



 **CYBONET**



# Cybowall Configuration Guide

Last Modified 27 May 2018



# Contents

<b>Introduction</b> .....	<b>5</b>
<b>Initial Configuration Steps</b> .....	<b>6</b>
<b>Network Scanning</b> .....	<b>7</b>
Before You Begin .....	7
Determining the Network Environment .....	7
Physical Server (Dedicated Hardware) .....	7
Virtual Environment .....	8
VMware .....	8
Hyper-V .....	9
Network Scanning Configuration.....	12
Enabling the Network.....	16
Adding Additional Networks/VLANs .....	17
Untagged Networks.....	17
Tagged Networks.....	19
Regaining Access to Cybowall.....	20
Physical Server (Dedicated Hardware) .....	20
Virtual Environment .....	20
VMware .....	20
Hyper-V .....	24
Adding Additional VLANs.....	26
<b>Port Mirroring</b> .....	<b>27</b>
Switch Configuration .....	27
Virtual Environment .....	28
Enabling Promiscuous Mode .....	28
VMware .....	28
Hyper-V .....	30
Setting the Mirroring Mode of the VM to Destination .....	30
Setting the Mirroring Mode of the External Port to Source .....	32
Verifying Port Mirroring Configuration.....	33
<b>WMI Access</b> .....	<b>34</b>
Cybowall GPO Configuration .....	34
Setting Firewall Rules .....	38



For Networks without Windows XP or 2003 computers ..... 38

Networks including Windows XP or 2003 computers ..... 39

Enabling Echo Reply ..... 41

Service Configuration ..... 42

Enabling Auditing..... 45

Enabling the GPO..... 50

Configuring Username and Password ..... 51

**Revision History ..... 52**

**About CYBONET ..... 53**



# Introduction

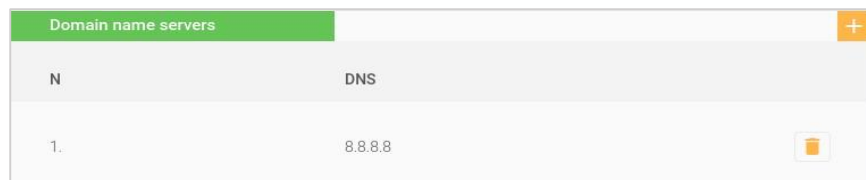
This guide details the steps required to configure the Cybowall solution. It is made up of four broad components:


1. Initial Configuration Steps
2. Network Scanning
3. Port Mirroring
4. WMI Access

# Initial Configuration Steps

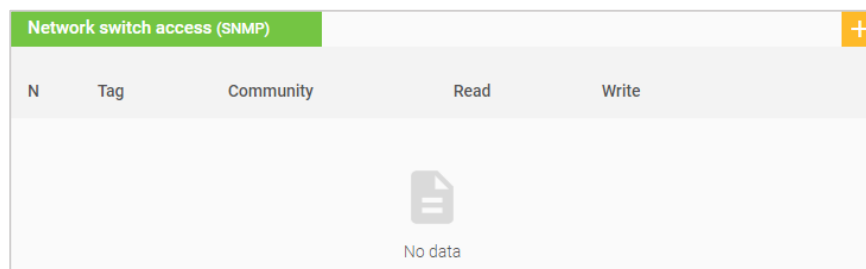
To start configuring Cybowall, follow the steps below.


1. Navigate to **System settings > Network devices** and in the **Domain name servers (DNS)** section, configure the relevant DNS servers in the organization's network:



Domain name servers		
N	DNS	
1.	8.8.8.8	

2. Cybowall connects to all network switches using SNMP. To allow this, add the SNMP information for all relevant switches by clicking the orange + icon to the right of the **Network switch access (SNMP)** section:



Network switch access (SNMP)					
N	Tag	Community	Read	Write	
 No data					

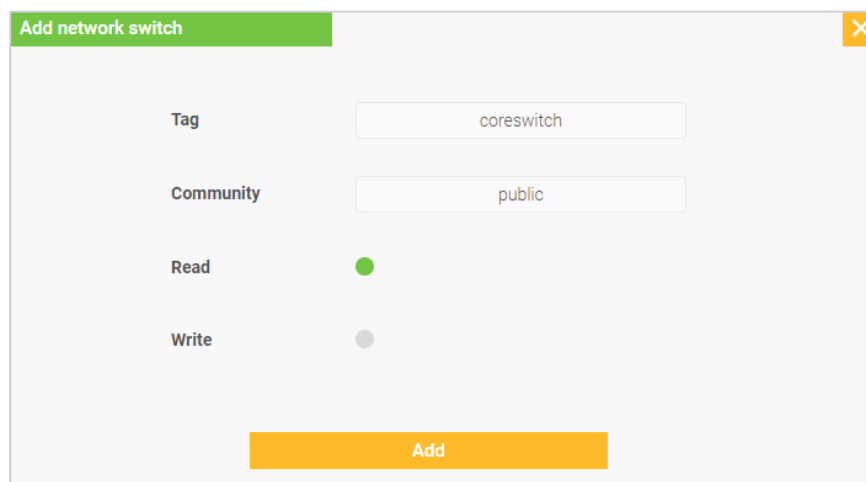
3. Complete the following information (at minimum):

**Tag** (description - one word, no spaces)

**Community**

**Read** (select to grant permission)

4. Click **Add**:



Tag	<input type="text" value="coreswitch"/>
Community	<input type="text" value="public"/>
Read	<input checked="" type="checkbox"/>
Write	<input type="checkbox"/>
<input type="button" value="Add"/>	



# Network Scanning

For an organization to know which systems and devices are connected to the network, asset mapping is required. In order for Cybowall to discover and map connected assets, it needs to perform network scans.

Network scans allow the organization to discover all devices with an IP address range, providing visibility of all connected devices and enabling effective monitoring of those assets. As a network evolves, network scanning allows a full picture of the network to be obtained and changes to be tracked.

## Before You Begin

Determine how the organization's network is configured in order to correctly configure Cybowall.

The network can be configured in one of the following ways:

- VLAN tagging (IEEE 802.1Q protocol) is utilized and the network has VLAN interfaces configured on the switch
- VLAN tagging is not utilized

## Determining the Network Environment

The method differs depending on the type of environment; physical server or virtual environment.

### Physical Server (Dedicated Hardware)

To verify if the network environment is tagged or untagged, access and check the switch configuration (which the server is connected to).

Since multiple types of switches exist, with their own setup, use the below link to access the manuals of known switch vendors (HP, Cisco, 3Com and others) in order to configure the port as a trunk port and assign to it the relevant VLANs:

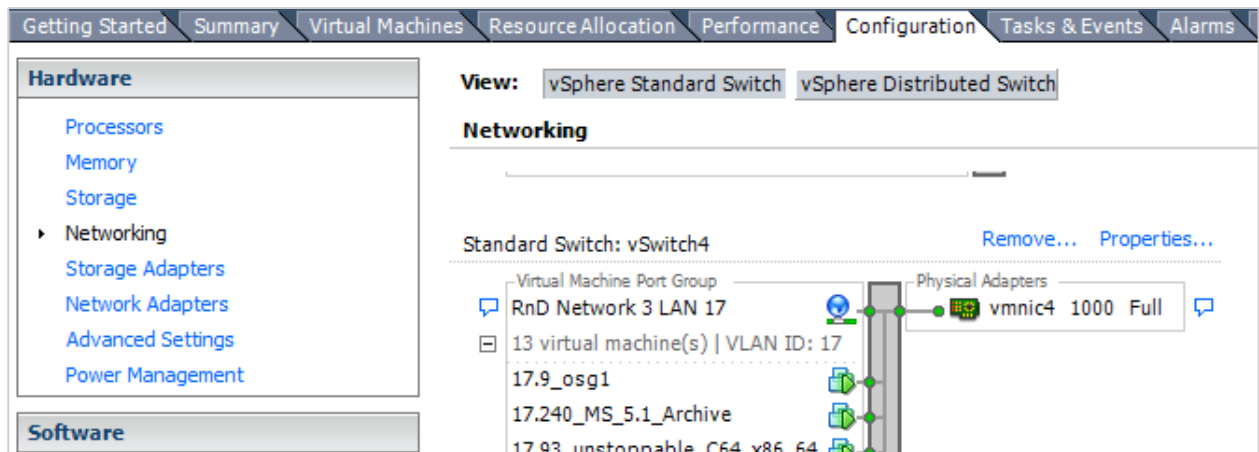
<https://wiki.wireshark.org/SwitchReference>

# Virtual Environment

To determine the type of network environment, review the set-up of VMware or Hyper-V.

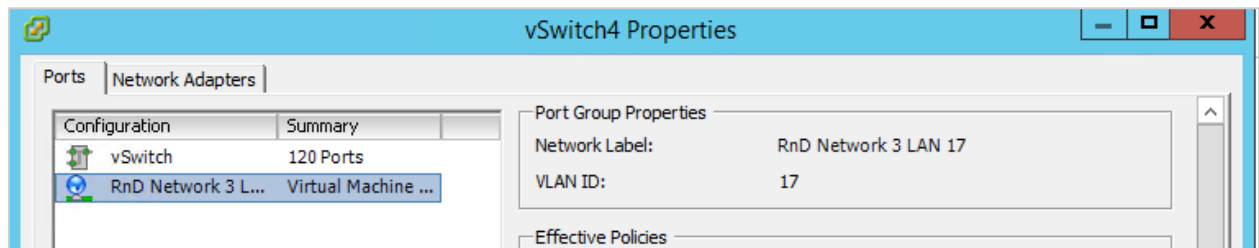
## VMware

1. Navigate to the VM host **Configuration > Networking** section:

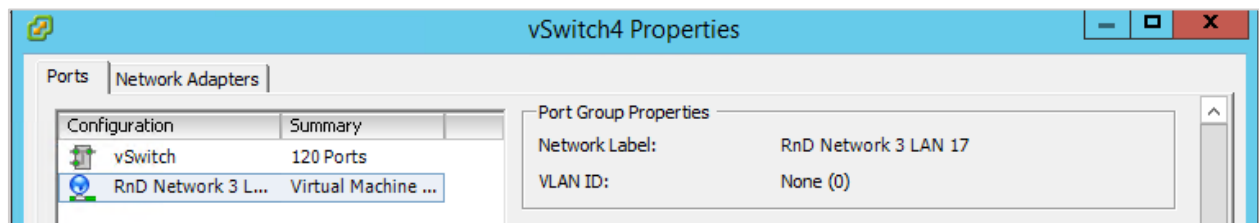


2. Click on the **vSwitch Properties**.

The presence of a **VLAN ID** indicates that VLAN tagging (IEEE 802.1Q protocol) is being used:



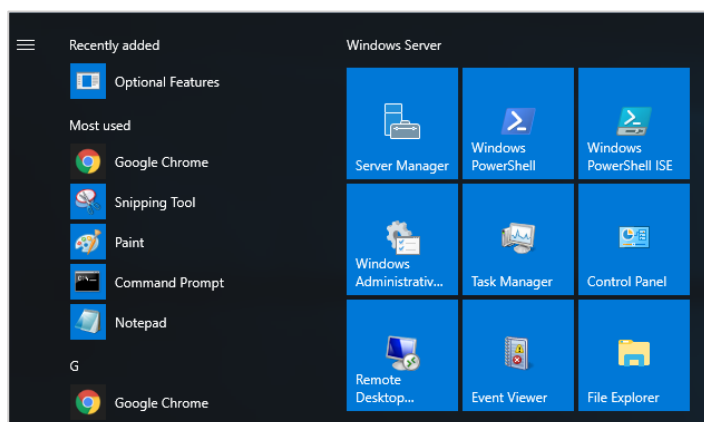
If there is no **VLAN ID**, this indicates an untagged environment:



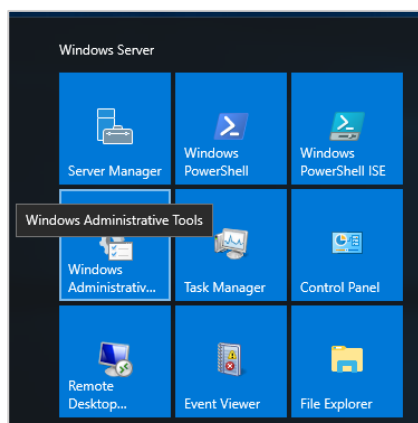


## Hyper-V

1. On the server on which Hyper-V is installed, click on the **Windows** key:

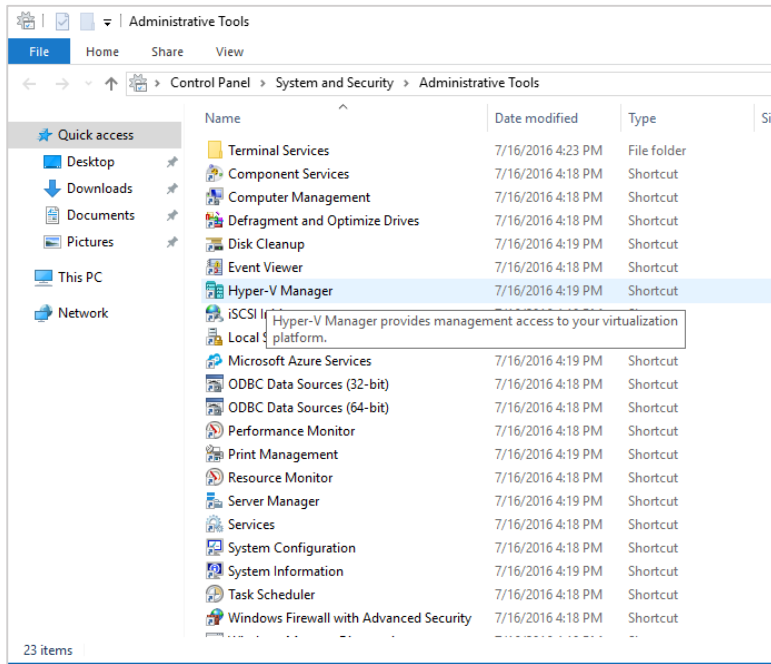


2. Click on the **Windows Administrative Tools** tile:

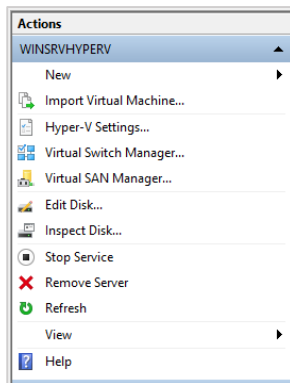




3. Double click **Hyper-V Manager**:



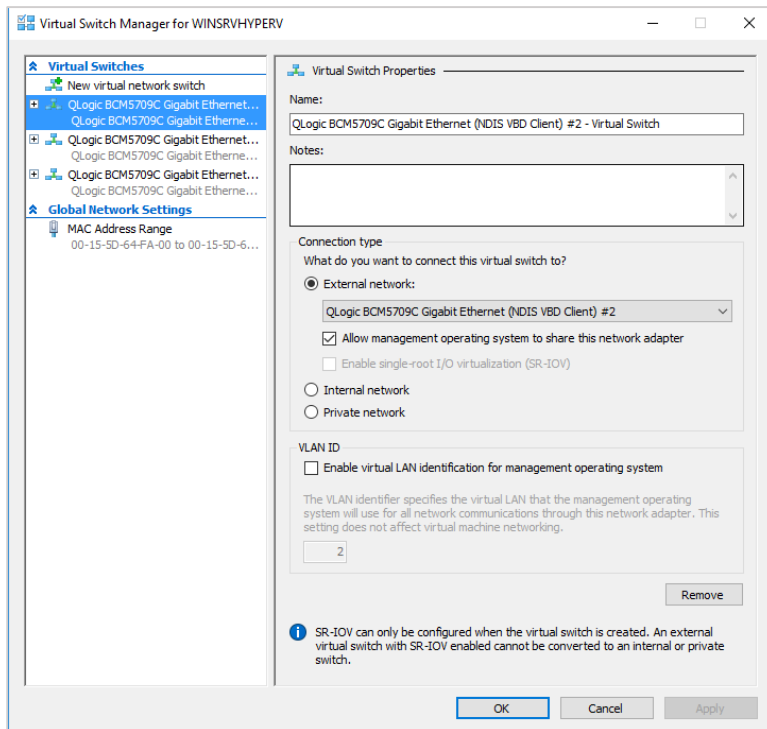
4. Under the **Actions** pane on the right, double click **Virtual Switch Manager**:





5. Select the relevant interface to show the interface properties.

If the checkbox under **VLAN ID** is checked, the environment is set up for VLAN tagging (IEEE 802.1Q protocol). If it is unchecked, the environment is untagged:



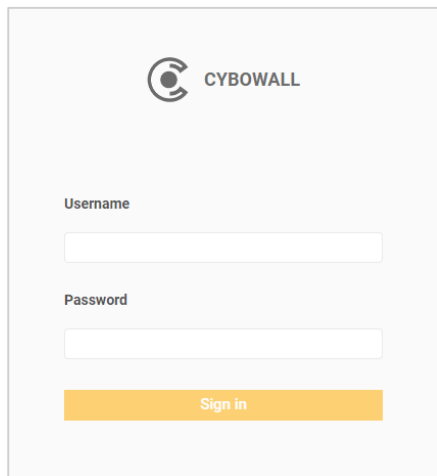
# Network Scanning Configuration

1. Login to the Cybowall UI using the IP address configured in the CLI – refer to the Cybowall Quick Installation Guide (QIG).

