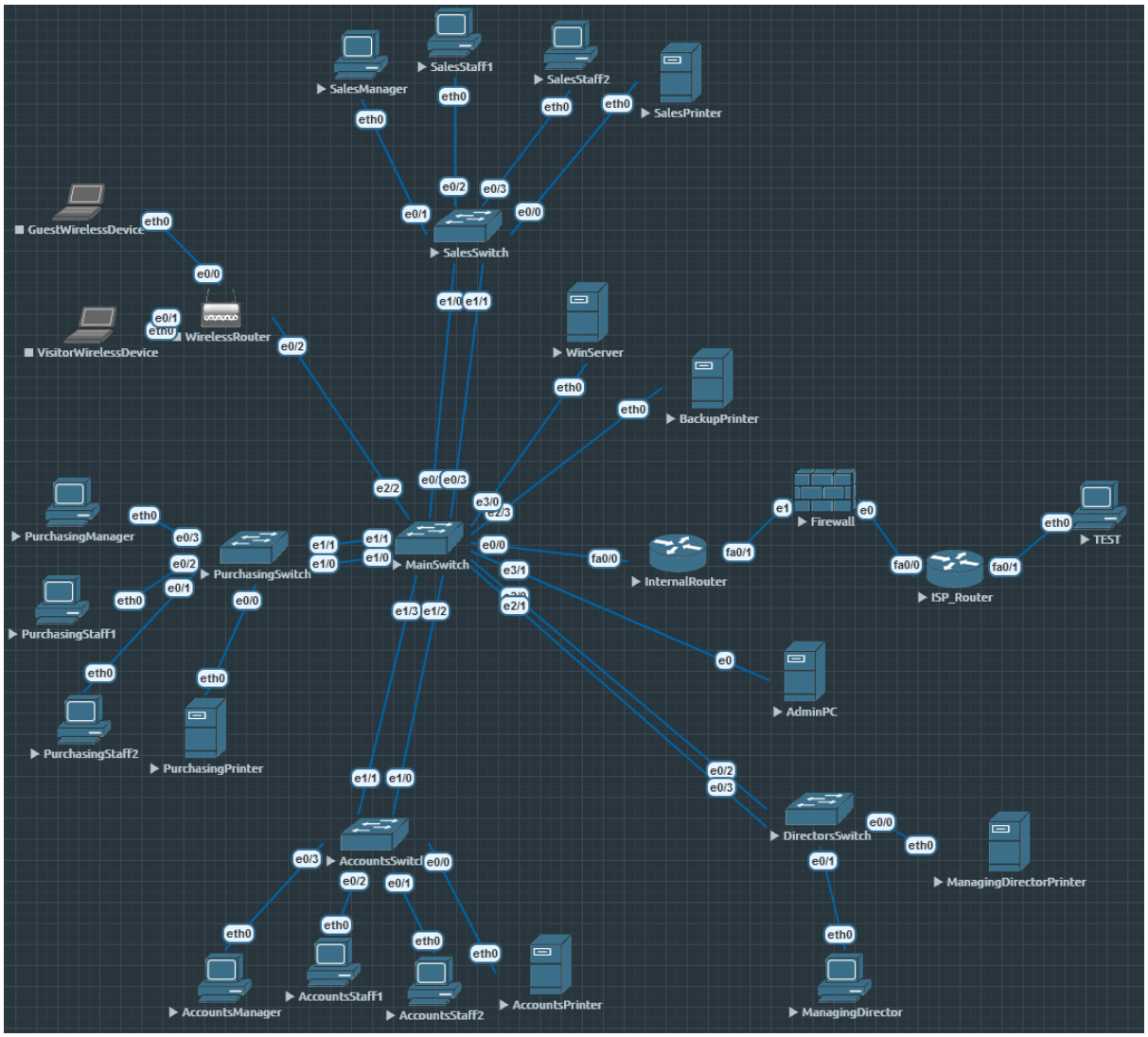
Purchasing and installing anti-malware software, encrypting hard disks, and implementing a screen locking policy.

Access Control and Identity Management

Password policy changes, lockout after incorrect guesses, and changing from passwords to passphrases.

2.2 - IMPLEMENTATION

In this section I will be implementing, documenting, testing, and justifying the changes made to the computer network. This will be conducted section by section for the five areas of security.



The completed proposed changes

2.2.1 - NETWORK SECURITY

Subnet the Network

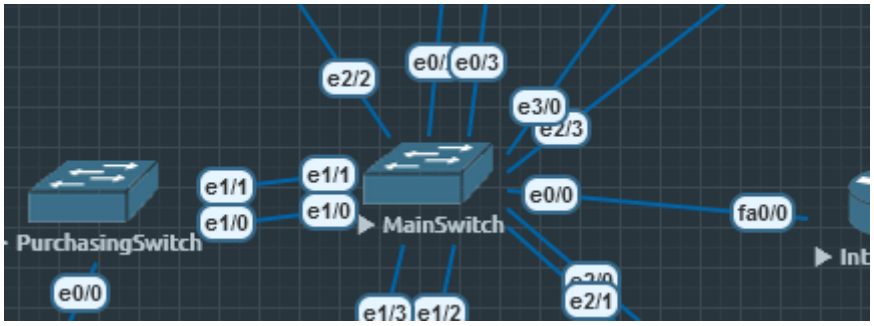
This prevents devices from seeing the whole network as well as accessing it without going through the internal router.[1] In combination with ACLs this is an incredible bolstering of security. Additionally, splitting the network into subnets will limit the broadcast domain which protects against ARP spoofing.[2]

This is achieved by using the following network addressing scheme:

SUBNET	DEVICE	IP ADDRESS
Sales		10.0.10.0/24
VLAN 10	SalesManager	10.0.10.11/24
	SalesStaff1	10.0.10.12/24
	SalesStaff2	10.0.10.13/24
	SalesPrinter	10.0.10.8/24
	InternalRT:fa0/0.10	10.0.10.1/24
Purchasing		10.0.20.0/24
VLAN 20	PurchasingManager	10.0.20.11/24
	PurchasingStaff1	10.0.20.12/24
	PurchasingStaff2	10.0.20.13/24
	PurchasingPrinter	10.0.20.8/24
	InternalRT:fa0/0.20	10.0.20.1/24
Accounting		10.0.30.0/24
VLAN 30	AccountingManager	10.0.30.11/24
	AccountingStaff1	10.0.30.12/24
	AccountingStaff2	10.0.30.13/24
	AccountingPrinter	10.0.30.8/24
	InternalRT:fa0/0.30	10.0.30.1/24
Director		10.0.40.0/24
VLAN 40	ManagingDirector	10.0.40.11/24
	ManagingDirectorPrinter	10.0.40.8/24
	InternalRT:fa0/0.40	10.0.40.1/24
Server		
VLAN 50	WindowsServer	10.0.50.11/24
	DebianServer	10.0.50.12/24
	BackupPrinter	10.0.50.8/24
	InternalRT:fa0/0.50	10.0.50.1/24
Wireless		
VLAN 60	Wireless DHCP Pool	10.0.60.10 - 10.0.60.30/24
	Wireless Router	
Firewall		
	InternalRT:fa0/1	10.0.100.1/24
	Firewall:e1	10.0.100.10/24

ISP		
	ISProuter:f0/0	10.0.200.1/24
	ISProuter:f0/1	192.168.10.1/24
	Firewall:e2	10.0.200.10/24
Note: TEST represents connection to external networks and can be considered the same as the internet	TEST	192.168.10.10/24
Management		
	InternalRT:fa0/0.101	10.0.101.1/24
	MainSwitch vlan 101	10.0.101.2/24

Combining Ports with Etherchannel



This section takes place on MainSwitch

Doubling up on connections between the Main Switch and the department switches provides efficiency, increased bandwidth, and redundancy which strengthens the network. The process is demonstrated below on the Main Switch and the Sales Switch.

```
MainSW(config)#int range e0/2 -3
MainSW(config-if-range)#switchport
MainSW(config-if-range)#switchport mode access
MainSW(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
MainSW(config-if-range)#channel-group 10 mode auto
Creating a port-channel interface Port-channel 10

MainSW(config-if-range)#
```

Selecting the interfaces connecting to the Sales Switch, putting them in access mode, setting them up to carry VLAN 10 [VLANS] and combining them into Port-Channel 10. The mode is set to 'auto' to receive PAgP packets.

```
SalesSW(config)#int range e1/0 -1
SalesSW(config-if-range)#switchport mode access
SalesSW(config-if-range)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
SalesSW(config-if-range)#channel-group 10 mode desirable
Creating a port-channel interface Port-channel 10

SalesSW(config-if-range)#
```

The process is repeated on the other end (Sales Switch) with the channel-group mode set to desirable so that it actively attempts to negotiate a PagP connection.

This process is repeated for all connections between the Main Switch and the department switches and Internal Router, changing the carried VLAN [VLANS] and channel-group to the appropriate values.

Configuring VLANs For Each Department

This section is demonstrated on SalesSwitch, but applies to all department switches.

The setup for the virtual local area networks is outlined in *fig i*, found in the section on subnetting. This is configured on the switches, as shown below.

VLANs reduce the broadcast domains to a single department, meaning broadcasts are not sent through the main router (and the rest of the network). This will reduce traffic congestion and prevent broadcasts being received by devices they are not intended for. This is often exploited by ARP spoofing attacks. [3]

```
SalesSW(config)#int range e0/0 -3
SalesSW(config-if-range)#switchport mode access
SalesSW(config-if-range)#switchport access vlan 10
SalesSW(config-if-range)#
```

Selecting the range of interfaces facing the Sales Department devices, setting their switchport mode to 'access' (to carry a single VLAN) and configuring the VLAN they will carry to VLAN 10. This process is repeated on all department switches for the appropriate VLANs.

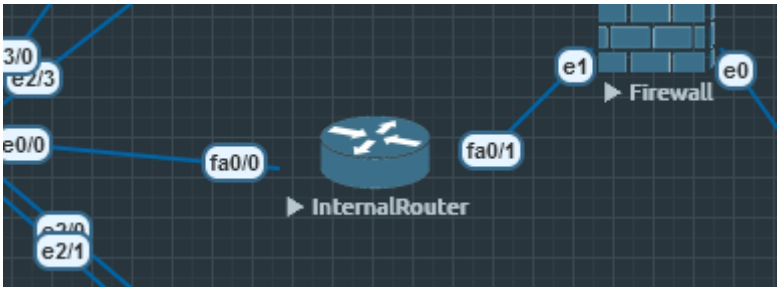
```
DirectorsSwitch
DirectorSW(config)#do show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
40   Directors Department             active    Et0/0, Et0/1, Po40
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ---------------- ----------------------------------------

DirectorSW(config)#
```

The completed VLAN table on the Directors Department Switch

```
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,40,50,60
 switchport mode trunk
 duplex auto
 channel-group 1 mode auto
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,40,50,60
 switchport mode trunk
 duplex auto
 channel-group 1 mode auto
!
interface Ethernet0/2

MainSW(config)#
```

The port on the Main Switch leading to the router is configured in trunk mode to carry all VLANs. This will is required for 'router on a stick' configuration.

Configuring Router on A Stick



This section takes place on the InternalRouter

To allow for communication between the different VLANs a 'Router on A Stick' setup will have to be configured. This involves setting up sub-interfaces on the router interface facing the network and setting the dot1q encapsulation for each VLAN.

```
InternalRT(config)#int fa0/0.20
InternalRT(config-subif)#encaps
InternalRT(config-subif)#encapsulation dot1q 20
InternalRT(config-subif)#ip address 10.0.20.1 255.255.255.0
InternalRT(config-subif)#
```

Selecting the sub-interface facing the main switch, assigning it encapsulation for a VLAN, and giving the sub-interface an IP address so it can function as a default gateway. This process is repeated for all VLANs and sub-interfaces.

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.0.10.1 255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.0.20.1 255.255.255.0
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.0.30.1 255.255.255.0
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 10.0.40.1 255.255.255.0
!
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 10.0.50.1 255.255.255.0
!
interface FastEthernet0/0.60
 encapsulation dot1Q 60
 ip address 10.0.60.1 255.255.255.0
```

The running config of the Internal Router, showing the sub-interfaces with their encapsulation and IP addresses.

Once configured the simplest way to test this is to have a client device from one subnet ping its default gateway (the corresponding router sub-interface) and then ping a device in a different subnet.

```
VPCS> ip 10.0.30.13/24 10.0.30.1
Checking for duplicate address...
PC1 : 10.0.30.13 255.255.255.0 gateway 10.0.30.1

VPCS> ping 10.0.30.1

84 bytes from 10.0.30.1 icmp_seq=1 ttl=255 time=9.678 ms
84 bytes from 10.0.30.1 icmp_seq=2 ttl=255 time=9.102 ms
^C
VPCS> ping 10.0.10.11

84 bytes from 10.0.10.11 icmp_seq=1 ttl=63 time=24.949 ms
84 bytes from 10.0.10.11 icmp_seq=2 ttl=63 time=14.997 ms
^C
VPCS>
```

Setting the IP address for AccountsStaff2, setting the default gateway, pinging the default gateway and then pinging SalesManager.

Configure Passwords on Routers/Switches

This section is demonstrated on SalesSwitch, but applies to the router and all switches in the network.

An essential part of device configuration is to set a password. This prevents unauthorised users from accessing the devices and making changes. The process to harden them is straightforward. For the example we will be using a dummy password of 'magic123', but **in deployment this should be something far stronger** and changed for each device.

```
MainSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MainSW(config)#enable secret magic123
MainSW(config)#exit
MainSW#exit
```

By using 'enable secret' instead of 'enable password', the password we enter will be encrypted in the running-config.

```
MainSW con0 is now available


Press RETURN to get started.


MainSW>enable
Password:
MainSW#show run | begin enable
enable secret 4 KPGGJ8oTopHGG6x4n3yS9mLLXJmHM.RSvg4KGNDWAZM
!
no aaa new-model
```

Note the requirement of a password to enter 'enable' mode and the encrypted password (the 'secret') showing in the running-config.

Furthermore, we can add a password to the console and vty lines to ensure security against remote logins. Again, the dummy password of 'magic123' will be used **for demonstration purposes only**. When configured on-site this must be changed for a more robust password.

```
MainSW(config)#line console 0
MainSW(config-line)#password magic123
MainSW(config-line)#login
MainSW(config-line)#line vty 0 4
MainSW(config-line)#password magic123
MainSW(config-line)#login
MainSW(config-line)#line aux 0
MainSW(config-line)#password magic123
MainSW(config-line)#login
MainSW(config-line)#exit
MainSW(config)#
```

Passwords are entered for the console, virtual terminals and auxiliary line. The use of 'login' on each enables password checking when users attempt to access them.

```
MainSW(config)#service password-encryption
MainSW(config)#
```

And finally, 'service password-encryption' is used to encrypt the passwords.

```
MainSW(config)#do show run | begin line
line con 0
 password 7 000912010D585A545C
 logging synchronous
 login
line aux 0
 password 7 000912010D585A545C
 login
line vty 0 4
 password 7 000912010D585A545C
 login
!
end

MainSW(config)#
```

The running-config showing the line passwords are encrypted.

A message of the day banner is good to set up on a device as it will warn anyone who accesses it without authorisation of the legal consequences.

```
MainSW(config)#banner motd &
Enter TEXT message.  End with the character '&'.
  __   __              _
 |  \/  | __ _   __ _(_) ___
 | |\/| |/ _` |/ _` | |/ __|
 | |  | | (_| | (_| | | (__
 |_|  |_|\__,_|\__, |_|\___|
  __   __       |___/                _
 |  \/  | ___ _ __ ___   ___  _ __(_) ___  ___
 | |\/| |/ _ \ '_ ` _ \ / _ \| '__| |/ _ \/ __|
 | |  | |  __/ | | | | | (_) | |  | |  __/\__ \
 |_|  |_|\___|_| |_| |_|\___/|_|  |_|\___||___/

>"MainSwitch"

/!\/!\  WARNING! UNAUTHORISED ACCESS TO  /!\/!\
        THIS DEVICE WILL RESULT IN LEGAL
        ACTION BEING TAKEN AGAINST YOU!
/!\/!\       YOU HAVE BEEN WARNED!       /!\/!\
&
MainSW(config)#
```

The banner will display when anyone connects to the switch.

Securing Remote Access

This section takes place on the Sales Switch, but can be configured on any switch or router as required when in deployment.

To save on having to go to the networking devices and physically connect the console cable for configuration management, we can set them up to take remote connections in using the passwords configured in the previous section. This was the purpose of securing the vty lines. They can even be configured to use a database of usernames and passwords for added security. This will prevent anyone who somehow manages to connect from merely having to guess a password. I will be using SSH as it is more secure than telnet, in which communications are sent unecnrypted (plaintext), making it easier to be read if intercepted. This is configured as follows:

```
MainSW(config)#ip default-gateway 10.0.101.1
MainSW(config)#interface vlan 101
MainSW(config-if)#ip address 10.0.101.2 255.255.255.0
MainSW(config-if)#exit
MainSW(config)#ip domain-name magicmemories.com
MainSW(config)#
```

The IP addressing must be configured before any remote connections can be used. I will be using the management network of 10.0.101.0/24, so the addresses are chosen thusly. The IP domain-name must also be configured.

```
MainSW(config)#crypto key generate rsa
The name for the keys will be: MainSW.magicmemories.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

MainSW(config)#
*May 29 16:09:21.357: %SSH-5-ENABLED: SSH 1.99 has been enabled
MainSW(config)#
```

In order to use SSH, RSA keys must be generated.

```
MainSW(config)#line vty 0 4
MainSW(config-line)#transport input ssh
MainSW(config-line)#login local
MainSW(config-line)#exit
MainSW(config)#username netadmin password magic123
MainSW(config)#service password-encryption
MainSW(config)#
```

*Configuring the vty lines, setting them to <u>only</u> take in SSH traffic, enabling login with the local database, creating a username and password to add to the database (note: password used here for **demonstration purposes only**, in deployment use a more secure password or passphrase), and encrypting the passwords in the configuration.*

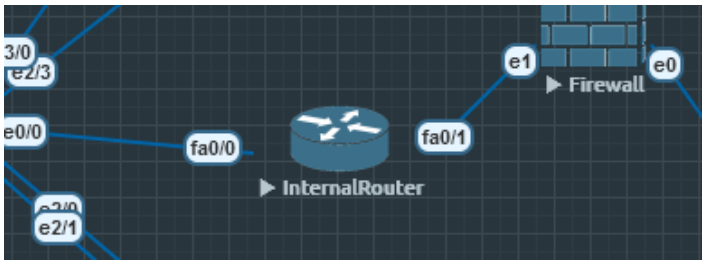
Next, to make sure the router is able to route incoming administrators, I will create a dedicated management sub-interface on the Internal Router, assign it the correct IP addressing and dot1q encapsualtion for the VLAN.

```
InternalRT(config)#interface fa0/0.101
InternalRT(config-subif)#encapsulation dot1q 101
InternalRT(config-subif)#ip address 10.0.101.1 255.255.255.0
InternalRT(config-subif)#
```

Creating and configuring the sub-interface for routing to VLAN 101 (Main Switch management interface)

From here everything is set up to configure the switch remotely. Unfrotunately, during the testing process I was unable to successfully log in from a host on the network, the Debian server (10.0.50.12). Pinging the fa0/0.101 interface was successful, pinging the VLAN 101 interface on the Main Switch from the Internal router was successful (and vice versa), but I was unable to get the Debian server to ping the VLAN 101 interface. All configruations were input correctly which leads me to suspect that it is either something I have missed out on the Internal Router, or less likely something at fault with the EVE-NG network virtualisation software.

Regulate Network Traffic



This section takes place on the InternalRouter

Network traffic can be regulated fairly easily with the use of access-control lists. These are lists of entries that either permit or deny network traffic using various criteria, such as source IP address or destination port number. I will be configuring the Internal Router with two access control lists. The type of access list used will be extended, as this allows for greater finese in the control of traffic. Specifically, the source, destination and TCP port number can be used in a control list entry.

To ensure correct configuration the lists of entries were written out beforehand and sorted into order. Access control lists work by looking for a match from the start of the list to the bottom. The router stops looking as soon as a match is found. If no match is found, the traffic is denied. The primary access control list was written as follows:

```
access-list 110 remark Master ACL for internal network
access-list 110 permit tcp any any eq smtp
access-list 110 permit tcp any any eq pop3
access-list 110 permit ip any host 10.0.50.8
access-list 110 permit ip any host 10.0.50.11
access-list 110 permit ip any host 10.0.50.12
access-list 110 permit tcp host 10.0.10.11 any eq 80
access-list 110 permit tcp host 10.0.10.11 any eq 8080
access-list 110 permit tcp host 10.0.10.11 any eq 443
access-list 110 deny ip host 10.0.20.8 any
access-list 110 permit tcp 10.0.20.8 0.0.0.7 any eq 80
access-list 110 permit tcp 10.0.20.8 0.0.0.7 any eq 8080
access-list 110 permit tcp 10.0.20.8 0.0.0.7 any eq 443
access-list 110 permit tcp host 10.0.30.11 any eq 80
access-list 110 permit tcp host 10.0.30.11 any eq 8080
access-list 110 permit tcp host 10.0.30.11 any eq 443
access-list 110 permit tcp host 10.0.40.11 any eq 80
access-list 110 permit tcp host 10.0.40.11 any eq 8080
access-list 110 permit tcp host 10.0.40.11 any eq 443
```

This access list will be applied to all sub-interfaces facing the employee departments and wireless network, and be applied in the “in” direction. A second access list will go on sub-interface fa0/0.50, as this faces the servers and backup printer. Rather than leaving that interface open, it will be restricted to just the devices specified with all others denied. This prevents unauthorised users connecting to the network from

the Server subnet. BackupPrinter shall be restricted to the internal network. This is as follows below:

```
access-list 150 remark ACL for Server subnet
access-list 150 permit ip host 10.0.50.8 10.0.0.0 0.255.255.255
access-list 150 permit ip host 10.0.50.11 any
access-list 150 permit ip host 10.0.50.12 any
```

These lists are entered into the Internal Router one entry at a time and then applied to an interface in either the inbound or outbound direction.

