2018

Deployment Guide

BLOCKBOX DISCOVERY APPLIANCE

REV 2.2, JAN 2018

Contents

Introduction

The BlockBox Appliance is a hardened Linux virtual appliance with an on-board web server designed to provide a richly detailed but easy to understand portrait of your IT environment.

The information capture elements of the BlockBox are designed to capture an exhaustive and accurate inventory of all endpoints - be they Windows PCs and Servers, Linux or Solaris systems, OSX devices, SNMP-enabled Layer 2 & Layer 3 devices, or even mobile devices connected to your wireless network.

The on-board reporting provided by the BlockBox is designed to be easy to use, to require the fewest clicks possible, and to answer key questions about the hardware and software present in your environment.

Requirements

For the BlockBox appliance to function properly, there are some ‘must haves’ that should be taken care of out of the gate.

Networking Requirements:

First off - you or someone with the appropriate access will need to provide a list of the appropriate subnet(s) to put into scope to ‘see’ all devices on the network(s)

- To function properly and be able to access and communicate with your entire environment, the BlockBox must be on a network segment that can route to any and all other segments. If there are unique ACLs on your routers or switches, they must allow the discovery appliance to communicate through to your endpoints.
- Access from the appliance through any network firewalls, intrusion prevention systems or endpoint protection. See Network Security Requirements below.

Network Security Requirements

Certain features of the appliance require a small amount of pre-work. We have endeavoured to create a platform that required zero client footprint - no agents, and no leave-behinds on your endpoints. To make that possible however, we require the ability to remotely administer these endpoints. Luckily, this is easily accomplished, and is a one-time effort.

The salient points are as follows:

- Network-based firewalls or Intrusion Prevention systems must allow communication from the appliance to your endpoints.

- Local firewalls or Endpoint Protection applications must also allow for communication from the appliance.

- The simplest method to ensure connectivity through your Endpoint Protection product, is to add a firewall and/or complete exception from the appliance's IP address to all endpoints over all ports and through all protections.

- Windows Inventory processes typically communicate over TCP ports 135, 139 and 445 (WMI, RPC, SMB) and UDP ports 137 and 138 (NetBIOS). Windows Inventory communicates over those ports using the following "services":
    - WMI
    - Remote Procedure Calls (RPC)
    - SMB (CIFS)

  To ensure these services respond to our inventory, please refer to Appendix 1.2 **–** Allowing Inventory services using Group Policy***...***

- OSX, Linux and Solaris Inventory processes are carried out over SSH (TCP port 22)

- SNMP Inventory processes are carried out over UDP ports 161 and/or 162

- VMware vCenter Inventory process are carried out over HTTPS (TCP port 443)

Windows Inventory Requirements:

- Administrator credentials with both domain and local administrator access for inventorying Windows machines. Typically, domain administrators have local administrator rights out of the gate, but if this is not the case in your environment, and you are not sure how to grant local administrator rights to a set of domain administrator credentials, please see Appendix 1.1: Granting A Domain User Local Administrative Rights
- Access through any local firewalls or endpoint protection systems to, at minimum, TCP ports 135, 139 and 445 (WMI, RPC and SMB) and UDP ports 135 and 139. See Network Security Requirements above.
- Additional Windows firewall exceptions may need to be set using Group Policy. See Appendix 1.2 - ***Windows Firewall…***

Apple OSX Inventory Requirements:

- OSX Administrator credentials for inventorying OSX machines
- SSH management must be enabled on the endpoint
- Access through any local firewalls or endpoint protection systems using TCP port 22 (SSH). See Network Security Requirements above.

Linux/Solaris Inventory Requirements:

- Credentials that can access the following resources for *nix systems:
    - Files in `/proc/`
    - `dmidecode` (ideal)
- Credentials that can access the following resources for Solaris systems:
    - `/usr/sbin/psrinfo`
    - `/usr/sbin/prtconf`
    - `/usr/sbin/smbios (`or `eeprom` or `sneep)`
- Access through any local firewalls or endpoint protection systems using TCP port 22 (SSH). See Network Security Requirements above.

VMware Inventory Requirements:

- vCenter SSO domain credentials in UPN format e.g. administrator@sso.mydomain.local
    - These credentials can also be Windows domain credentials.
- Access through any local firewalls or endpoint protection systems using TCP port 443 (HTTPS). See Network Security Requirements above.

SNMP Inventory Requirements:

- SNMP v1 or v2c read-only community strings
- SNMP v3 credentials for inventorying the network devices. These would include:
    - Username
    - Password
    - Context
    - Security level
    - Authentication and encryption protocols
    - Encryption key
- Access through any local firewalls or endpoint protection systems using UDP ports 161 and 162. See Network Security Requirements above.

Information Collection

The BlockBox can collect an inventory of all devices on the network, though if you have an alternate solution already collecting this data, you can simply choose to not enable the Inventory functions of the BlockBox, and import flatfiles of your existing inventory yourself in the ‘Utilities’ section of the BlockBox GUI.

Should you use the BlockBox to collect an inventory of your environment, information is collected in the following fashion:

Scanning

First, a list of viable targets is generated via a multi-level scan of the environment. This has been engineered to have the lowest impact to the network possible. First, a list of possible targets is gathered by conducting a scan of provided subnets via TCP SYN requests. The results of these scans are combined and used as a list of viable targets within the environment.

Fingerprinting

Optionally, and recommended on all but the most fragile of networks, further information can be collected about the devices that have been uncovered without a full-blown inventory being conducted, via OS fingerprinting. This is carried out by investigating the manner in which the device responds to a small number of TCP and UDP probes over a period of a few milliseconds. This can be disabled if chosen.

Inventory

Once a possible candidate for inventory has been detected and validated, an inventory of that endpoint can be optionally carried out. For Windows and OSX machines, a full list of installed software, as well as the hardware specifications and serial numbers of the machines are gathered. For SNMP devices (such as printers, switches, routers, and firewalls), the full complement of MIBs is dumped, and information such as manufacturer, model, serial number, etc. is gathered. For Linux, Unix, Solaris and similar variants, hardware information, package lists, and certain files pertaining to software installations are gathered.

Reporting

Almost of your interactions with the BlockBox will take place through a browser. We hope you'll find the reports provided useful in gaining a quick and easy understanding of what you have - and more importantly, what you need to know about it. But first, you'll need to configure the appliance for your unique environment.