<https://ipaddress:7443>


**Username:** admin

**Password:** CBWadminPa\$\$



The screenshot shows the Cybowall login interface. At the top left is the Cybowall logo. Below it are two input fields: 'Username' and 'Password'. At the bottom is a yellow 'Sign in' button.



2. Navigate to the **System settings > Network devices** tab:

Management service						
Device	IP	Speed	MTU	UI port (HTTPS)	VLAN id	
eth0	172.16.100.100/24	AUTO	1500	7443		

General settings	
Hostname	Cybowall 
Default gateway	192.168.7.254 

These screenshots show the initial IP address and **Default gateway** for the Management service interface set up in the QIG.


Setting the Management IP, as above, automatically adds the network that the Management IP is a part of:

VLAN access interface list (IEEE 802.1Q)							+
N	VLAN name	VLAN address range	VLAN id	Type	IP	Device	
1.	172.16.100.0/24	172.16.100.0/24		STATIC	172.16.100.100/24	eth0	 

3. Navigate to the **Policy > Network scanner** tab:


Default network definitions	Save default
<b>DHCP Server</b>	<b>DNS Server</b>
<input type="text" value="Default DHCP server"/>	<input type="text" value="Default DNS server"/>

4. Add the primary **DHCP Server** and **DNS Server** in the **Default network definitions** section.  
When new subnets are added, they automatically inherit the default network definition, unless otherwise specified.
5. **\*Note:** If any of the networks contain alternate DHCP and DNS servers, this step can be skipped. Add the information for each network in the **Networks** section:

Networks										
N	Name	Address range	Risk factor	Malware hunter	Default gateway	DNS servers	DHCP servers	Protected	Enabled	
1.	172.16.100.0/24	172.16.100.0/24	1	Normal				<input type="checkbox"/>	<input checked="" type="checkbox"/>	




6. Return to **Systems settings > Network devices** to configure the **Network traps service (Honeypots)**. Click the orange **Edit icon** to the right of this section:

Network traps service (Honeypots)		
Device	IP	VLAN id
eth0	172.16.30.7/24	 

- a. **For untagged networks:** choose a **Device**, enter a free **IP address and subnet mask** and leave the **VLAN id** field blank. Click **Update**, then **Apply changes**:

### Update network traps interface ✕

**Device**  

Select the network interface to configure (the interface used for "Sniffer service" will **not** be available here)

**IP address and subnet mask (CIDR notation)**

Please enter a valid IP address and subnet mask using a CIDR notation

**VLAN id**

From 1 to 4094

**Update**



- b. For tagged networks: choose a **Device**, enter a free **IP address and subnet mask** and enter the relevant **VLAN id**. Click **Update**, then **Apply changes**:

### Update network traps interface ✕

<b>Device</b>	<input type="text" value="eth0"/> <span>▼</span>
	Select the network interface to configure (the interface used for "Sniffer service" will <b>not</b> be available here)
<b>IP address and subnet mask (CIDR notation)</b>	<input type="text" value="172.16.30.7/24"/>
	Please enter a valid IP address and subnet mask using a CIDR notation
<b>VLAN id</b>	<input type="text" value="30"/>
	From 1 to 4094

**Update**

# Enabling the Network

In order to start the scanning process, it is necessary to enable the network.

1. Click the orange **Edit icon** on the right of the **Networks** section. The following window appears:

**Update network** ✕

**Important** If you need to change *IP range* field, you should delete it and create a new one with all corresponding network definitions in **System settings / Network devices / VLAN access interface list**. Please note that deleting the network is an *irreversible operation* and will cause all hosts and statistic related to this *IP range* to be deleted.

IP address and subnet mask (CIDR notation)

Network name

Default gateway

DNS servers  +

DHCP servers  +

Network risk factor

Malware hunter profile  ▼

Status

**Update**

**Default gateway**, **DNS servers** and **DHCP servers** configuration are optional. It is relevant only if the network in question has its own DHCP server. Complete the information if relevant. If not, leave blank.

2. In order to enable scanning, toggle the **Enabled** status switch to the green 'on' position, and click **Update**.

If configured correctly, the **Protected** toggle turns green shortly after, indicating that Cybowall is able to scan the network segment:

N	Name	Address range	Risk factor	Malware hunter	Default gateway	DNS servers	DHCP servers	Protected	Enabled	
1.	172.16.100.0/24	172.16.100.0/24	1	Normal				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

**\*Note:** If the organization's network consists of one network only, no additional network scanning configuration is required. Continue to the Port Mirroring section of this guide.





# Adding Additional Networks/VLANs

If more than one network needs to be scanned by Cybowall, these must be added.

The following steps differ for tagged and untagged networks (refer to the Before You Begin section of this guide above).

## Untagged Networks

Requires that Cybowall have as many interfaces as the organization has subnets.

Cybowall's minimum requirements specify 2 network interfaces; one for scanning and one for port mirroring. Additional subnets require that additional interfaces are added to Cybowall.

### \*Note: Eth0 cannot be used for additional networks/subnets

Eth0 is used for management and scanning. Eth1 is used for port mirroring.

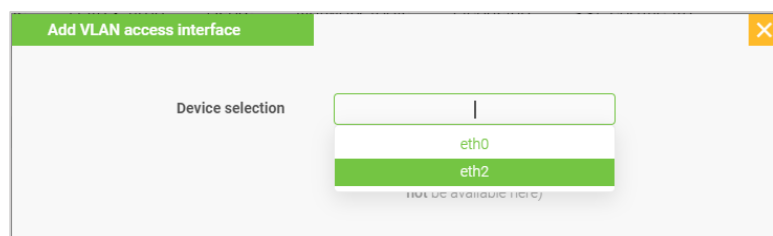
### Example:

- A network has 2 subnets: 172.16.100.0/24 and 192.168.1.0/24
- In this scenario, Eth0 is used for the 172.16.100.0/24 network
- Eth1 is reserved for port mirroring and cannot be used
- It is necessary to add Eth2 to scan 192.168.1.0/24

In a virtual environment, the number of interfaces required must be added.

In the case of a physical server, verify that there are sufficient physical interfaces.

1. To add another network, navigate to **System settings > Network devices**.
2. In the **VLAN access interface list** click the orange + icon:





3. Ensure that the correct interface is chosen (**Eth0 cannot be used again**).
4. Add a free **IP address and subnet mask**, choose the **Untagged** option, click **Add** and then **Apply Changes**:

Add VLAN access interface
✕

**Device selection**  ✕ ▼

Select the network interface to configure  
(the interface used for "Shiffer service" will not be available here)

**IP address type**  Static (Manual)  DHCP

DHCP is only allowed to be configured for fully-configured VLANs, go to Policy / Network scanner to configure the VLAN in full first

**IP address and subnet mask (CIDR notation)**

Please enter a valid IP address and subnet mask using a CIDR notation

**Tagged / Untagged**  Tagged  Untagged

Is this VLAN tagged (for IEEE 802.1Q access) or untagged (native VLAN)?

Add

The new network is added to the list:

VLAN access interface list (IEEE 802.1Q)							+
N	VLAN name	VLAN address range	VLAN id	Type	IP	Device	
1.	172.16.100.0/24	172.16.100.0/24		STATIC	172.16.100.100/24	eth0	
2.	192.168.1.0/24	192.168.1.0/24		STATIC	192.168.1.10/24	eth2	

5. Navigate to **Policy > Network scanner** to enable the newly added network:

Networks										
N	Name	Address range	Risk factor	Malware hunter	Default gateway	DNS servers	DHCP servers	Protected	Enabled	
1.	172.16.100.0/24	172.16.100.0/24	1	Normal				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
2.	192.168.1.0/24	192.168.1.0/24	1	Normal				<input type="checkbox"/>	<input type="checkbox"/>	

6. Click the **Edit icon**, and follow the steps outlined above in the Enabling the Network section of this guide.

# Tagged Networks

If VLAN tagging is in use, only two interfaces are required.

1. Navigate to **System Settings > Network devices** and click the **Edit icon** on the right of the **Management service** section.
2. Add the relevant **VLAN id**, click **Update** and then **Apply Changes**:

### Update management interface

Device	<input type="text" value="eth0"/>
	Select the network interface to configure (the interface used for "Sniffer service" will not be available here)
IP address and subnet mask (CIDR notation)	<input type="text" value="172.16.100.100/24"/>
	Please enter a valid IP address and subnet mask using a CIDR notation
MTU	<input type="text" value="1500"/>
	From 68 to 1500
UI port (HTTPS)	<input type="text" value="7443"/>
	From 1024 to 65535
Speed	<input type="text" value="AUTO"/>
VLAN id	<input type="text" value="1"/>
	From 1 to 4094

**Update**

**\*Note:** Expect access to the unit to be lost at this stage.



# Regaining Access to Cybowall

To regain access to Cybowall, follow the steps below.

## Physical Server (Dedicated Hardware)

1. To restore access, go the switch and change the role of the port that Cybowall is connected to via eth0 (Management interface) from an access port to a trunk port and allow all relevant VLANs.

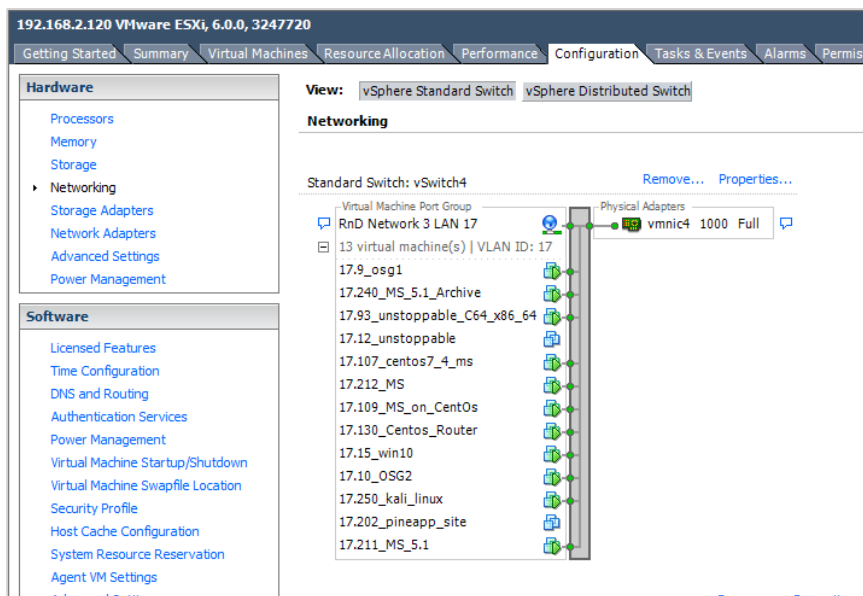
Access to the Cybowall UI is restored.

2. If Cybowall is a virtual machine (VM), make changes to the virtual environment as well.

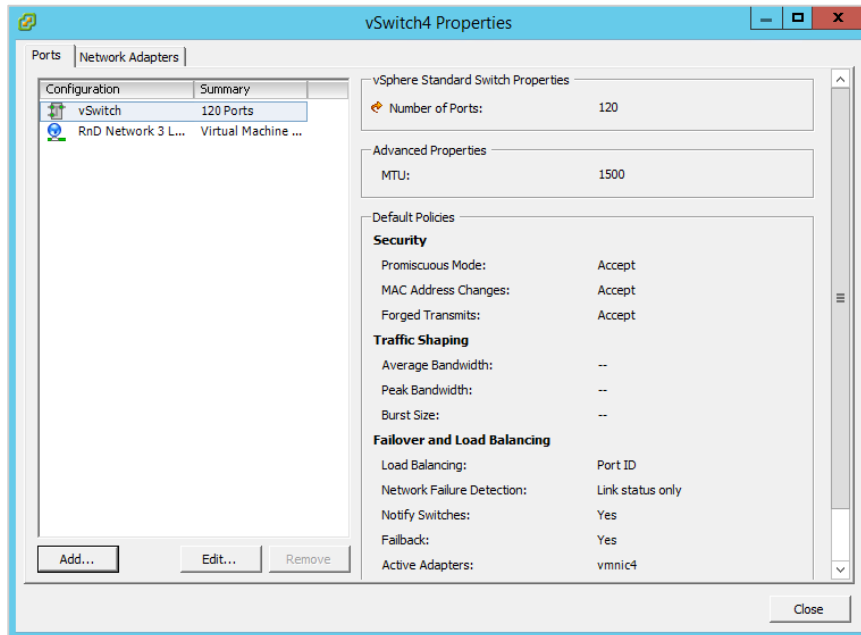
## Virtual Environment

### VMware

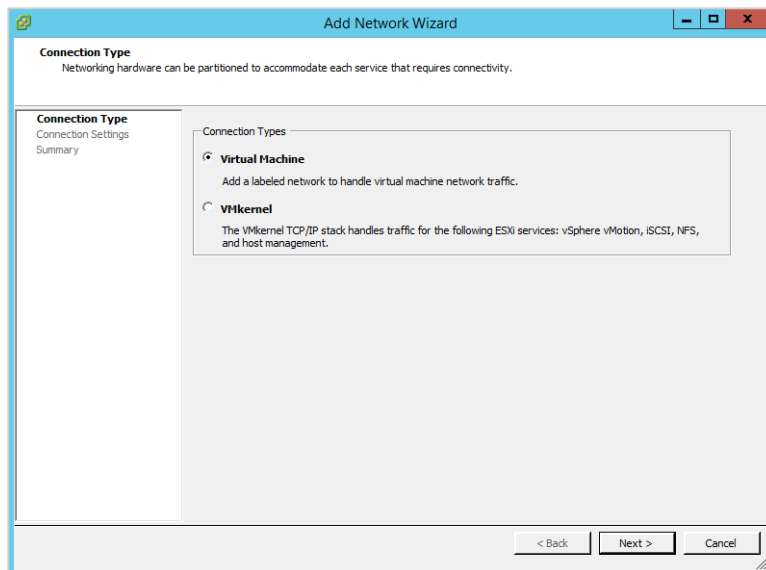
1. Navigate to the VM host **Configuration > Networking** section:



2. Open the relevant vSwitch Properties:

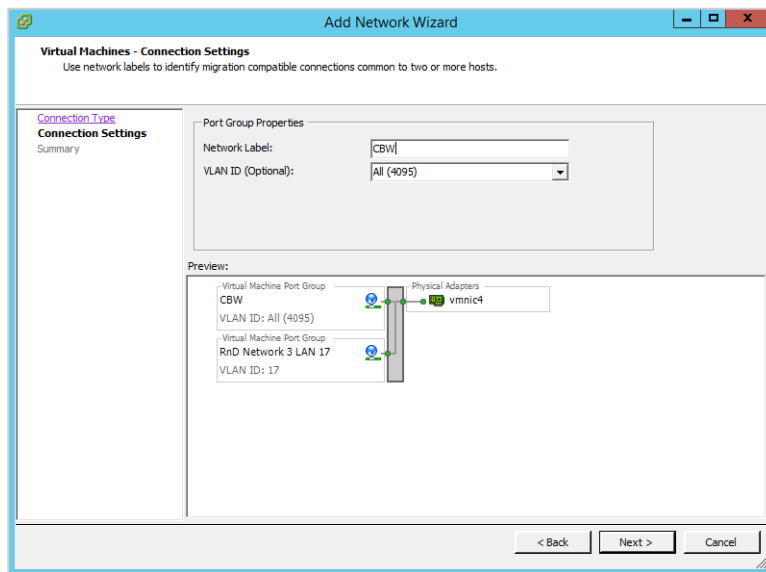


3. Click Add:

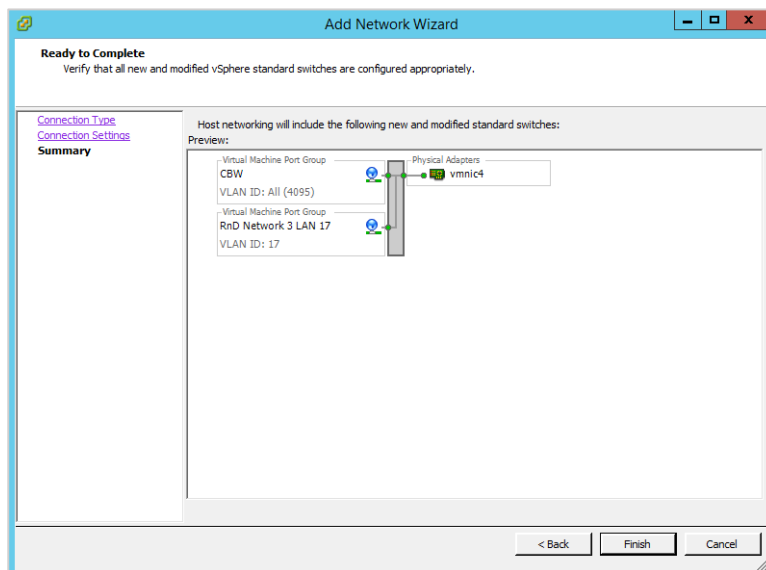




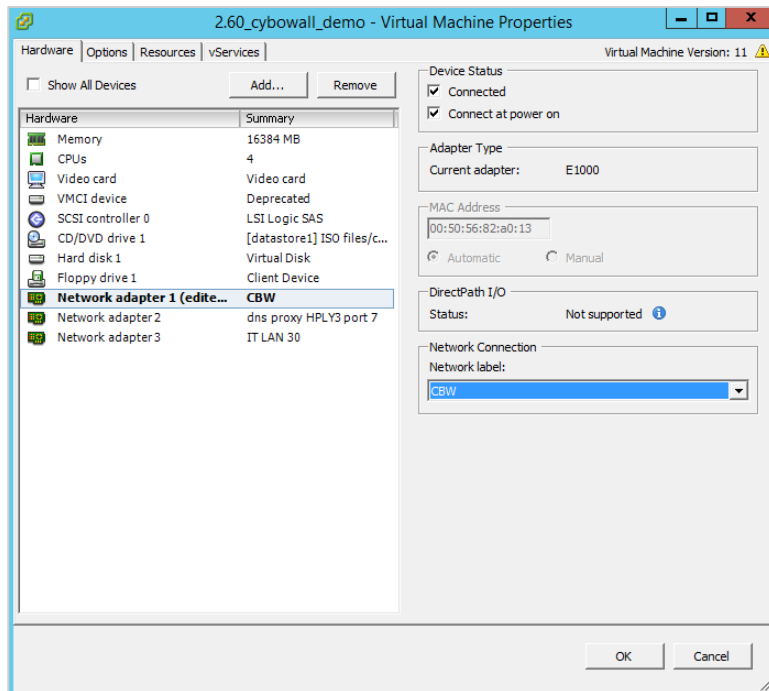
4. Give it a name under **Network Label**, select **All (4095)** under **VLAN ID**, and click **Next**:



5. Click **Finish**:



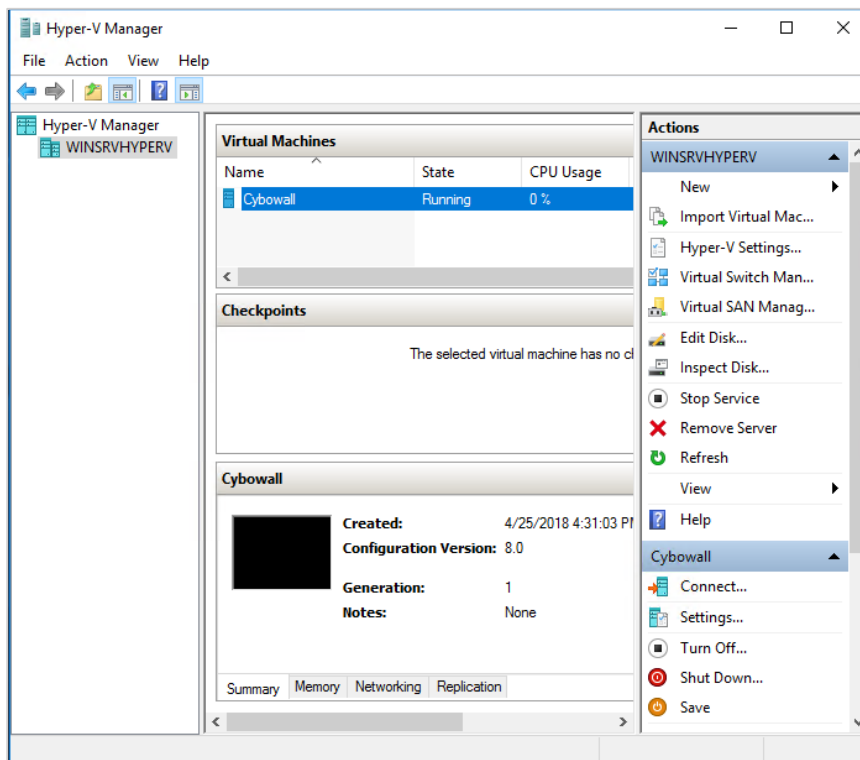
6. Open the Cybowall **Virtual Machine Properties** and change the **Network Connection** to the newly created one.
7. Click **OK**:



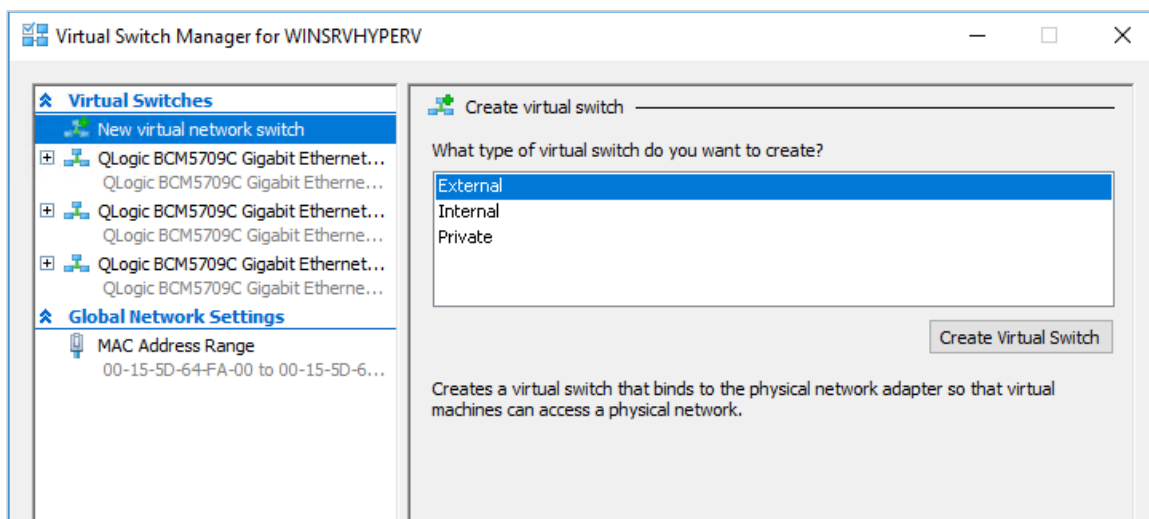
After completion of these steps, the Cybowall UI is accessible once more.

## Hyper-V

1. Open Hyper-V Manager:

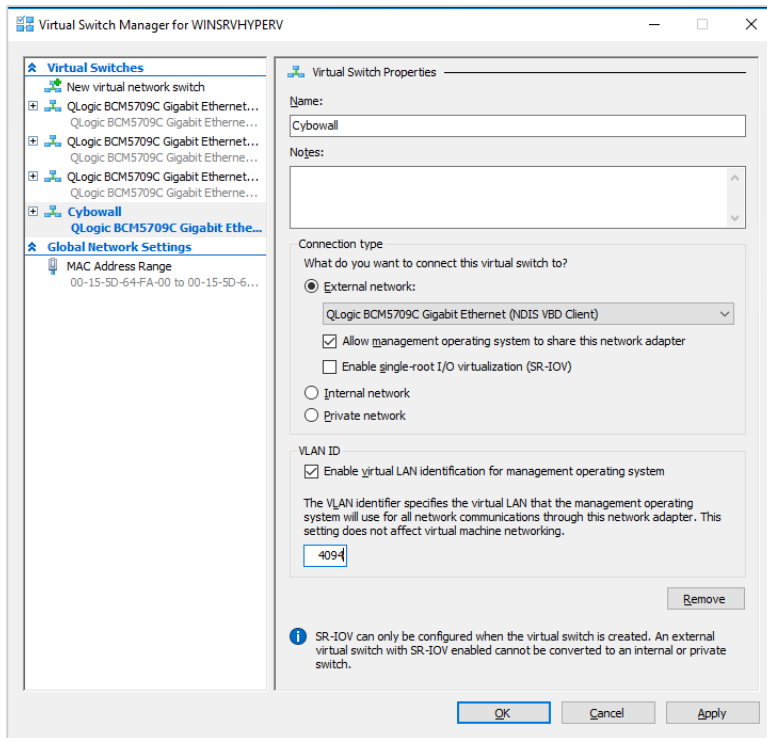


2. Double click the **Virtual Switch Manager** and create a **New virtual network switch**:

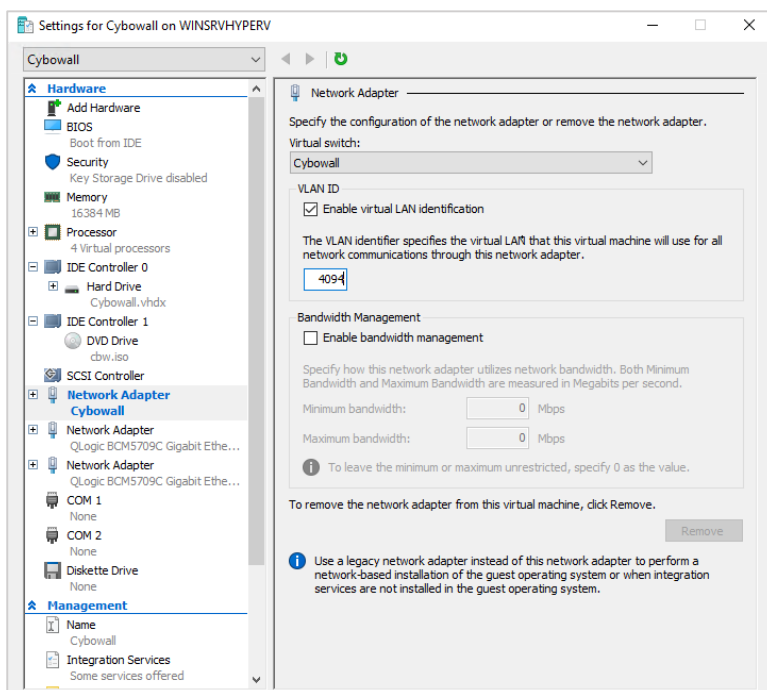




3. Name the new virtual switch, check **VLAN ID** and add **4094** (to indicate all VLANs) and click **OK**:



4. Navigate to Cybowall VM **Settings**. Select the newly created virtual switch, check **VLAN ID** and add **4094** as the VLAN ID as click **OK**:



After completion of these steps, the Cybowall UI is accessible once more.

## Adding Additional VLANs

Additional VLANs to be scanned by Cybowall can be added.

1. Navigate to **System settings > Network devices** and click the orange **+** icon to the right of the **VLAN access interface list**.
2. In the **Device** selection field, select **eth0**.
3. Provide a free **IP address and subnet mask**, and select **Tagged**.
4. Add the relevant **VLAN id** and click **Add**:

### Add VLAN access interface

**Device selection**  ✕ ▼  
Select the network interface to configure (the interface used for "Sniffer service" will not be available here)

**IP address type**  Static (Manual)  DHCP  
DHCP is only allowed to be configured for fully-configured VLANs, go to Policy / Network scanner to configure the VLAN in full first

**IP address and subnet mask (CIDR notation)**   
Please enter a valid IP address and subnet mask using a CIDR notation

**Tagged / Untagged**  Tagged  Untagged  
Is this VLAN tagged (for IEEE 802.1Q access) or untagged (native VLAN)?

**VLAN id**   
What is the VLAN id for this? (check your network equipment settings to be sure please)

**Add**

5. After the VLAN is created, it needs to be enabled. Refer to the Enabling the Network section of this guide above.
6. Repeat the process in order to add all network VLANs for scanning by Cybowall.

# Port Mirroring

Port mirroring, also known as port monitoring or Switched Port Analyzer (SPAN), is a method of replicating network traffic. It enables the switch to send a copy of all network traffic going through a port/ports, or an entire VLAN, to another port. This port, where the traffic is analyzed, is known as the monitoring port.