```
InternalRT(config)#do show run | begin access-list
access-list 110 remark Master ACL for internal network
access-list 110 permit tcp any any eq smtp
access-list 110 permit tcp any any eq pop3
access-list 110 permit ip any host 10.0.50.8
access-list 110 permit ip any host 10.0.50.11
access-list 110 permit ip any host 10.0.50.12
access-list 110 permit tcp host 10.0.10.11 any eq www
access-list 110 permit tcp host 10.0.10.11 any eq 8080
access-list 110 permit tcp host 10.0.10.11 any eq 443
access-list 110 deny   ip host 10.0.20.8 any
access-list 110 permit tcp 10.0.20.8 0.0.0.7 any eq www
access-list 110 permit tcp 10.0.20.8 0.0.0.7 any eq 8080
access-list 110 permit tcp 10.0.20.8 0.0.0.7 any eq 443
access-list 110 permit tcp host 10.0.30.11 any eq www
access-list 110 permit tcp host 10.0.30.11 any eq 8080
access-list 110 permit tcp host 10.0.30.11 any eq 443
access-list 110 permit tcp host 10.0.40.11 any eq www
access-list 110 permit tcp host 10.0.40.11 any eq 8080
access-list 110 permit tcp host 10.0.40.11 any eq 443
access-list 150 remark ACL for Server subnet
access-list 150 permit ip host 10.0.50.8 10.0.0.0 0.255.255.255
access-list 150 permit ip host 10.0.50.11 any
access-list 150 permit ip host 10.0.50.12 any
!
!
!
!

InternalRT(config)#
```

The access lists showing in the running-config.

```
InternalRT(config)#int fa0/0.10
InternalRT(config-subif)#ip access-group 110 in
InternalRT(config-subif)#
```

Selecting the sub-interface and applying the ACL to inbound traffic. This process is repeated for all sub-interfaces facing the internal network <u>except</u> sub-interface fa0/0.50, for which ACL 150 is applied.

To test the ACLs we can perform a few pings from a couple of computers. For example, SalesManager should not be able to communicate with AccountsPrinter.

```
SalesManager
VPCS> ping 10.0.30.8

*10.0.10.1 icmp_seq=1 ttl=255 time=5.705 ms (ICMP type:3,
code:13, Communication administratively prohibited)
*10.0.10.1 icmp_seq=2 ttl=255 time=5.806 ms (ICMP type:3,
code:13, Communication administratively prohibited)
*10.0.10.1 icmp_seq=3 ttl=255 time=4.852 ms (ICMP type:3,
code:13, Communication administratively prohibited)
*10.0.10.1 icmp_seq=4 ttl=255 time=4.826 ms (ICMP type:3,
code:13, Communication administratively prohibited)
^C
VPCS>
```

The pings fail due, the ACL is working

Another test is to make sure devices can access BackupPrinter.

```
SalesManager
VPCS> ping 10.0.50.8

84 bytes from 10.0.50.8 icmp_seq=1 ttl=63 time=29.881 ms
84 bytes from 10.0.50.8 icmp_seq=2 ttl=63 time=13.579 ms
84 bytes from 10.0.50.8 icmp_seq=3 ttl=63 time=17.447 ms
84 bytes from 10.0.50.8 icmp_seq=4 ttl=63 time=17.238 ms
84 bytes from 10.0.50.8 icmp_seq=5 ttl=63 time=18.300 ms

VPCS>
```

SalesManager can reach BackupPrinter (and therefore the Server subnet).

And to test the Server subnet ACL, WinServer should be able to ping the external interface of InternalRouter (fa0/1) but BackupPrinter should not.

```
WinServer
VPCS> ping 192.168.0.1

84 bytes from 192.168.0.1 icmp_seq=1 ttl=255 time=9.153 ms
84 bytes from 192.168.0.1 icmp_seq=2 ttl=255 time=7.658 ms
84 bytes from 192.168.0.1 icmp_seq=3 ttl=255 time=1.227 ms
84 bytes from 192.168.0.1 icmp_seq=4 ttl=255 time=6.935 ms
84 bytes from 192.168.0.1 icmp_seq=5 ttl=255 time=6.768 ms

VPCS>
```

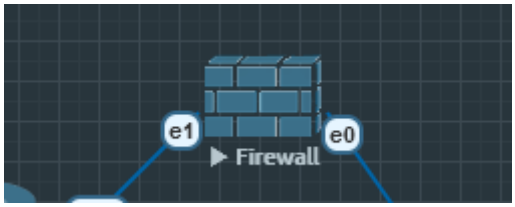
Success!

```
BackupPrinter
VPCS> ping 192.168.0.1

*10.0.50.1 icmp_seq=1 ttl=255 time=4.818 ms (ICMP type:3, code:13, Communication
administratively prohibited)
*10.0.50.1 icmp_seq=2 ttl=255 time=1.730 ms (ICMP type:3, code:13, Communication
administratively prohibited)
*10.0.50.1 icmp_seq=3 ttl=255 time=10.617 ms (ICMP type:3, code:13, Communication
 administratively prohibited)
*10.0.50.1 icmp_seq=4 ttl=255 time=4.721 ms (ICMP type:3, code:13, Communication
administratively prohibited)
*10.0.50.1 icmp_seq=5 ttl=255 time=5.134 ms (ICMP type:3, code:13, Communication
administratively prohibited)

VPCS>
```

The failure to ping outside the network is also a success!

As before, the configuration is saved with `write` and `copy running-config startup-config`.

Implementing a Hardware Firewall



This section takes place on Firewall

To further secure the network, a hardware firewall shall be put in place between the ISProuter and InternalRouters to strictly regulate the flow of traffic to and from the broader internet. The firewall operating system being used is pfSense because it is free and open source.

After specificying which interface is WAN and which is LAN the IP addresses have to be set. This is simple enough to do.

```
Available interfaces:

1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 10.0.200.10

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.0.200.1
```

Setting the IP address and default gateway for the WAN interface. The LAN interface is configured the same way, though without a default gateway

```
Enter a host name or IP address: 10.0.100.1

PING 10.0.100.1 (10.0.100.1): 56 data bytes
64 bytes from 10.0.100.1: icmp_seq=0 ttl=255 time=12.231 ms
64 bytes from 10.0.100.1: icmp_seq=1 ttl=255 time=5.605 ms
64 bytes from 10.0.100.1: icmp_seq=2 ttl=255 time=1.047 ms

--- 10.0.100.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.047/6.294/12.231/4.592 ms

Press ENTER to continue.
```

Testing the LAN interface by pinging the InternalRouter interface.

```
Enter a host name or IP address: 10.0.200.1

PING 10.0.200.1 (10.0.200.1): 56 data bytes
64 bytes from 10.0.200.1: icmp_seq=1 ttl=255 time=2.013 ms
64 bytes from 10.0.200.1: icmp_seq=2 ttl=255 time=1.076 ms

--- 10.0.200.1 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 1.076/1.544/2.013/0.468 ms

Press ENTER to continue.
```

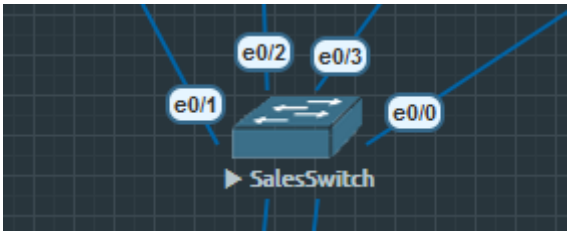
The WAN interface IP address tested by pinging the ISProuter.

```
Enter a host name or IP address: 10.10.10.10

PING 10.10.10.10 (10.10.10.10): 56 data bytes
64 bytes from 10.10.10.10: icmp_seq=0 ttl=63 time=3020.256 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=63 time=4996.305 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=63 time=6956.934 ms

--- 10.10.10.10 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3020.256/4991.165/6956.934/1607.146 ms

Press ENTER to continue.
```

The firewall can ping the TEST computer.

For ease of management, the pfSense firewall uses a webConfigurator site that can be access from within the LAN. A computer can connect from the LAN side with a web browser and the traffic leaving the network can be configured with a user-friendly ACL system.

Close Unused Network Interfaces



This section takes place on the switches. For demonstration purposes the SalesSwitch will be used.

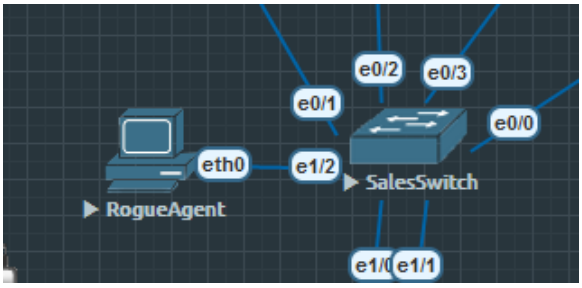
As not all interfaces on the switches will be used by computers there will be spaces where additional devices can be plugged in. Cisco switches have all interfaces up by default. A malicious actor could connect their own device and listen in to network traffic if the interfaces are not shut down. This is very easy to do.

```
SalesSW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SalesSW(config)#int range e1/2-3
SalesSW(config-if-range)#shutdown
SalesSW(config-if-range)#
*May 18 16:52:22.011: %LINK-5-CHANGED: Interface Ethernet1/2, changed state to a
dministratively down
*May 18 16:52:22.016: %LINK-5-CHANGED: Interface Ethernet1/3, changed state to a
dministratively down
*May 18 16:52:23.015: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
2, changed state to down
*May 18 16:52:23.025: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
3, changed state to down
SalesSW(config-if-range)#exit
```

Configuring the range of unusued interfaces, issuing the shutdown command and seeing the report from each interface that they have been shut down.

```
interface Ethernet1/2
 shutdown
 duplex auto
!
interface Ethernet1/3
 shutdown
 duplex auto
```

The interfaces in the running-config showing in the shutdown state



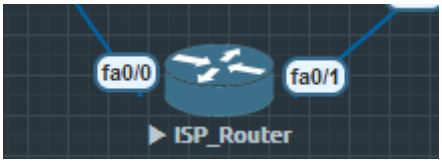
Testing the shut down interface with a rogue computer

```
VPCS> ping 10.0.10.1

host (10.0.10.1) not reachable

VPCS>
```

The rogue computer cannot ping the default gateway as the interface is shut down.

This process is repeated on all interfaces on all switches that are left unused. This is unnecessary for the routers as Cisco router interfaces are shut down by default.

Implement NAT on The ISP Router



This section takes place on the ISP Router

The implementation of network address translation (NAT) prevents the interior addresses of the network being broadcast out to the public, obscuring the network structure and improving security.[5] The ISP Router will translate inside addresses to a publicly viewable global address. For Magic Memories I will configure port address translation (PAT), which uses one public IP address and dynamically assigns a TCP port number to the inside devices sending/receiving traffic.

```
ISProuter(config)#ip access-list standard INSIDE-HOSTS
ISProuter(config-std-nacl)#permit 10.0.0.0 0.255.255.255
ISProuter(config-std-nacl)#int fa0/0
ISProuter(config-if)#ip address 10.0.200.1 255.255.255.0
ISProuter(config-if)#ip nat inside
ISProuter(config-if)#int fa0/1
ISProuter(config-if)#ip address 192.168.10.1 255.255.255.0
ISProuter(config-if)#ip nat outside
ISProuter(config-if)#exit
ISProuter(config)#ip nat inside source list INSIDE-HOSTS int fa0/0 overload
ISProuter(config)#
```

Creating the access-list to select the entire 10.0.0.0/8 block of addresses, assigning IP addresses and NAT sides to the two interfaces, and configuring NAT to use the address block on the WAN interface with PAT.

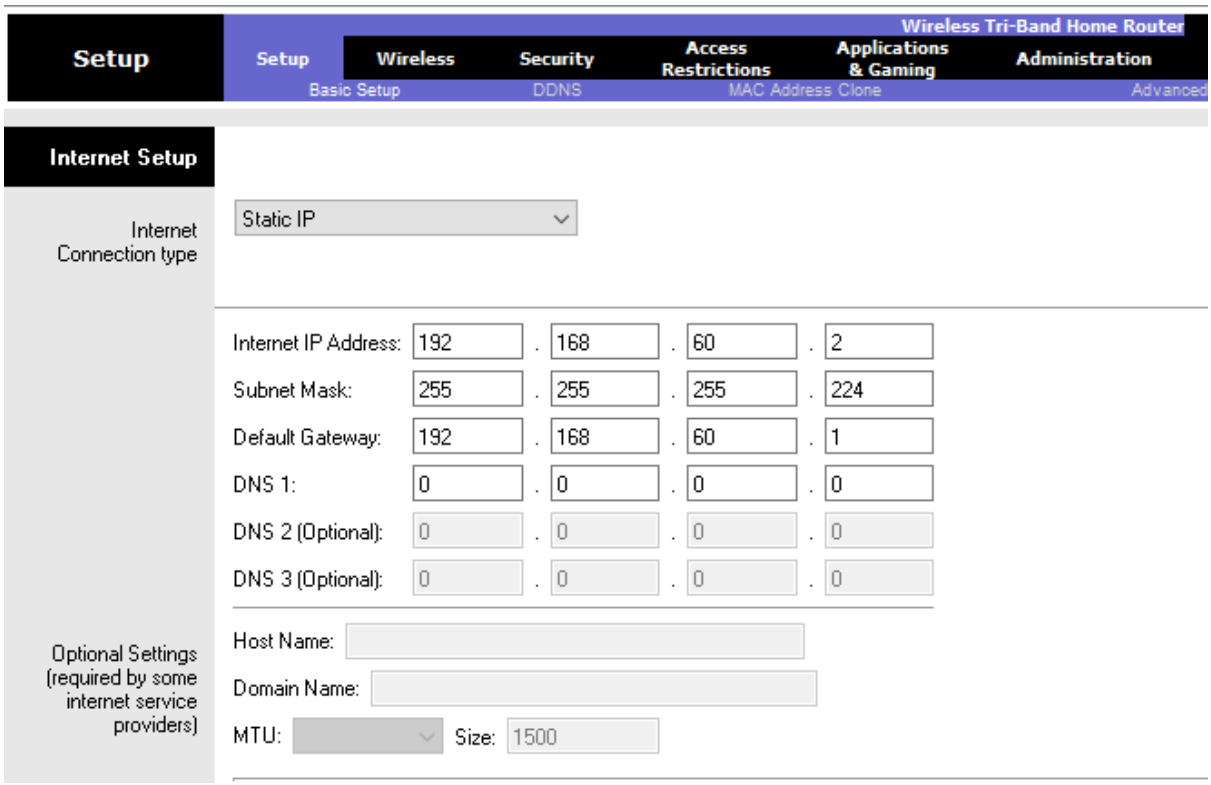
```
Enter a host name or IP address: 192.168.10.10

PING 192.168.10.10 (192.168.10.10): 56 data bytes
64 bytes from 192.168.10.10: icmp_seq=1 ttl=63 time=13.614 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=19.493 ms

--- 192.168.10.10 ping statistics ---
3 packets transmitted, 2 packets received, 33.3% packet loss
round-trip min/avg/max/stddev = 13.614/16.553/19.493/2.939 ms

Press ENTER to continue.
```

A test ping from the firewall shows a successful PAT has taken place!

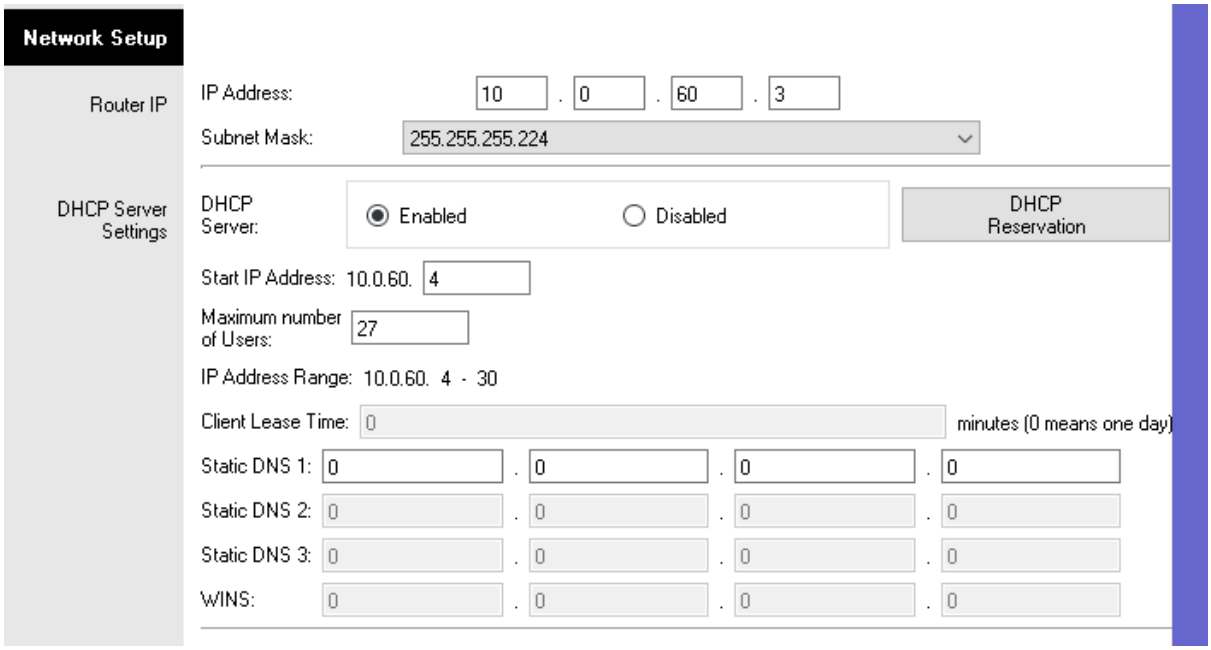
Fix Issues With The Wireless Network

This section takes place on the wireless router in Packet Tracer

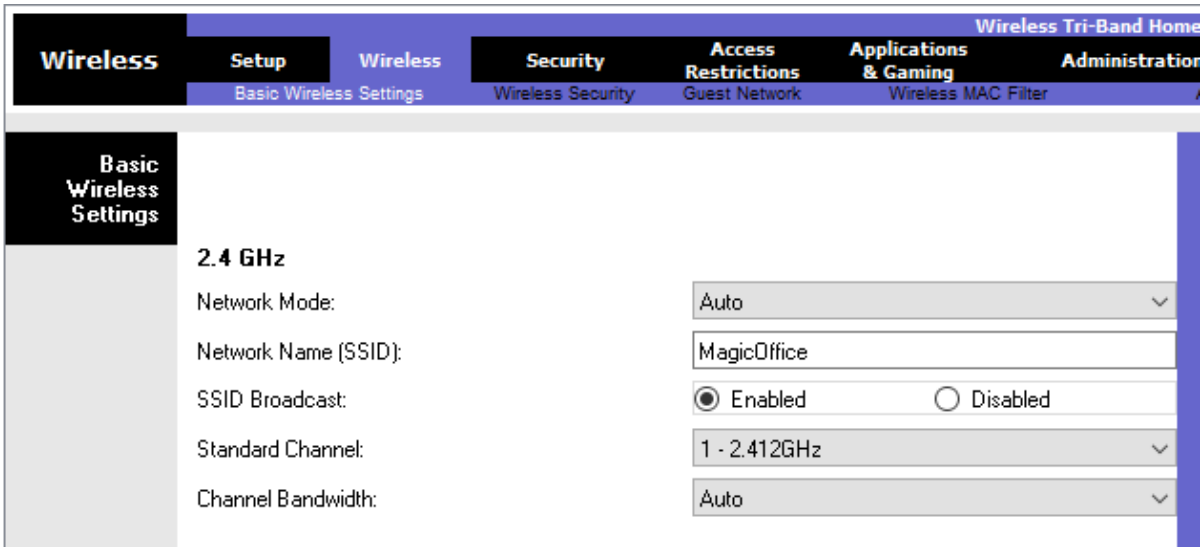
For working on the wireless network I will be switching to Packet Tracer. This is because EVE-NG does not allow for wireless virutalisation and Packet Tracer has fully competent wireless simulation. To harden the wireless network I will enforce WPA2-AES encryption and reduce the DHCP lease time. WPA2-AES is the most secure wireless standard available for this wireless router and utilises encryption and longer password requirements to prevent unauthorised access. By limiting the DHCP lease time I can prevent an accidental (or intentional) DHCP starvation attack. These are configured below via the wireless router's GUI.



Configuring the wireless router's IP addressing. Note: the network address of 192.168.60.0/27 is for ***demonstration purposes only****. This is used due to the limitations of Packet Tracer, which reserves the 10.0.0.0/24 address space for VLAN1 by default, with no way to change it.*

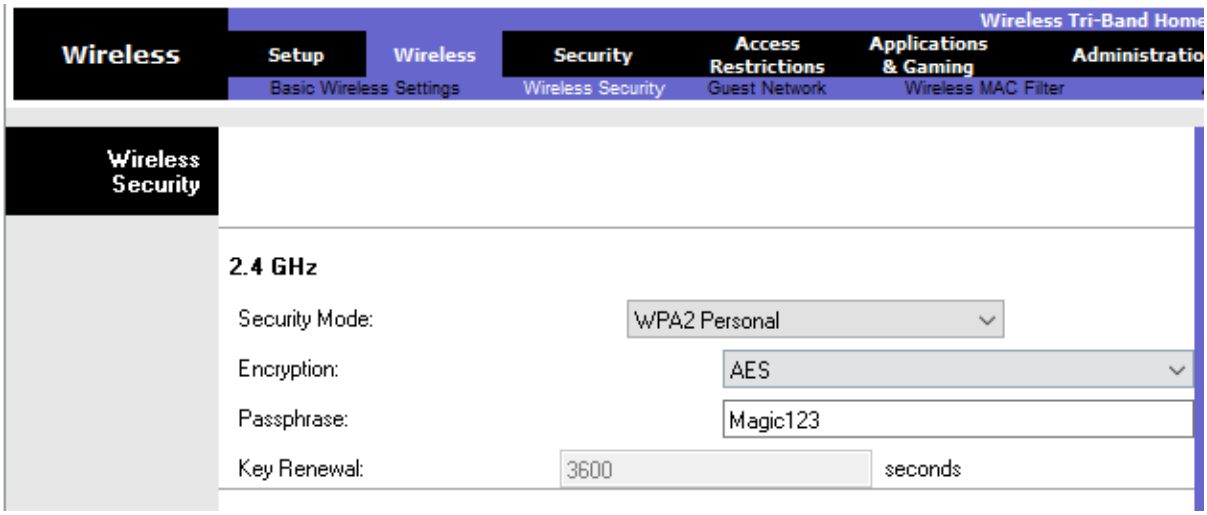


Configuring the IP addresses used in the DHCP pool. As the number of expected addresses in use per day is 20, the best fit subnet is /27. Note: due to the limitations of Packet Tracer, the client lease time is unable to be altered on this model of wireless router. In deployment, this value will be set to 240 minutes.

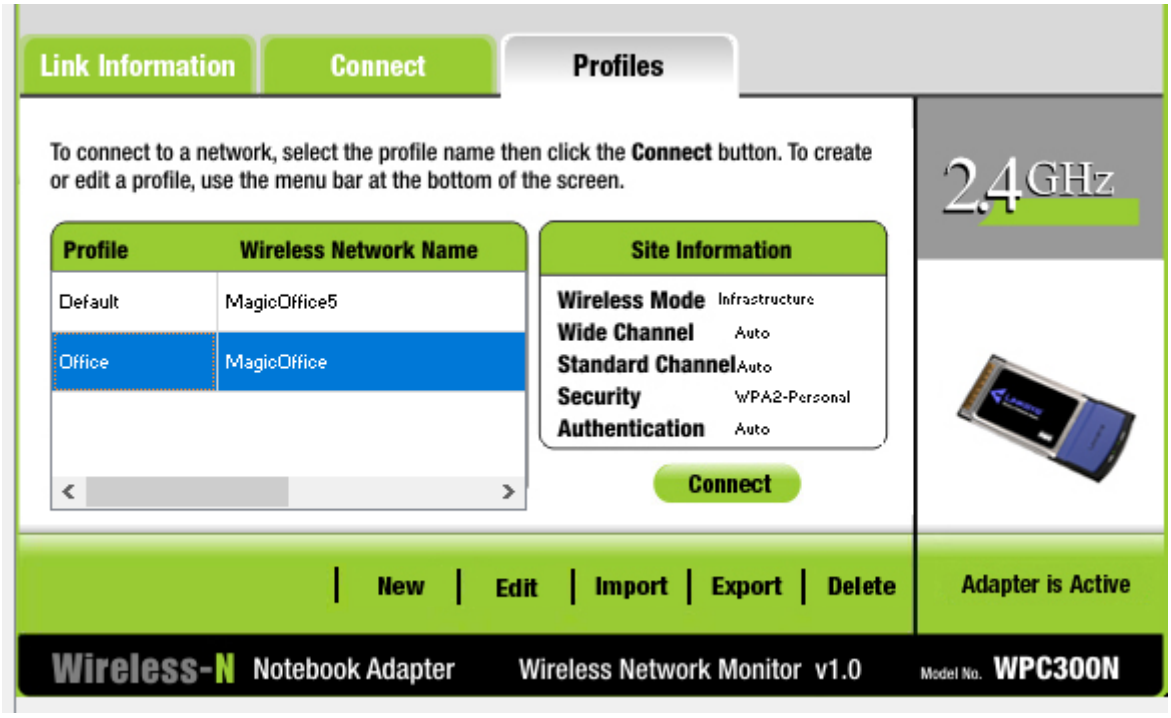


As guests will be connecting to the network the SSID will be broadcast.

Hiding the SSID is sometimes recommended as a security option, but this is *not* a security feature. Devices that already know the SSID and are attempting to reconnect will be broadcasting the SSID. Anyone sniffing the wifi will be able to find the SSID, rendering this ineffective at detering intrustion.



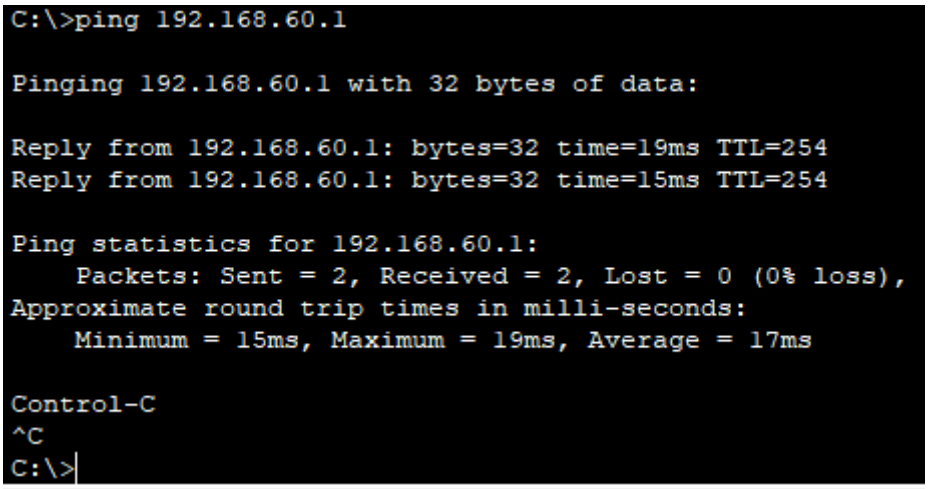
It is very important to select WPA2 and use AES to encrypt the password. The password used here, "Magic123", is for ***demonstration purposes only****. In deployment a more secure password or passphrase should be used. As will be discussed later, a passphrase is more memorable for users while still being secure.*



The connectivity wizard on the laptop is used to test the connection.

The connection is successful!

The DHCP service is working