Initial Setup

Console Setup

First things first! Hopefully by now you have downloaded a copy of the virtual appliance and deployed it on your chosen virtualization platform, and have an IP Address handy that you can assign to the appliance. The first job you'll have is to, from the console, log into the device:

```
      blockbox login: _
```

The login and the password are both by default ‘blockbox’, though you will be asked to change this upon your first login. After you’ve successfully logged in, simply type ‘./config’ at the prompt to configure the network:

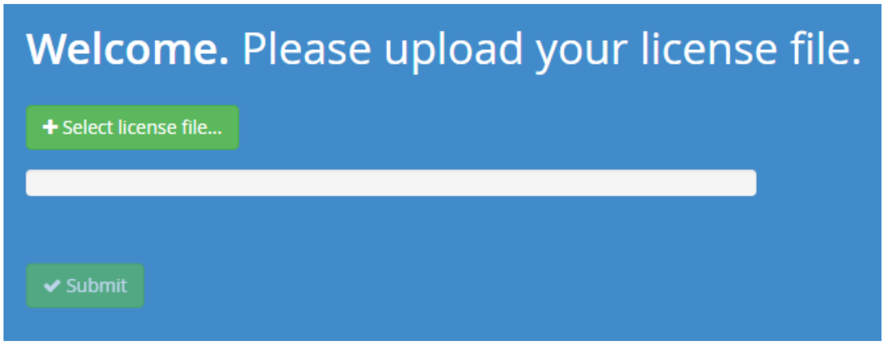
```
      blockbox@blockbox:~$ _ ./config
```

You will be asked to supply the desired netmask, gateway, ip address, DNS servers and DNS suffixes for the appliance:

```
Configuring BlockBox for first use!

Please enter the Netmask associated with this appliance: [255.255.255.0]
255.255.255.0

Please enter the gateway associated with this appliance: [xxx.xxx.x.x]
192.168.1.1

Please enter the IP Address assigned to this appliance:  [xxx.xxx.x.xx]
192.168.1.96

Please enter your Domain Name Server(s) (DNS) assigned to this appliance.
Please separate each DNS with a space: [8.8.8.8 9.9.9.9]

Please enter your Domain Suffix(es) (DNS) assigned to this appliance

. Please separate each suffix with a space: [domain.local
subdomain.domain.local]

Changes Applied. Please reset the appliance to continue.
```

Web UI Setup

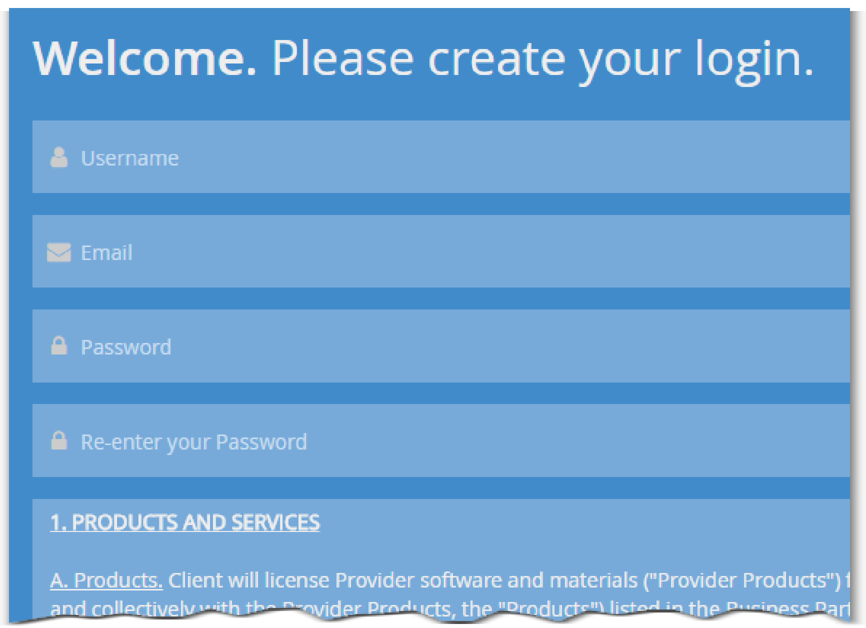
After configuring the device IP address and resetting the device, you should be able to navigate via browser to the GUI for further configuration. **Make sure to use ‘https’ as the IP prefix.** You may want to bookmark this page for easy re-visiting once you’ve arrived. The first screen you see should be like this:



Welcome. Please upload your license file.

You should have received a license file (“license.dat”) that you can upload using the browser interface. If you haven’t, contact your representative and we’ll get you sorted out right away!

From here, you’ll want to input the credentials you plan to use with the appliance. Make sure you write them down or keep them on hand somewhere!

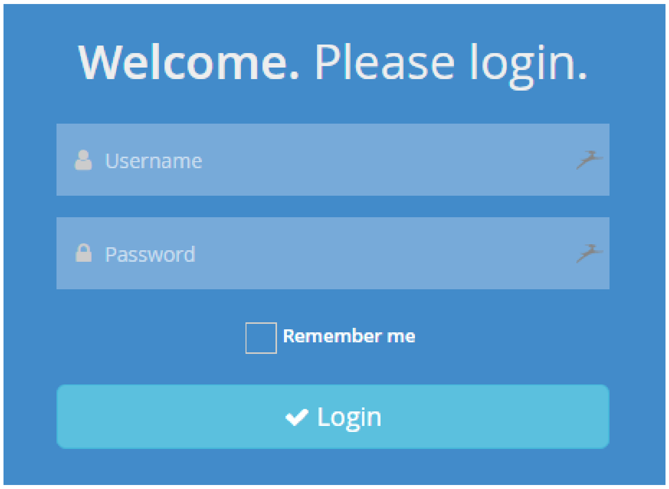


Welcome. Please create your login.

1. PRODUCTS AND SERVICES

A. Products. Client will license Provider software and materials ("Provider Products") t and collectively with the Provider Products, the "Products") listed in the Business Part

Once created, you be dropped into the login page. Use the credentials you just created to authenticate, and you're on to the configuration wizard!



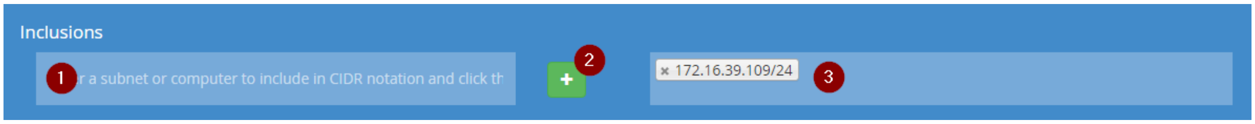
Welcome. Please login.

Configuration Wizard

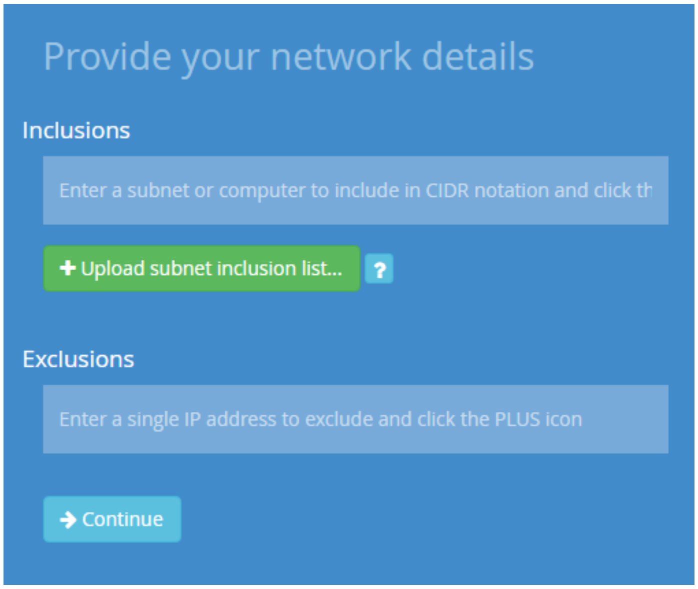
You should be directed to the "Configuration Wizard" on first landing.

Note: The rule of thumb for entering data into most fields in the Configuration Wizard, is to:

1. Enter the value in the field at left
2. *Click the + (plus) sign to…*
3. …transfer that value to the field at right


Inclusions
1
r a subnet or computer to include in CIDR notation and click th
2
+
× 172.16.39.109/24
3

Configuration Wizard: Network


Provide your network details

Inclusions

Enter a subnet or computer to include in CIDR notation and click th

Exclusions

Enter a single IP address to exclude and click the PLUS icon

Inclusions

You will first enter in the network subnets intended for inclusion in the scanning process.

