How to Configure Windows Remote Management (WinRM)

Task. Configure WinRM.

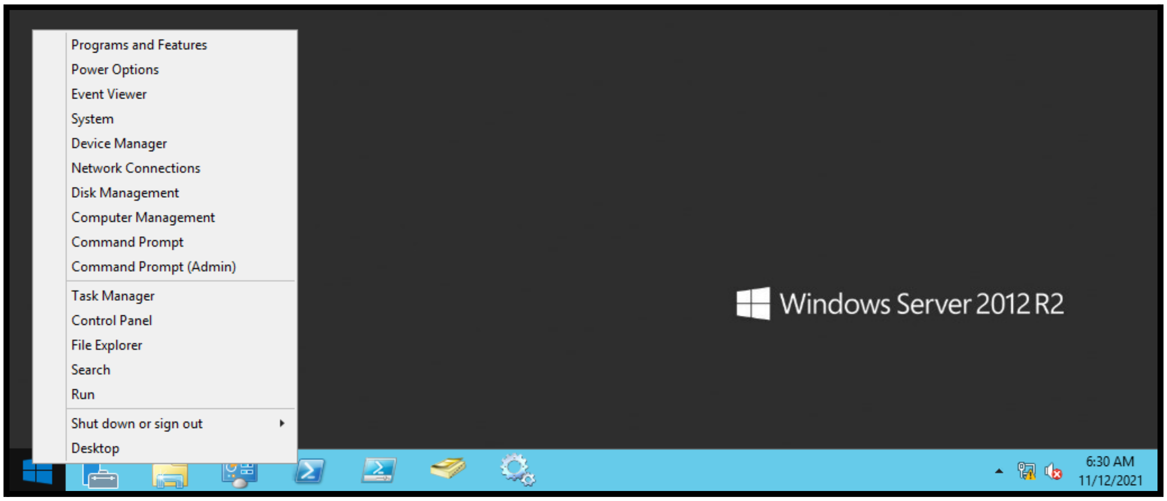
Purpose. Windows Event Forwarding and PowerShell Remoting use WinRM listeners to send and receive data. WinRM listeners exchange data via the HTTP or HTTPS protocol. Said data is encrypted using Kerberos, regardless of if HTTP or HTTPS is used. If WinRM is not enabled or configured correctly, administrators will not be able to collect Windows events, remotely manage the domain, etc.

Conditions. You have domain administrator privileges and access to either a domain controller or a workstation with Remote Server Administration Tools (RSAT) installed.

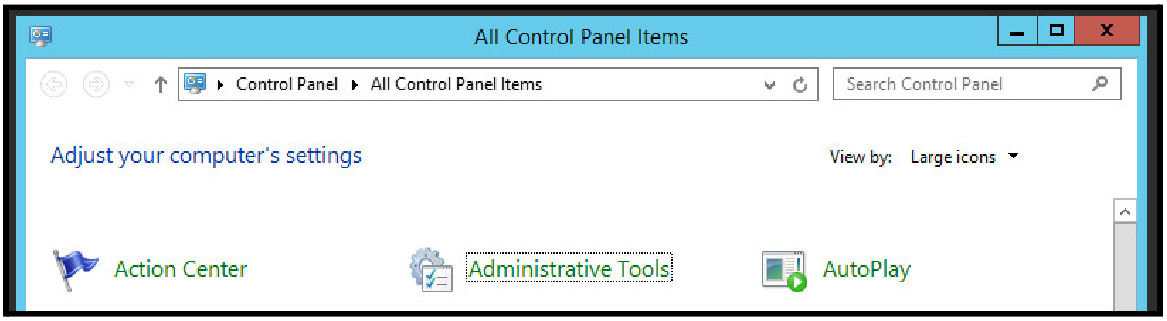
Standard. You were able to create a Group Policy Object (GPO) for WinRM.

Step 1. Login to your domain administrator account on either a domain controller or a workstation with RSAT installed.

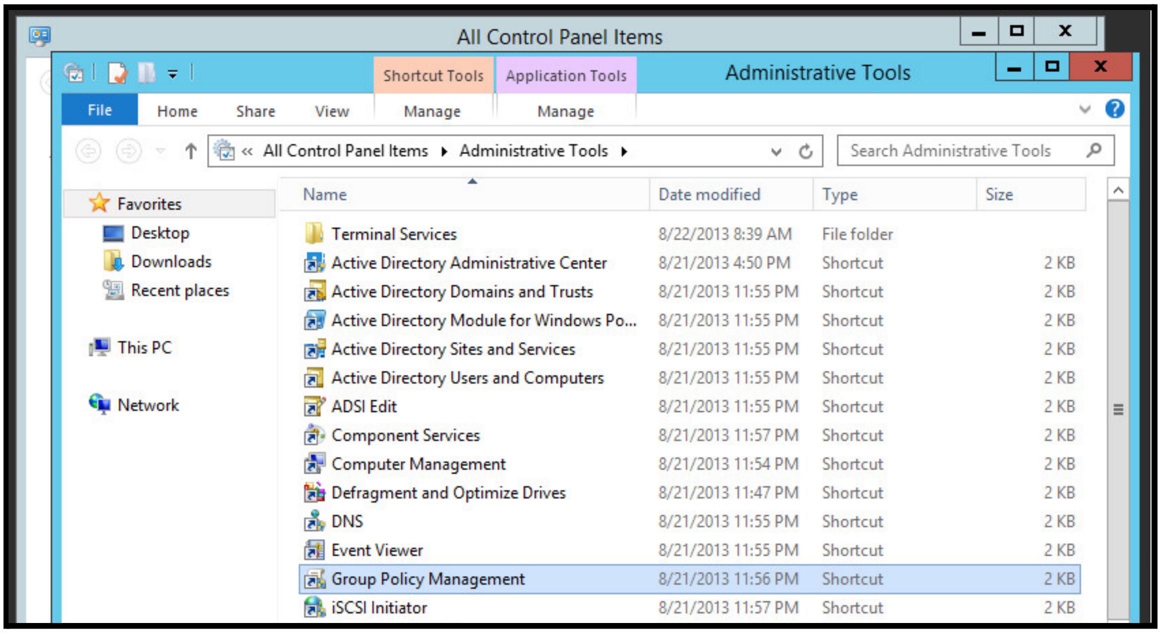
Step 2. Right-click the Windows icon in the bottom-left corner and select "Control Panel."



Step 3. Click-on "Administrative Tools."