```
C:\>ping 192.168.60.1

Pinging 192.168.60.1 with 32 bytes of data:

Reply from 192.168.60.1: bytes=32 time=19ms TTL=254
Reply from 192.168.60.1: bytes=32 time=15ms TTL=254

Ping statistics for 192.168.60.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 19ms, Average = 17ms

Control-C
^C
C:\>
```

Pinging the InternalRT is also successful

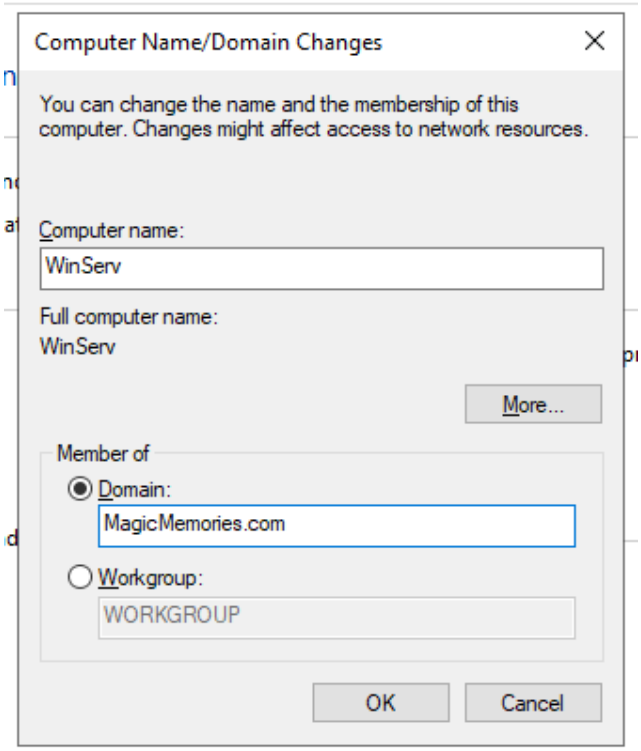
```
C:\>ping 10.0.10.11

Pinging 10.0.10.11 with 32 bytes of data:

Reply from 10.0.10.11: bytes=32 time=18ms TTL=126
Reply from 10.0.10.11: bytes=32 time=10ms TTL=126

Ping statistics for 10.0.10.11:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 18ms, Average = 14ms