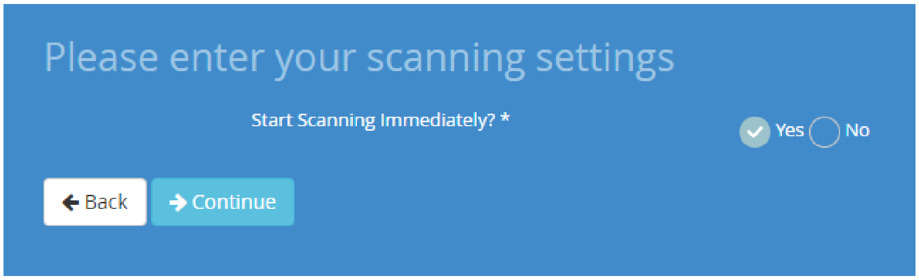
Note that the ideal is to enter the smallest possible subnets that cover all of your endpoints. So while your LAN may be using a class A network (10.x.x.x/8), unless you have millions of endpoints (!), you should consider entering some more logical subnets into the appliance's scanning ranges.

Desired Range	Proper CIDR Notation	# of Possible Hosts
192.168.1.1	192.168.1.1/32	1
192.168.1.0-255	192.168.1.0/24	256
172.16.0-255.0-255	172.16.0.0/16	65,536
10.0-255.0-255.0-255	10.0.0.0/8	16,777,216

Exclusions

Enter any individual IP addresses that you would prefer to be excluded from scans or inventories. (Examples of these may be ER systems in health care organizations or reactor systems in energy organizations)

Configuration Wizard: Scanning

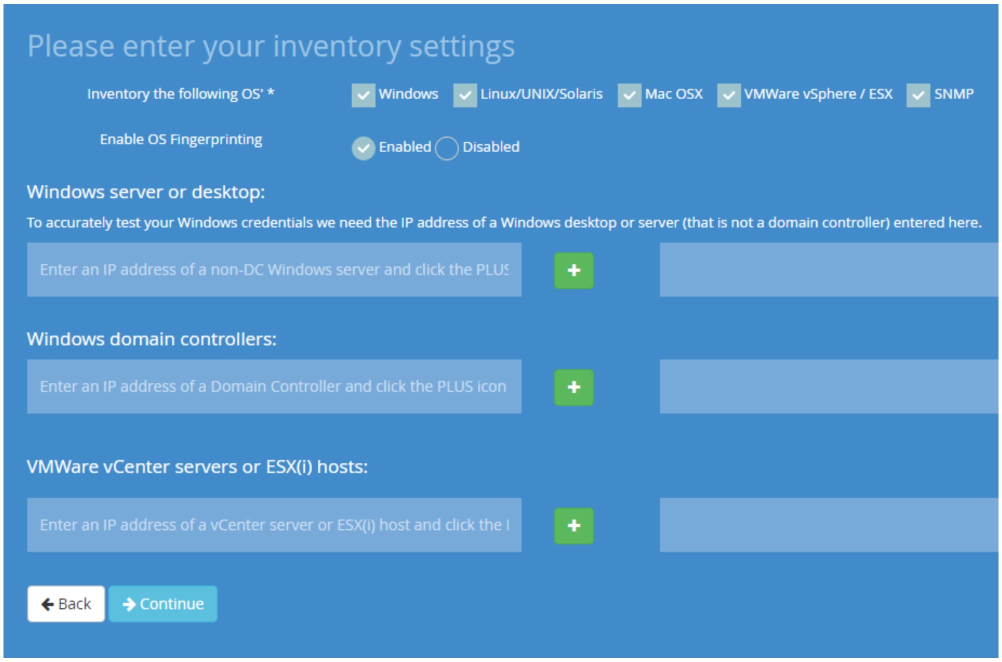


Please enter your scanning settings

Start Scanning Immediately? * ● Yes ○ No

Here you can opt to start scanning immediately (highly recommended) or postpone the scan to a later time.

Configuration Wizard: Inventory



Please enter your inventory settings

Inventory the following OS' * ☑ Windows ☑ Linux/UNIX/Solaris ☑ Mac OSX ☑ VMWare vSphere / ESX ☑ SNMP

Enable OS Fingerprinting ● Enabled ○ Disabled

Windows server or desktop:

To accurately test your Windows credentials we need the IP address of a Windows desktop or server (that is not a domain controller) entered here.

Enter an IP address of a non-DC Windows server and click the PLUS

Windows domain controllers:

Enter an IP address of a Domain Controller and click the PLUS icon

VMWare vCenter servers or ESX(i) hosts:

Enter an IP address of a vCenter server or ESX(i) host and click the I

Inventory the following OS'

You can enable or disable the inventory of Windows, Linux/UNIX/Solaris, OSX, VMware and/or SNMP devices.

Enable OS Fingerprinting

Immediately prior to inventory, we can use our OS fingerprinting technology to determine a device's type, making it easier for us to target a style of inventory.

Windows Server or Desktop

Enter a Windows server or workstation IP address here that is not a domain controller.

The purpose here is for checking local administrator privileges once we have entered some credentials in the Security tab of the wizard.

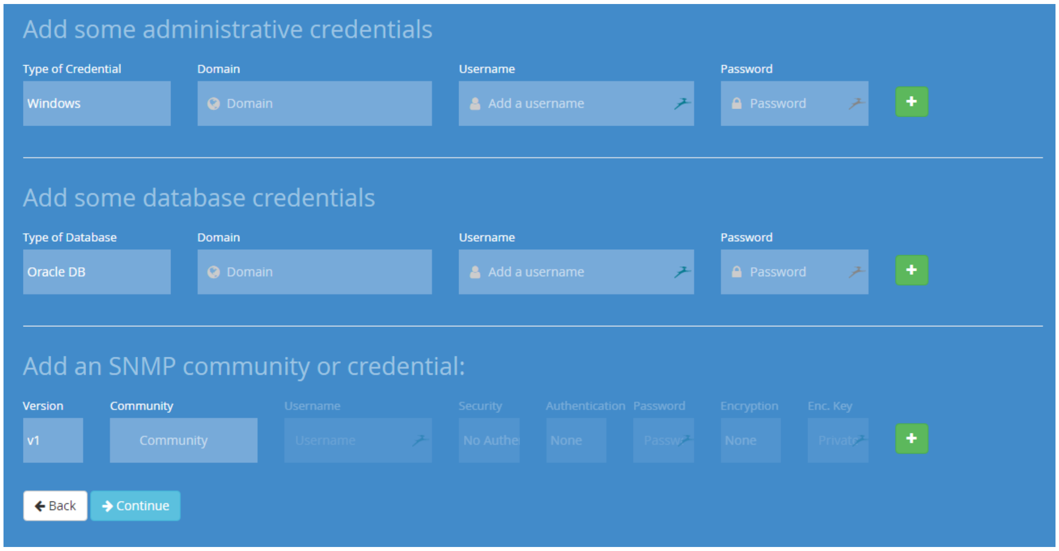
Windows Domain Controllers

Enter the IP address(es) of your domain controller(s) that are as close to the top of your Active Directory forest as possible.