Cybowall employs port mirroring in order to act as an Intrusion Detection System (IDS). An IDS inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack.

The Cybowall solution deploys a Sensor within the network that uses TAP/port mirroring to take a copy of all inbound and outbound traffic to provide full network visibility. Captured network traffic is analyzed to identify any abnormal/ suspicious user or service activity.

## Switch Configuration

Most network core switches have the ability to copy network traffic from one port on the switch to another. Configuring a mirroring/monitoring port on the switch varies from vendor to vendor.

The below link provides instructions on how to configure a switch for port mirroring for commonly used switch vendors (HP, Cisco, 3Com and others):

<https://wiki.wireshark.org/SwitchReference>

The **Sniffer service** automatically assigns the second interface (**eth1**) to be the target for port mirroring:

Sniffer service
Device
eth1

Port mirroring is configured on the switch – copying the traffic from the port that connects the network to the internet, to the target port (the port that eth1 is connected to).

# Virtual Environment

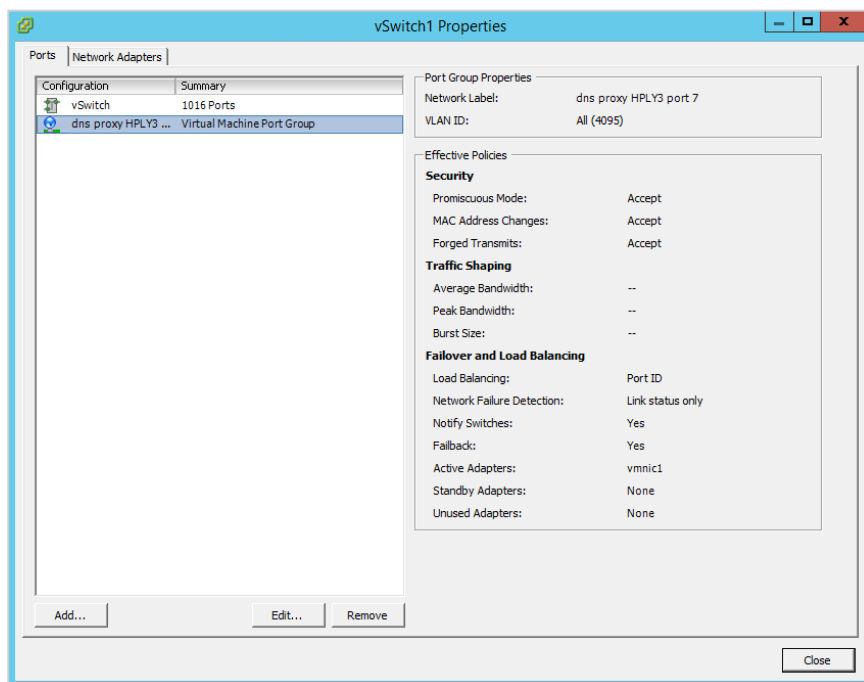
If Cybowall is installed as a VM, additional steps are required for the sniffer interface to receive the mirrored traffic.

## Enabling Promiscuous Mode

In a virtual environment, it is necessary to enable promiscuous mode on the virtual switch that the Cybowall interface is connected to.

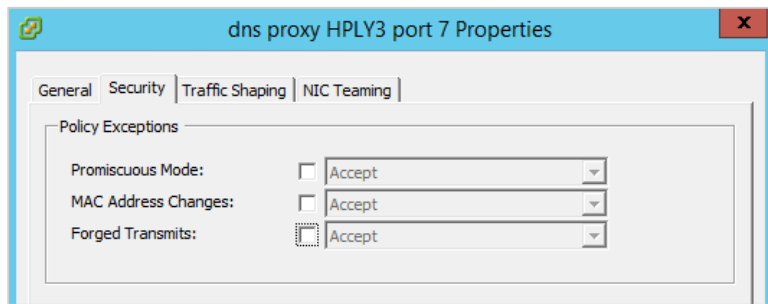
### VMware

1. Navigate to VM host **Configuration > Networking** section.
2. Double click on the relevant **vSwitch Properties**.
3. Select the **Port Group** that the Cybowall second interface is connected and click **Edit**:

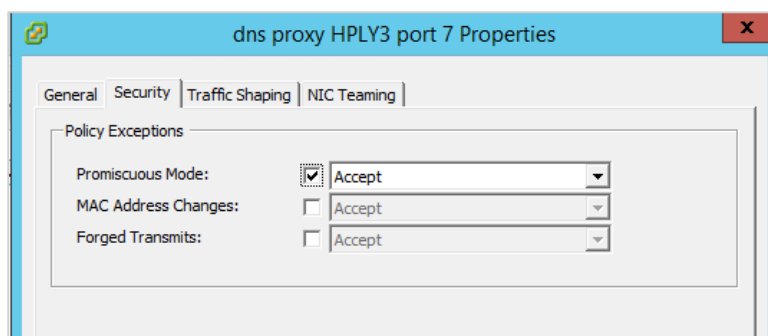




4. Navigate to the **Security** tab:



5. Check **Promiscuous Mode** and set the drop down menu to **Accept**:



6. Click **OK**.

For reference, VMware documentation can be accessed via the link below:

[https://kb.vmware.com/selfservice/microsites/search.do?language=en\\_US&cmd=displayKC&externalId=1002934](https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1002934)

## Hyper-V

By default, the mirroring mode will only allow a VM to capture from the virtual switch that the VM is attached to.

In order to enable the VM to also capture traffic hitting the mirrored port that the host is connected to, the following steps are required:

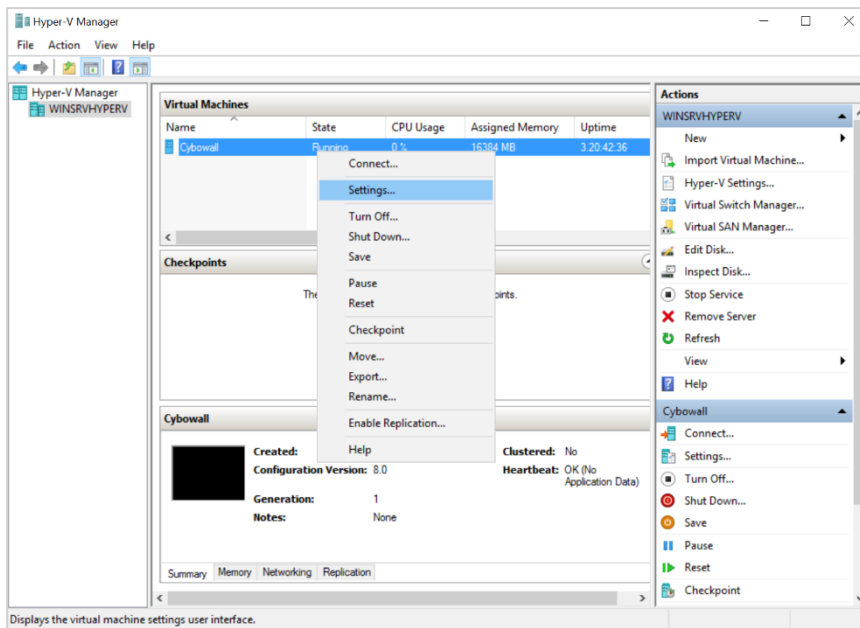
1. Set the mirroring mode of the capturing VM to **Destination**.
2. Set the mirroring mode on the external port of the virtual switch the VM is attached to reflect the **Source**.
3. Configure the destination VM Network Interface Card (NIC) to trunk mode and specify the VLANs it is to receive traffic from.

These steps are broken down below.

### Setting the Mirroring Mode of the VM to Destination

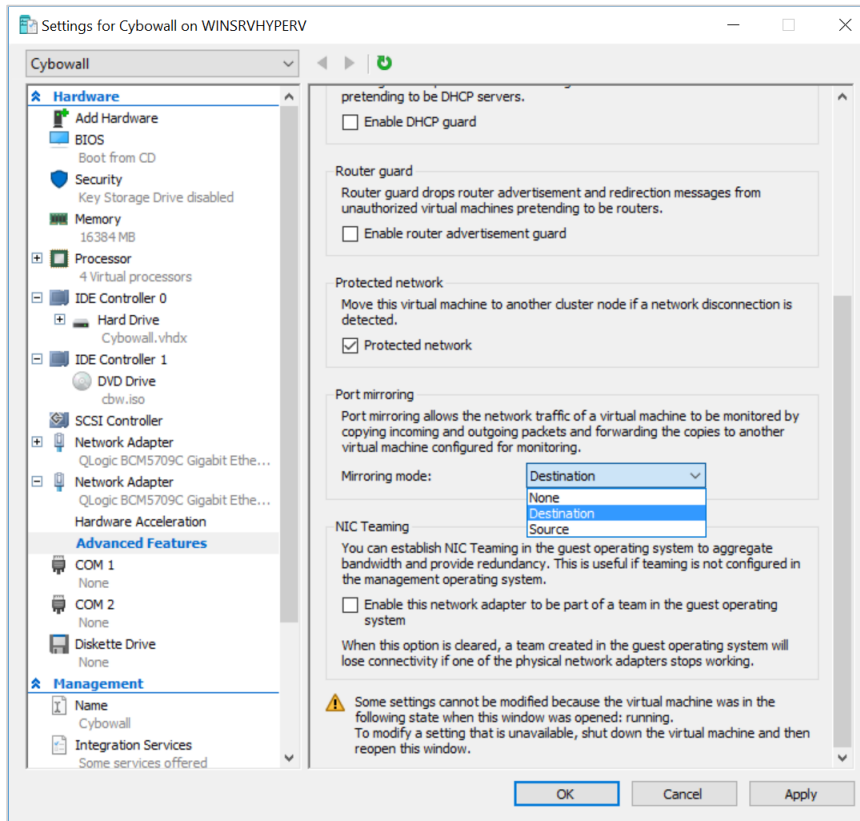
On the VM where the mirrored traffic is to be captured:

1. Navigate to the Cybowall **Virtual Machines > Settings** from the Hyper-V console:



2. Expand the respective network adapter and click on **Advanced Features**.

3. Select the **Mirroring mode** under the **Port mirroring** section and set it to **Destination**:



When port mirroring is configured, it needs to be configured as a pair. A Source and a Destination are configured so that the Source knows where to forward the information to.

The above steps set one of the interfaces (virtual ports) of the virtual switch to Destination.



## Setting the Mirroring Mode of the External Port to Source

It is necessary to let the virtual switch know that any traffic that hits the external port has to be forwarded to the port previously configured as Destination.

All traffic hitting the Hyper-V host also hits the external port of the virtual switch.

For the NIC on the VM to receive these packets, it is necessary to mirror this switch port (on the virtual switch) so that packets will be forwarded to the Destination previously configured.

1. The PowerShell command below sets the external port to **Source** mirroring mode:

```
$a = Get-VMSystemSwitchExtensionPortFeature -FeatureId 776e0ba7-94a1-41c8-8f28-951f524251b5
$a.SettingData.MonitorMode = 2
add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName <name of the switch> -VMSwitchExtensionFeature $a
```

Replace **<name of the switch>** with the name of the virtual switch.

**MonitorMode = 2** sets the Mirror mode to Source.

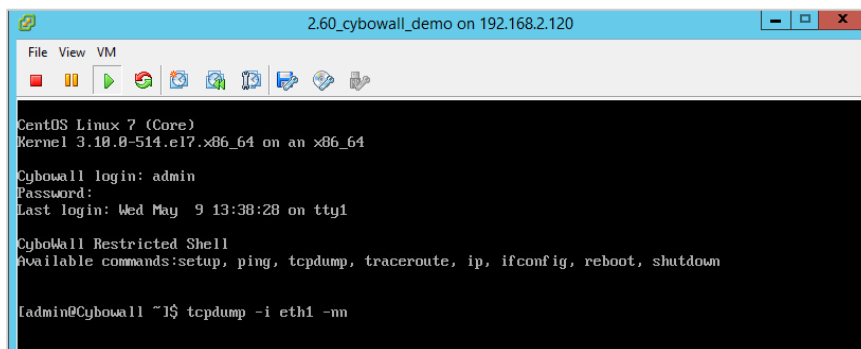
For reference, consult the documentation provided via the link below:

<https://blogs.technet.microsoft.com/networking/2015/10/16/setting-up-port-mirroring-to-capture-mirrored-traffic-on-a-hyper-v-virtual-machine/>



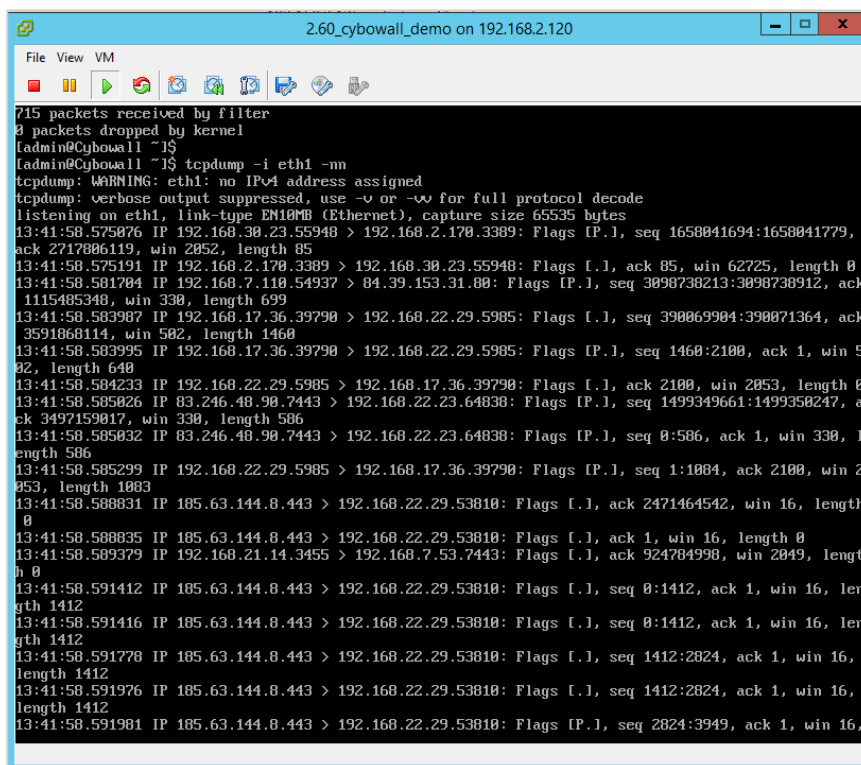
# Verifying Port Mirroring Configuration

1. Login to the Cybowall console as admin.
2. Run the `tcpdump` on eth1 as shown in the screenshot:



```
2.60_cybowall_demo on 192.168.2.120
File View VM
CentOS Linux 7 (Core)
Kernel 3.10.0-514.el7.x86_64 on an x86_64
Cybowall login: admin
Password:
Last login: Wed May  9 13:38:28 on tty1
Cybowall Restricted Shell
Available commands:setup, ping, tcpdump, traceroute, ip, ifconfig, reboot, shutdown
[admin@Cybowall ~]# tcpdump -i eth1 -nn
```