Control-C
^C
C:\>
```

Pinging a host on another subnet also works. Note: when in deployment this will not be possible due to the ACLs in place on the InternalRT interface. As this Packt Tracer environment was only used for wireless testing, the ACLs have not been configured here. Packet Tracer is also known for not fully simulating ACL functionality.

Configuring the Windows Server

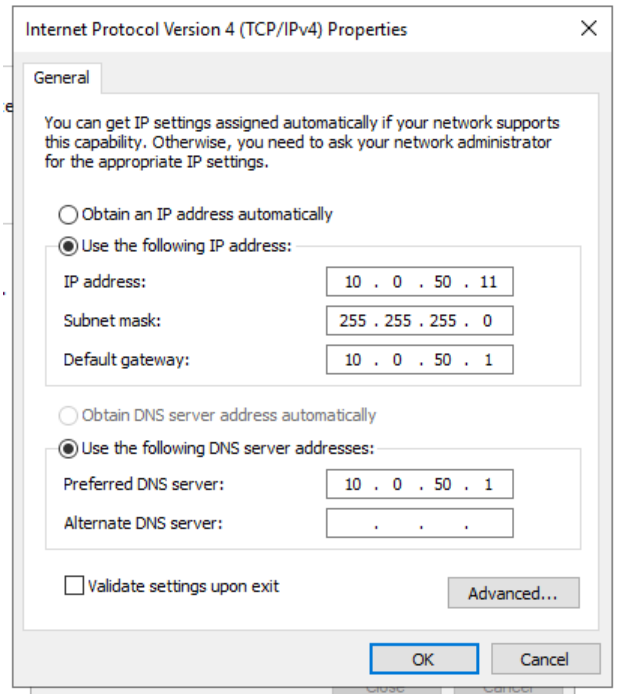
To accommodate the required needs of Magic Memories a Windows Server will be used. This will allow for the use of features such as the Active Directory Domain Services.

After the installation of Windows Server is complete, the Active Directory Domain Service can be set up. The Active Directory service will allow for the management of permissions and the control of access to resources on Magic Memories' network.



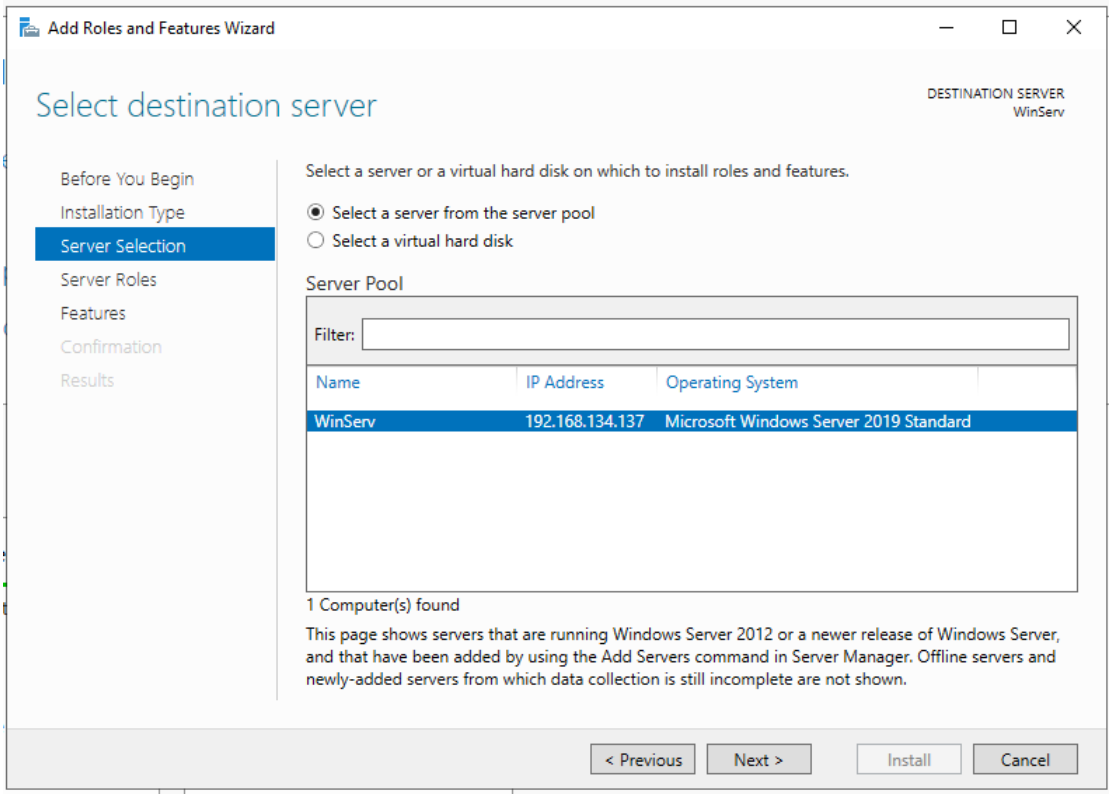
As a quick first step, the server name is changed and the domain is configured.

The server I am configuring here is running on a virtual machine, so whilst the configuration is valid and would work in deployment, it is not connected to the virtualised network. The differences between the two are negligable and so the configuration will continue as though it were connected.

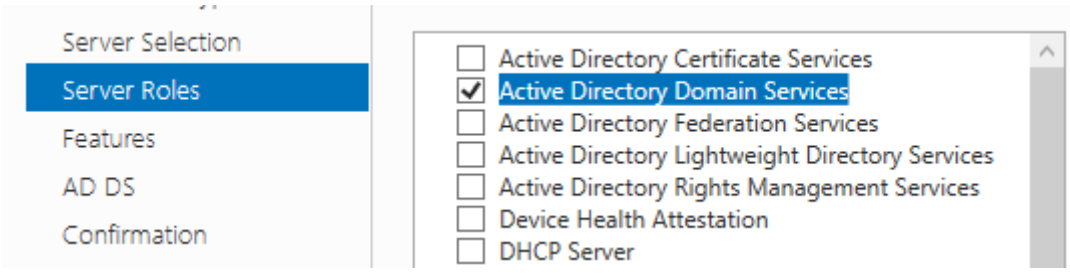


The IP address is configured.

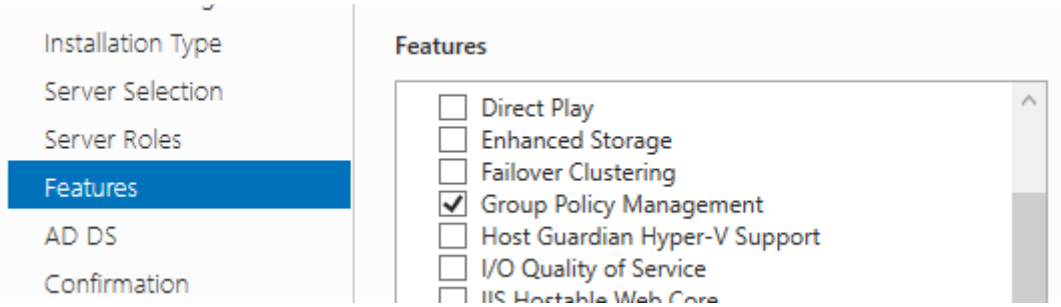
The Active Directory Domain Service is easily added with the server manager. The process for this is shown in the screenshots below, with configuration for Magic Memories' specific needs being covered later.



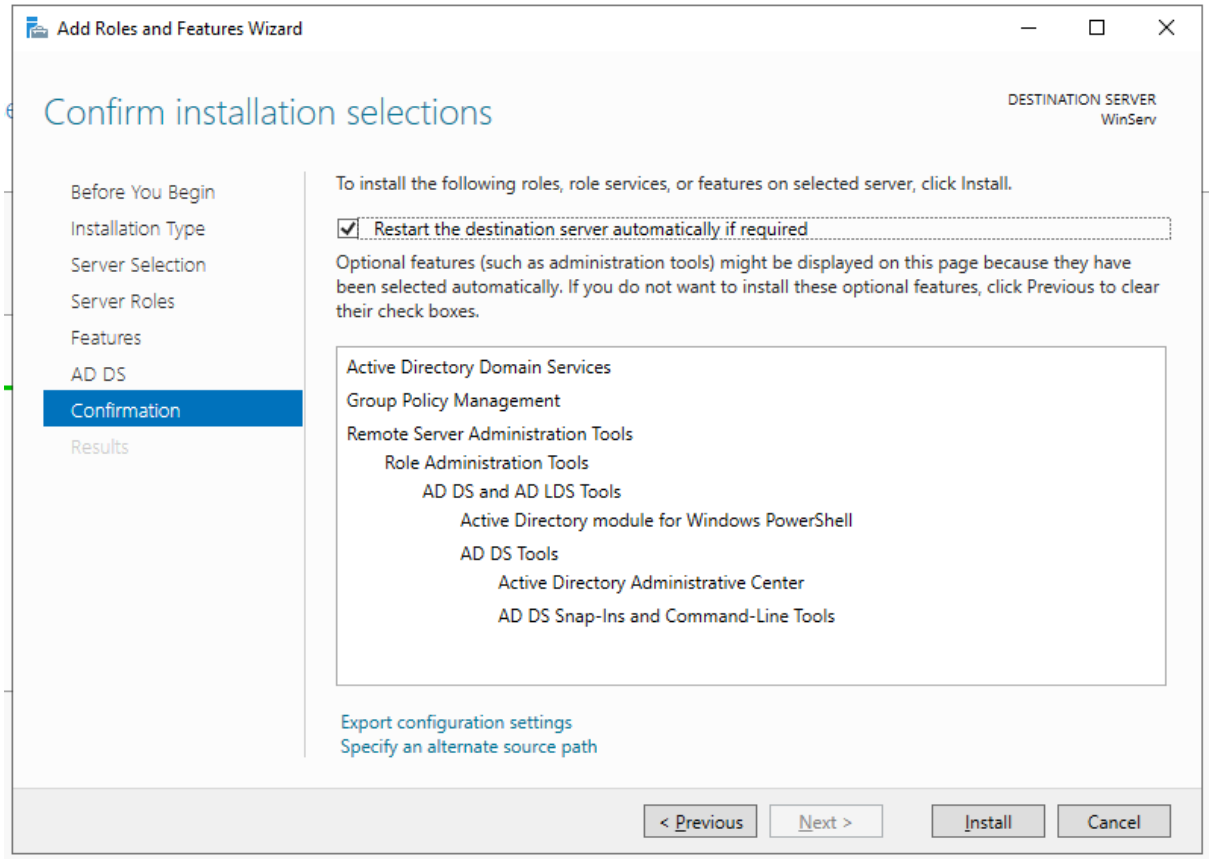
It's important to select the Magic Memories server when choosing where to install roles and features to.



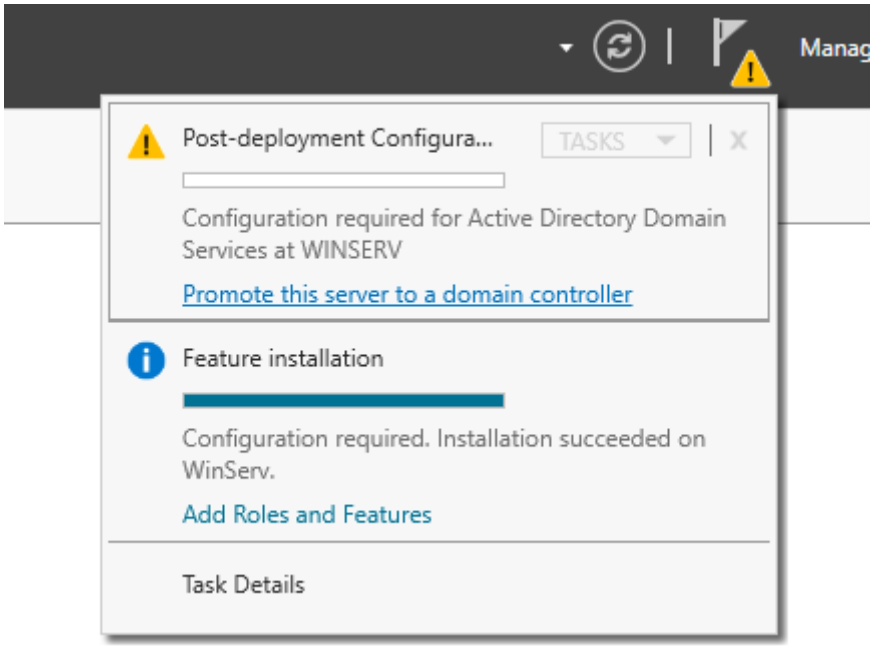
The role to be added is the Active Directory Domain Services.



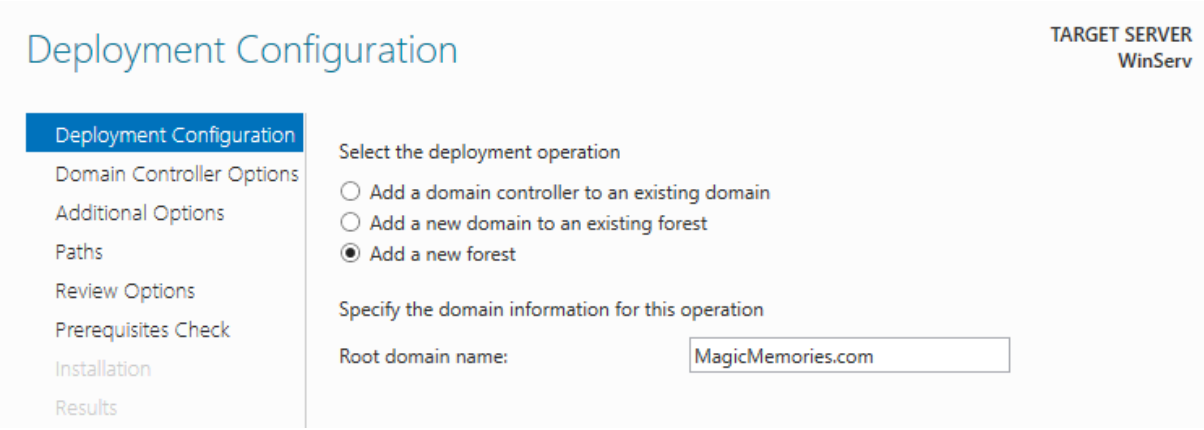
Group Policy Management will also be needed for managing permissions



The summary of the chosen changes to be made. If a restart is required the wizard will conduct this itself as the check box is ticked.

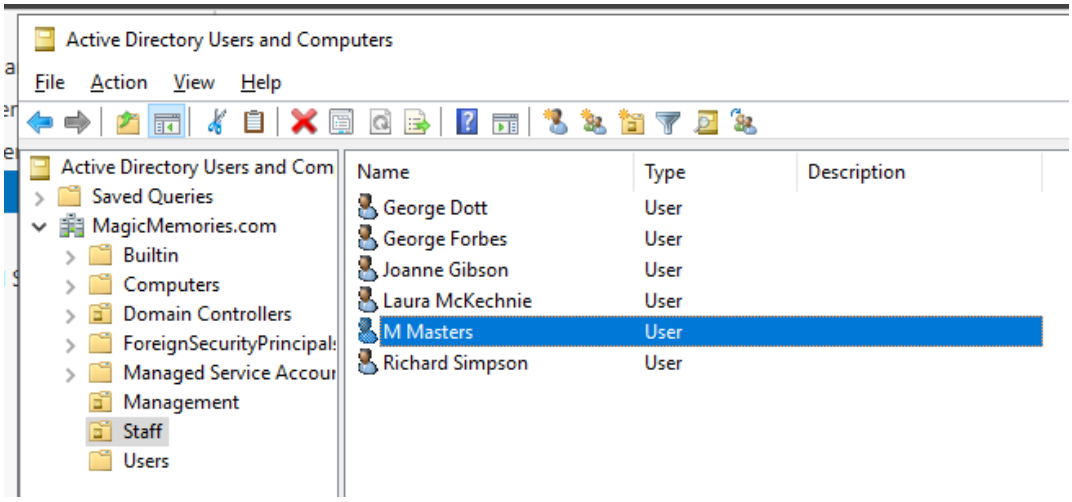


We can start configuring the Active Directory by promoting the server to a domain controller

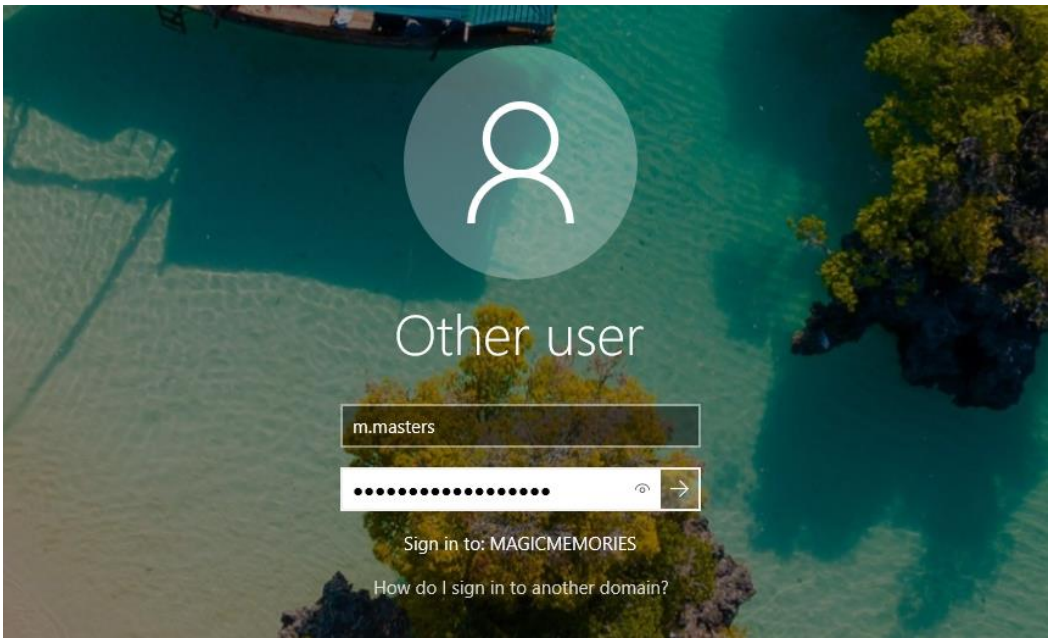


The new forest we'll use for the ADDS will be called MagicMemories.com

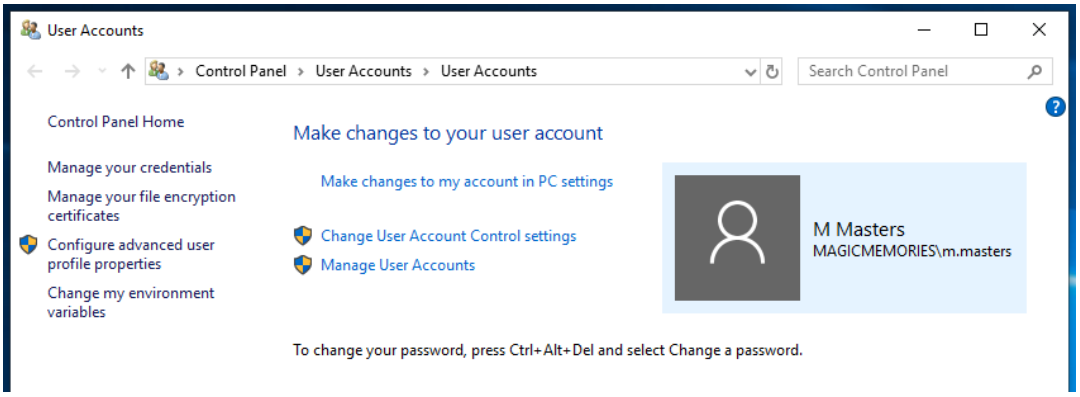
Once created, some user accounts will be made. As different policies are being applied to different sets of users, Organisational Units and User Groups will be used.



Some users created in the "Staff" group under the MagicMemories.com organisational unit.

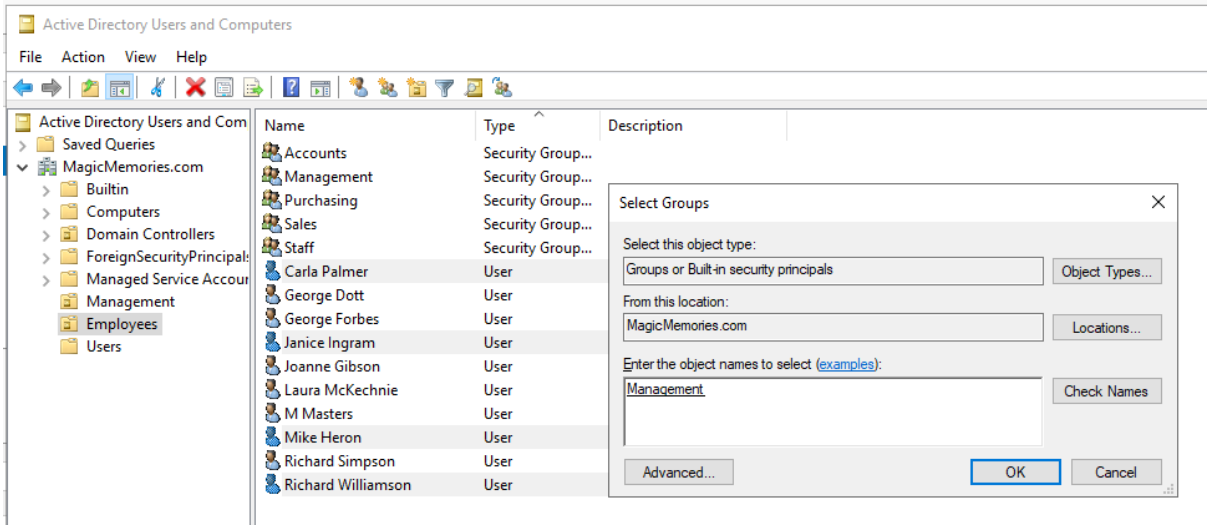


Logging in from a client computer with M Masters' account…



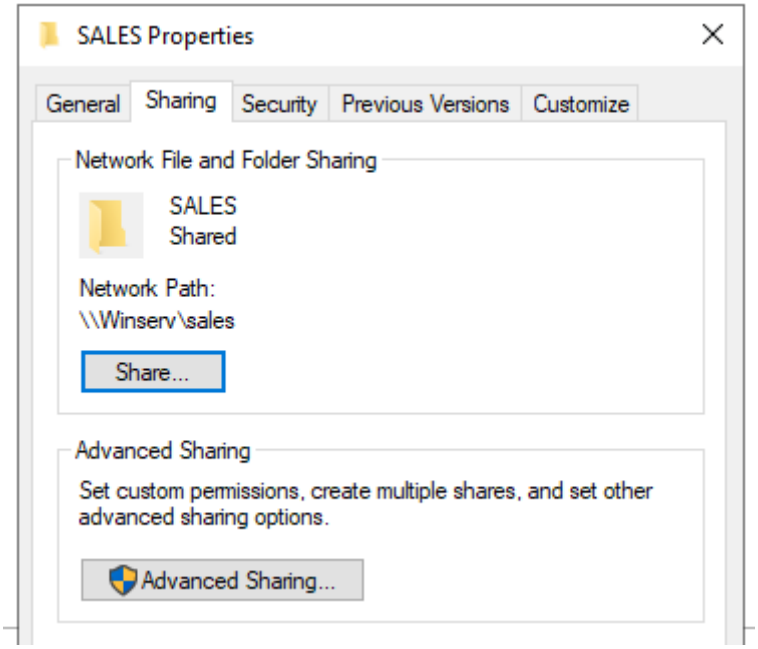
Success! Clients can log into the domain.

Now with staff and management able to connect to the domain, their personal drives must be set up with appropriate permissions, as per the project brief.

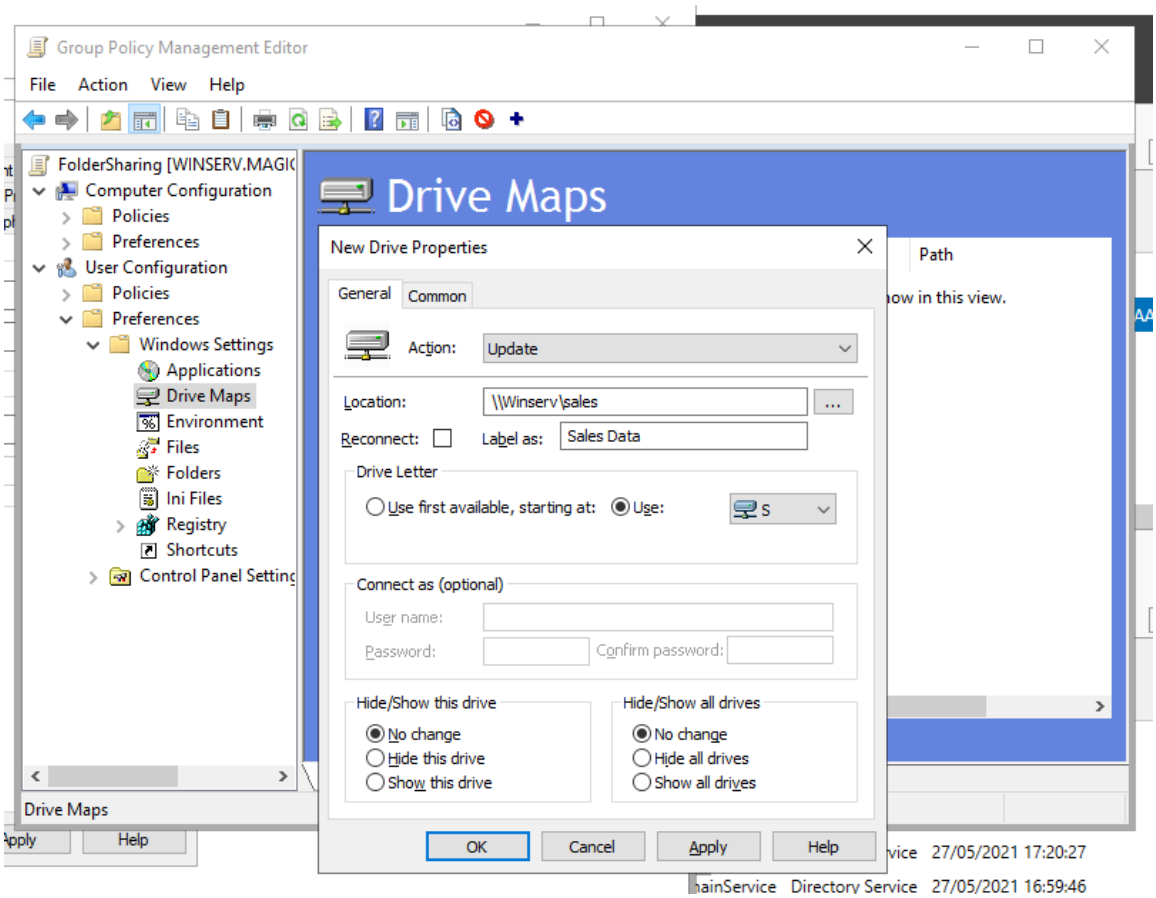


Sorting the user accounts, creating groups and adding the appropriate employees to the groups. Some groups will be doubled over, for example Mike Heron will be in both the "Management" and "Sales" groups as he is the Sales Manager.

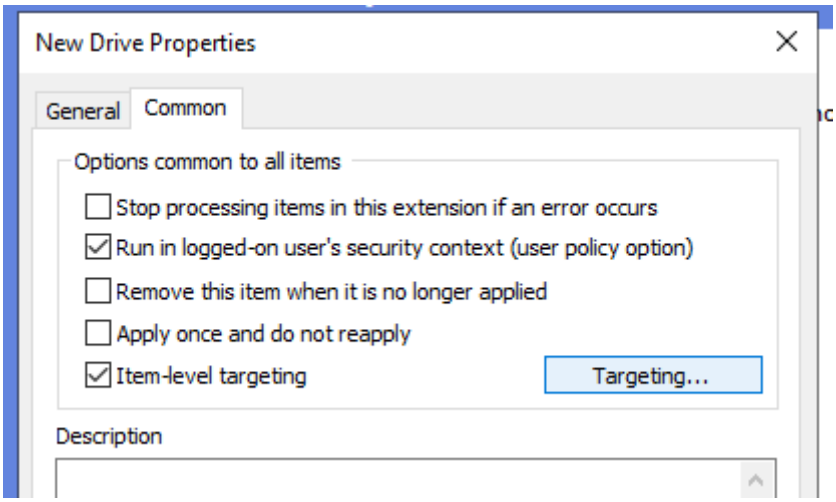
The permissions for accessing the private/department folders can be achieved with a Group Policy Object (GPO). The process will be demonstrated below with the Sales department but can be repeated across all departments as necessary. The effect of this will be that employees will be able to access the shared folder of their own department but not others, and managers will be able to access



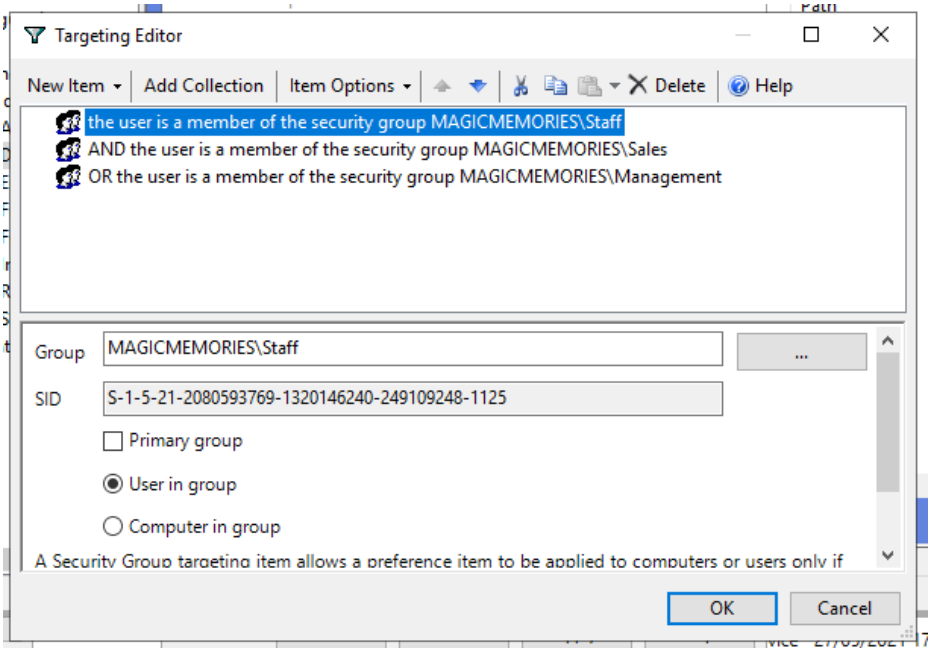
The folders should be shared on the network for this to work.



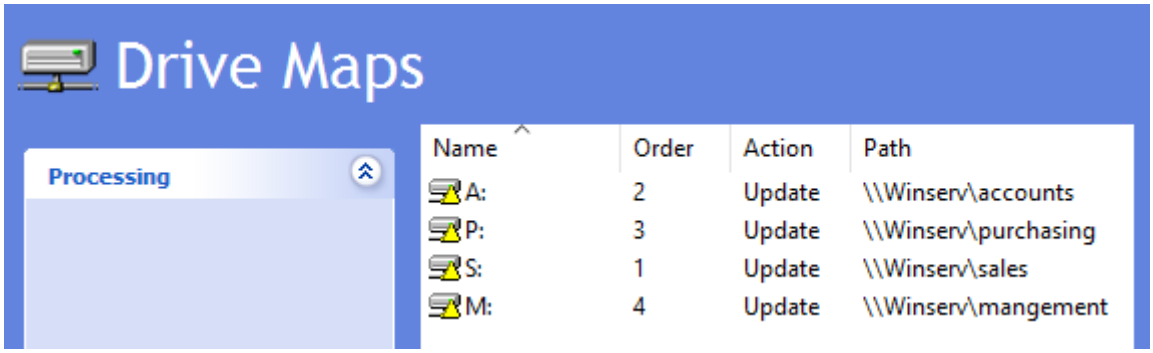
The location of the GPO and the details for configuring a new networked drive. For this example we will be using the Sales department.



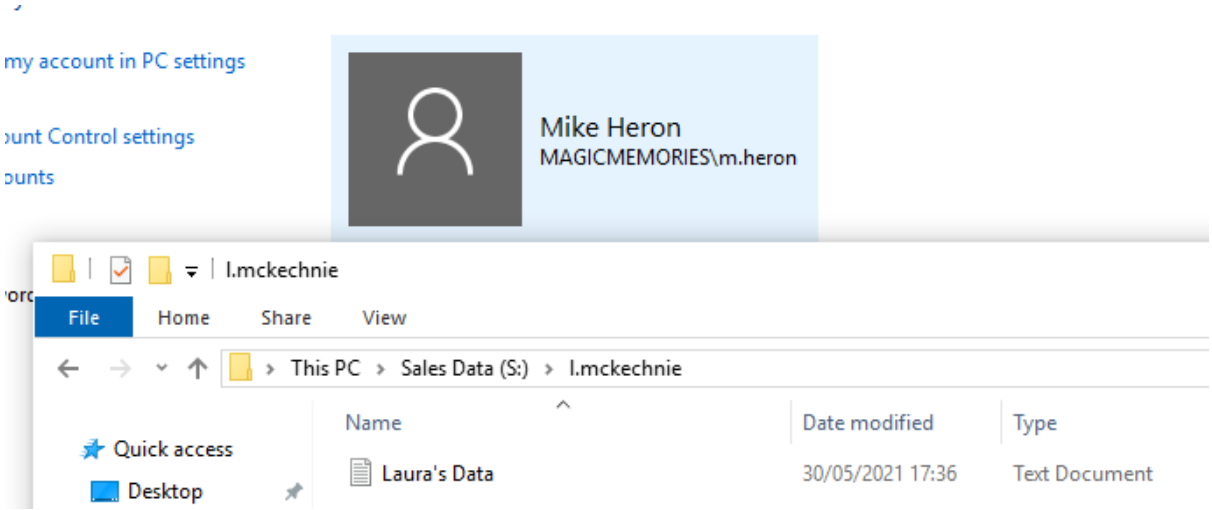
In the Common tab we can use Item-level targeting to select the groups to which this drive will be applied.



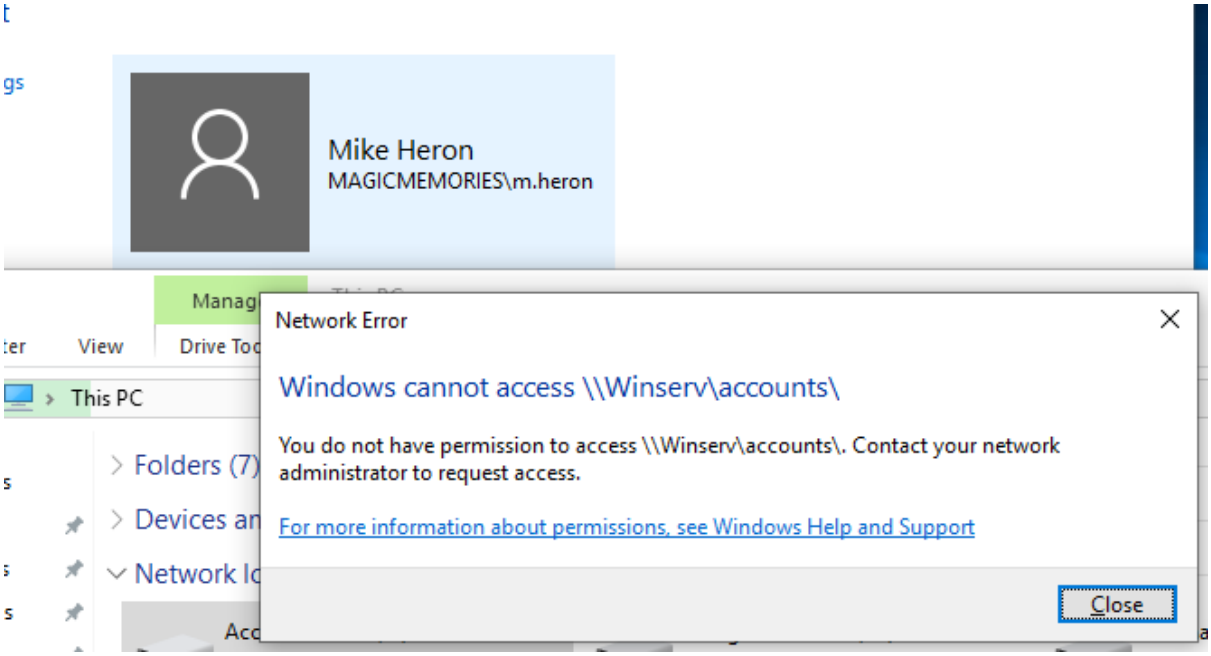
The targeting is set up so that only managers or satff in the Sales department can access this drive.



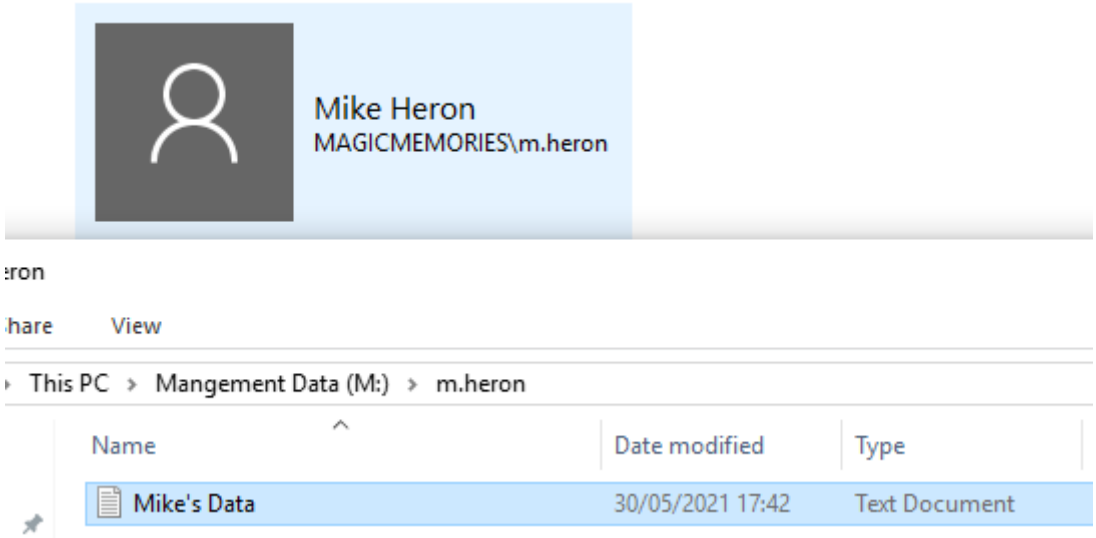
The full set of mapped drives. These will now show up for users as per the security groups assigned to them.



Logged in as the manager, we can see a department employee's data…



…but we cannot see another department's data.



And finally, the management data drive is available to the manager. Success!

Configuring The Debian Server

As per the questions with the directing manager and the project specification, a Debian server will be installed and configured to host a web server and a VPN server. I will be using Debian for the operating system, Apache2 for the web hosting server, and OpenVPN because they are Free Open Source Software (FOSS) applications, they are regularly updated, and are relatively simple to configure. This means cutting edge software with no licensing fees. During the configuration process the server will be connected to the internet via the internal router and obtain an IP address through DHCP.

After installing Debian to the server and setting up accounts (username sysadmin and password “magic123” selected for **demonstration purposes only**) a useful tool I’ll set up is ‘sudo’. Sudo allows a regular user to execute commands with root level permissions and is highly configurable. This means specific permissions can be given to groups of users and prevent any account save root having total control over the operating system. As users use sudo with their own passwords it prevents anyone but the system administrator from knowing the root password, enhancing security.

This is installed by logging in as the root user, running `apt-get install sudo`, and editing the configuration file located at /etc/sudoers to add the desired users and their permission levels. In this example we’re using the demonstration account sysadmin and giving it full permissions.

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
sysadmin ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

*Sudoers file with the sysadmin user added with full permissions. Again, this is for **demonstration purposes only**. When configured in deployment permission should be set per user.*

From here I can log in as sysadmin and upate the server with `sudo apt-get update && sudo apt-get upgrade`.

Installing And Configuring OpenVPN

I'll set up the OpenVPN server first. To pass incoming network packets to clients on other networks, IP forwarding has to be enabled by editing the config file, located at /etc/systctl.conf.