VMware vCenter server or ESX(i) hosts

Enter the IP address of your vCenter server. If you do not have a vCenter server, enter the IP addresses of your virtual hosts.

Configuration Wizard: Security



Add some administrative credentials

Type of Credential: Windows

Add some database credentials

Type of Database: Oracle DB

Add an SNMP community or credential:

Version: v1

Security: No Authe

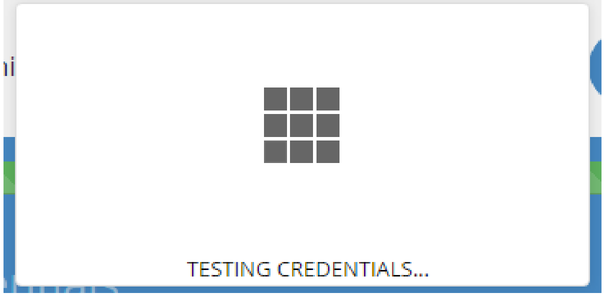
Authentication: None

Encryption: None

Here you will enter your OS administrative credentials, Oracle database credentials and/or SNMP community strings or SNMPv3 credentials.

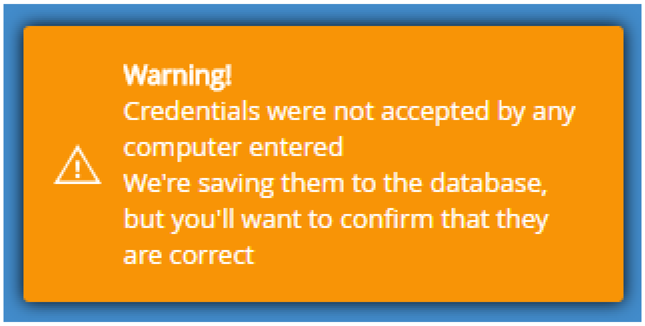
Administrative credentials:

As you enter your credential sets, and click the + sign, in the case of Windows and VMware credentials, we will try and test those credentials against the systems entered under the Inventory tab.



TESTING CREDENTIALS...

In the case where we are unable to authenticate the credentials against those systems, you will receive the following notice:



Warning!
Credentials were not accepted by any computer entered
We're saving them to the database, but you'll want to confirm that they are correct

As noted, we would recommend that you ensure the credentials were entered correctly, or that the systems entered in the Inventory tab would be able to authenticate them properly.

Database Credentials:

Primarily designed to take in Oracle Database credentials.

SNMP Credentials:

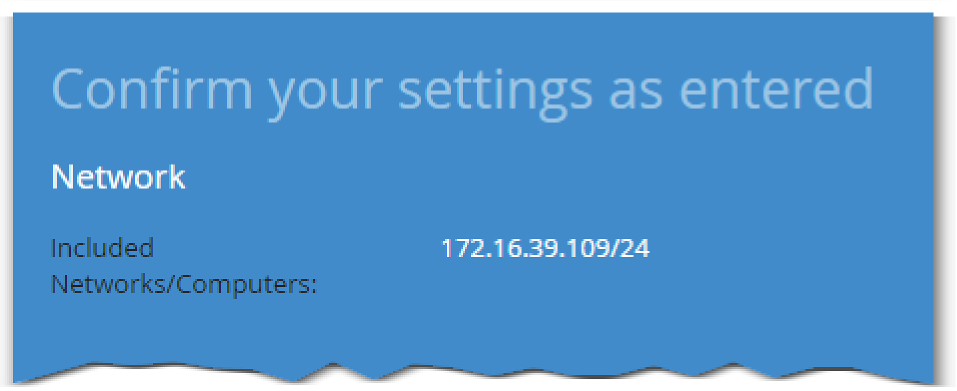
For v1 or v2c SNMP credentials, enter your community string.

For v3 SNMP credentials, you will need to enter:

- Username
- Password
- Context
- Security level
- Authentication and encryption protocols
- Encryption key

Configuration Wizard: Confirmation

You're all set! Check that the desired settings have been entered and click the Submit button.



Confirm your settings as entered

Network

Included Networks/Computers: 172.16.39.109/24

From here you will be taken to the Status screen which will display how your scanning and inventory processes are proceeding.

That’s Just About It!

There should be nothing to do at this point but sit back and let the tool do its work. Within 10-15 minutes, you should begin to see devices showing up in the ‘Discovery Status’ report.

Should you have any questions, concerns or require assistance of any kind, please contact info@block64.com and we will be back to you post haste!

Appendix 1.1: Granting A Domain User Local Administrative Rights

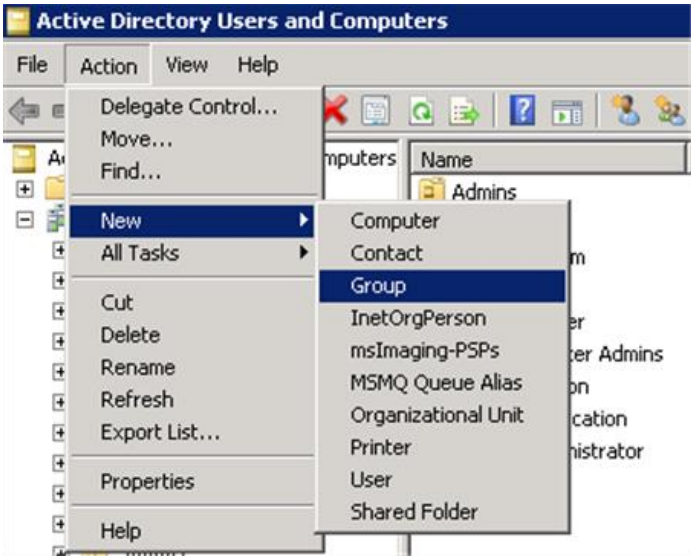
(From https://social.technet.microsoft.com/wiki/contents/articles/7833.how-to-make-a-domain-user-the-local-administrator-for-all-pcs.aspx):

Step 1 : Creating a Security Group

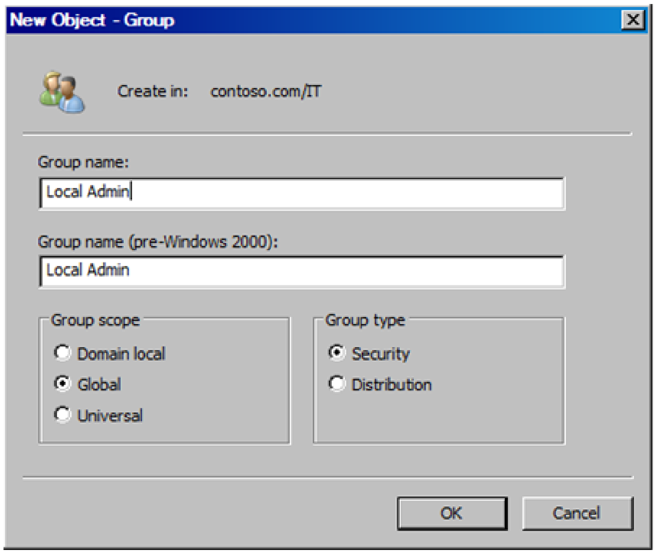
First you need to create a security group called Local Admin

Log onto a Domain Controller, open Active Directory Users and Computers (dsa.msc)

Create a security Group name it Local Admin. From the top menu, select Action | New | Group



Name the group **'Local Admin'**.