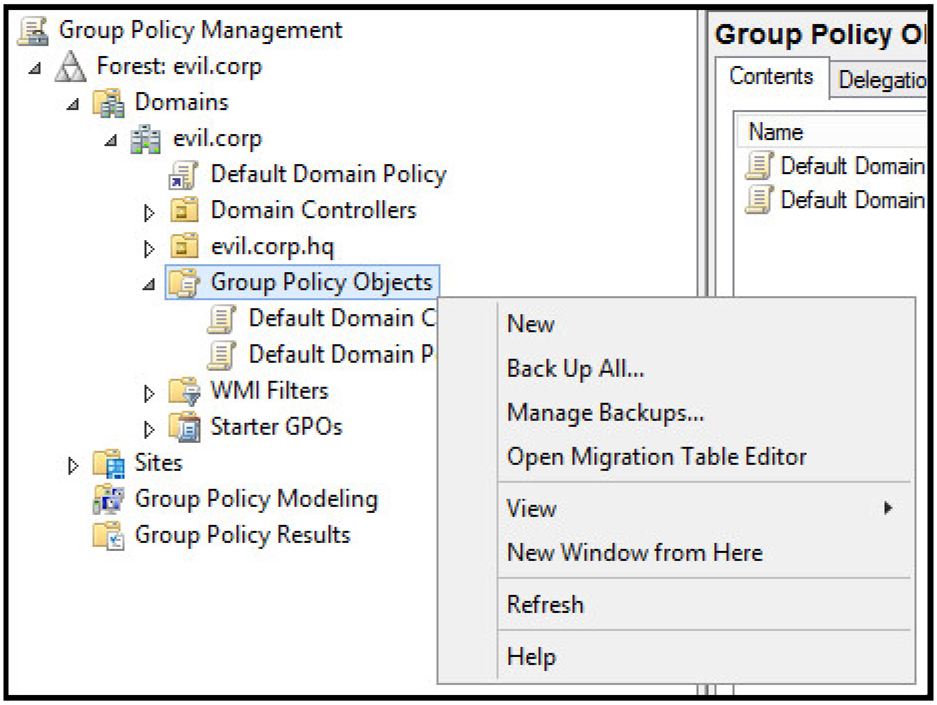


Step 4. Double-click "Group Policy Management."

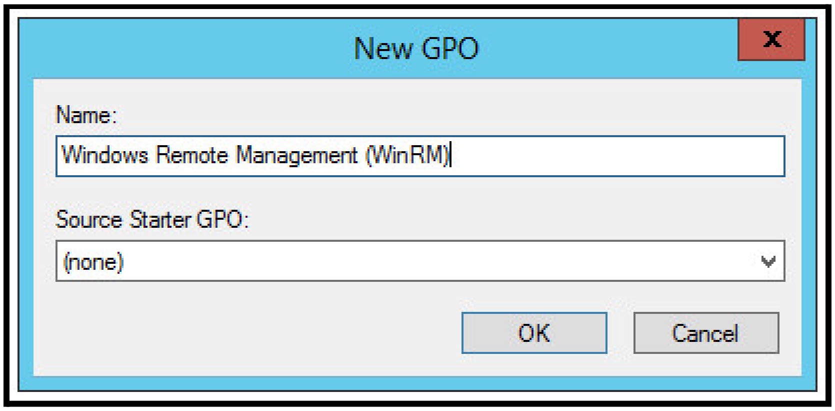


Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Active Directory Administrative Center	8/21/2013 4:50 PM	Shortcut	2 KB
Active Directory Domains and Trusts	8/21/2013 11:55 PM	Shortcut	2 KB
Active Directory Module for Windows Po...	8/21/2013 11:55 PM	Shortcut	2 KB
Active Directory Sites and Services	8/21/2013 11:55 PM	Shortcut	2 KB
Active Directory Users and Computers	8/21/2013 11:55 PM	Shortcut	2 KB
ADSI Edit	8/21/2013 11:55 PM	Shortcut	2 KB
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
DNS	8/21/2013 11:55 PM	Shortcut	2 KB
Event Viewer	8/21/2013 11:55 PM	Shortcut	2 KB
Group Policy Management	8/21/2013 11:56 PM	Shortcut	2 KB
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2 KB

Step 5. Right-click the "Group Policy Objects" container and select "New."



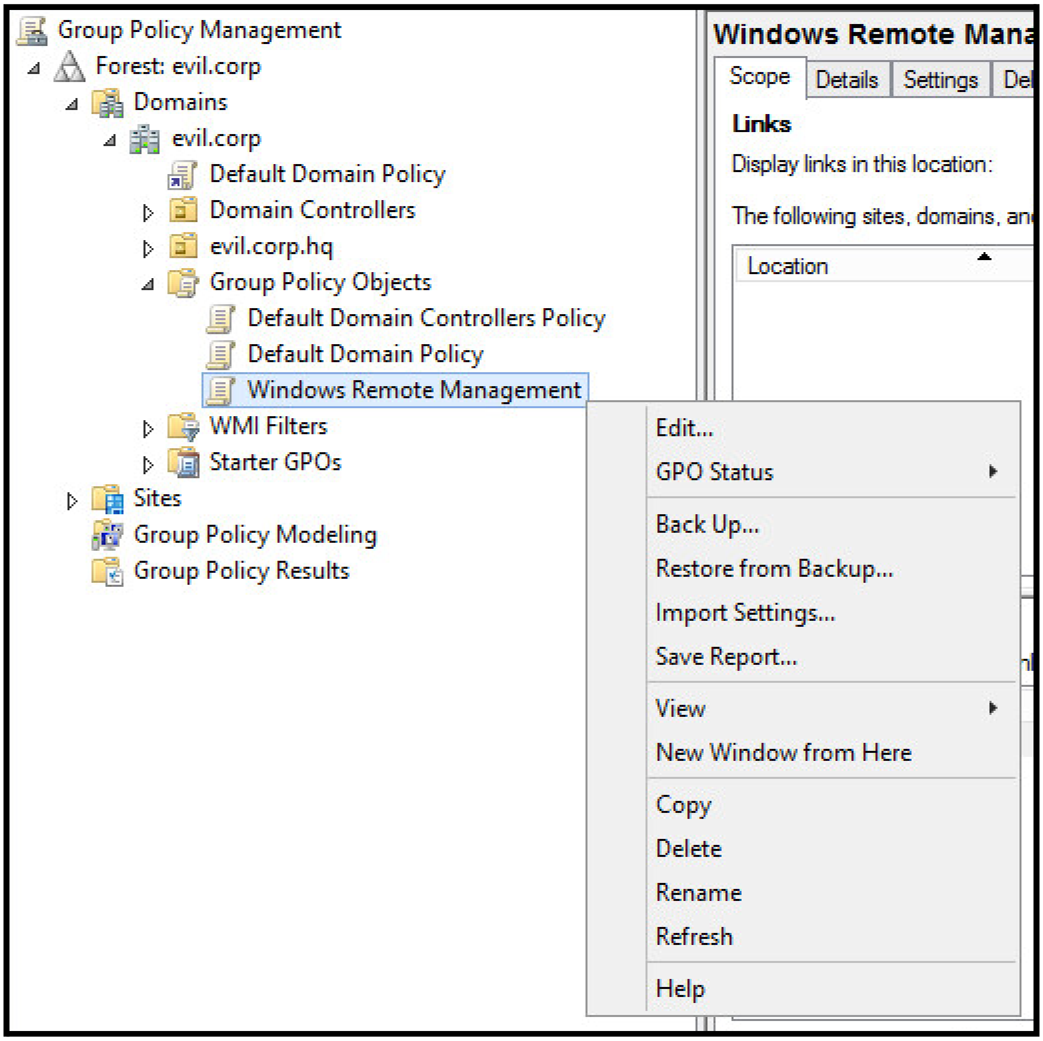
Step 6. Type “Windows Remote Management (WinRM)” in the “Name” field.