```
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

Note the line 'net.ipv4.ip_forward = 1' is uncommented

To apply the changes run `sudo sysctl -p`. The output will be `net.ipv4.ip_forward = 1`. There is a script I will be using for installing and configuring OpenVPN that makes the process much faster. Once downloaded and modified to be executable it's a simple case of running it and entering the appropriate IP adddresses; 10.0.50.12 for the server IP and 192.168.33.1 for the public IP address (note; this public IP is for **demonstration purposes only**, the public IP address for the company can be obtained by visiting a website such as https://ip4.me/ in a web browser from inside the company network).

```
What port do you want OpenVPN to listen to?
   1) Default: 1194
   2) Custom
   3) Random [49152-65535]
Port choice [1-3]: 2
Custom port [1-65535]: 10512
```

*A custom port number helps deter opportunistic attacks. [4] Any non-standard port number can be used here, 10512 is used for **demonstration purposes only**.*

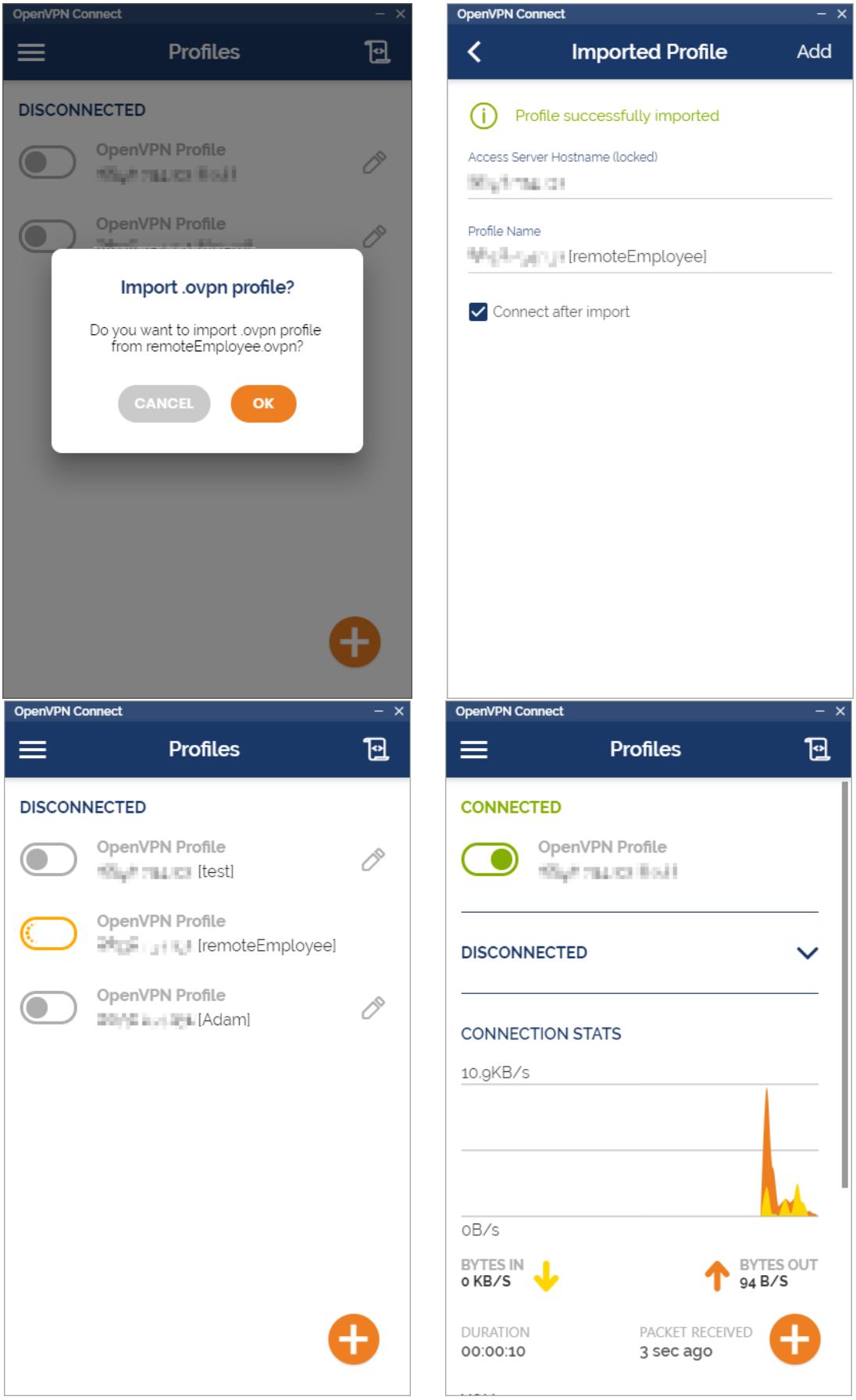
UDP is selected as the protocol as it is faster and the DNS resolver shall be Clourflare. We don't want to use compression (vulnerable to VORACLE attack, as advised in the script) and we don't want to customise the encryption settings. The choices presented in the script are safe enough.

The script is finished from here and the installation begins. Afterwards, we will make our client.

```
Tell me a name for the client.
The name must consist of alphanumeric character. It may also include an underscore or a dash.
Client name: remoteEmployee

Do you want to protect the configuration file with a password?
(e.g. encrypt the private key with a password)
   1) Add a passwordless client
   2) Use a password for the client
Select an option [1-2]: 1

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1d  10 Sep 2019
Generating an EC private key
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-4704.8gqmTH/tmp.kEZOrg'
-----
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-4704.8gqmTH/tmp.owUFQB
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'remoteEmployee'
Certificate is to be certified until Jul 22 13:47:13 2023 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Client remoteEmployee added.

The configuration file has been written to /home/sysadmin/remoteEmployee.ovpn.
Download the .ovpn file and import it in your OpenVPN client.
sysadmin@debServ:~$
```

Creating the client outputs an .ovpn file which the client can use with the OpenVPN client application to connect to the network.

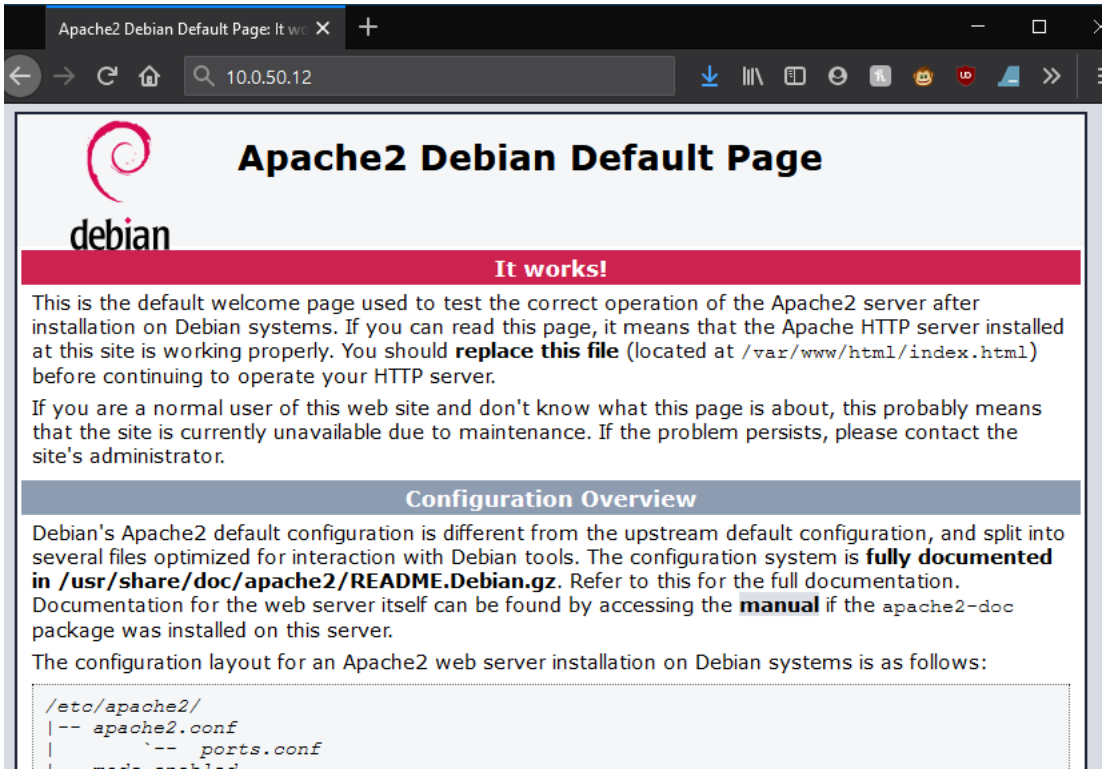
After this is all set up the connection can be tested from a client in another network. The .ovpn file is exported from the server (this can be done via ftp) and imported to the client. From there, the file is imported to OpenVPN Connect. The screenshots below show the testing process.



The test was successful, we have connection to the network!

Installing And Configuring Apache2

Apache2 requires very little configuration after installation. The command to install is `sudo apt-get install apache2`. Once the installation is finished Apache2 can be tested by entering the IP address of the server.



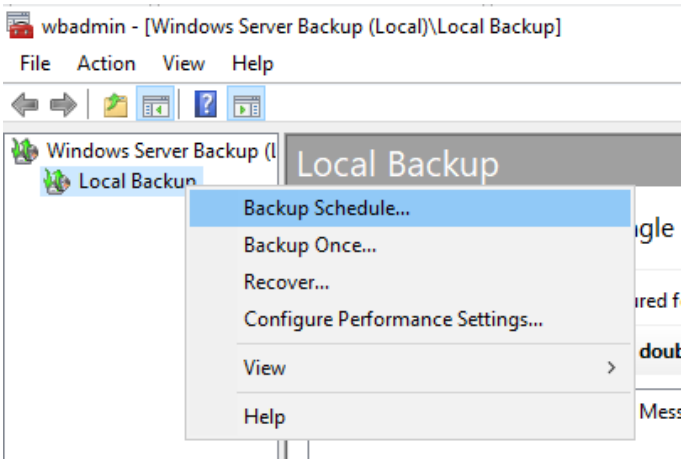
The page loads correctly, Apache2 is working.

Now we can import the Magic Memories website to /var/www/html and overwrite the default file. The web developers can take it from here.

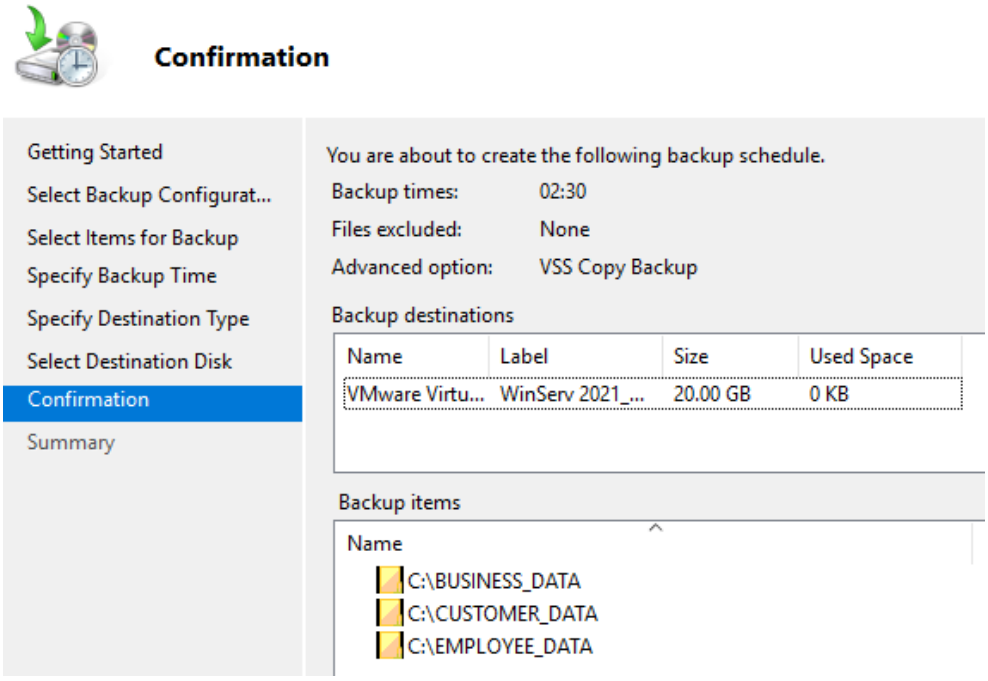
2.2.2 - COMPLIANCE AND OPERATIONAL SECURITY

Configure Daily Backups

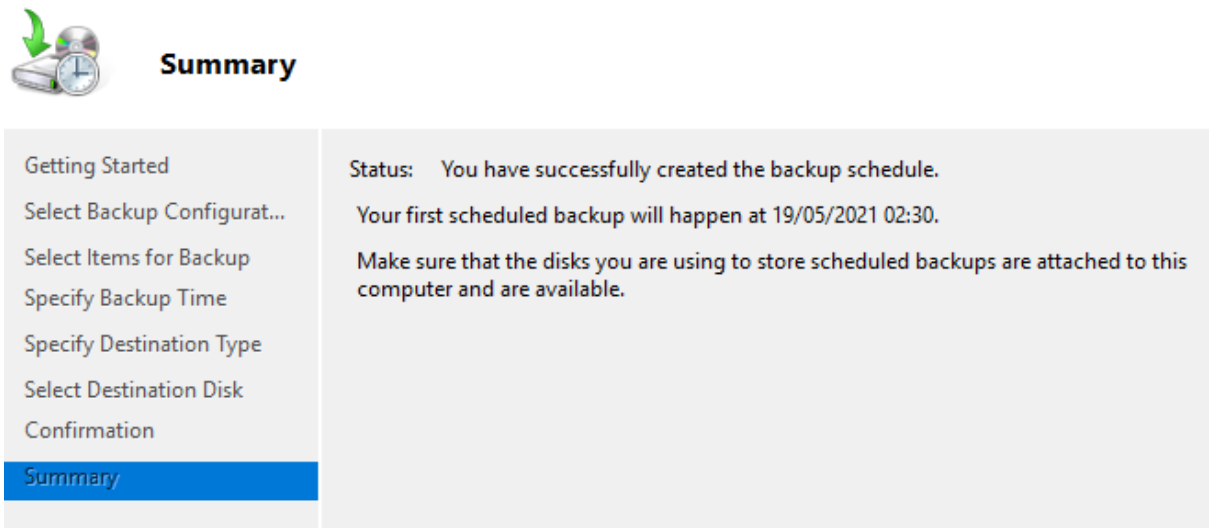
Backups are essential in case of data loss. As all client data is held on the Windows Server it is vital that this is regularly backed up. Fortunately, Windows Server has options to do this that are easy to configure. The Windows Server Backup tool is a feature that is added using the “Add Roles and Features” wizard. Once installed it is configured as below.



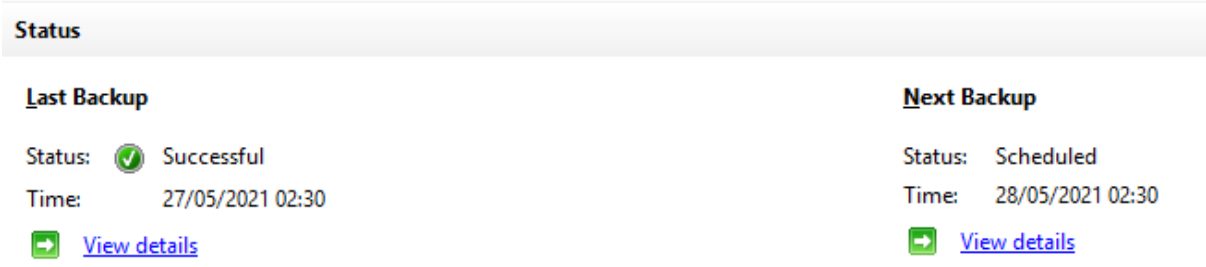
The Windows Server Backup tool has a backup schedule built in. This is what I’ll be using to configure weekly backups.



Summary of the backup configuration. The time (0230) was chosen as there are not going to be any employees using the system at this hour. The destination disk is a designated backup drive (configured from a RAID set up in the next section)



The backups have been scheduled and will now take place every dat at 0230.

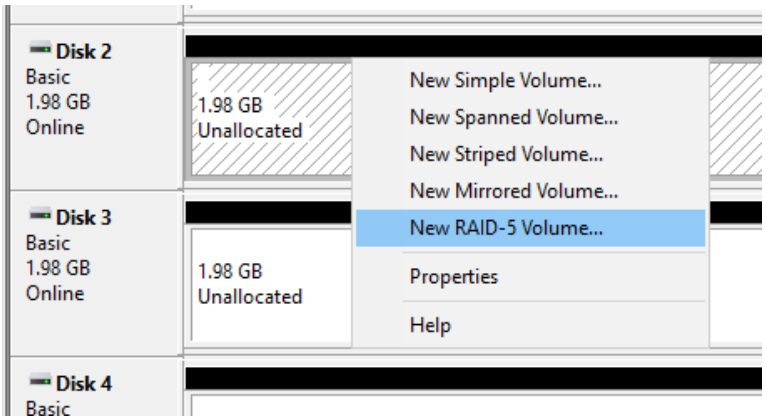


After leaving the server on all night the backup has been completed.

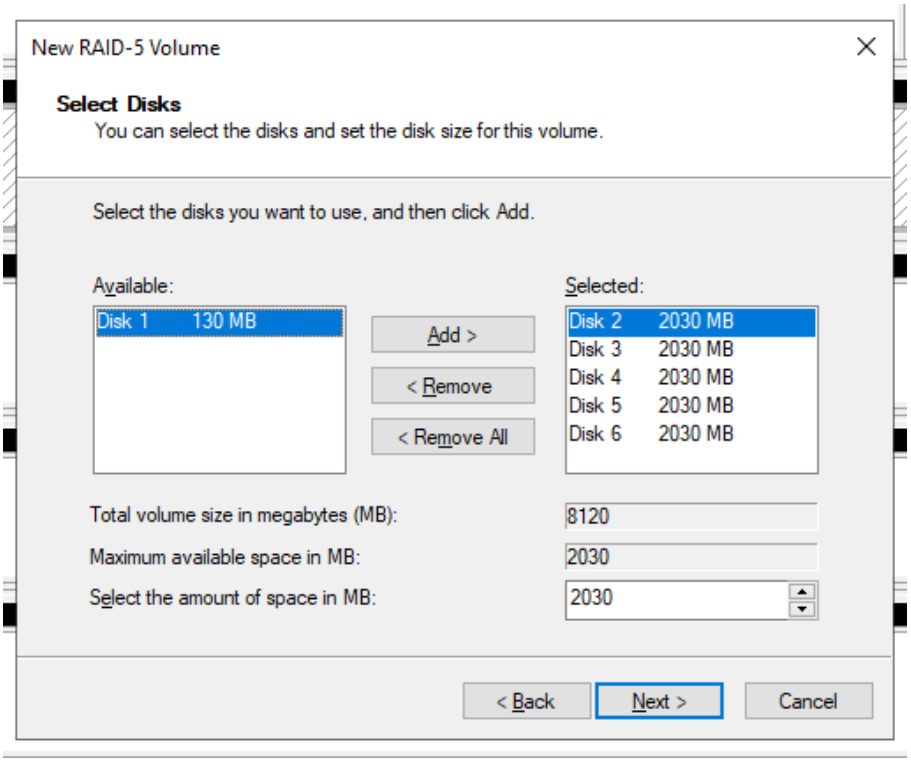
Configure RAID

A RAID (redundant array of independent disks) is a way of combining multiple storage devices to act as one unit for the purposes of increasing resistance against data loss and corruption. There are different RAID levels that work through different methods. For the important data on the Windows Server (the backup drive) I will combine several drives into a single RAID 5 storage pool. RAID 5 works by spreading the data across the disks involved and including a parity data on each drive. This is used to recalculate any missing data, allowing the array to withstand the failure of a whole drive.