New Object - Group

Create in: contoso.com/IT

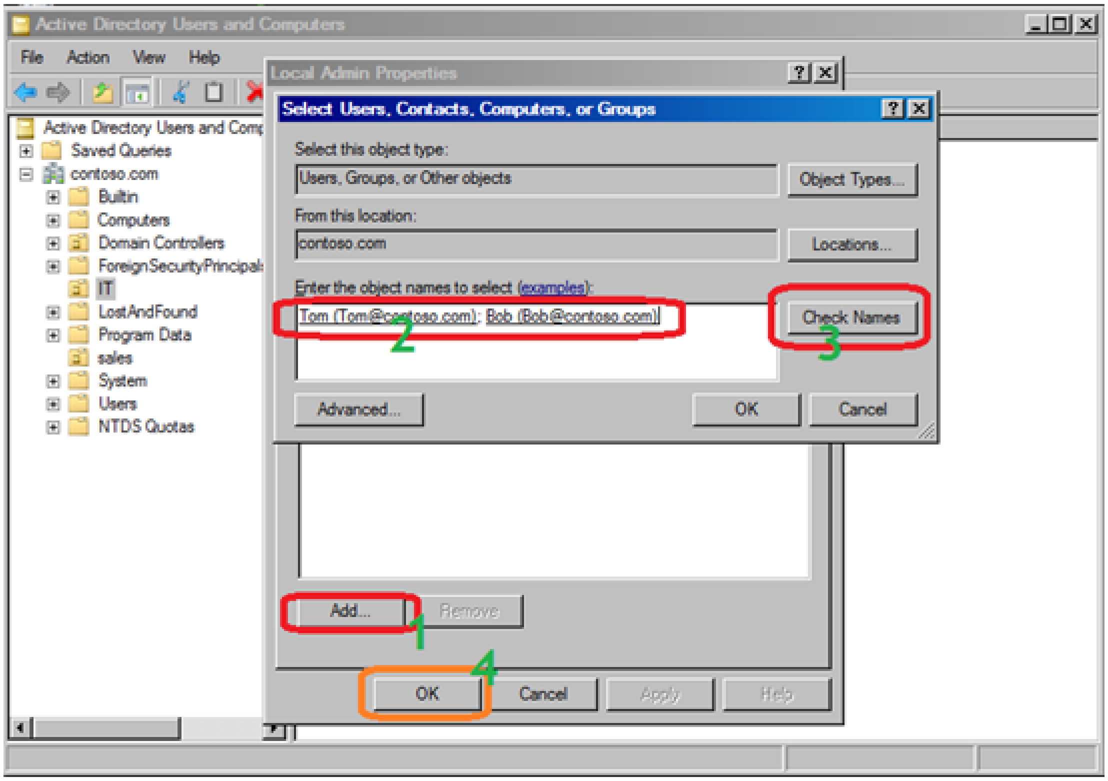
Group name:
Local Admin

Group name (pre-Windows 2000):
Local Admin

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Add the Help Desk members to Local Admin group. I will add two users say Tom and Bob.



Select Users, Contacts, Computers, or Groups

Select this object type:
Users, Groups, or Other objects

From this location:
contoso.com

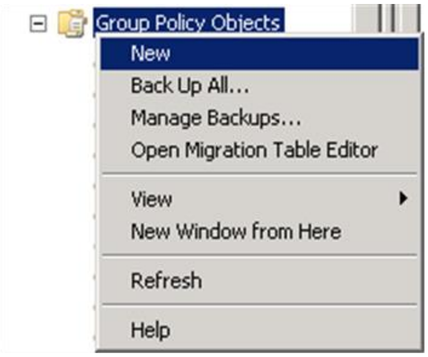
Enter the object names to select (examples):
Tom (Tom@contoso.com); Bob (Bob@contoso.com)

Step 2: Create Group Policy.

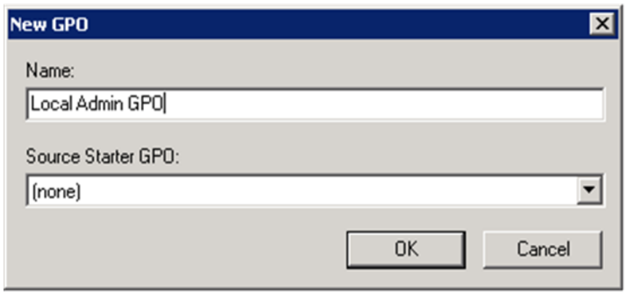
Next you need to create a group policy called “Local Admin GPO”

Open Group Policy Management Console (gpmc.msc)

Right click on Group Policy Objects and select New.



Type the name of the policy "Local Admin GPO"



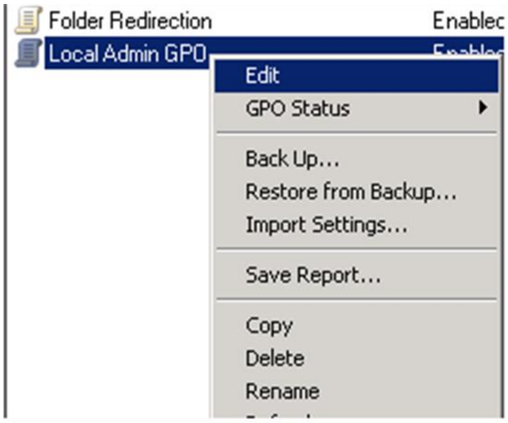
Name:
Local Admin GPO

Source Starter GPO:
(none)

Step 3: Configure the policy to add the “Local Admin” group as Administrators

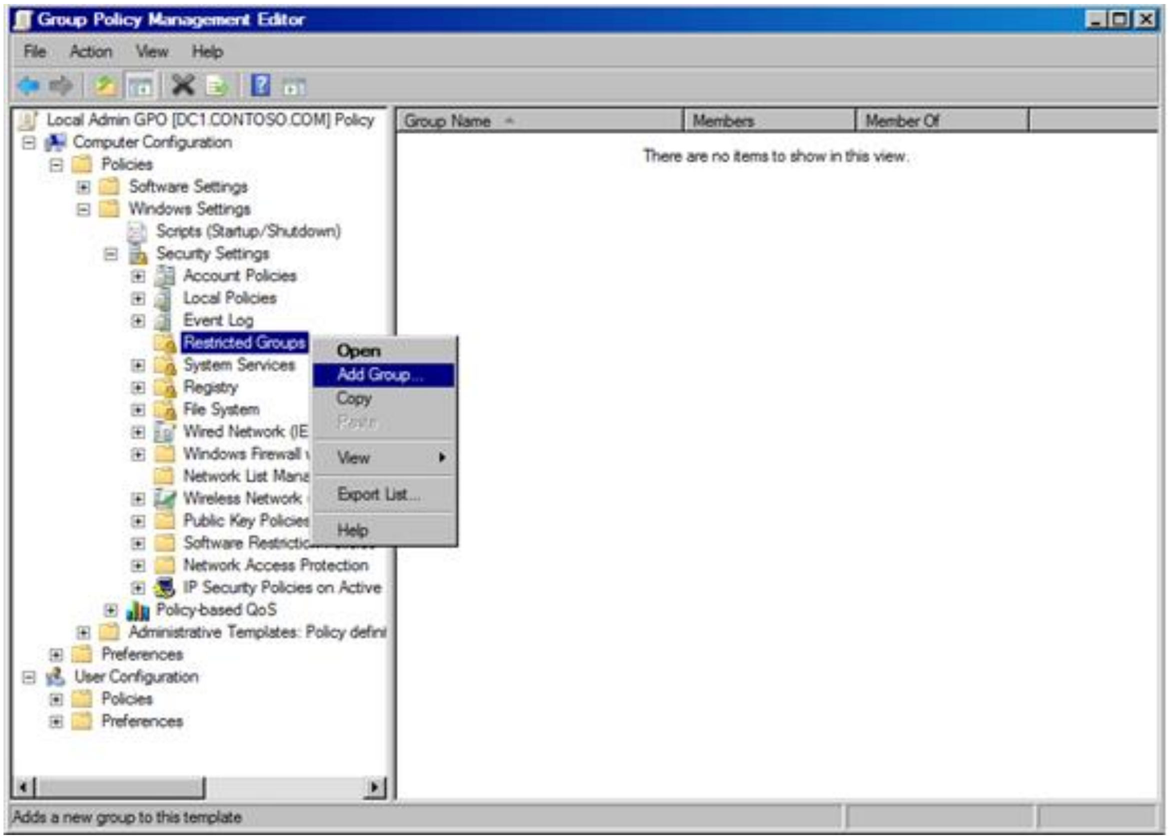
Here you will add the Local Admin group to the Local Admin GPO policy and put them in the groups you wish them to use.