In the case of a successful configuration, the traffic is visible:



```
2.60_cybowall_demo on 192.168.2.120
File View VM
715 packets received by filter
0 packets dropped by kernel
[admin@Cybowall ~]#
[admin@Cybowall ~]# tcpdump -i eth1 -nn
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
13:41:58.575876 IP 192.168.30.23.55948 > 192.168.2.170.3389: Flags IP., seq 1650041694:1650041779,
ack 2717806119, win 2052, length 85
13:41:58.575191 IP 192.168.2.170.3389 > 192.168.30.23.55948: Flags [..], ack 85, win 62725, length 0
13:41:58.581784 IP 192.168.7.110.54937 > 84.39.153.31.80: Flags IP., seq 3098738213:3098738912, ack
1115485348, win 330, length 699
13:41:58.583987 IP 192.168.17.36.39790 > 192.168.22.29.5985: Flags [..], seq 390069904:390071364, ack
3591868114, win 502, length 1460
13:41:58.583995 IP 192.168.17.36.39790 > 192.168.22.29.5985: Flags IP., seq 1460:2100, ack 1, win 5
02, length 640
13:41:58.584233 IP 192.168.22.29.5985 > 192.168.17.36.39790: Flags [..], ack 2100, win 2053, length 0
13:41:58.585026 IP 83.246.48.90.7443 > 192.168.22.23.64838: Flags IP., seq 1499349661:1499350247, a
ck 3497159017, win 330, length 586
13:41:58.585032 IP 83.246.48.90.7443 > 192.168.22.23.64838: Flags IP., seq 0:586, ack 1, win 330, l
ength 586
13:41:58.585299 IP 192.168.22.29.5985 > 192.168.17.36.39790: Flags IP., seq 1:1884, ack 2100, win 2
053, length 1883
13:41:58.588031 IP 185.63.144.8.443 > 192.168.22.29.53810: Flags [..], ack 2471464542, win 16, length
0
13:41:58.588035 IP 185.63.144.8.443 > 192.168.22.29.53810: Flags [..], ack 1, win 16, length 0
13:41:58.589379 IP 192.168.21.14.3455 > 192.168.7.53.7443: Flags [..], ack 924784998, win 2049, lengt
h 0
13:41:58.591412 IP 185.63.144.8.443 > 192.168.22.29.53810: Flags [..], seq 0:1412, ack 1, win 16, len
gth 1412
13:41:58.591416 IP 185.63.144.8.443 > 192.168.22.29.53810: Flags [..], seq 0:1412, ack 1, win 16, len
gth 1412
13:41:58.591778 IP 185.63.144.8.443 > 192.168.22.29.53810: Flags [..], seq 1412:2824, ack 1, win 16,
length 1412
13:41:58.591976 IP 185.63.144.8.443 > 192.168.22.29.53810: Flags [..], seq 1412:2824, ack 1, win 16,
length 1412
13:41:58.591981 IP 185.63.144.8.443 > 192.168.22.29.53810: Flags IP., seq 2824:3949, ack 1, win 16,
```

# WMI Access

It is also necessary to configure Windows Management Instrumentation (WMI) to allow Cybowall to access windows hosts. In order to allow WMI access, a Group Policy Object (GPO) needs to be created.

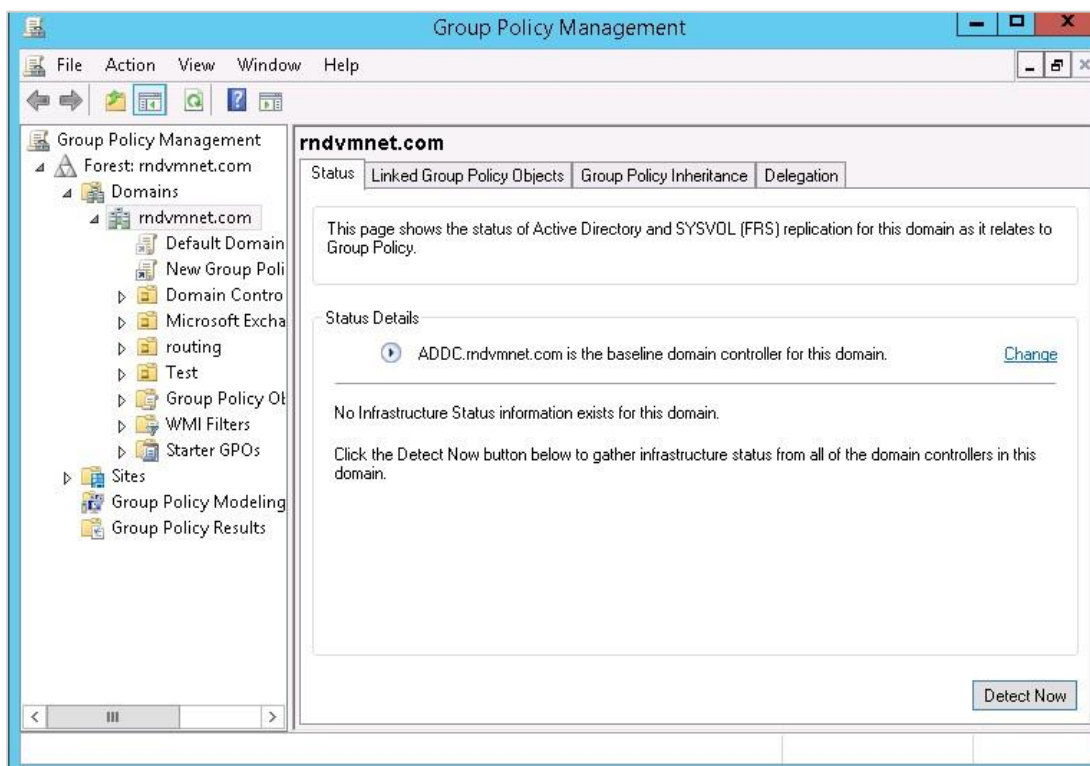
## Cybowall GPO Configuration

This section details how to configure the GPO in order to enable remote access to WMI.

1. Navigate to **Control Panel\System and Security\Administrative Tools**:

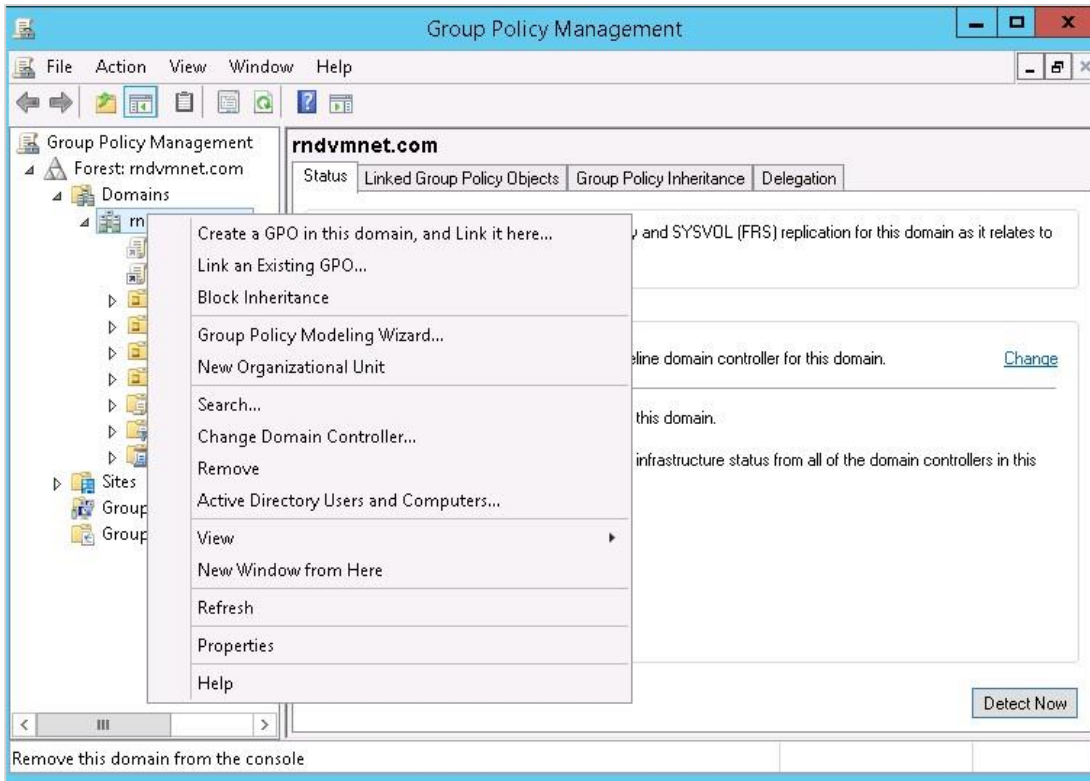


2. Open **Group Policy Management**:

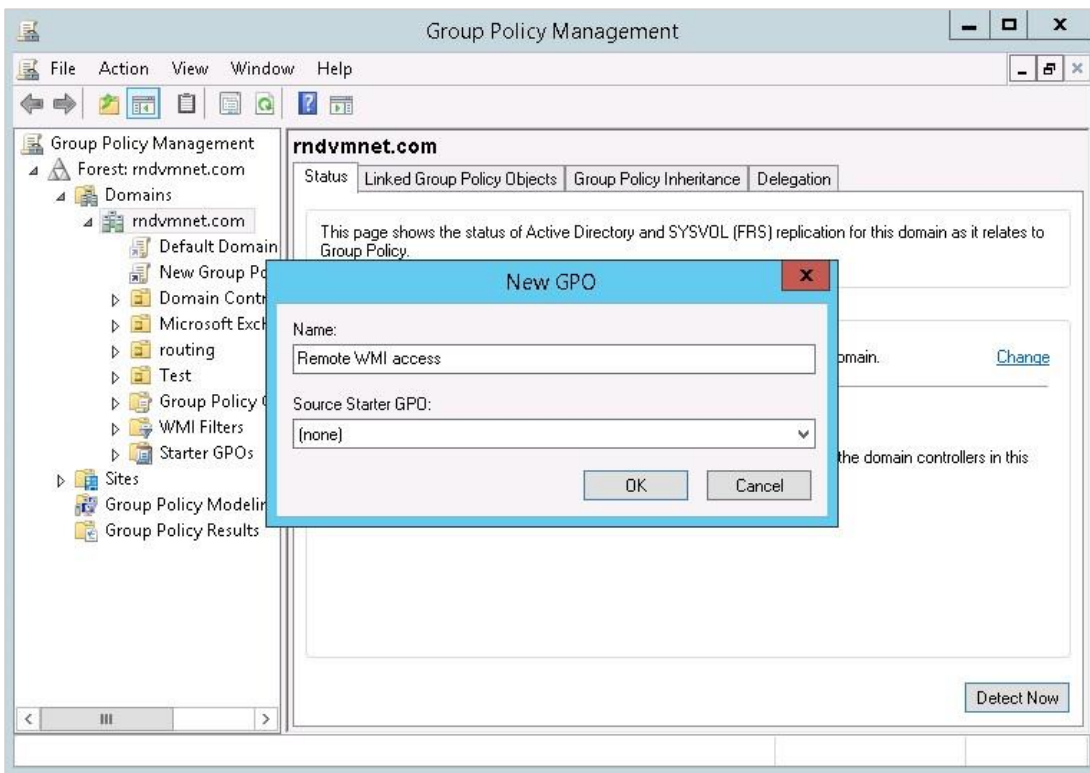




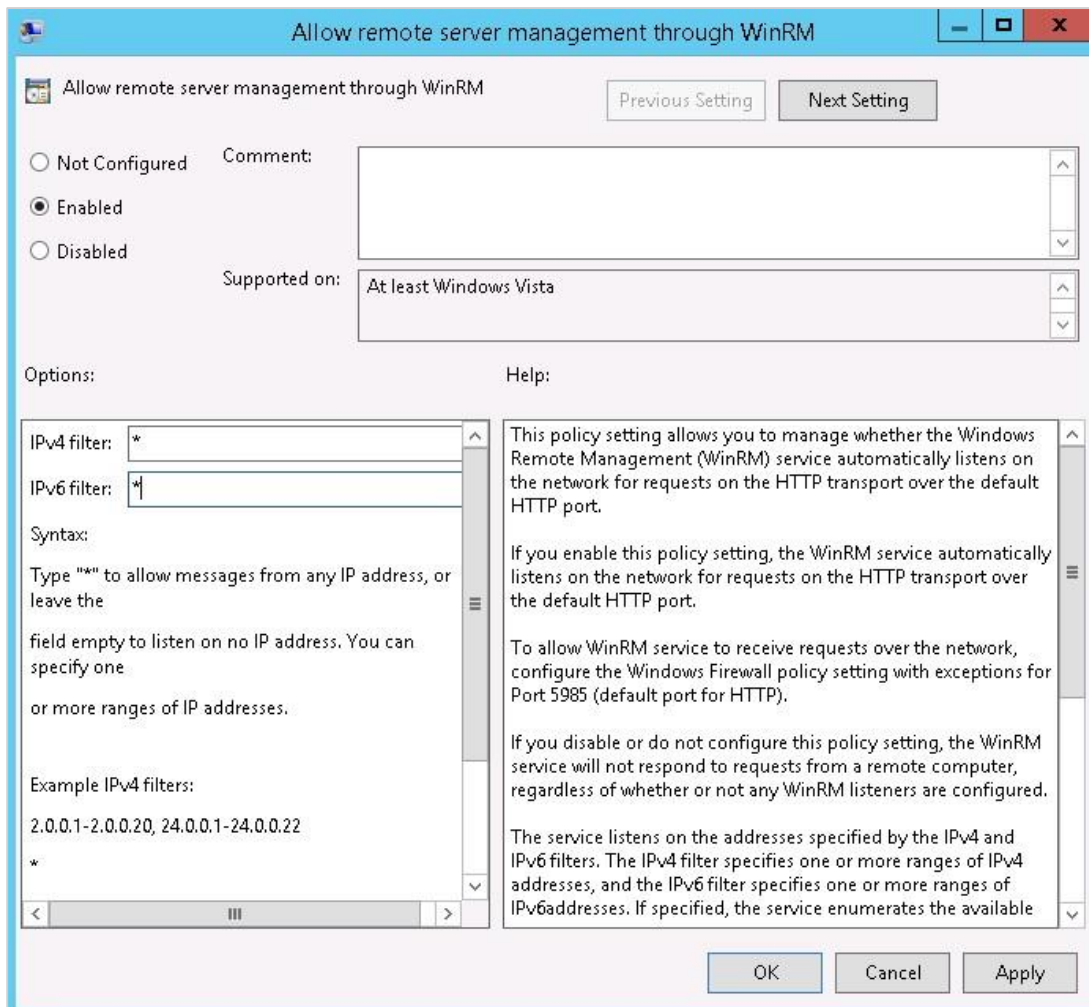
- 3. Create a GPO template by clicking **Create a GPO in this domain, and Link it here...**:



- 4. Choose a relevant **Name** (for example, Remote WMI access) and click **OK**:

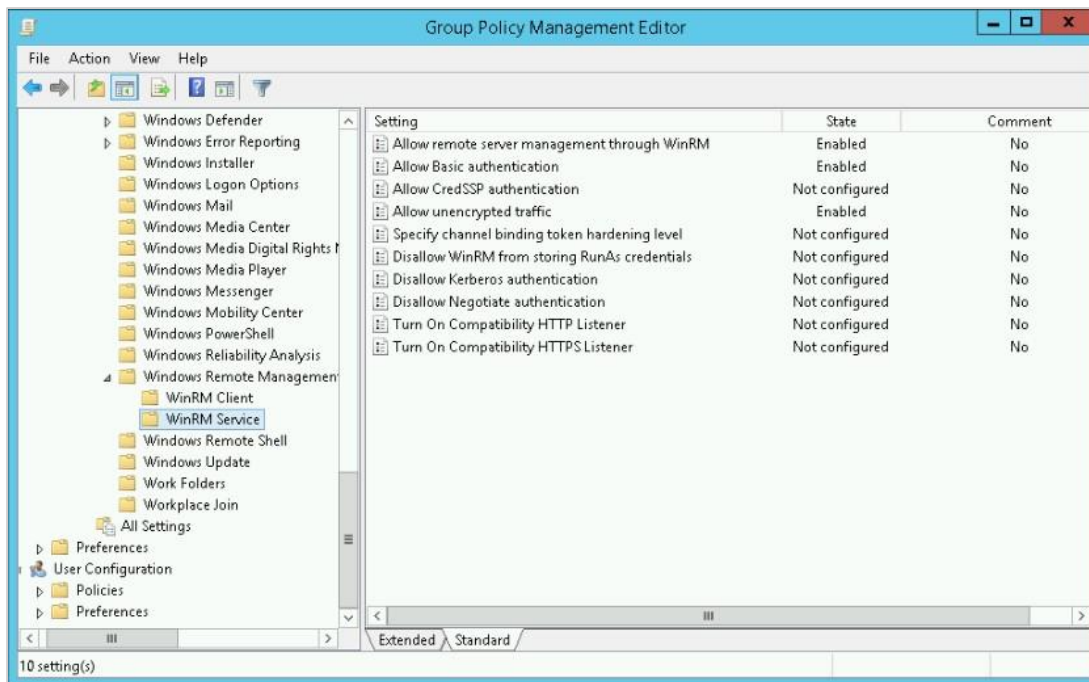


5. Right click the newly created GPO and select **Edit**.
6. Navigate to **Computer configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service**.
7. Double click on **Allow Basic authentication**, choose **Enable** and click **OK**.
8. Double click on **Allow unencrypted traffic**, choose **Enable** and click **OK**.
9. Double click on **Allow remote server management through WinRM**, (could be named **Allow automatic configuration of listeners**).
10. Set policy to **Enabled**.
11. Set both IPv4 filter and IPv6 filter to **\***.
12. Click **OK**:





The view appears as follows:



# Setting Firewall Rules

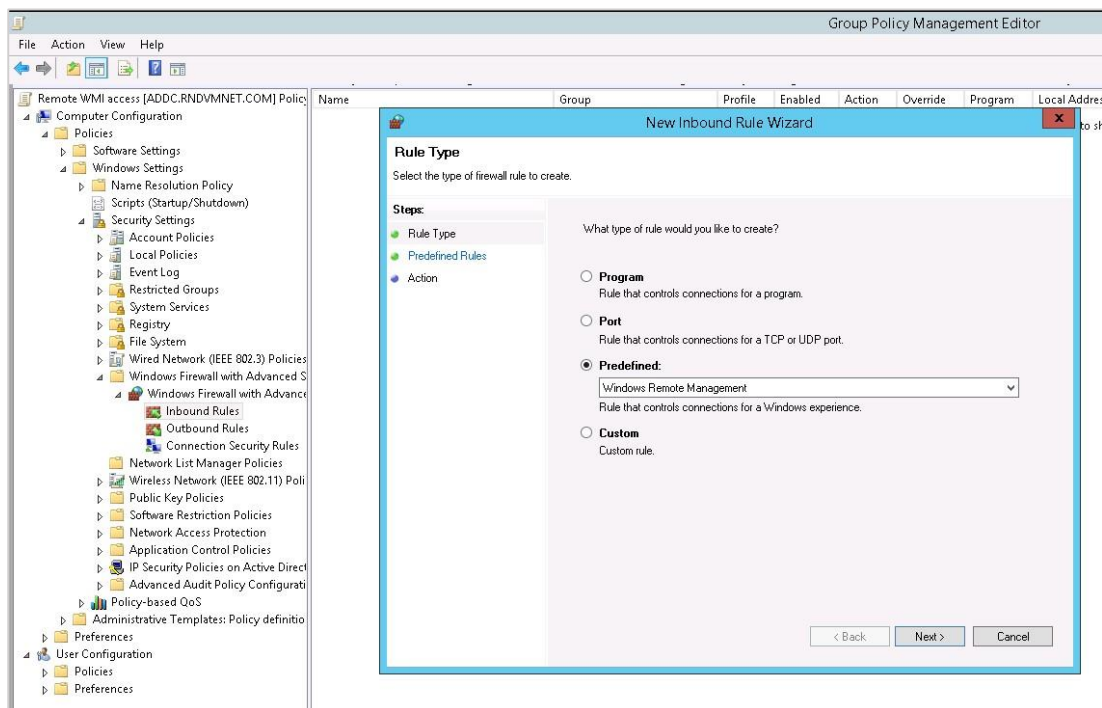
## For Networks without Windows XP or 2003 computers

If there are no Windows XP or 2003 computers on the network, the newer Firewall with Advanced Features policy can be used to configure the rule.

Additionally, this should be configured from a Windows 7 / 2008 R2 machine because of a difference in the pre-defined rule.

Carry out the following steps:

1. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall... > Inbound Rules**.
2. Right click and choose **New Rule...**
3. Under **Predefined** choose the **Windows Remote Management** rule.
4. Click **Next** to see that the pre-defined rule has been added (2 lines).
5. Click **Next**.
6. Choose to **Allow** the connection, and then **Finish**:

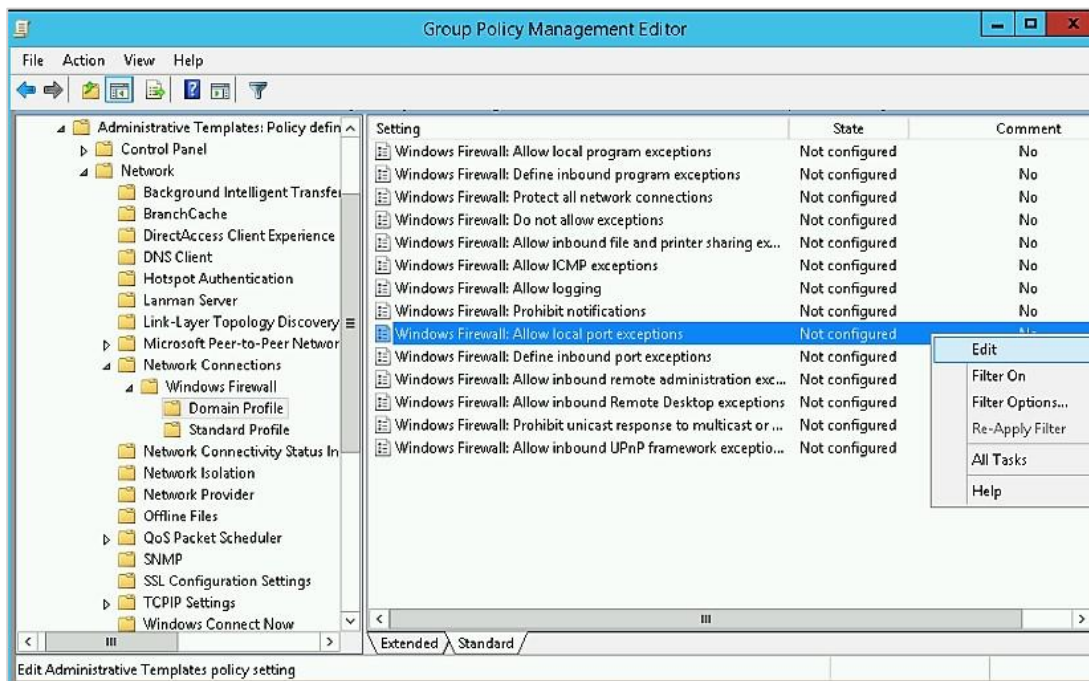


## Networks including Windows XP or 2003 computers

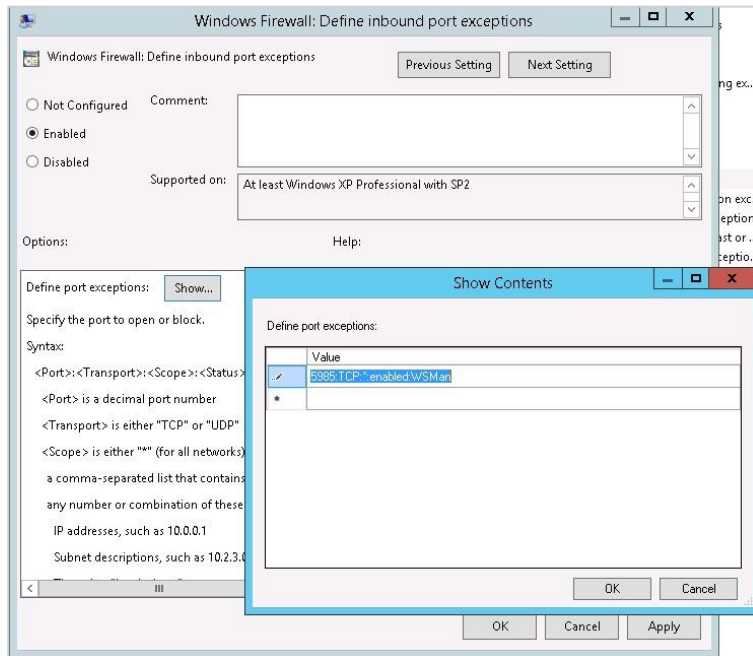
If there are Windows XP or 2003 computers on the network, the steps in the above section will not be effective on these computers.

It is necessary to carry out the following steps:

1. Navigate to (or continue under) **GPO Management Editor**, navigate to **Computer configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**.
2. Right click on **Windows Firewall Define inbound port exceptions > Edit**.
3. Set policy to **Enable**:



4. Click on **Show...** and add the following string: **5985:TCP:\*.enabled:WSMan**.
5. Instead of the **\*** insert the Cybowall server IP address.
6. Click **OK** and **OK** again:

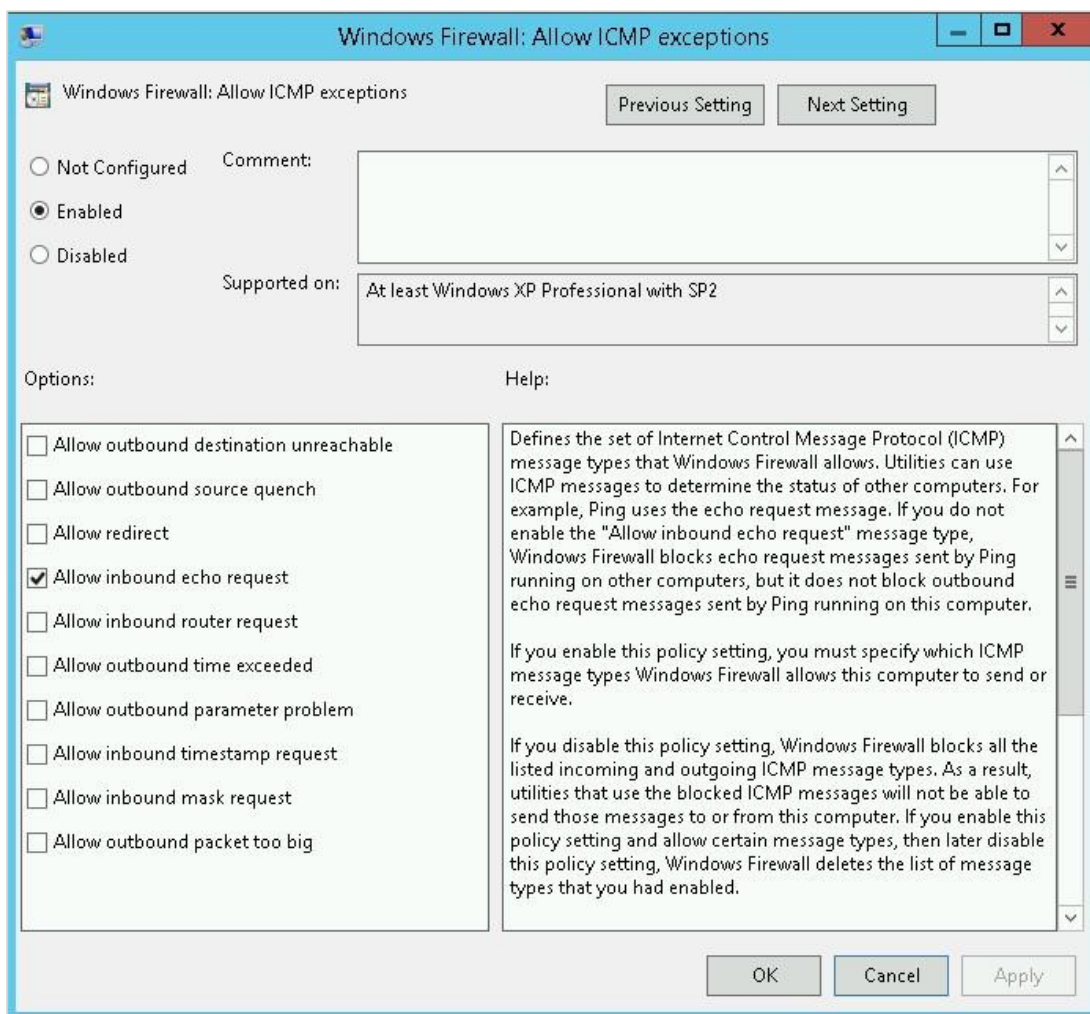




# Enabling Echo Reply

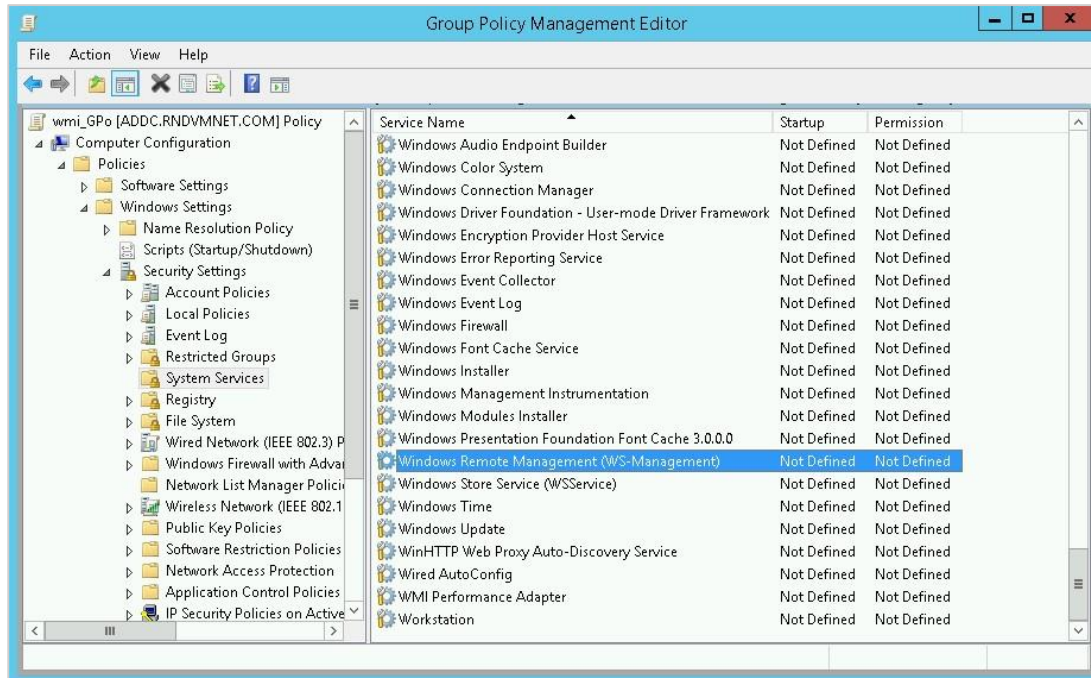
These steps are required to enable Echo Reply to gain visibility.