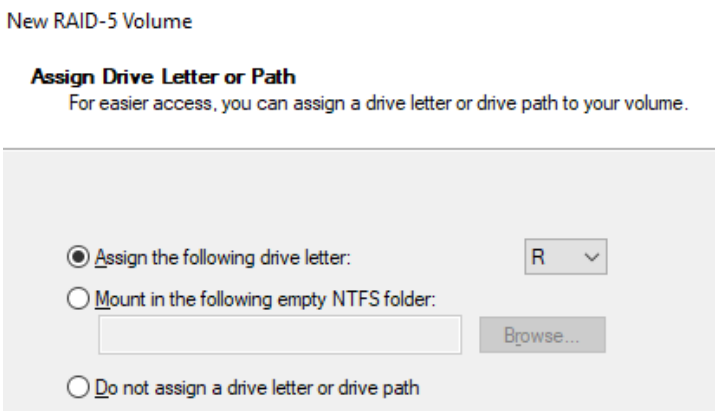
For **demonstration purposes** 5 drives of 2GB are used, but in practice RAID 5 supports 3 or more drives of any size.



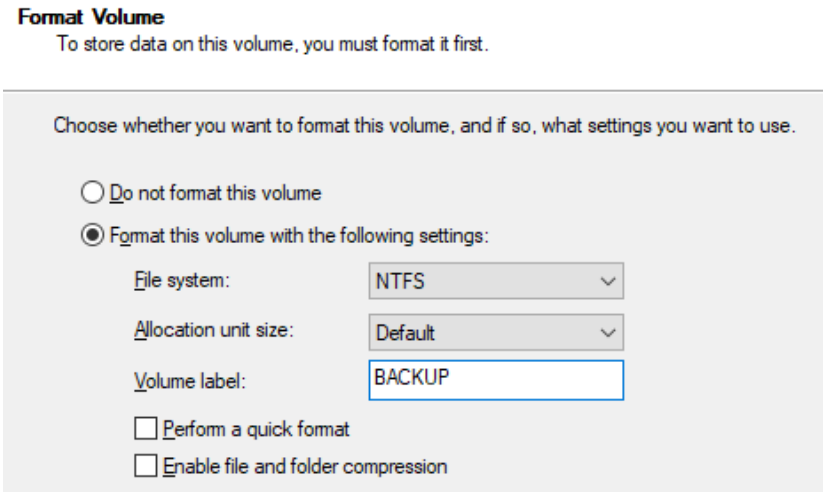
The array is built in Disk Management.



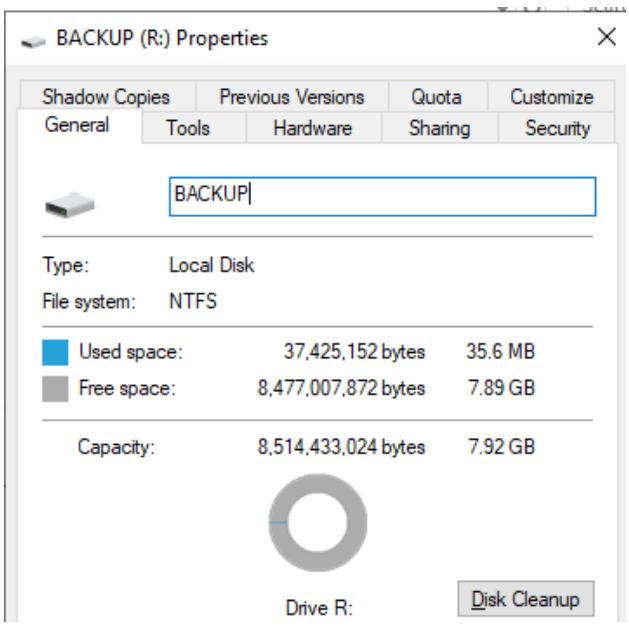
The disks are added to the array.



The drive letter is assigned in the next page of the wizard.



Formatting options…

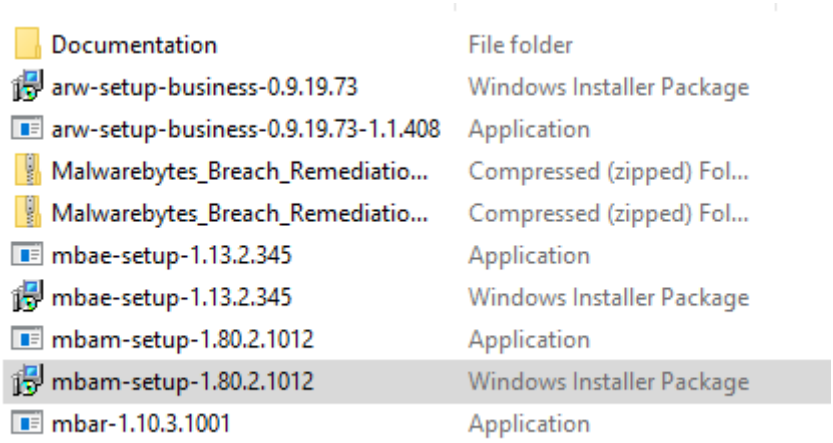


The completed array shows as a single volume, R. Note the reduced storage size caused by the parity data.

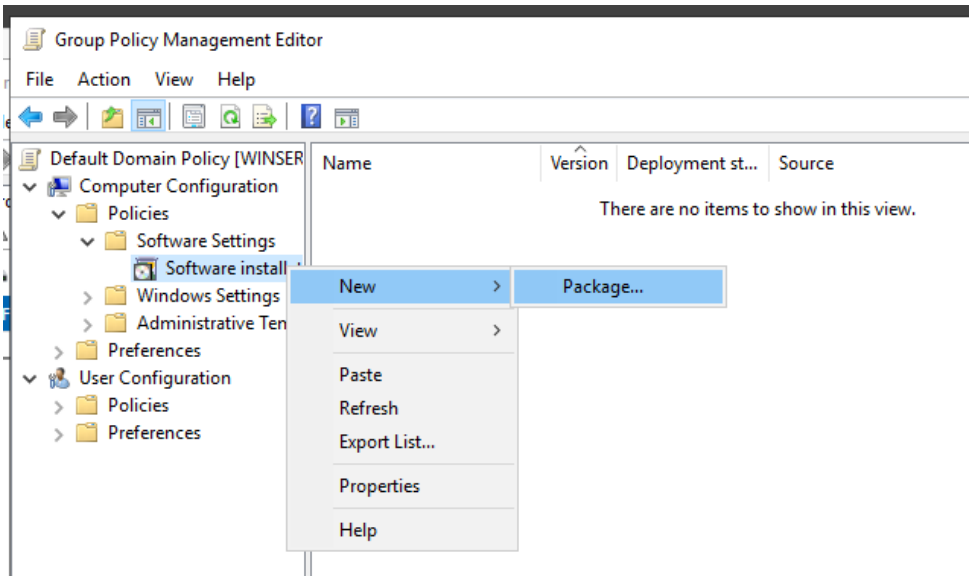
2.2.3 - THREATS AND VULNERABILITIES

Purchase and Install Anti-Malware Software

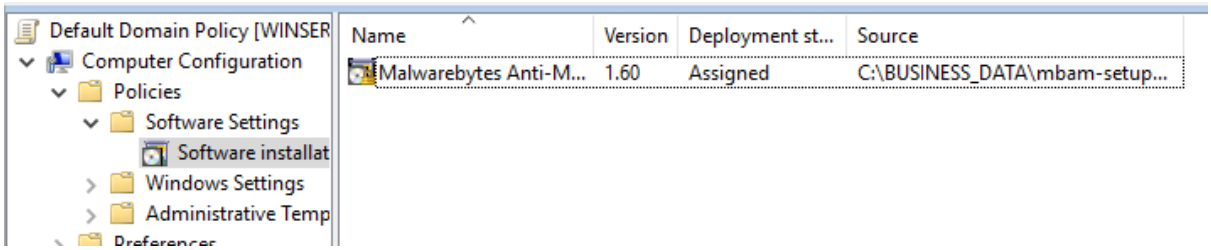
Through the use of a GPO on the Windows Server, the software for the anti-malware can be distributed to every client computer on the network when the users log on. For the anti-malware software, I will be installing Malwarebytes Antimalware for Business. Once installed, the license details can be entered to activate the software for the company. I'll be using a GPO to distribute this software to each computer that logs in. The default GPO is being used



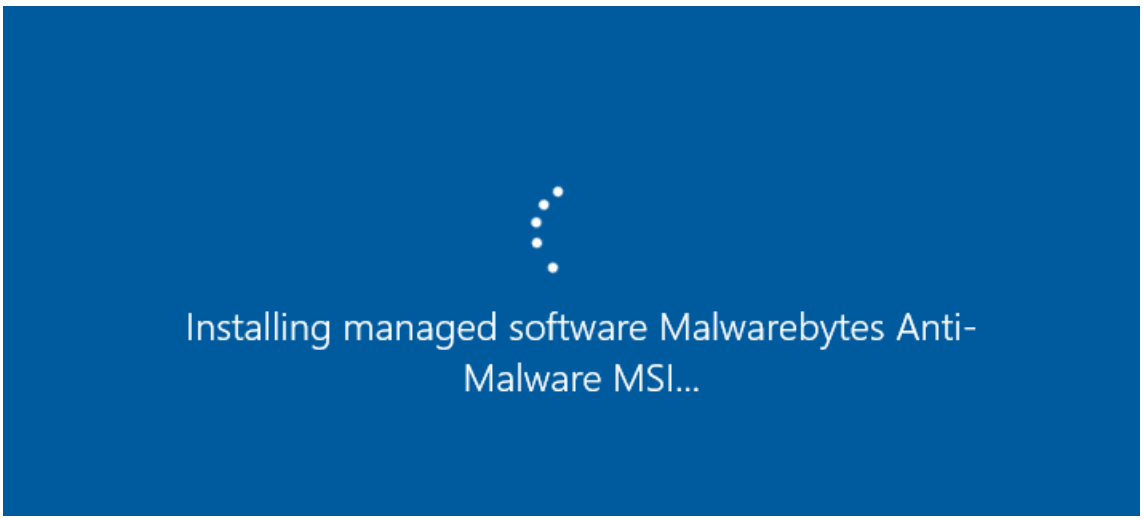
The installation file must specifically be a Windows Installer Package. Once downloaded, this is placed in a shared directory where it can be accessed by all computers in the domain.



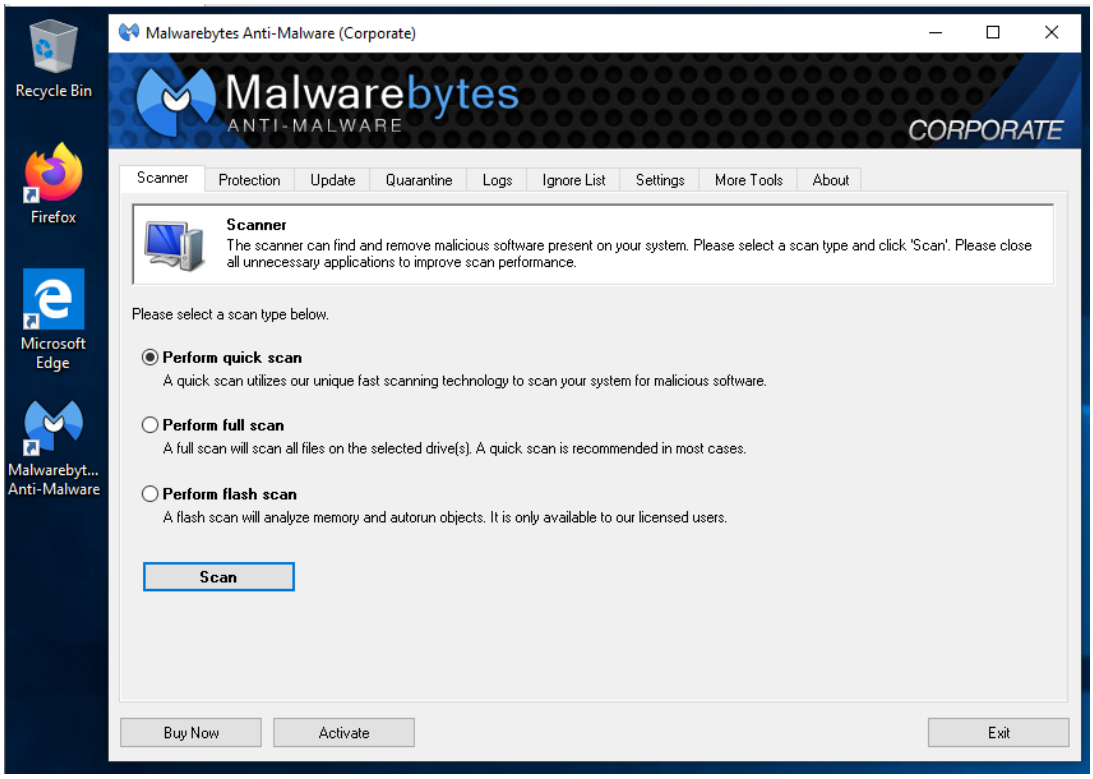
Where the software package is added to the policy.



The MSI package that will be deployed to users.

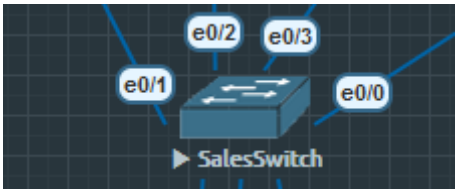


Booting a client computer (vm) connected to the domain shows a promising sign…



After logging in as a user, Malwarebytes is on the desktop and launches. Success!

Configure Switchport Security

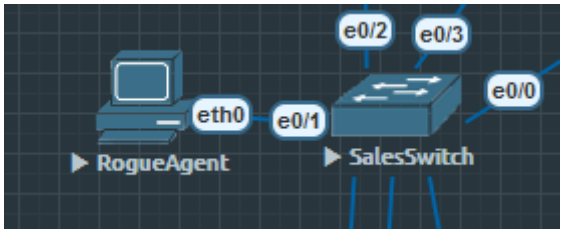


This section takes place on the department switches.

Switchport security can be configured to ensure that only authorized devices are connected to the switch interfaces. The switchport can be set to only accept a maximum number of mac address. I will be setting this to a single device for security purposes. This device/mac address can be specified with an exact address or set to be learned with “sticky” mode, in which the next connected device is remembered. The remembered device can then be forgotten after a period if desired, but as per the interview questions with the managing director it would be safer to keep it static as no other devices will be connecting. This will prevent unknown devices connecting and becoming the new learned “sticky” mac address. Furthermore, the switchports can be configured so that when an unknown device connects and the mac address is not recognized, the switch will drop the traffic and log the incident. All three of these features will be configured on the department switches.

```
SalesSW(config)#interface e0/1
SalesSW(config-if)#switchport port-security mac-address sticky
SalesSW(config-if)#switchport port-security maximum 1
SalesSW(config-if)#switchport port-security violation restrict
SalesSW(config-if)#
```

The commands to configure the three port-security options



We bring back the RogueAgent to test the security by plugging him into the interface previously used by SalesManager

```
VPCS> ping 10.0.10.12

host (10.0.10.12) not reachable

VPCS>
```

As expected, pinging SalesStaff1 fails as all traffic from the unknown MAC address is dropped by the switch.

Enable Access, Events and Security Logs

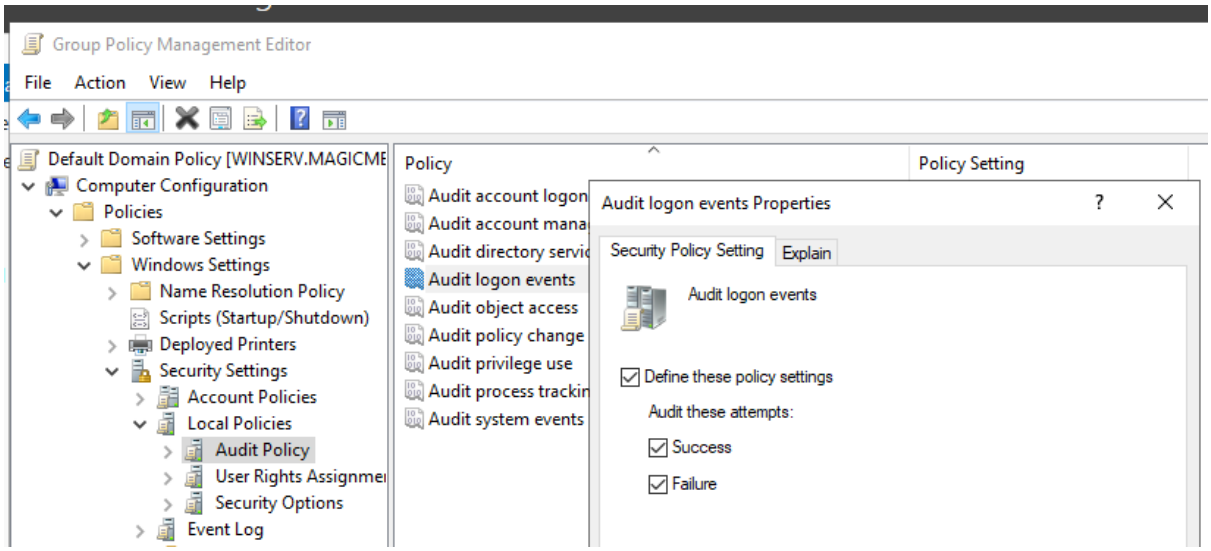
To assist in security, logs can be kept to be looked through as part of regular maintenance or in response to an incident. Continuous logging is encouraged to ensure logs are always available.

Logging can be enabled on the routers quite easily. Using the Debian server as a syslog server, we can send all logs there by from the routers. This is demonstrated on the Internal Router but can be configured on the ISP Router too.

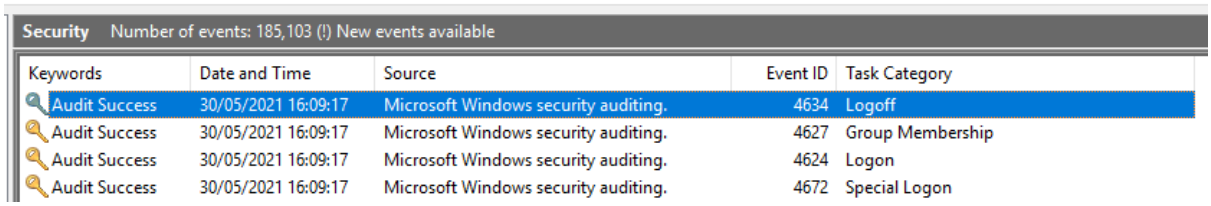
```
InternalRT(config)#logging host 10.0.50.12
InternalRT(config)#logging trap
InternalRT(config)#logging on
InternalRT(config)#service timestamps log datetime
InternalRT(config)#
```

Specifying the location for the logs, the types of logs, enabling the logs and ensuring that timestamps are added to the logs.

Windows Server keeps a lot of logs, viewable in the Event Viewer, but we can also specifically audit for events such as users logging on to the domain (or failing to log on in the case of entering an incorrect password). This can be achieved with a GPO which will be applied to all users.



Location of the group policy object and the settings used for it.



Security Number of events: 185,103 (!) New events available

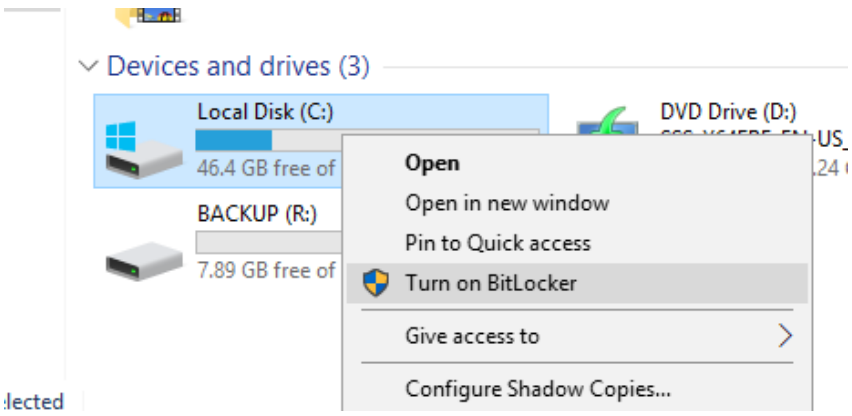
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	30/05/2021 16:09:17	Microsoft Windows security auditing.	4634	Logoff
Audit Success	30/05/2021 16:09:17	Microsoft Windows security auditing.	4627	Group Membership
Audit Success	30/05/2021 16:09:17	Microsoft Windows security auditing.	4624	Logon
Audit Success	30/05/2021 16:09:17	Microsoft Windows security auditing.	4672	Special Logon

After logging off the client VM the logoff entry is visible in the Event Viewer. Success!

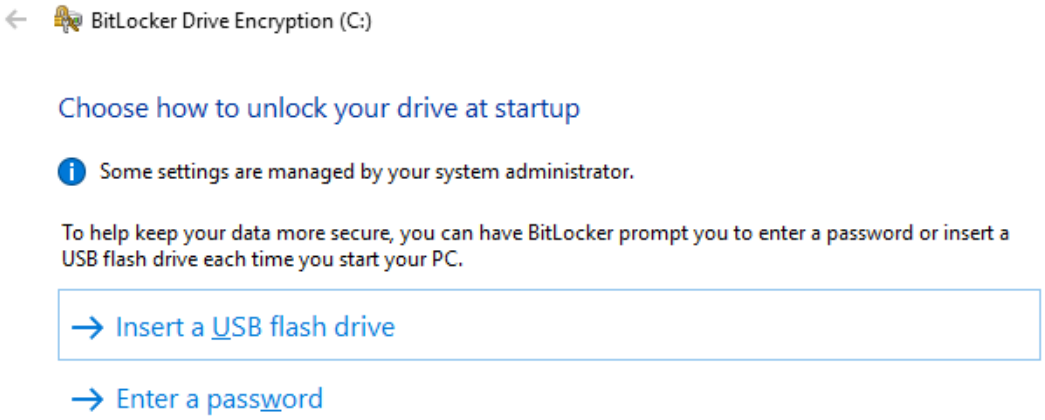
2.2.4 - APPLICATION, DATA AND HOST SECURITY

Encrypt Hard Disks

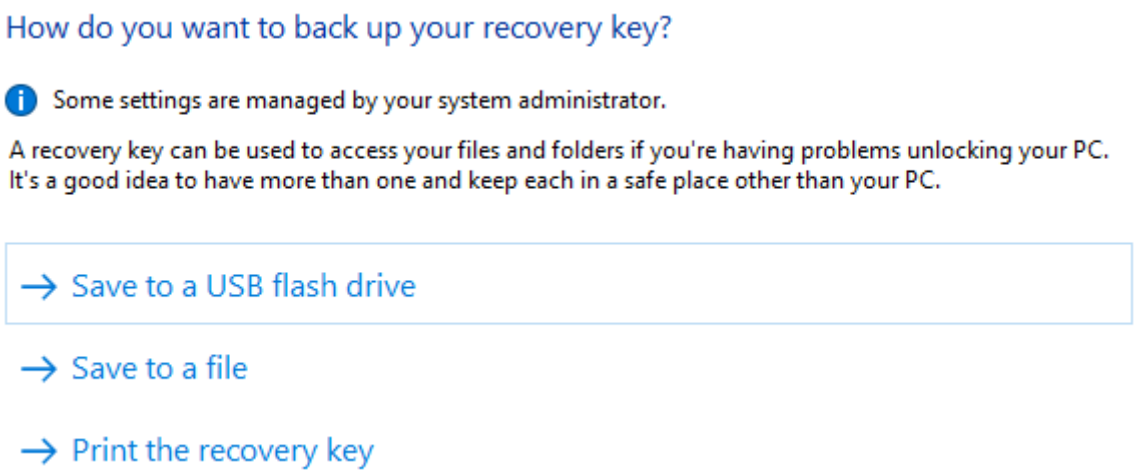
Hard drive encryption prevents unauthorised access to the drives. One of the methods to achieve this is to use Windows' BitLocker feature. This will require a password at boot before the hard drive can be used, rendering the data inaccessible even if the hard drives are removed from the computers and stolen.