Name:
Windows Remote Management (WinRM)

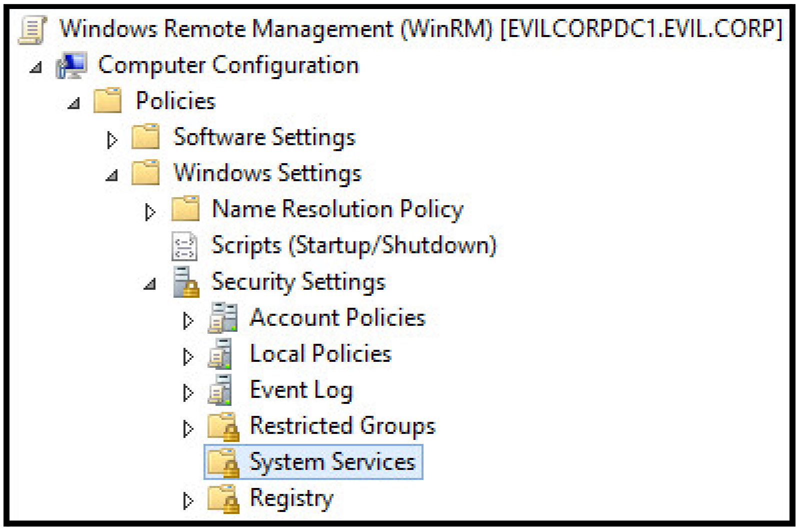
Source Starter GPO:
(none)

Step 7. Right-click the GPO you created and select “Edit.”



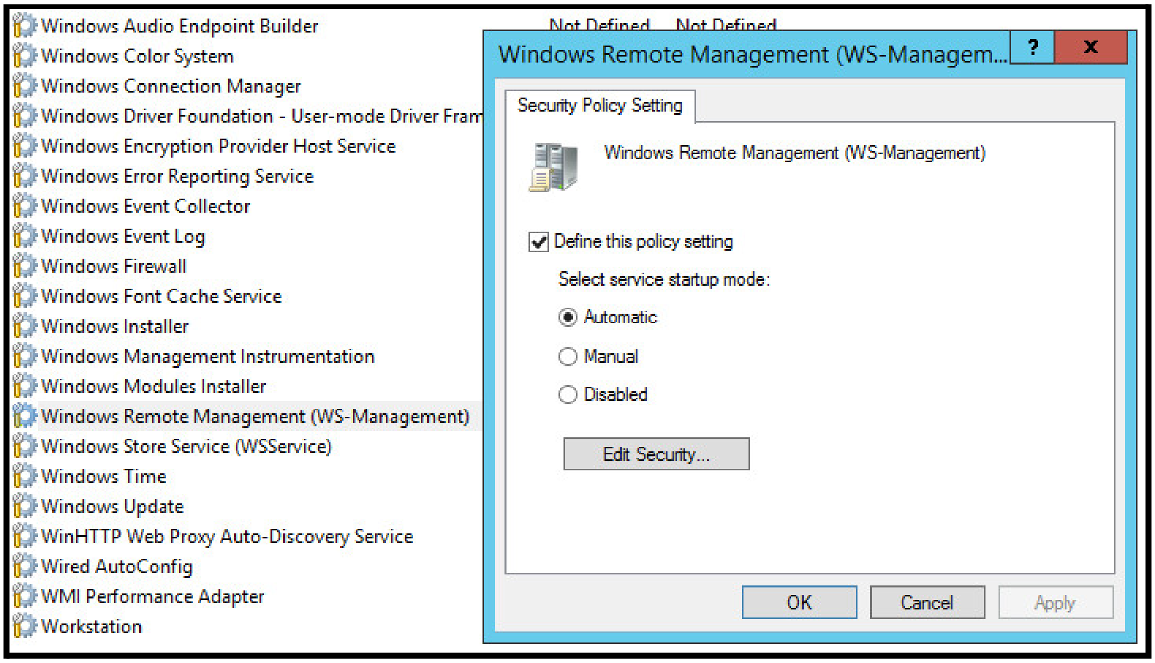
How to Configure Windows Remote Management (WinRM)

Step 8. With the GPO open, navigate to the following path: “Computer Configuration” > “Policies” > “Windows Settings” > “Security Settings” > “System Services.”



Windows Remote Management (WinRM) [EVILCORPDC1.EVIL.CORP]
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry

Step 9. In the pane on the right, right-click “Windows Remote Management (WS-Management),” select “Properties,” and configure the service startup mode to be “Automatic.” Click-on “Apply.”



Windows Audio Endpoint Builder — Not Defined — Not Defined
Windows Color System
Windows Connection Manager
Windows Driver Foundation - User-mode Driver Fram
Windows Encryption Provider Host Service
Windows Error Reporting Service
Windows Event Collector
Windows Event Log
Windows Firewall
Windows Font Cache Service
Windows Installer
Windows Management Instrumentation
Windows Modules Installer
Windows Remote Management (WS-Management)
Windows Store Service (WSService)
Windows Time
Windows Update
WinHTTP Web Proxy Auto-Discovery Service
Wired AutoConfig
WMI Performance Adapter
Workstation

Windows Remote Management (WS-Managem...