Right click “Local Admin GPO” Policy then select Edit.



Expand Computer configuration\Policies\Windows Settings\Security Settings\Restricted Groups

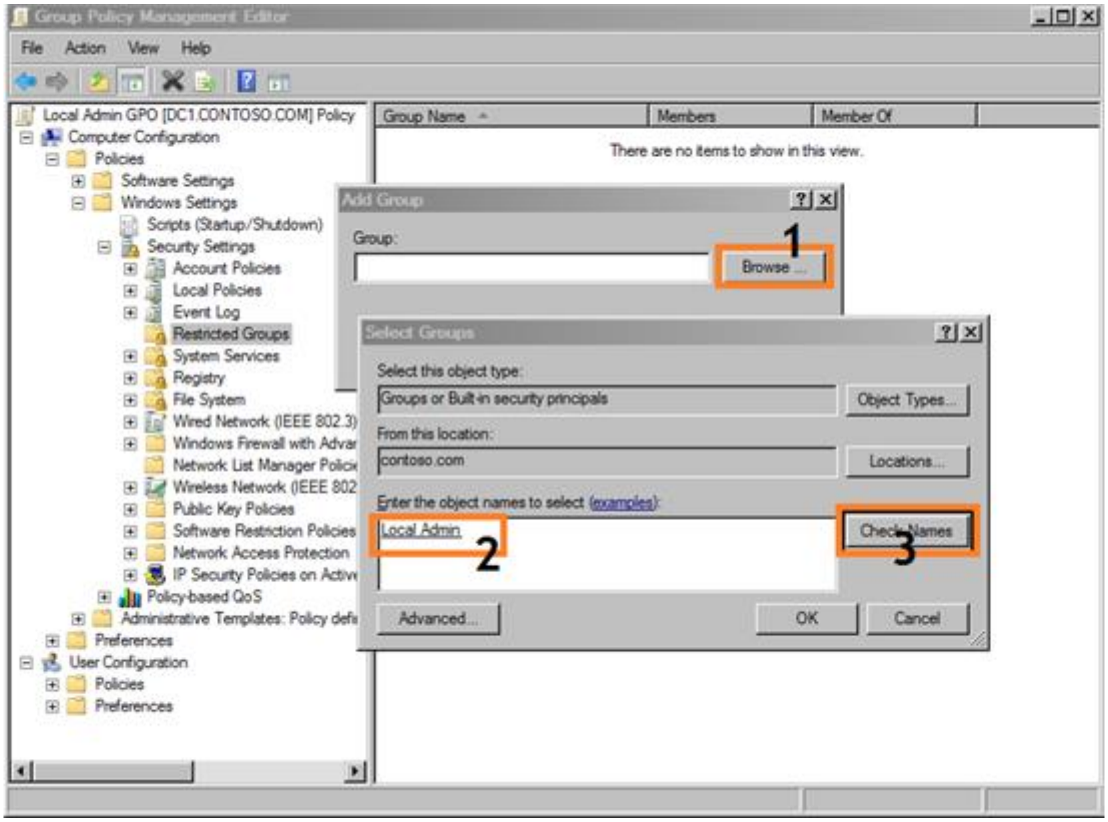
In the Left pane on Restricted Groups, Right Click and select “Add Group“



There are no items to show in this view.

Adds a new group to this template

In the Add Group dialog box, select browse and type Local Admin and then click “Check Names“

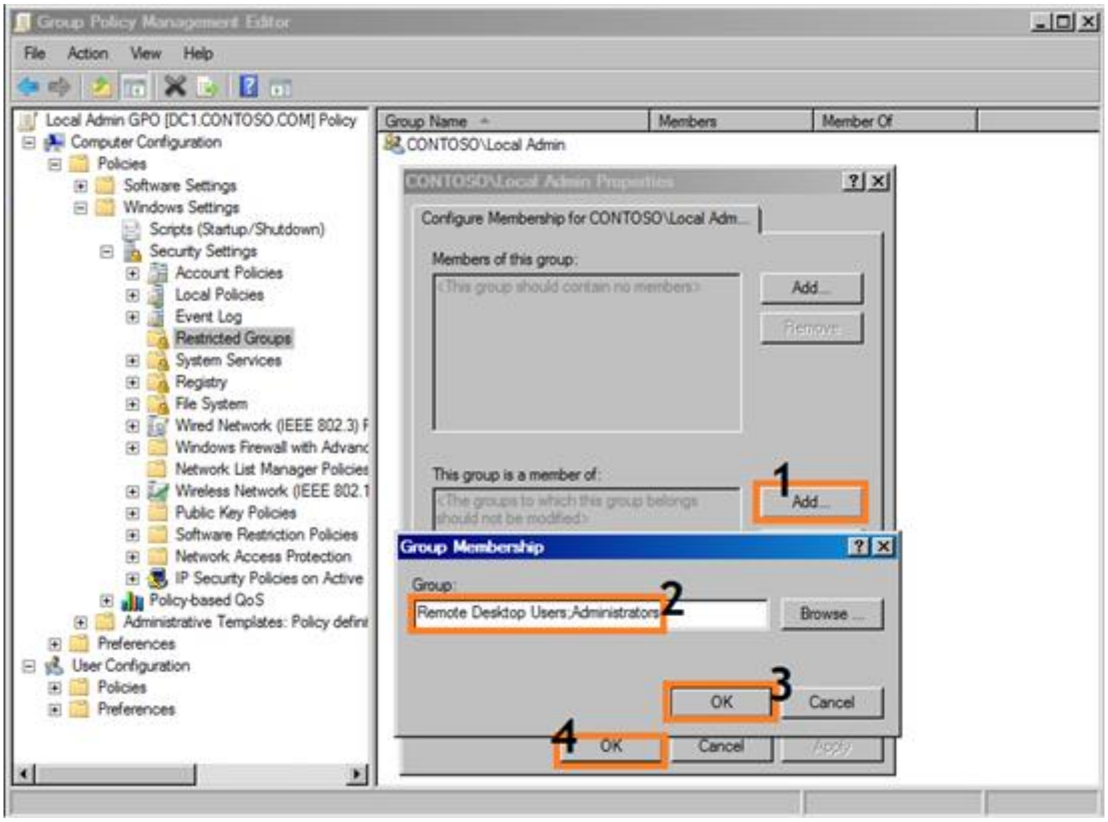


Select this object type: Groups or Built-in security principals

From this location: contoso.com

Enter the object names to select (examples): Local Admin

Click OK twice to close the dialog box.