1. Under **GPO Management Editor**, navigate to **Computer configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**.
2. Click on **Windows Firewall: Allow ICMP exceptions**.
3. Click on **Enabled**.
4. Check **Allow inbound echo request**.
5. Click **OK**:



# Service Configuration

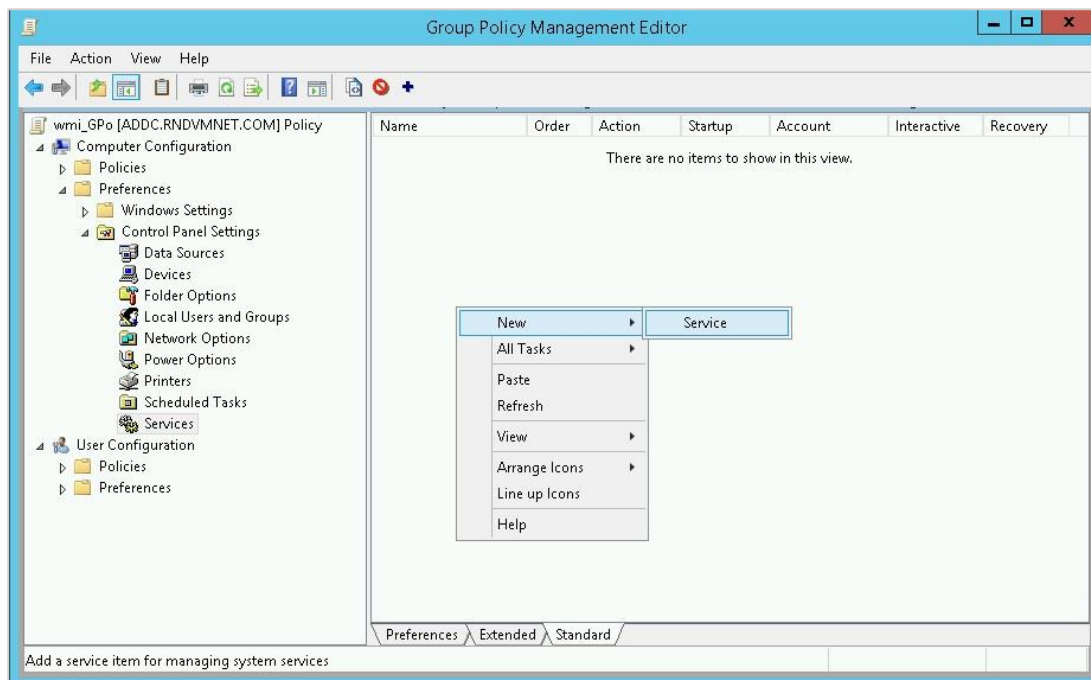
1. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > System Services > Windows Remote Management (WS-Management)**:



2. Check **Define this policy setting**.
3. Under **Select service startup mode** select **Automatic**.
4. Click **OK**:



5. Navigate to **Computer Configuration > Preferences > Control Panel Settings > Services**.
6. Right click and choose **New > Service**:

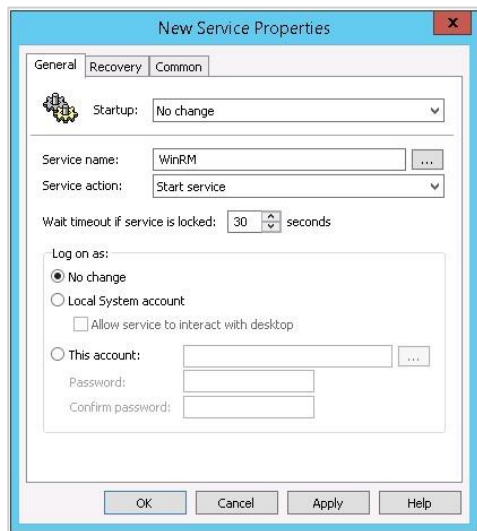


7. On the **General** tab select the following parameters:

**Startup:** No change

**Service name:** WinRM

**Service action (optional):** Start service



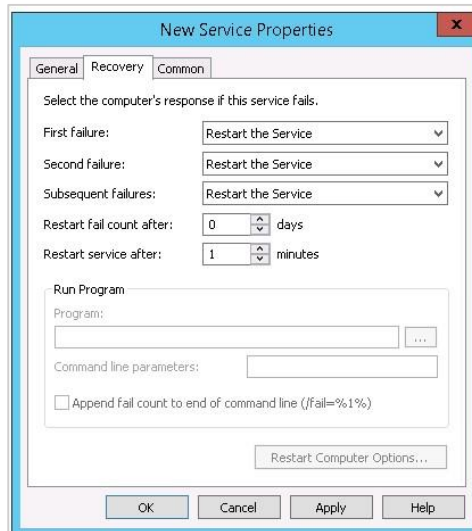
8. On the **Recovery** tab select the following parameters:

**First failure:** Restart the Service

**Second failure:** Restart the Service

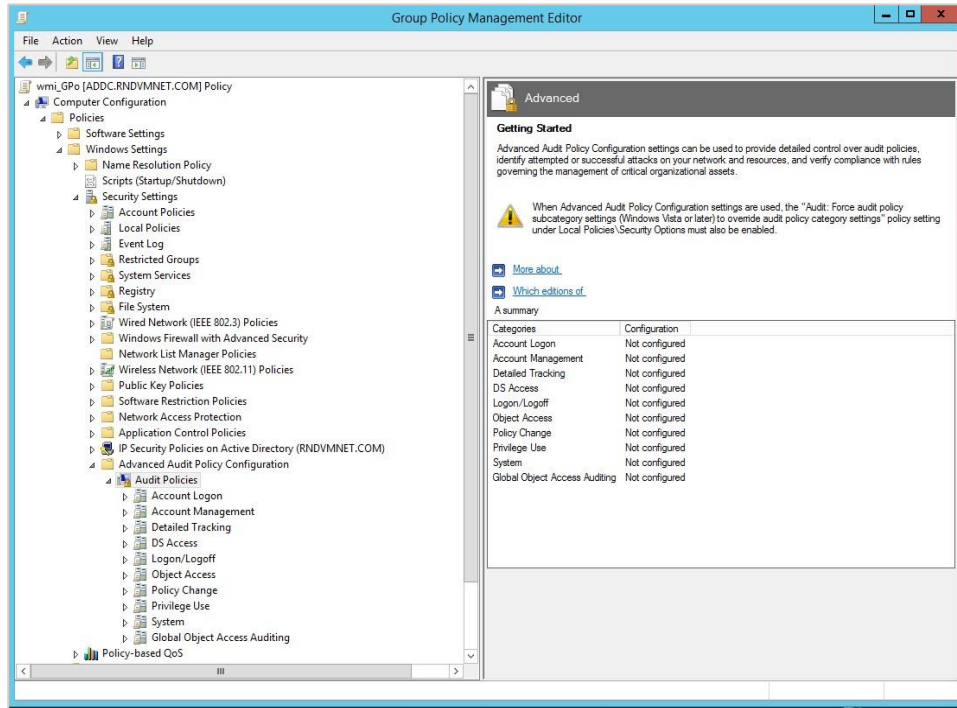
**Subsequent failures:** Restart the Service

9. Click **OK**:

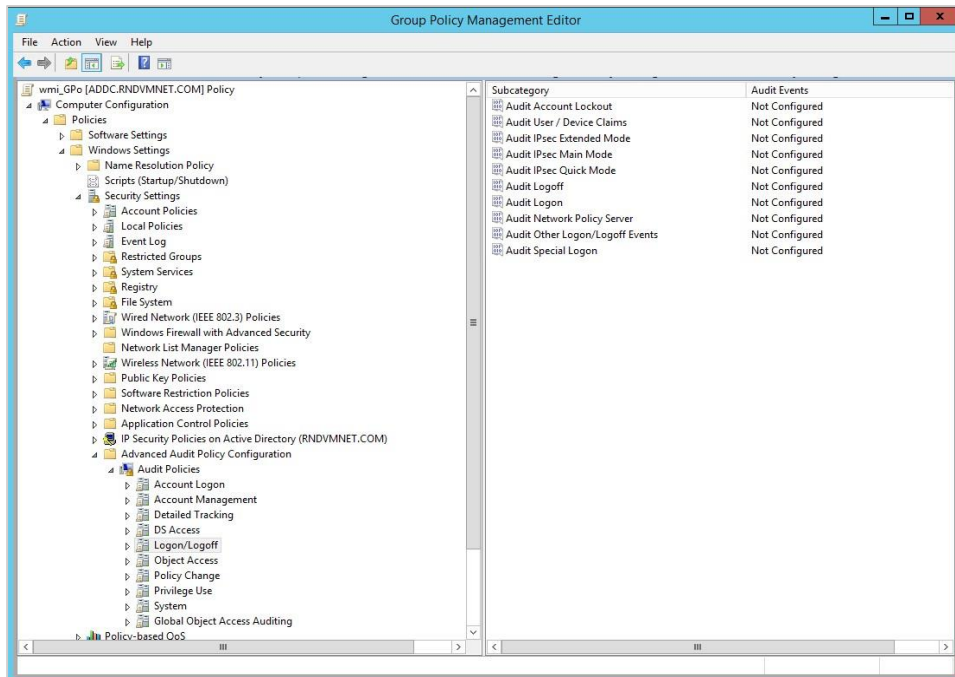


# Enabling Auditing

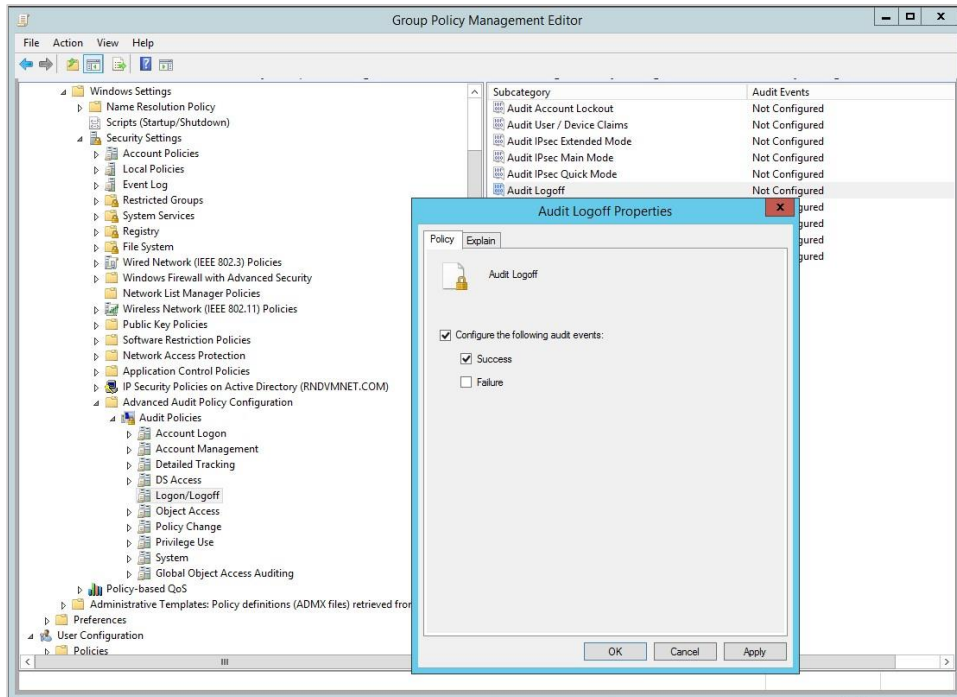
1. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies**:



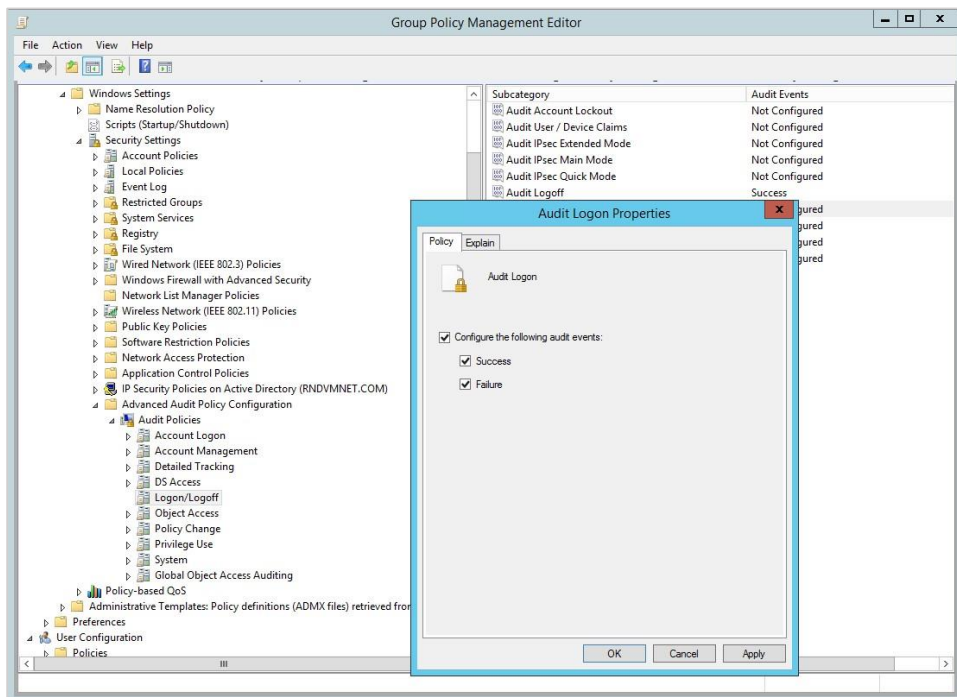
2. Expand **Logon/Logoff**:



3. Double click **Audit Logoff**, check **Configure the following audit events** and check **Success**.
4. Click **OK**:

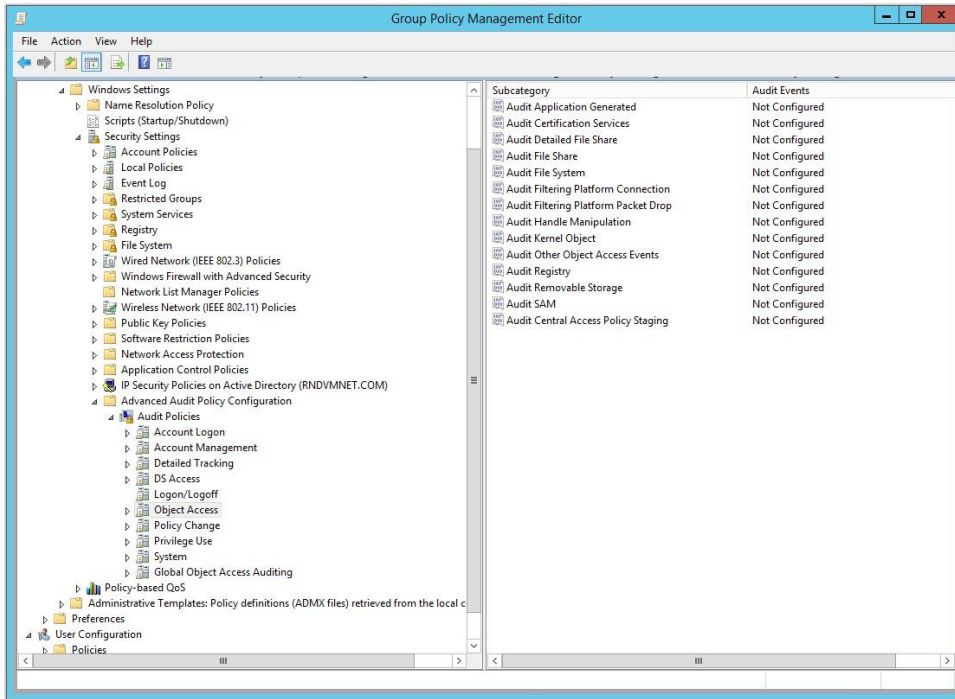


5. Double click **Audit Logon**, check **Configure the following audit events**, check **Success** and **Failure**.
6. Click **OK**:



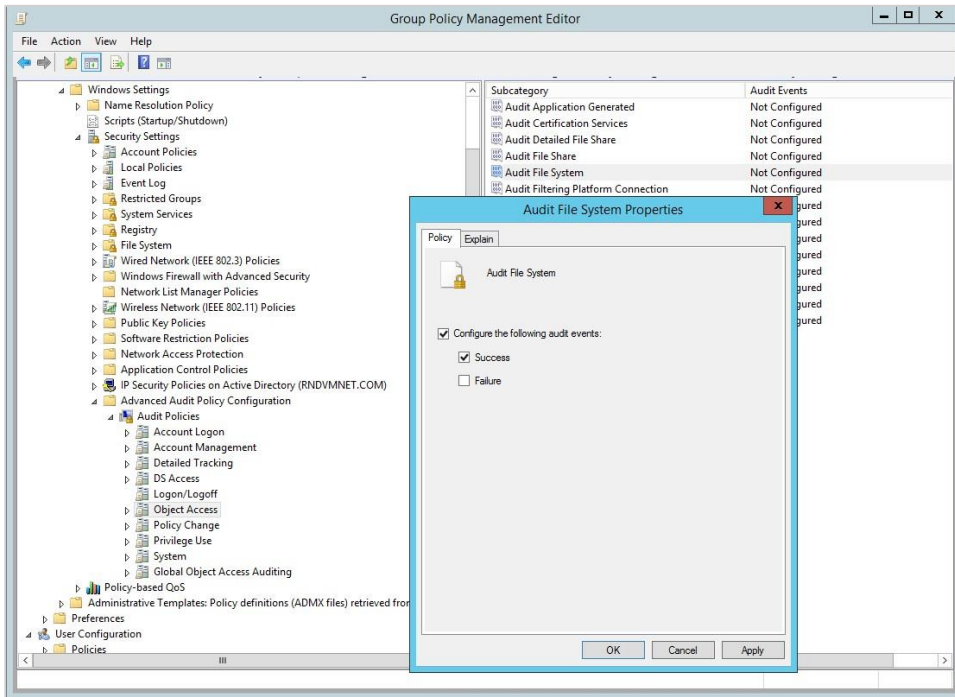


7. Expand Object Access:



8. Double click **Audit File System**, check **Configure the following audit events** and check **Success**.

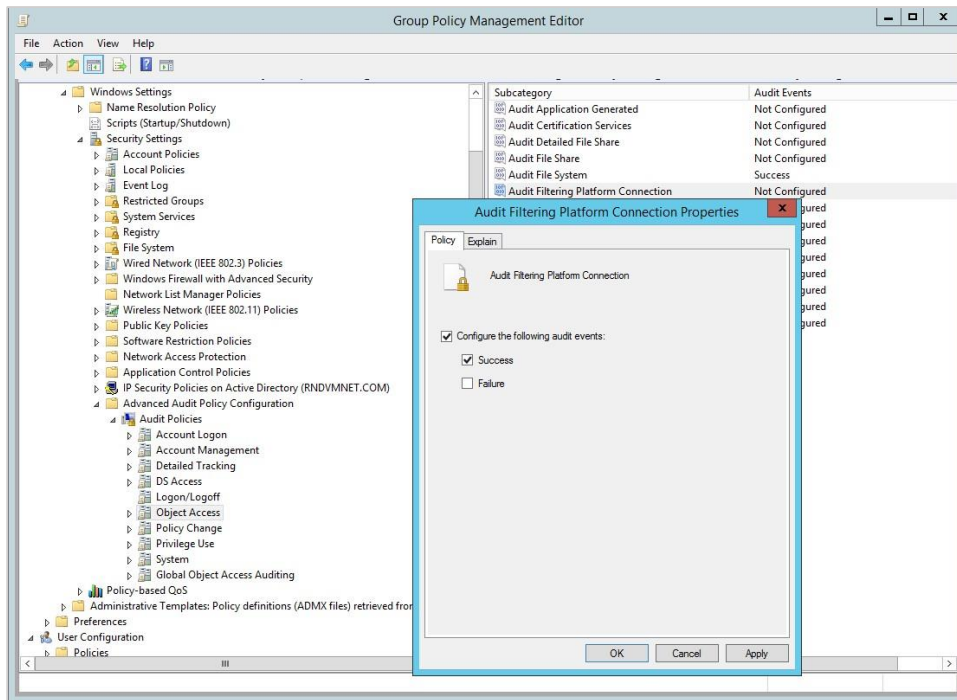
9. Click **OK**:





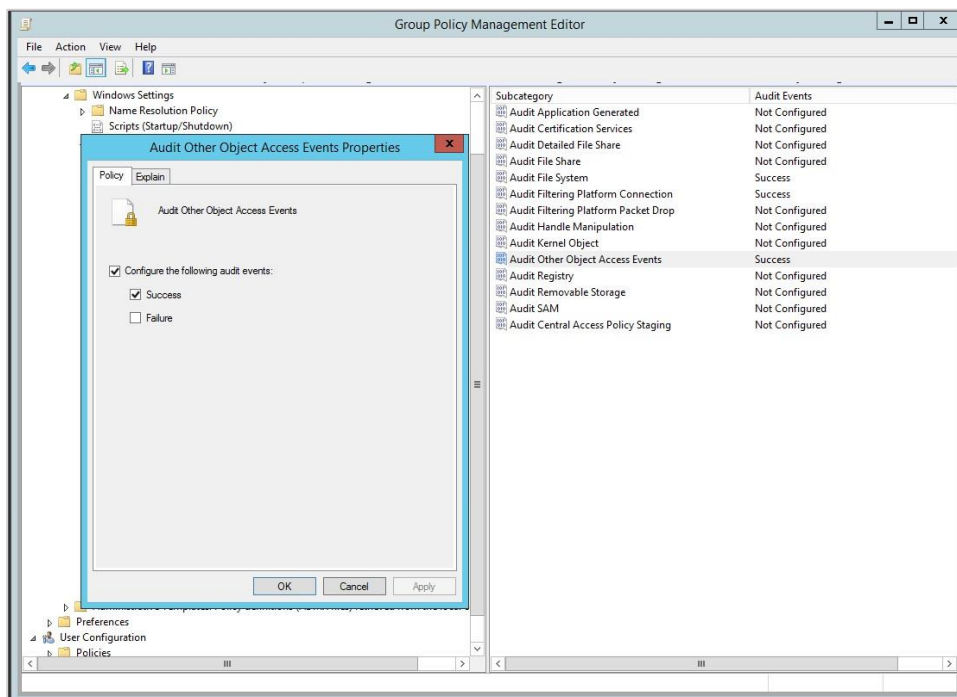
10. Double click **Audit Filtering Platform Connection**, check **Configure the following audit events** and check **Success**.

11. Click **OK**:



12. Double click **Audit Other Object Access Events**, check **Configure the following audit events** and check **Success**.

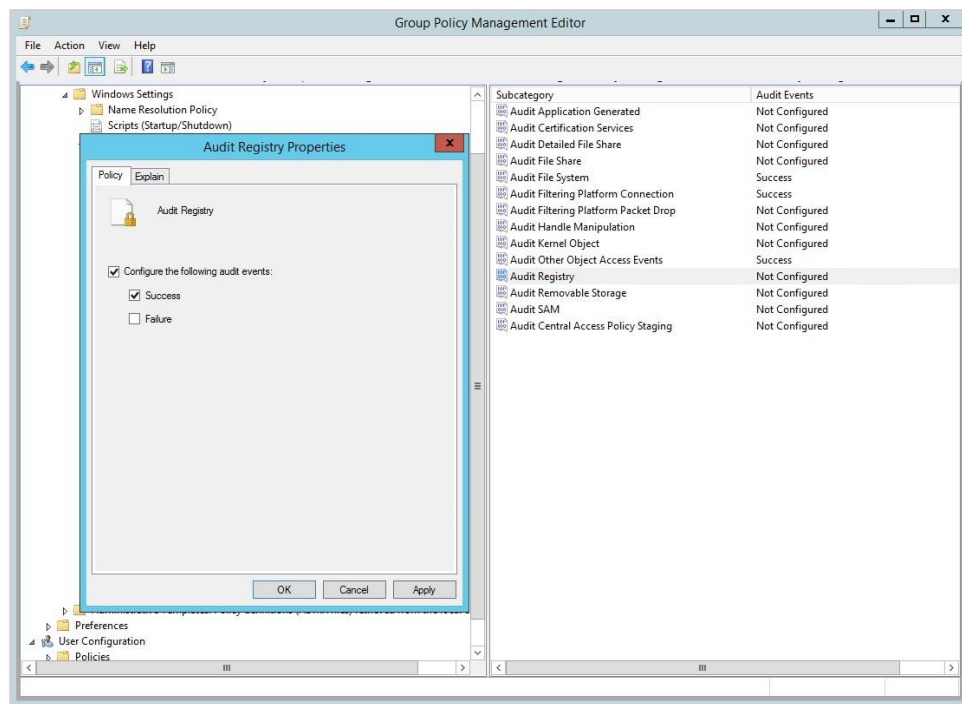
13. Click **OK**:





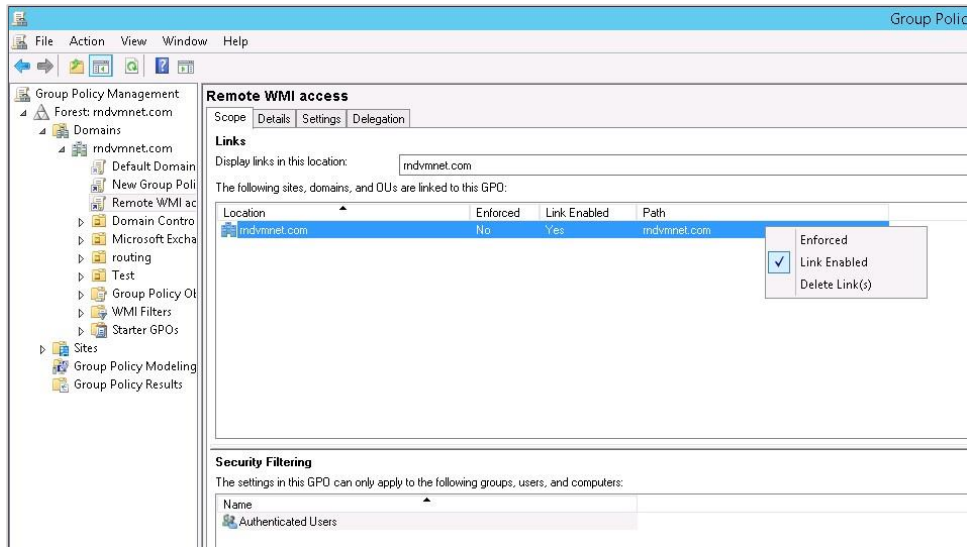
14. Double click **Audit Registry**, check **Configure the following audit events** and check **Success**.

15. Click **OK**:

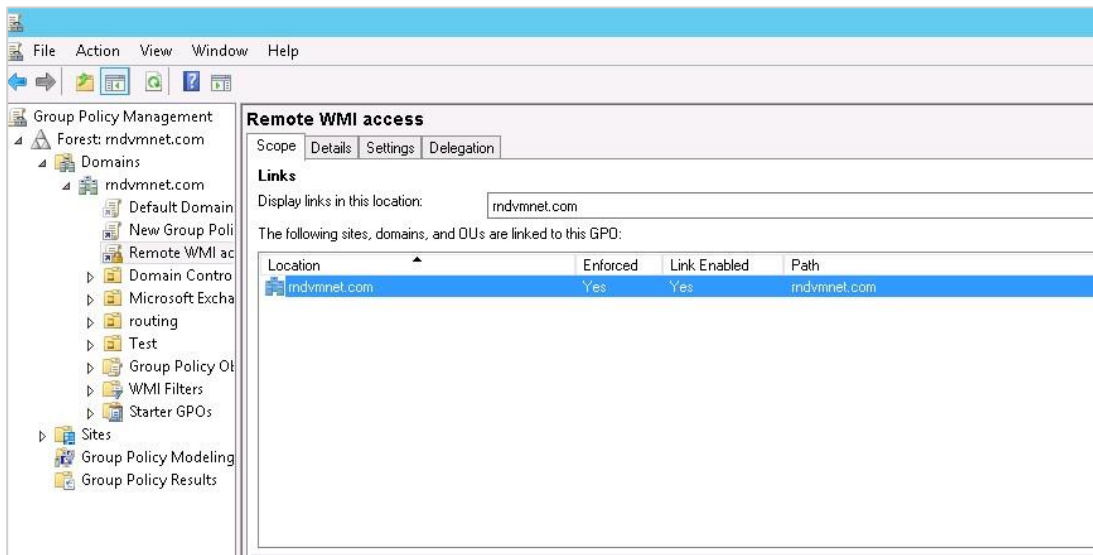


# Enabling the GPO

1. In order to enable the GPO, open **Group Policy Management** and double click the new GPO (named Remote WMI access in the example).
2. Right click and check **Enforced**:



3. Confirm that the **Enforced** field changes to **Yes**:





# Configuring Username and Password

Take these steps to configure the domain settings after deploying GPO.

1. Navigate to the **Policy > WMI** tab.
2. Add the **Domain settings (Domain, User, and Password)**:

Domain settings	Update	
Domain	User	Password
rndvmnet.com	administrator	Password is set



# Revision History

Date	Description	Section
27/05/2018	Cybowall Password updated	Network Scanning Configuration



## About CYBONET

CYBONET, formerly PineApp, was originally established as an email security solutions company. Since 2002, CYBONET has been providing easy to deploy, flexible and scalable security solutions that empower organizations of all sizes to actively safeguard their networks in the face of today's evolving threats. CYBONET's product suite includes our new Cybowall solution for network visibility, vulnerability management and breach detection, our flagship PineApp Mail Secure for comprehensive email security, and our carrier-grade Outbound Spam Guard (OSG). With a continued emphasis on developing and delivering high quality solutions, and in conjunction with our valued partner community, CYBONET is dedicated to security. For further details, please contact [info@cybonet.com](mailto:info@cybonet.com) [www.cybonet.com](http://www.cybonet.com)