Security Policy Setting

Windows Remote Management (WS-Management)

☑ Define this policy setting

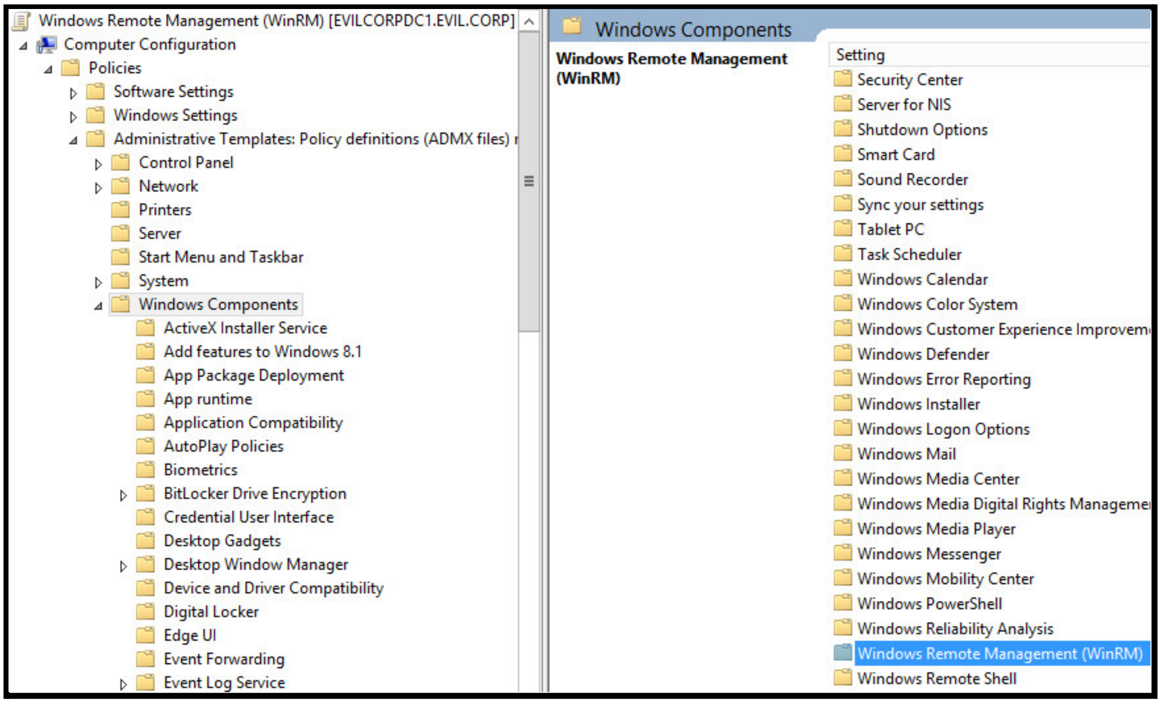
Select service startup mode:

● Automatic

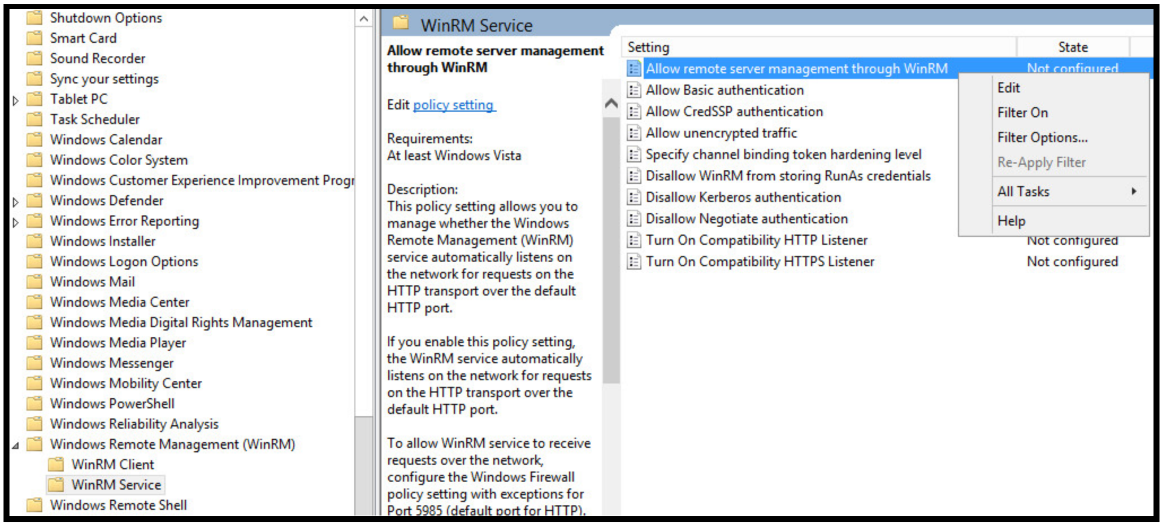
○ Manual

○ Disabled

Step 10. With the GPO still open, navigate to the following path: “Computer Configuration > Policies” > “Administrative Templates” > “Windows Components” > “Windows Remote Management (WinRM).”



Step 11. Double-click “Windows Remote Management (WinRM).” Double-click “WinRM Service.” Right-click “Allow remote service management through WinRM” and select “Edit.”