Group Policy Management Editor
File
Action
View
Help
Local Admin GPO [DC1.CONTOSO.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) F
Windows Firewall with Advanc
Network List Manager Policies
Wireless Network (IEEE 802.1
Public Key Policies
Software Restriction Policies
Network Access Protection
IP Security Policies on Active
Policy-based QoS
Administrative Templates: Policy defini
Preferences
User Configuration
Policies
Preferences
Group Name
Members
Member Of
CONTOSO\Local Admin
CONTOSO\Local Admin Properties
Configure Membership for CONTOSO\Local Adm...
Members of this group:
<This group should contain no members>
Add...
Remove
This group is a member of:
<The groups to which this group belongs should not be modified>
1
Add...
Group Membership
Group:
2
Browse ...
3
OK
Cancel
4
OK
Cancel
Apply

Group: Remote Desktop Users;Administrators

Click Add under “This group is a member of:”

Add the “Administrators” Group.

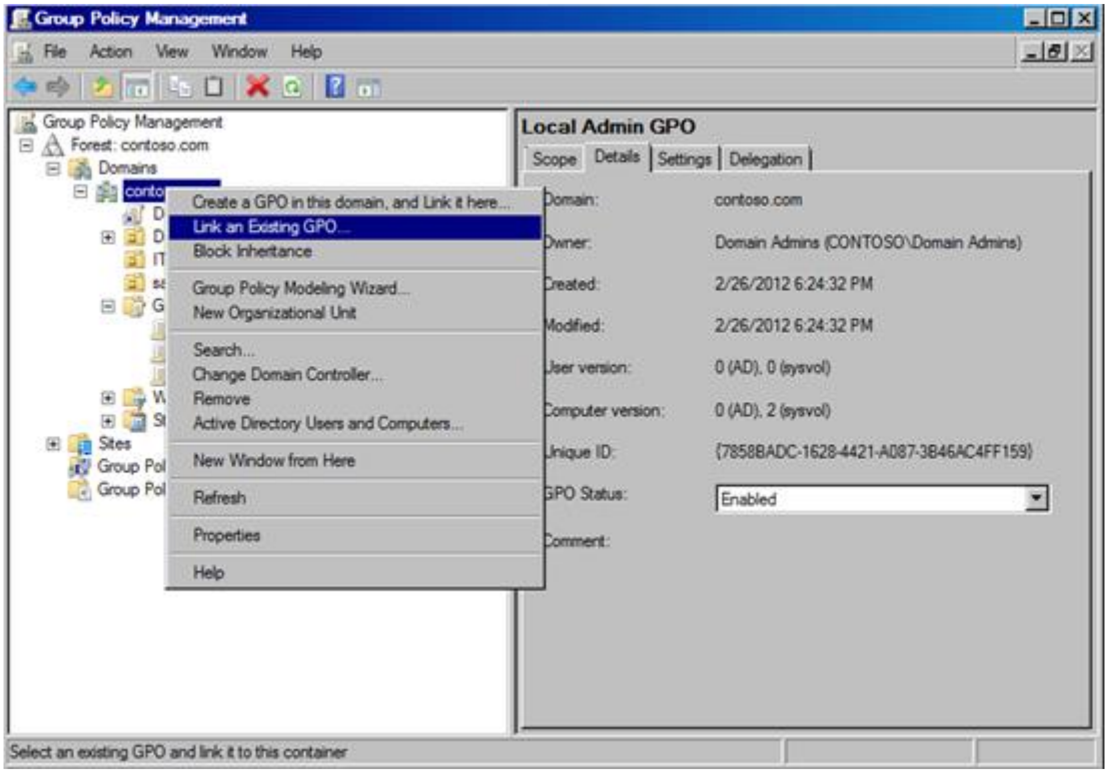
Add “Remote Desktop Users”

Click OK twice

Note: When adding groups, you can add whatever you want, the GPO will match the group on the *system, if you type “Admins” it will match a local group called Admins if it exists and put “Local Admin” in that group.*

Step 4: Linking GPO

In Group policy management console, right click on the domain or the OU and select Link an Existing GPO



Local Admin GPO

Domain: contoso.com

Owner: Domain Admins (CONTOSO\Domain Admins)

Created: 2/26/2012 6:24:32 PM

Modified: 2/26/2012 6:24:32 PM

User version: 0 (AD), 0 (sysvol)

Computer version: 0 (AD), 2 (sysvol)

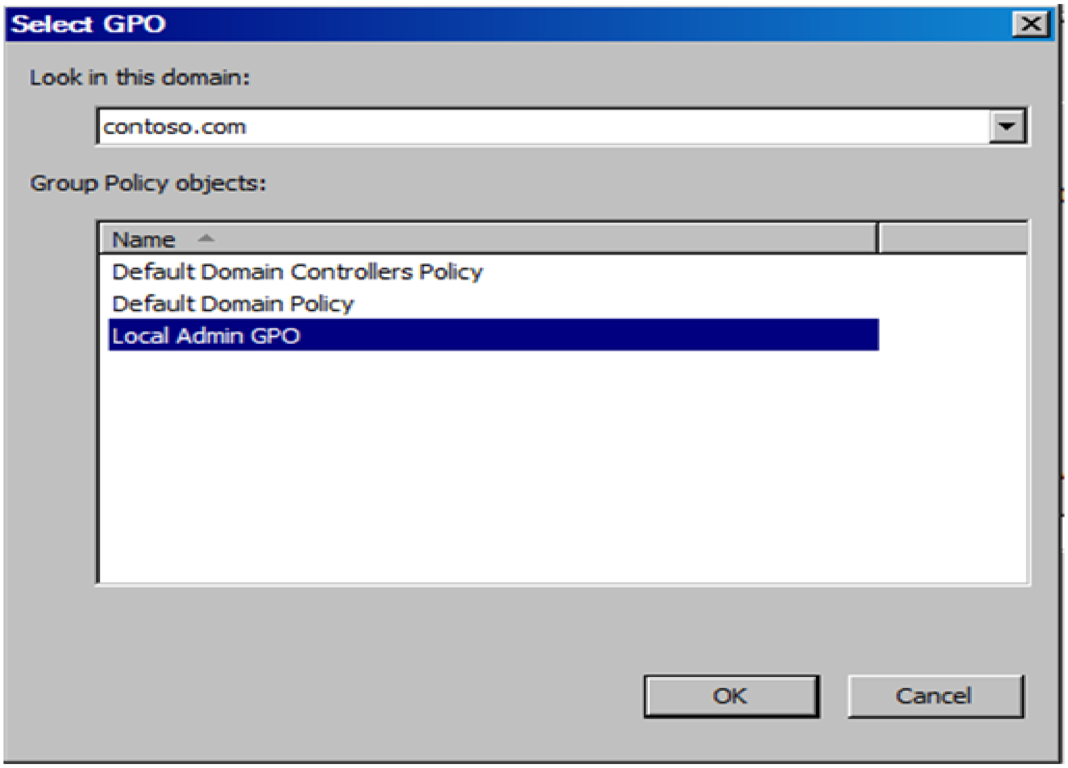
Unique ID: {7858BADC-1628-4421-A087-3B46AC4FF159}

GPO Status: Enabled

Comment:

Select an existing GPO and link it to this container

Select the Local Admin GPO



Step 5: Testing GPOs

Log on to a PC which is join to the domain and then run gpupdate /force and check the local administrators group. You should see Local Admin in that group now. Make sure all PCs you want to access should be move to an OU and properly link above GPO. Tom and Bob domain users can now access all PCs remotely as a local administrator.