The easiest way to configure BitLocker is to right click on the drive to be encrypted and choose the option. This takes us to the BitLocker wizard.



There are two options in the wizard. A standard password or passphrase can be used, or a USB flash drive can be configured as a key. I will be using a password ***for demonstration purposes only****. In deployment, the most secure option is to use a flash drive, adding another layer of security to the encryption as the 'key' drive will also have to be stolen to access the data.*



*The recovery option I will be using here is to print the key. This is **for demonstration purposes only.** The safest (and recommended for deployment) method is to save the key as a file to a remote location, to a USB flash drive, and to make a physical note. Multiple recovery options keep the drive data from being lost, but more copies mean more things to secure. My recommendation is to print a recovery document and keep it in the company safe.*

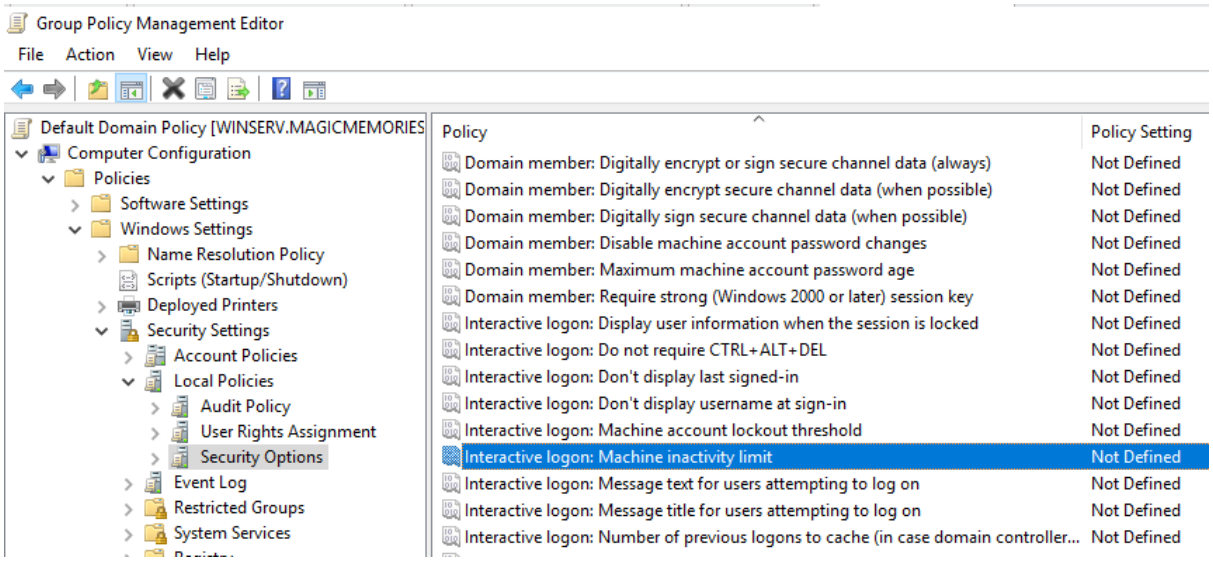
From here, a few options are selected such as choosing whether to encrypt the whole disk or just the space used. These are configured as required by the deployment. The last step is to restart the computer to enable the encryption.

*After restarting the prompt appears to enter the password. Note: the password used is **for demonstration purposes only** and in deployment a much stronger password or passphrase is recommended if a password is to be used in lieu of a USB flash drive key.*

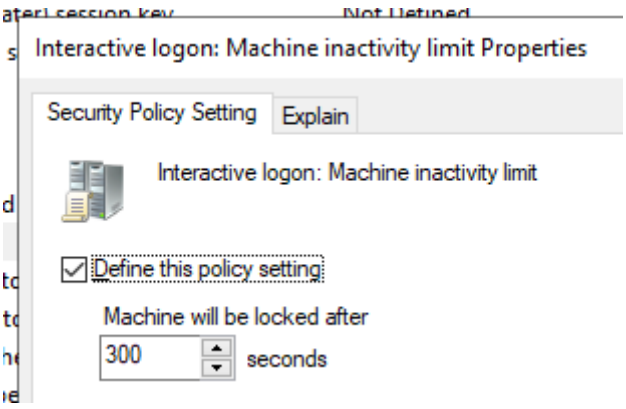
The encryption process can be repeated on every hard drive as needed.

Implement Screen-Locking Policy

All staff should lock their computer screen upon leaving their desk. This prevents any shoulder-surfing attacks. Realistically, some employees will forget so we can use a Group Policy Object on the Windows Server to help them out. By applying this GPO to the default domain policy, it will affect *all* users.



Location of the policy to enforce.



If a user is inactive for 5 minutes the screensaver starts and the screen locks. This value can be changed as per the business needs.

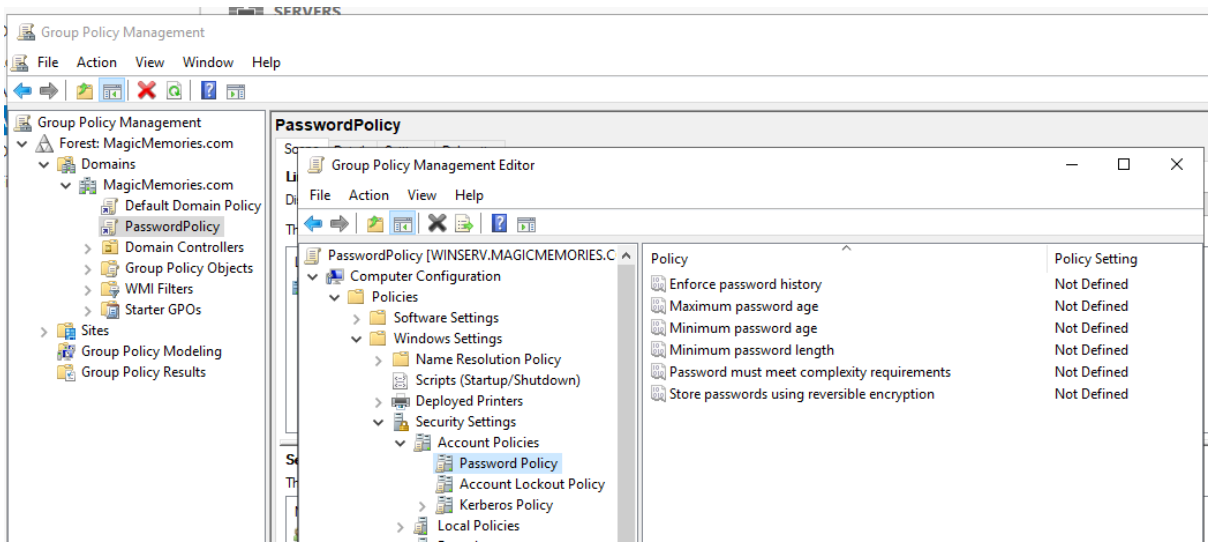
2.2.5 - ACCESS CONTROL AND IDENTITY MANAGEMENT

Creating A Password Policy

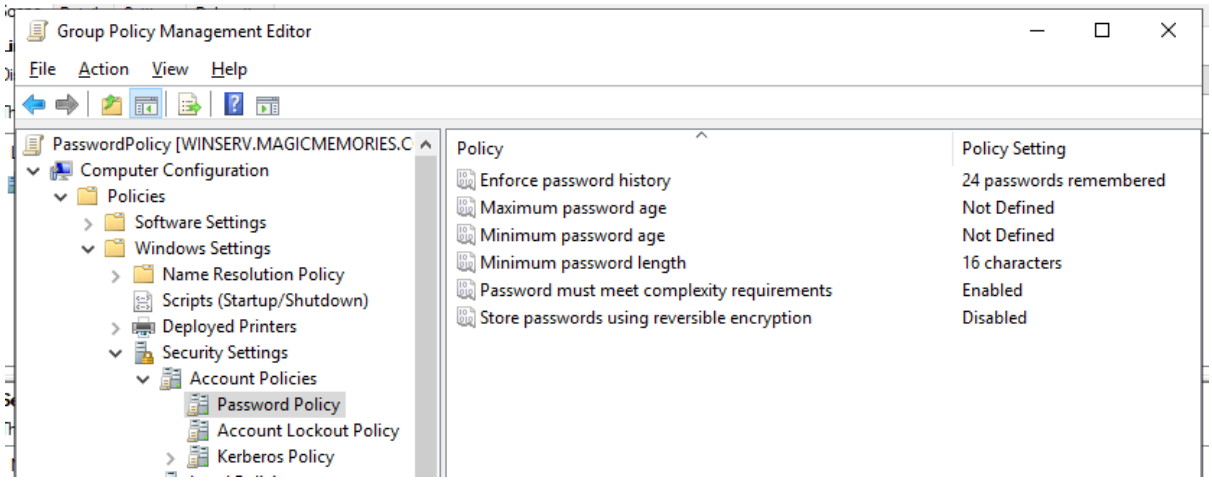
As per the proposed solution, a password policy shall be put into place to enhance the security of individuals' accounts. The policy shall be as follows:

- Passphrases encouraged over passwords
- Minimum length of 16 characters
- Passwords cannot contain the user's name or account name
- No mandatory password changes (passwords should be changed at suspected compromise instead)
- The last 24 entered passwords cannot be re-used.
- Passwords cannot be changed by the user for 2 days after last change (prevents brute-forcing of password expiration to enable use of previous, compromised password).
- Enforce complexity requirements, at least three from:
    - Uppercase characters
    - Lowercase characters
    - Digits 0 - 9
    - Non-alphanumeric symbols (!, $, &, {, etc.).
- Account lockout after three incorrect attempts

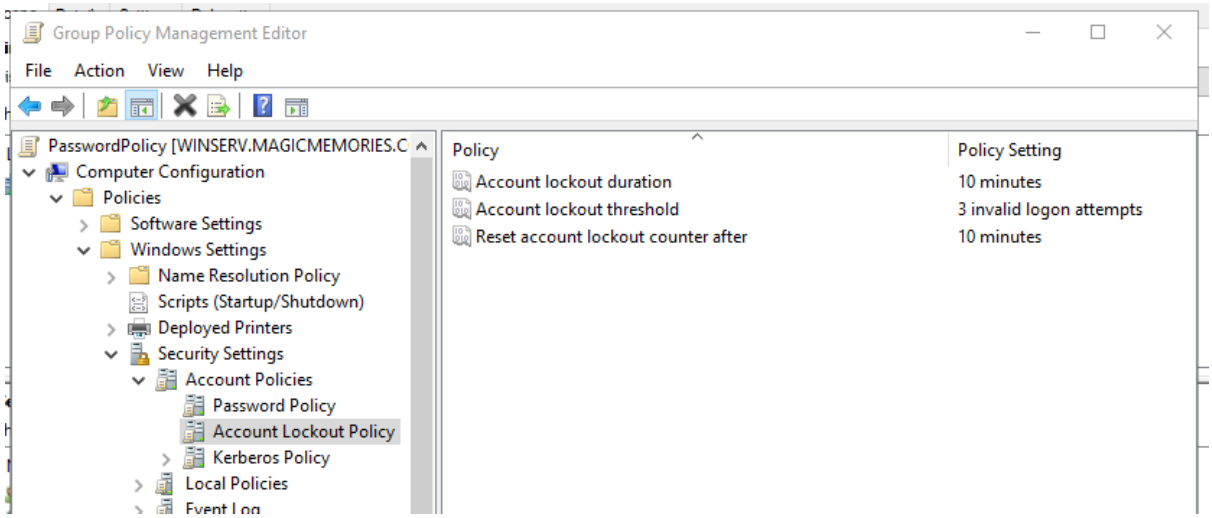
A Group Policy Object can be used for controlling the password policy.



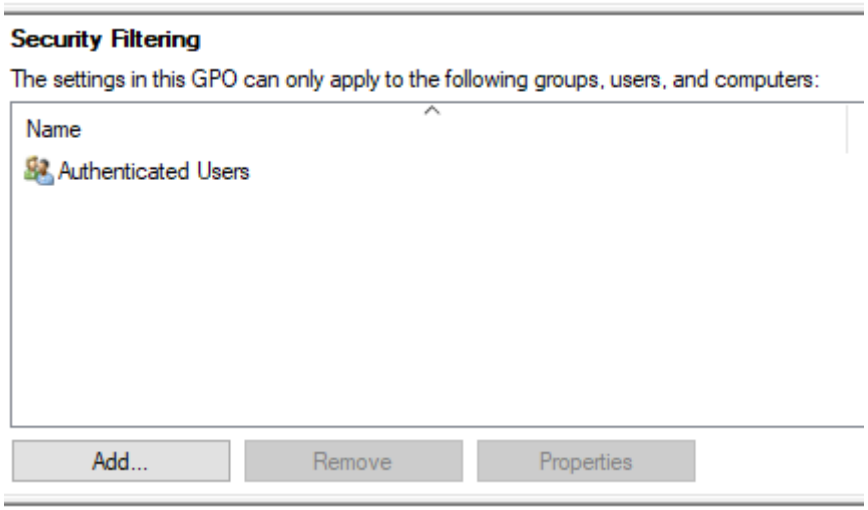
The GPO can be edited in here by right clicking each policy, editing its properties and clicking 'Apply'.



The updated GPO showing the password policy in place.

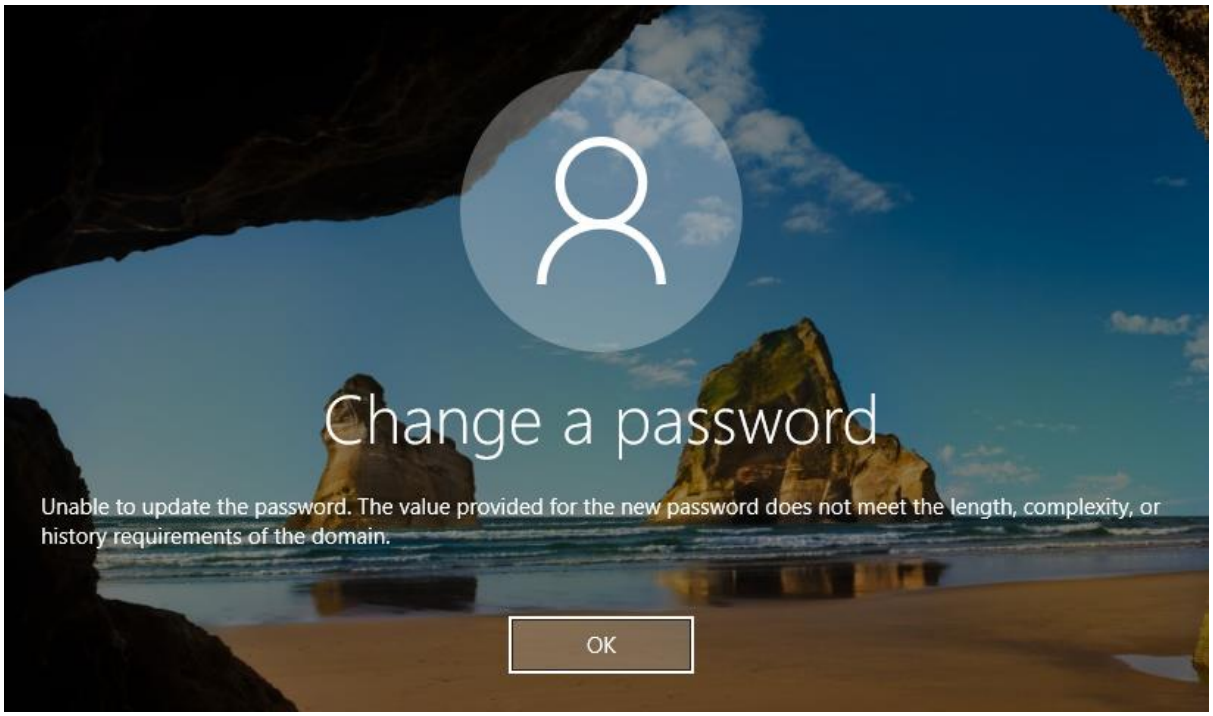


To adjust the account lockout settings, changes must be made to the Account Lockout Policy, as seen here.



The GPO must be applied to all authenticated users.

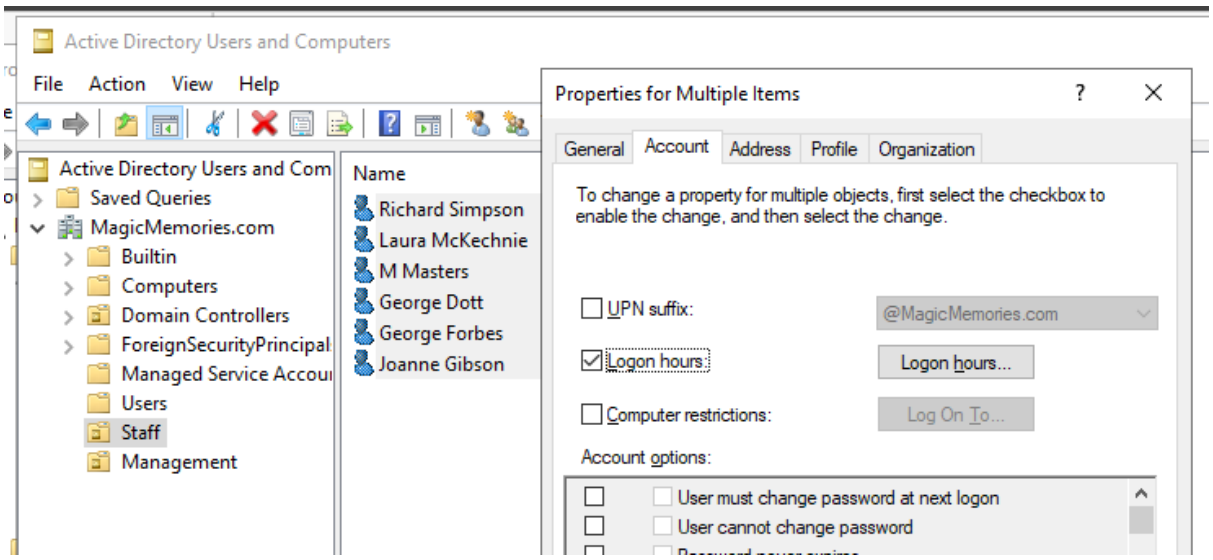
Attempting to change the password to one that does not meet the requirements…



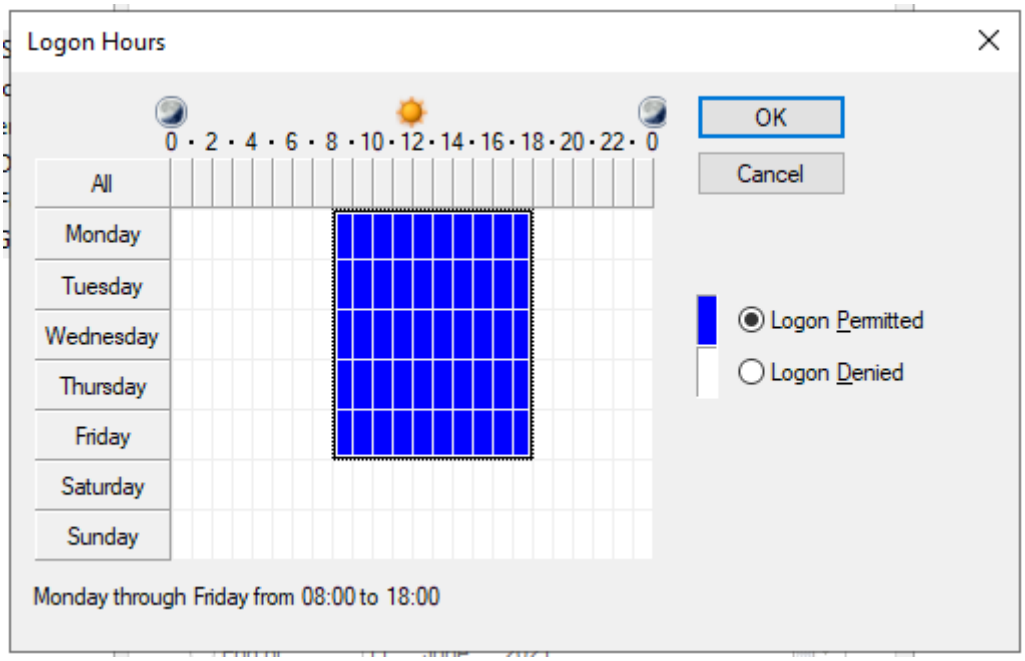
…the password is not accepted, policy successfully implement.

Restricting Logon Hours

As per the discussion with the managing director, the hours in which non-management staff can log into the system will be reduced to 0800 to 1800. The reasoning is that these are the working hours when staff would normally be logging in. Anything outside of this time could be suspicious.This can be achieved by editing the users in the Staff OU.



The logon hours checkbox must be ticked before the longon hours can be configured.



The configured logon hours.

The testing is simple. Try to log on after 6pm. Test successful.