Allow remote server management through WinRM

Edit policy setting

Requirements:
At least Windows Vista

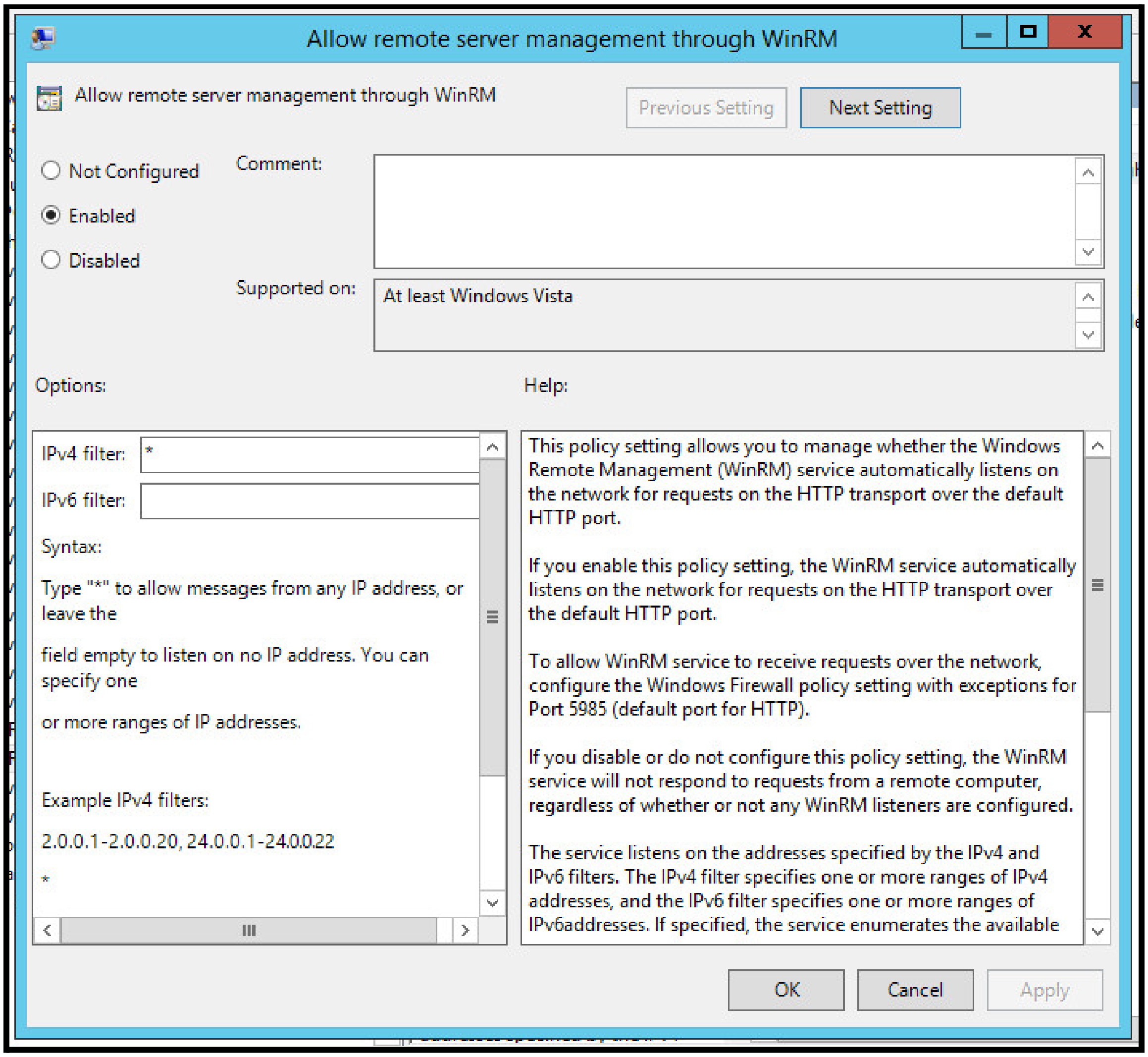
Description:
This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

If you enable this policy setting, the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting with exceptions for Port 5985 (default port for HTTP),

Setting	State
Allow remote server management through WinRM	Not configured
Allow Basic authentication	
Allow CredSSP authentication	
Allow unencrypted traffic	
Specify channel binding token hardening level	
Disallow WinRM from storing RunAs credentials	
Disallow Kerberos authentication	
Disallow Negotiate authentication	
Turn On Compatibility HTTP Listener	Not configured
Turn On Compatibility HTTPS Listener	Not configured

Step 12. Select “Enabled,” type “*” in the IPv4 filter field, click-on “Apply,” and click-on “OK.”



Allow remote server management through WinRM

Allow remote server management through WinRM

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

IPv4 filter: *

IPv6 filter:

Syntax:

Type "*" to allow messages from any IP address, or leave the

field empty to listen on no IP address. You can specify one

or more ranges of IP addresses.

Example IPv4 filters:

2.0.0.1-2.0.0.20, 24.0.0.1-24.0.0.22

*

Help:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

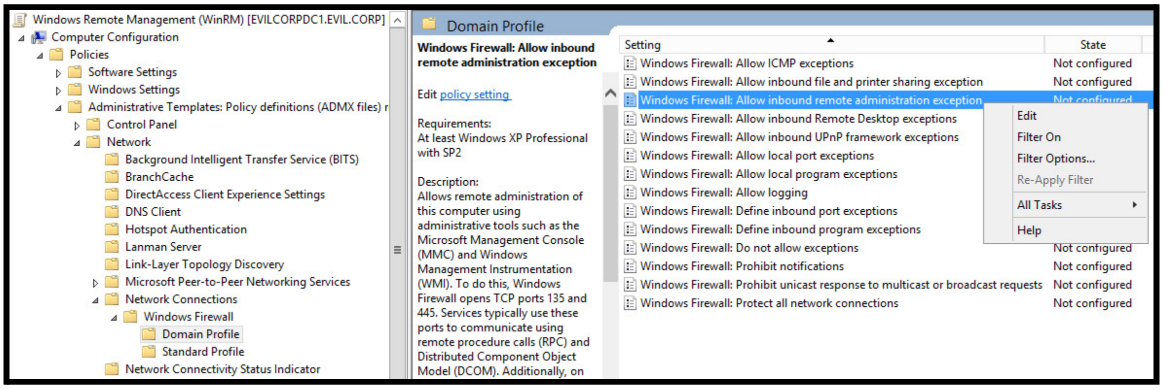
If you enable this policy setting, the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting with exceptions for Port 5985 (default port for HTTP).

If you disable or do not configure this policy setting, the WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.

The service listens on the addresses specified by the IPv4 and IPv6 filters. The IPv4 filter specifies one or more ranges of IPv4 addresses, and the IPv6 filter specifies one or more ranges of IPv6addresses. If specified, the service enumerates the available

Step 13. With the GPO still open, navigate to the following path: “Computer Configuration” > “Policies” > “Administrative Templates” > “Network” > “Network Connections” > “Windows Firewall” > “Domain Profile.” Right-click “Windows Firewall: Allow inbound remote administration exception” and select “Edit.”



- Windows Remote Management (WinRM) [EVILCORPDC1.EVIL.CORP]
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy definitions (ADMX files) r
        - Control Panel
        - Network
          - Background Intelligent Transfer Service (BITS)
          - BranchCache
          - DirectAccess Client Experience Settings
          - DNS Client
          - Hotspot Authentication
          - Lanman Server
          - Link-Layer Topology Discovery
          - Microsoft Peer-to-Peer Networking Services
          - Network Connections
            - Windows Firewall
              - Domain Profile
              - Standard Profile
          - Network Connectivity Status Indicator

Domain Profile

Windows Firewall: Allow inbound remote administration exception

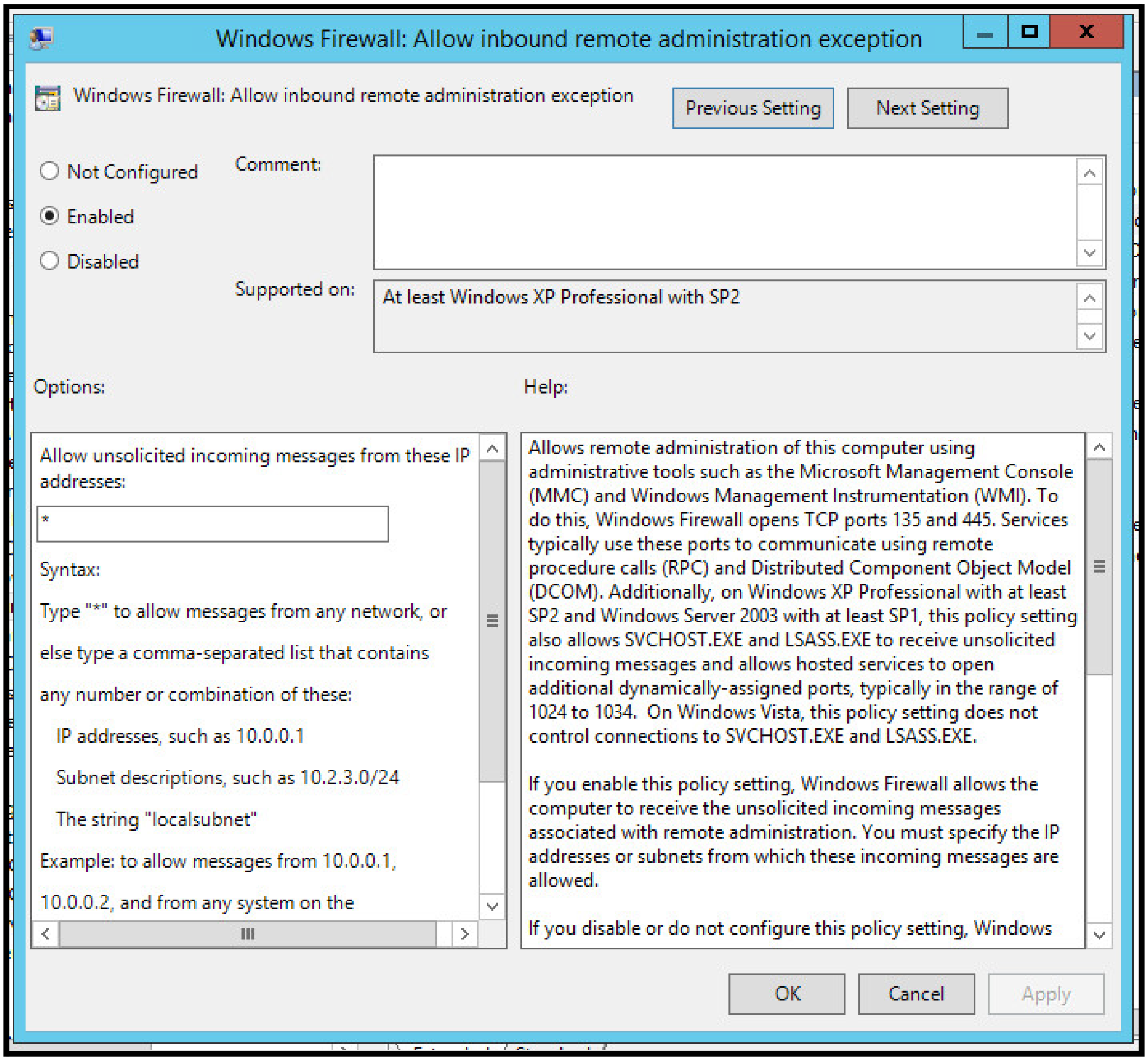
Edit policy setting

Requirements:
At least Windows XP Professional with SP2

Description:
Allows remote administration of this computer using administrative tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object Model (DCOM). Additionally, on

Setting	State
Windows Firewall: Allow ICMP exceptions	Not configured
Windows Firewall: Allow inbound file and printer sharing exception	Not configured
Windows Firewall: Allow inbound remote administration exception	Not configured
Windows Firewall: Allow inbound Remote Desktop exceptions	
Windows Firewall: Allow inbound UPnP framework exceptions	
Windows Firewall: Allow local port exceptions	
Windows Firewall: Allow local program exceptions	
Windows Firewall: Allow logging	
Windows Firewall: Define inbound port exceptions	
Windows Firewall: Define inbound program exceptions	
Windows Firewall: Do not allow exceptions	Not configured
Windows Firewall: Prohibit notifications	Not configured
Windows Firewall: Prohibit unicast response to multicast or broadcast requests	Not configured
Windows Firewall: Protect all network connections	Not configured

Step 14. Select “Enabled,” type “*” in the “Allow unsolicited incoming messages from these IP addresses,” click-on “Apply,” and click-on “OK.”



Windows Firewall: Allow inbound remote administration exception

Windows Firewall: Allow inbound remote administration exception

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows XP Professional with SP2

Options:

Allow unsolicited incoming messages from these IP addresses:

*

Syntax:

Type "*" to allow messages from any network, or

else type a comma-separated list that contains

any number or combination of these:

IP addresses, such as 10.0.0.1

Subnet descriptions, such as 10.2.3.0/24

The string "localsubnet"