2.3 - TESTING

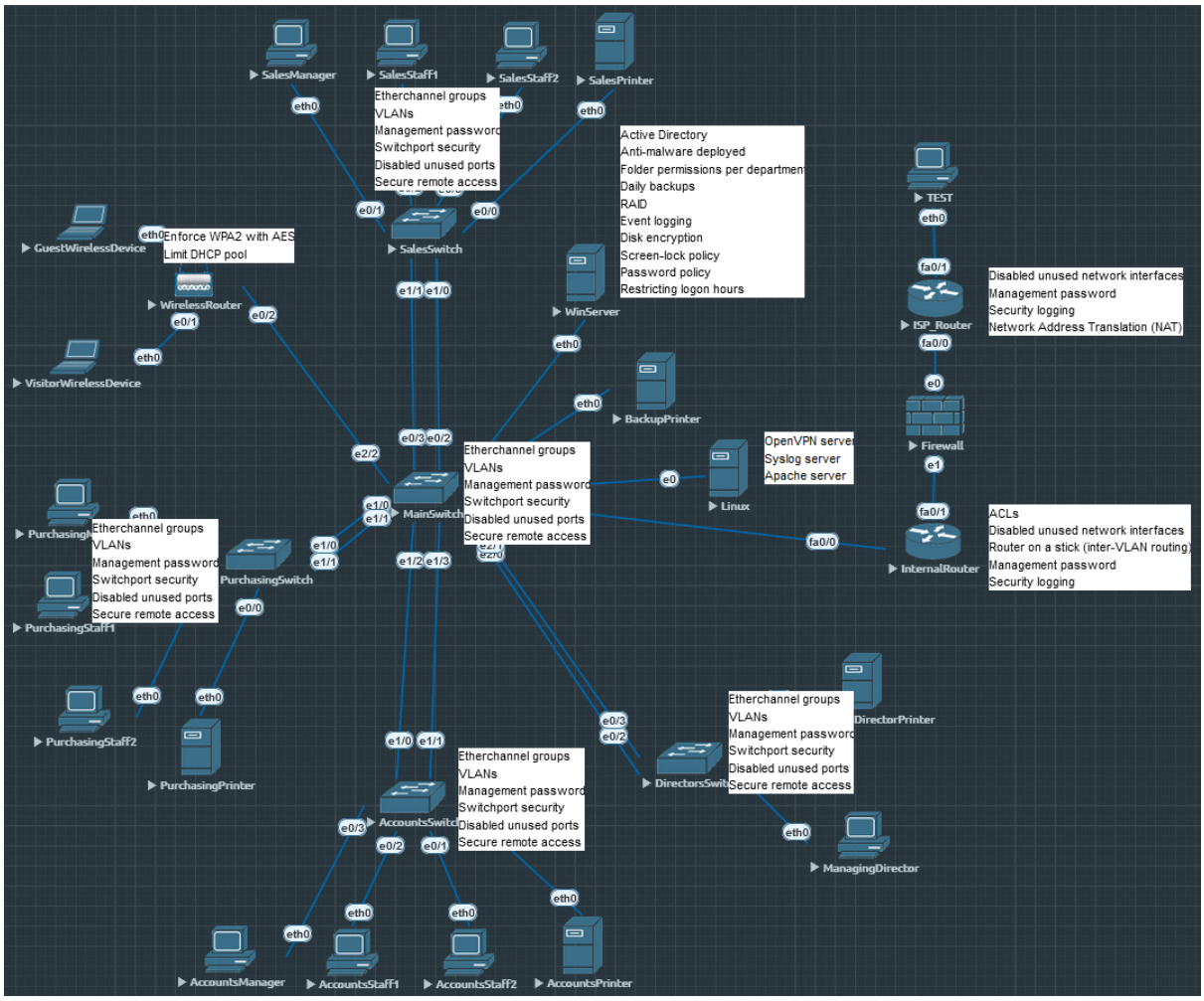
Testing of the implementations was conducted throughout the process, often immediately after a feature was configured. This approach saved coming back to each item later when my head may be in another space. The results of the test are included in the implementation section, but a summary test log is included below.

NETWORK SECURITY	TEST METHOD	RESULT	DATE	SIGNED
Subnet the network	Ping default gateway, IP address in another network from a staff computer	Success	19/05/2021	A.G.
Combining ports with Etherchannel				
Implement VLANs per department				
Configure “router on a stick”				
Set management passwords on the routers/switches	Log in via console, check entries in running-config	Success	19/05/2021	A.G.
Implement ACLS	Ping devices in another subnet from a staff computer	Ping successfully blocked	19/05/2021	A.G.
Configure hardware firewall				
Restrict open network interfaces	Ping default gateway from a forbidden interface	Ping fails to get through	19/05/2021	A.G.
Implement NAT on the ISP router	Ping test computer from inside the network	Success	19/05/2021	A.G.
Harden Wireless	Connect and receive IP address via DHCP	Success	20/05/2021	A.G.
	Ping default gateway and host on another subnet	Success	20/05/2021	A.G.
COMPLIANCE AND OPERATIONAL SECURITY	**TEST METHOD**	**RESULT**	**DATE**	**SIGNED**
Daily local backups	Leave server on past scheduled backup time	Success	27/05/2021	A.G.
Configure RAID	Mount the RAID drive on the server for use as storage	Success	27/05/2021	A.G.
THREATS AND VULNERABILITIES	**TEST METHOD**	**RESULT**	**DATE**	**SIGNED**
Purchase anti-malware software	Install anti-malware software via deployment by GPO	Success	24/05/2021	A.G.
Configure switchport security	Attempt to connect a rogue device on the switchport	Device traffic successfully blocked	20/05/2021	A.G.
Disable unused switchports	Attempt to connect a rogue device to an unused switchport	Device unable to connect, success	20/05/2021	A.G.
Keep access, events, and security logs	Log in and out of the domain with a client and view the event in the Event Viewer	Success	30/05/2021	A.G.

APPLICATION, DATA AND HOST SECURITY	TEST METHOD	RESULT	DATE	SIGNED
Purchase and install anti-malware software	Log in as client to see if software installed	Success	25/05/2021	A.G.
Encrypt hard disks	Boot computer after enabling BitLocker encryption	Success	23/05/2021	A.G.
Implement screen locking policy when employees away from desk	Leave desktop unattended for duration of timeout before locking	Success	26/05/2021	A.G.
ACCESS CONTROL AND IDENTITY MANAGEMENT	**TEST METHOD**	**RESULT**	**DATE**	**SIGNED**
Implement password policy changes	Change password to unacceptable, receive prompt	Success	25/05/2021	A.G.
Lockout after incorrect guesses	Use incorrect password 3 times	Success	25/05/2021	A.G.
Restrict logon hours	Attempt to log in as client outside of configured hours	Success	25/05/2021	A.G.

2.4 - NETWORK DIAGRAM WITH UPDATES

The network upgrades have been demonstrated so included below is a diagram of the Magic Memories network with the changes labelled for use as a quick guide to what has been done.



The completed network upgrade

2.5 - NETWORK DEVICES RUNNING CONFIGS

In this section I have included the running configurations of the various networking devices. These have been copied directly from console access after the network was completed.

Internal Router

```
Current configuration : 4243 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime
service password-encryption
!
hostname InternalRT
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$W73u$eJ8FFD.QroYqPPUgw6DEN0
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
```

```
!
!
!
!
interface Port-channel1
 no ip address
 hold-queue 0 in
!
interface Port-channel1.10
 encapsulation dot1Q 10
!
interface Port-channel1.20
 encapsulation dot1Q 20
!
interface Port-channel1.30
 encapsulation dot1Q 30
!
interface Port-channel1.40
 encapsulation dot1Q 40
!
interface Port-channel1.50
 encapsulation dot1Q 50
!
interface Port-channel1.60
 encapsulation dot1Q 60
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.0.10.1 255.255.255.0
 ip access-group 110 in
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.0.20.1 255.255.255.0
 ip access-group 110 in
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.0.30.1 255.255.255.0
!
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 10.0.40.1 255.255.255.0
!
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 10.0.50.1 255.255.255.0
 ip access-group 150 in
!
interface FastEthernet0/0.60
 encapsulation dot1Q 60
 ip address 10.0.60.1 255.255.255.0
!
interface FastEthernet0/0.99
 encapsulation dot1Q 99
 ip address 10.0.99.1 255.255.255.0
!
interface FastEthernet0/0.101
```

```
 encapsulation dot1Q 101
 ip address 10.0.101.1 255.255.255.0
 ip access-group 101 in
 ip access-group 101 out
!
interface FastEthernet0/1
 ip address 10.0.100.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 no ip address
 speed auto
 half-duplex
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface vmi99
 no ip address
!
ip forward-protocol nd
ip route 10.0.0.0 255.255.255.0 FastEthernet0/1
ip route 10.0.100.0 255.255.255.0 FastEthernet0/1
ip route 10.0.200.0 255.255.255.0 FastEthernet0/1
ip route 192.168.10.0 255.255.255.0 FastEthernet0/1
!
!
ip http server
no ip http secure-server
!
logging 10.0.50.12
access-list 101 permit ip any any
access-list 110 remark Master ACL for internal network
access-list 110 permit tcp any any eq smtp
access-list 110 permit tcp any any eq pop3
access-list 110 permit ip any host 10.0.50.8
access-list 110 permit ip any host 10.0.50.11
access-list 110 permit ip any host 10.0.50.12
access-list 110 permit tcp host 10.0.10.11 any eq www
access-list 110 permit tcp host 10.0.10.11 any eq 8080
access-list 110 permit tcp host 10.0.10.11 any eq 443
access-list 110 deny   ip host 10.0.20.8 any
access-list 110 permit tcp 10.0.20.8 0.0.0.7 any eq www
access-list 110 permit tcp 10.0.20.8 0.0.0.7 any eq 8080
access-list 110 permit tcp 10.0.20.8 0.0.0.7 any eq 443
access-list 110 permit tcp host 10.0.30.11 any eq www
access-list 110 permit tcp host 10.0.30.11 any eq 8080
access-list 110 permit tcp host 10.0.30.11 any eq 443
access-list 110 permit tcp host 10.0.40.11 any eq www
access-list 110 permit tcp host 10.0.40.11 any eq 8080
access-list 110 permit tcp host 10.0.40.11 any eq 443
access-list 150 remark ACL for Server subnet
access-list 150 permit ip host 10.0.50.8 10.0.0.0 0.255.255.255
access-list 150 permit ip host 10.0.50.11 any
access-list 150 permit ip host 10.0.50.12 any
!
!
!
!
```

```
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner motd ^C

  __  __              _
 |  \/  | __ _  __ _(_) ___
 | |\/| |/ _` |/ _` | |/ __|
 | |  | | (_| | (_| | | (__
 |_|  |_|\__,_|\__, |_|\___|
  __  __        |___/                _
 |  \/  | ___ _ __ ___   ___  _ __(_) ___  ___
 | |\/| |/ _ \ '_ `  _ \ / _ \| '__| |/ _ \/ __|
 | |  | |  __/ | | | | | (_) | |  | |  __/\__ \
 |_|  |_|\___|_| |_| |_|\___/|_|  |_|\___||___/

>"InternalRouter"

/!\/!\  WARNING! UNAUTHORISED ACCESS TO  /!\/!\
        THIS DEVICE WILL RESULT IN LEGAL
        ACTION BEING TAKEN AGAINST YOU!
/!\/!\       YOU HAVE BEEN WARNED!       /!\/!\
^C
!
line con 0
 password 7 121404101B085D5679
 login
line aux 0
line vty 0 4
 password 7 0702204B470A59544541
 login
 transport input ssh
!
!
end
```

ISP_Router

```
Current configuration : 1922 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISProuter
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$mjsX$l9WArbyxpXBkapgwL1AQX0
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.200.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
```

```
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 speed auto
 full-duplex
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1 100
ip route 10.0.0.0 255.255.255.0 FastEthernet0/1
ip route 10.10.10.0 255.255.255.0 FastEthernet0/1
!
!
ip http server
no ip http secure-server
ip nat inside source list INSIDE-HOSTS interface FastEthernet0/0 overload
!
ip access-list standard INSIDE-HOSTS
 permit 10.0.0.0 0.255.255.255
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
banner motd ^C
  __   __              _
 |  \/  | __ _  __ _(_) ___
 | |\/| |/ _` |/ _` | |/ __|
 | |  | | (_| | (_| | | (__
 |_|  |_|\__,_|\__, |_|\___|
  __   __        |___/                _
 |  \/  | ___ _ __ ___   ___  _ __(_) ___  ___
 | |\/| |/ _ \ '_ ` _ \ / _ \| '__| |/ _ \/ __|
 | |  | |  __/ | | | | | (_) | |  | |  __/\__ \
 |_|  |_|\___|_| |_| |_|\___/|_|  |_|\___||___/

>"ISP_Router"
```

```
/!\/!\  WARNING! UNAUTHORISED ACCESS TO  /!\/!\
        THIS DEVICE WILL RESULT IN LEGAL
        ACTION BEING TAKEN AGAINST YOU!
/!\/!\       YOU HAVE BEEN WARNED!       /!\/!\

^C
!
line con 0
 password magic123
 login
line aux 0
line vty 0 4
 password magic123
 login
 transport input ssh
!
!
end
```

Main Switch

```
Current configuration : 2354 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname MainSW
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
clock timezone EET 2 0
!
ip cef
!
!
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Port-channel40
 switchport
 switchport access vlan 40
 switchport mode access
!
interface Port-channel30
 switchport
 switchport access vlan 30
 switchport mode access
!
interface Port-channel20
 switchport
 switchport access vlan 20
 switchport mode access
!
interface Port-channel10
 switchport
 switchport access vlan 10
```

```
 switchport mode access
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 duplex auto
!
interface Ethernet0/2
 switchport access vlan 10
 switchport mode access
 duplex auto
 channel-group 10 mode auto
!
interface Ethernet0/3
 switchport access vlan 10
 switchport mode access
 duplex auto
 channel-group 10 mode auto
!
interface Ethernet1/0
 switchport access vlan 20
 switchport mode access
 duplex auto
 channel-group 20 mode auto
!
interface Ethernet1/1
 switchport access vlan 20
 switchport mode access
 duplex auto
 channel-group 20 mode auto
!
interface Ethernet1/2
 switchport access vlan 30
 switchport mode access
 duplex auto
 channel-group 30 mode auto
!
interface Ethernet1/3
 switchport access vlan 30
 switchport mode access
 duplex auto
 channel-group 30 mode auto
!
interface Ethernet2/0
 switchport access vlan 40
 switchport mode access
 duplex auto
 channel-group 40 mode auto
!
interface Ethernet2/1
 switchport access vlan 40
 switchport mode access
 duplex auto
 channel-group 40 mode auto
!
interface Ethernet2/2
 duplex auto
!
interface Ethernet2/3
 switchport access vlan 50
 switchport mode access
 duplex auto
!
interface Ethernet3/0
 switchport access vlan 50
```

```
 switchport mode access
 duplex auto
!
interface Ethernet3/1
 switchport access vlan 50
 switchport mode access
 duplex auto
!
interface Ethernet3/2
 duplex auto
!
interface Ethernet3/3
 duplex auto
!
!
no ip http server
!
!
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Sales Switch

```
Current configuration : 2202 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname SalesSW
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 KPGGJ8oTopHGG6x4n3yS9mLLXJmHM.RSvg4KGNDWAZM
!
no aaa new-model
clock timezone EET 2 0
!
ip cef
!
!
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Port-channel10
 switchport
 switchport access vlan 10
 switchport mode access
!
interface Ethernet0/0
 switchport access vlan 10
 switchport mode access
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address 0050.7966.680e
 duplex auto
```

```
!
interface Ethernet0/2
 switchport access vlan 10
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 switchport access vlan 10
 switchport mode access
 duplex auto
!
interface Ethernet1/0
 switchport access vlan 10
 switchport mode access
 duplex auto
 channel-group 10 mode desirable
!
interface Ethernet1/1
 switchport access vlan 10
 switchport mode access
 duplex auto
 channel-group 10 mode desirable
!
interface Ethernet1/2
 shutdown
 duplex auto
!
interface Ethernet1/3
 shutdown
 duplex auto
!
!
no ip http server
!
!
!
!
!
control-plane
!
banner motd ^C
  __  __              _
 |  \/  | __ _  __ _(_) ___
 | |\/| |/ _` |/ _` | |/ __|
 | |  | | (_| | (_| | | (__
 |_|  |_|\__,_|\__, |_|\___|
  __  __        |___/                _
 |  \/  | ___ _ __ ___   ___  _ __(_) ___  ___
 | |\/| |/ _ \ '_ `  _ \ / _ \| '__| |/ _ \/ __|
 | |  | |  __/ | | | | | (_) | |  | |  __/\__ \
 |_|  |_|\___|_| |_| |_|\___/|_|  |_|\___||___/

>"SalesSW"

/!\/!\  WARNING! UNAUTHORISED ACCESS TO  /!\/!\
        THIS DEVICE WILL RESULT IN LEGAL
        ACTION BEING TAKEN AGAINST YOU!
/!\/!\       YOU HAVE BEEN WARNED!       /!\/!\

^C
!
line con 0
 password 7 141A130C05077B7977
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 13081615020F447B7977
```

```
 login
 transport input ssh
!
end
```

Purchasing Switch

```
Current configuration : 2049 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname PurchasingSW
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 KPGGJ8oTopHGG6x4n3yS9mLLXJmHM.RSvg4KGNDWAZM
!
no aaa new-model
clock timezone EET 2 0
!
ip cef
!
!
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Port-channel20
 switchport
 switchport access vlan 20
 switchport mode access
!
interface Ethernet0/0
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport access vlan 20
```

```
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet1/0
 switchport access vlan 20
 switchport mode access
 duplex auto
 channel-group 20 mode desirable
!
interface Ethernet1/1
 switchport access vlan 20
 switchport mode access
 duplex auto
 channel-group 20 mode desirable
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
!
no ip http server
!
!
!
!
!
control-plane
!
banner motd ^C
  __   __              _
 |  \/  | ___ _  ___ _(_) ___
 | |\/| |/ _` |/ _` | |/ __|
 | |  | | (_| | (_| | | (__
 |_|  |_|\__,_|\__, |_|\___|
  __   __        |___/                 _
 |  \/  | ___ _ __ ___   ___  _ __(_) ___   ___
 | |\/| |/ _ \ '_ `_ \ / _ \| '__| |/ _ \/ __|
 | |  | |  __/ | | | | | (_) | |  | |  __/\__ \
 |_|  |_|\___|_| |_| |_|\___/|_|  |_|\___||___/

>"PurchasingSW"


/!\/!\  WARNING! UNAUTHORISED ACCESS TO  /!\/!\
        THIS DEVICE WILL RESULT IN LEGAL
        ACTION BEING TAKEN AGAINST YOU!
/!\/!\       YOU HAVE BEEN WARNED!       /!\/!\

^C
!
line con 0
 password 7 060B0E26454D584B56
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 0702204B470A59544541
 login
 transport input ssh
!
end
```

Accounts Switch

```
Current configuration : 2045 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname AccountsSW
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 KPGGJ8oTopHGG6x4n3yS9mLLXJmHM.RSvg4KGNDWAZM
!
no aaa new-model
clock timezone EET 2 0
!
ip cef
!
!
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Port-channel30
 switchport
 switchport access vlan 30
 switchport mode access
!
interface Ethernet0/0
 switchport access vlan 30
 switchport mode access
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 30
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport access vlan 30
```

```
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 switchport access vlan 30
 switchport mode access
 duplex auto
!
interface Ethernet1/0
 switchport access vlan 30
 switchport mode access
 duplex auto
 channel-group 30 mode desirable
!
interface Ethernet1/1
 switchport access vlan 30
 switchport mode access
 duplex auto
 channel-group 30 mode desirable
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
!
no ip http server
!
!
!
!
!
control-plane
!
banner motd ^C
  __   __              _
 |  \/  | ___ _  ___ _(_) ___
 | |\/| |/ _` |/ _` | |/ __|
 | |  | | (_| | (_| | | (__
 |_|  |_|\__,_|\__, |_|\___|
  __   __        |___/                 _
 |  \/  | ___ _ __ ___   ___  _ __(_) ___   ___
 | |\/| |/ _ \ '_ `_ \ / _ \| '__| |/ _ \/ __|
 | |  | |  __/ | | | | | (_) | |  | |  __/\__ \
 |_|  |_|\___|_| |_| |_|\___/|_|  |_|\___||___/

>"AccountsSW"


/!\/!\  WARNING! UNAUTHORISED ACCESS TO  /!\/!\
        THIS DEVICE WILL RESULT IN LEGAL
        ACTION BEING TAKEN AGAINST YOU!
/!\/!\       YOU HAVE BEEN WARNED!       /!\/!\

^C
!
line con 0
 password 7 000912010D585A545C
 logging synchronous
 login
line aux 0
line vty 0 4
 password 7 020B055C02054F701E1D
 login
 transport input ssh
!
end
```

DirectorsSwitch

```
Current configuration : 1945 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname DirectorsSW
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 KPGGJ8oTopHGG6x4n3yS9mLLXJmHM.RSvg4KGNDWAZM
!
no aaa new-model
clock timezone EET 2 0
!
ip cef
!
!
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
interface Port-channel40
 switchport
 switchport access vlan 40
 switchport mode access
!
interface Ethernet0/0
 switchport access vlan 40
 switchport mode access
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 40
```

```
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport access vlan 40
 switchport mode access
 duplex auto
 channel-group 40 mode desirable
!
interface Ethernet0/3
 switchport access vlan 40
 switchport mode access
 duplex auto
 channel-group 40 mode desirable
!
interface Ethernet1/0
 duplex auto
!
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/2
 duplex auto
!
interface Ethernet1/3
 duplex auto
!
!
no ip http server
!
!
!
!
!
control-plane
!
banner motd ^C
  __  __              _
 |  \/  | __ _  __ _(_) ___
 | |\/| |/ _` |/ _` | |/ __|
 | |  | | (_| | (_| | | (__
 |_|  |_|\__,_|\__, |_|\___|
  __  __       |___/                _
 |  \/  | ___ _ __ ___   ___  _ __(_) ___  ___
 | |\/| |/ _ \ '_ `  _ \ / _ \| '__| |/ _ \/ __|
 | |  | |  __/ | | | | | (_) | |  | |  __/\__ \
 |_|  |_|\___|_| |_| |_|\___/|_|  |_|\___||___/

>"DirectorsSW"

/!\/!\  WARNING! UNAUTHORISED ACCESS TO  /!\/!\
        THIS DEVICE WILL RESULT IN LEGAL
        ACTION BEING TAKEN AGAINST YOU!
/!\/!\       YOU HAVE BEEN WARNED!       /!\/!\

^C
!
line con 0
 password 7 09414F0E1006464058
 logging synchronous
 login
line aux 0
line vty 0 4
```

```
 password 7 141A130C05076A7A767B
 login
 transport input ssh
!
end
```