Example: to allow messages from 10.0.0.1,

10.0.0.2, and from any system on the

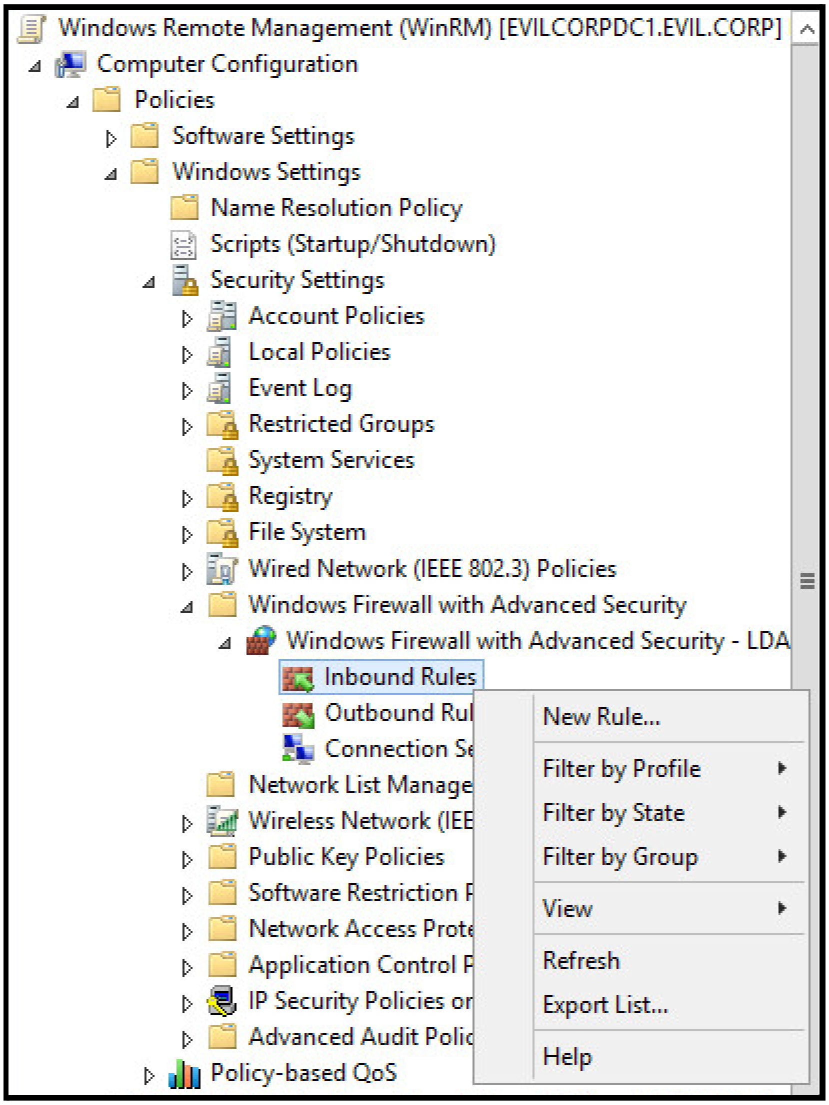
Help:

Allows remote administration of this computer using administrative tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object Model (DCOM). Additionally, on Windows XP Professional with at least SP2 and Windows Server 2003 with at least SP1, this policy setting also allows SVCHOST.EXE and LSASS.EXE to receive unsolicited incoming messages and allows hosted services to open additional dynamically-assigned ports, typically in the range of 1024 to 1034. On Windows Vista, this policy setting does not control connections to SVCHOST.EXE and LSASS.EXE.

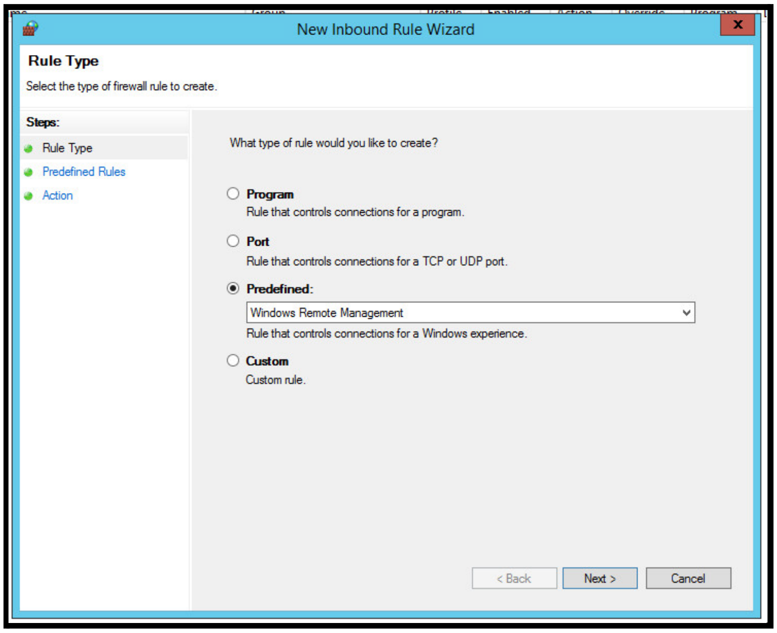
If you enable this policy setting, Windows Firewall allows the computer to receive the unsolicited incoming messages associated with remote administration. You must specify the IP addresses or subnets from which these incoming messages are allowed.

If you disable or do not configure this policy setting, Windows

Step 15. With the GPO still open, navigate to the following path: “Computer Configuration” > “Policies” > “Windows Settings” > “Security Settings” > “Windows Firewall with Advanced Security” > “Windows Firewall with Advanced Security.” Right-click “Inbound Rules” and select “New Rule.”



Step 16. In the “Predefined” drop-down menu, select “Windows Remote Management.” Click “Next.”



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Predefined Rules
- Action

What type of rule would you like to create?

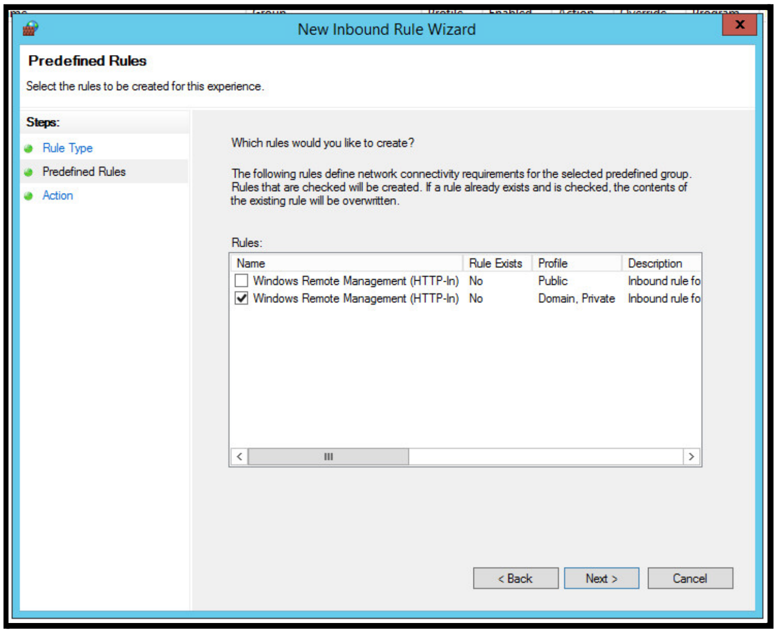
○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

● **Predefined:**
Windows Remote Management
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Step 17. Deselect “Windows Remote Management (HTTP-In)” for the “Public” profile. Select “Windows Remote Management (HTTP-In)” for the “Domain, Private” profile. Click “Next.”



New Inbound Rule Wizard

Predefined Rules

Select the rules to be created for this experience.

Steps:
- Rule Type
- Predefined Rules
- Action

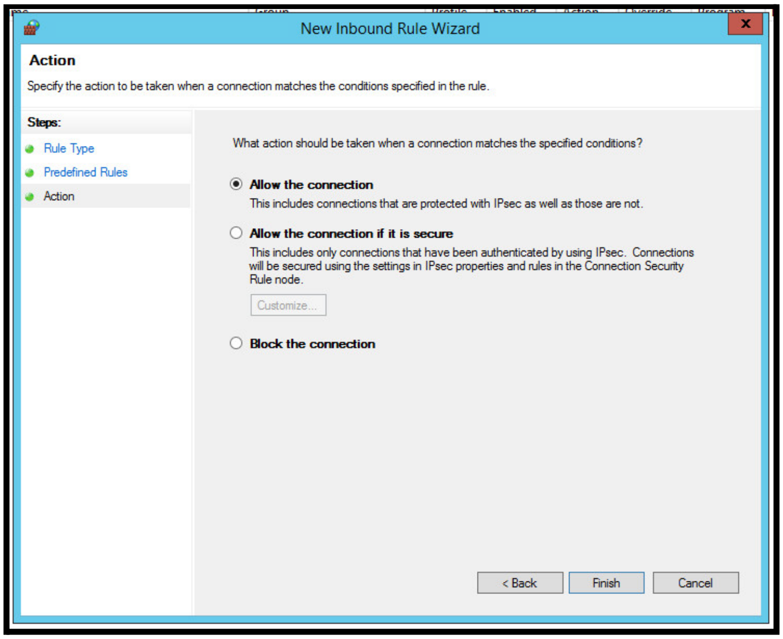
Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Rules:

Name	Rule Exists	Profile	Description
□ Windows Remote Management (HTTP-In)	No	Public	Inbound rule fo
☑ Windows Remote Management (HTTP-In)	No	Domain, Private	Inbound rule fo

Step 18. Select “Allow the connection.” Click “Finish” and close the GPO.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Predefined Rules
- Action

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

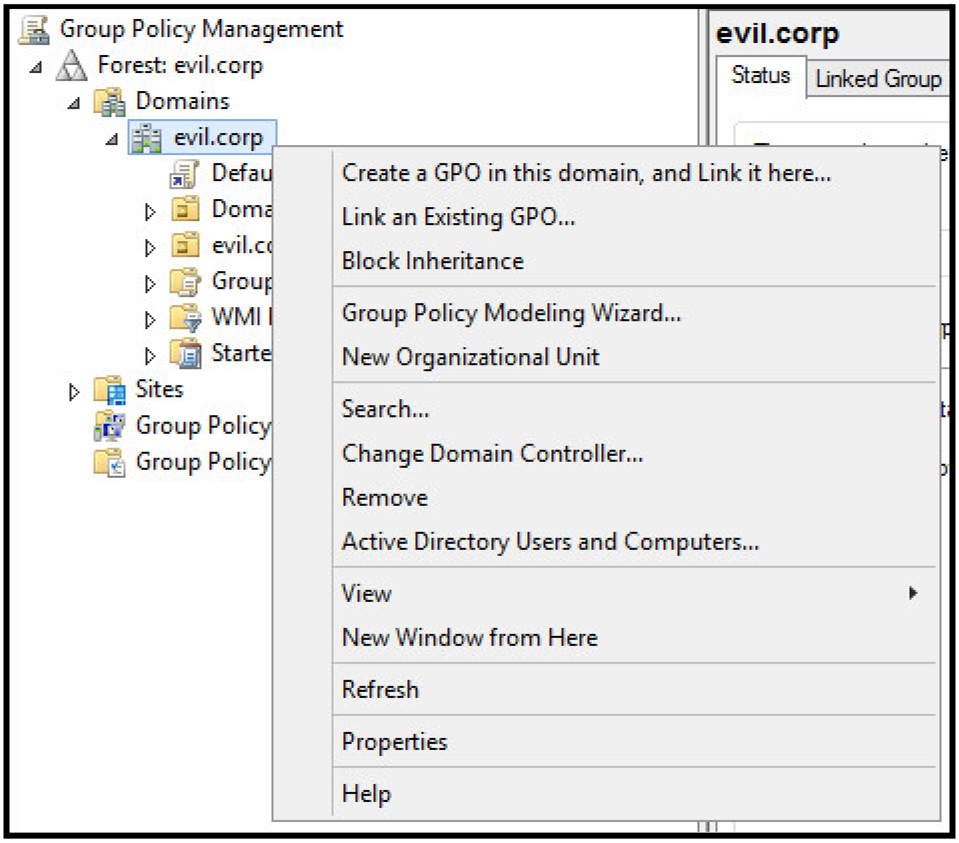
○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Customize...

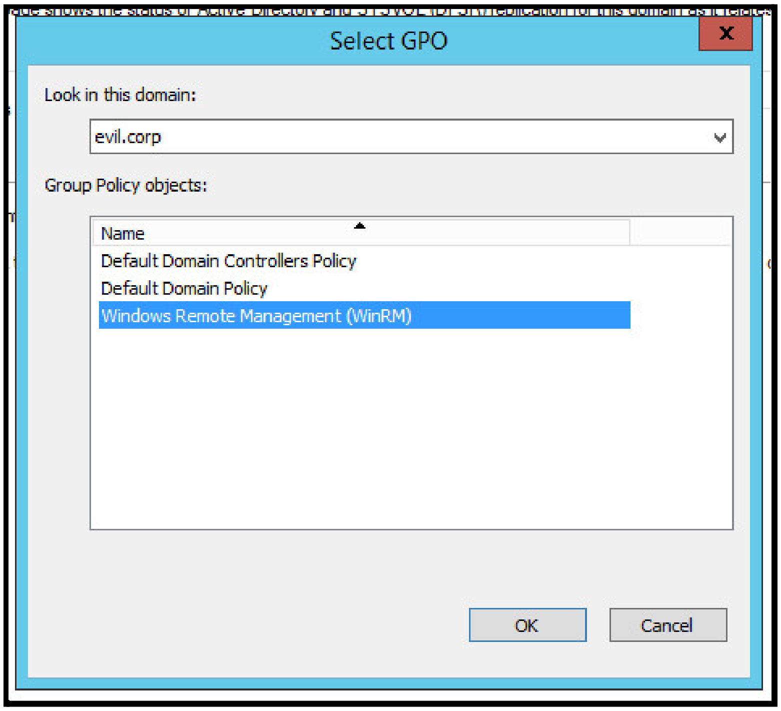
○ **Block the connection**

< Back | Finish | Cancel

Step 19. Right-click your domain and select “Link an Existing GPO…”



Step 20. Select the GPO you created and click-on "OK."



Look in this domain: evil.corp

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
Windows Remote Management (WinRM)