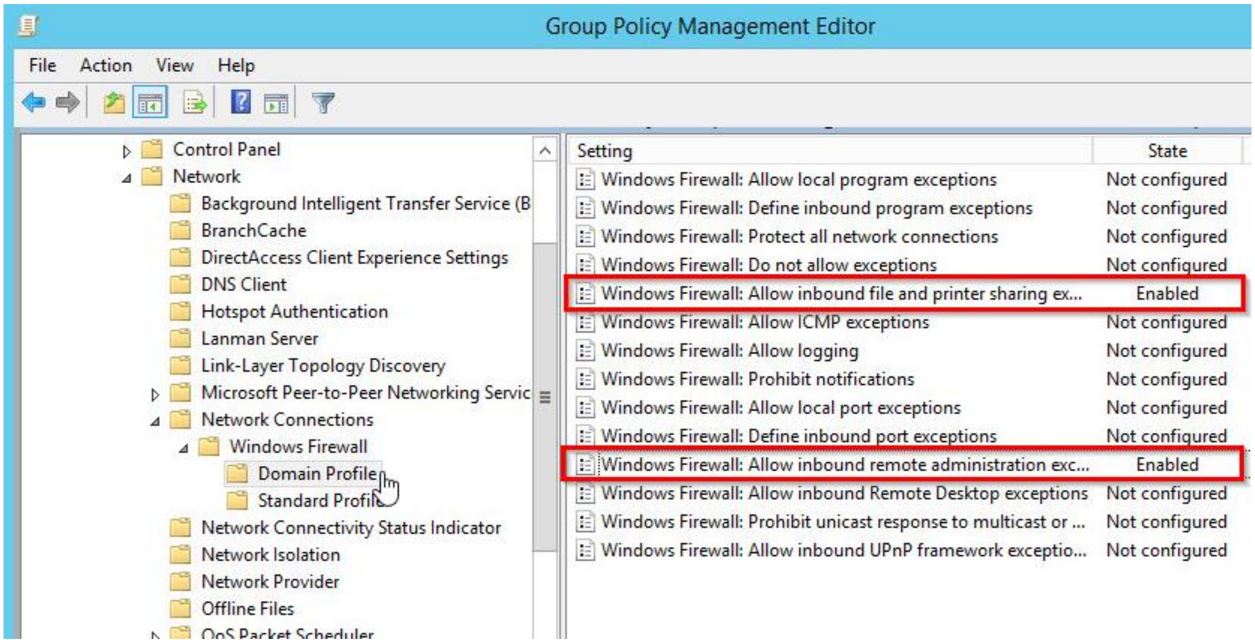
Appendix 1.2: Allowing Inventory services using Group Policy

The Windows Inventory functions of our technology require the ability to remotely access 'File and Printer Sharing' services, 'WMI' and 'Remote Administration'. This is what allows our solution to remain agentless - luckily, the steps to allow access to these services can be easily enabled through Group Policy:

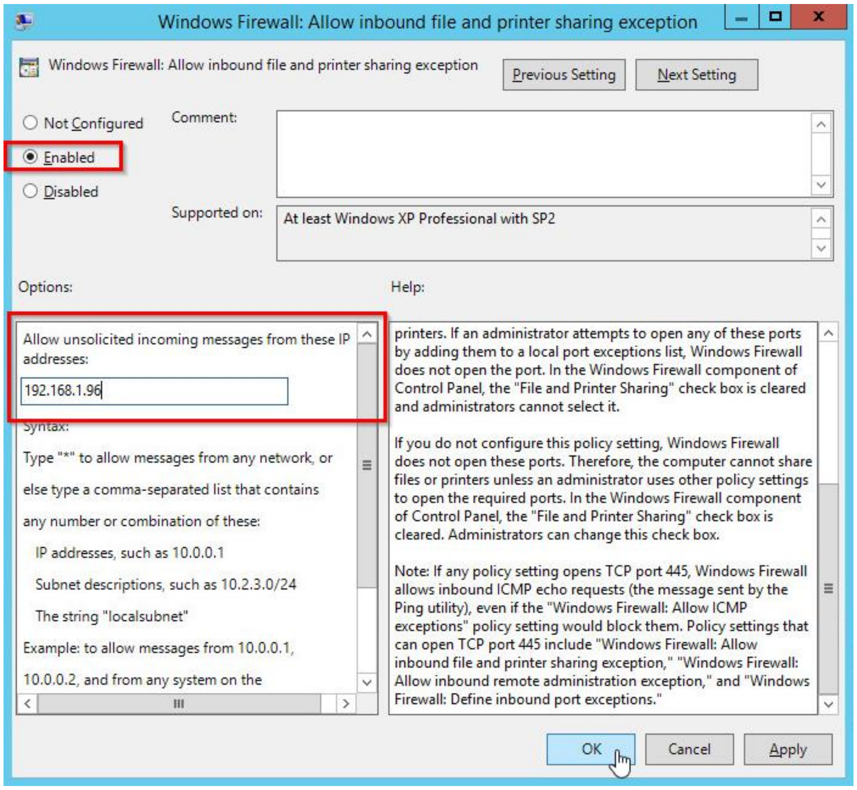
1. Using the Group Policy Management console, create a new Group Policy Object (GPO) called BlockBox (for example) and then Edit that GPO

2. In the new GPO, navigate to Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile
If you do not have this entry, and/or are working with legacy Domain Controllers (Windows 2008R2 or older), go to step 4 below.

3. You should then enable the Allow inbound file and printer sharing exception and Allow inbound remote administration exception rules for the discovery appliance's IP address.



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



Windows Firewall: Allow inbound file and printer sharing exception

Windows Firewall: Allow inbound file and printer sharing exception

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows XP Professional with SP2

Options:

Allow unsolicited incoming messages from these IP addresses:

192.168.1.96

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:

printers. If an administrator attempts to open any of these ports by adding them to a local port exceptions list, Windows Firewall does not open the port. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is cleared and administrators cannot select it.

If you do not configure this policy setting, Windows Firewall does not open these ports. Therefore, the computer cannot share files or printers unless an administrator uses other policy settings to open the required ports. In the Windows Firewall component of Control Panel, the "File and Printer Sharing" check box is cleared. Administrators can change this check box.

Note: If any policy setting opens TCP port 445, Windows Firewall allows inbound ICMP echo requests (the message sent by the Ping utility), even if the "Windows Firewall: Allow ICMP exceptions" policy setting would block them. Policy settings that can open TCP port 445 include "Windows Firewall: Allow inbound file and printer sharing exception," "Windows Firewall: Allow inbound remote administration exception," and "Windows Firewall: Define inbound port exceptions."

That’s it! The following steps are only for Windows 2008R2 or older.

4. Navigate to Computer Configuration > Policies > Security Settings > Windows Firewall with Advanced Security > Inbound Rules

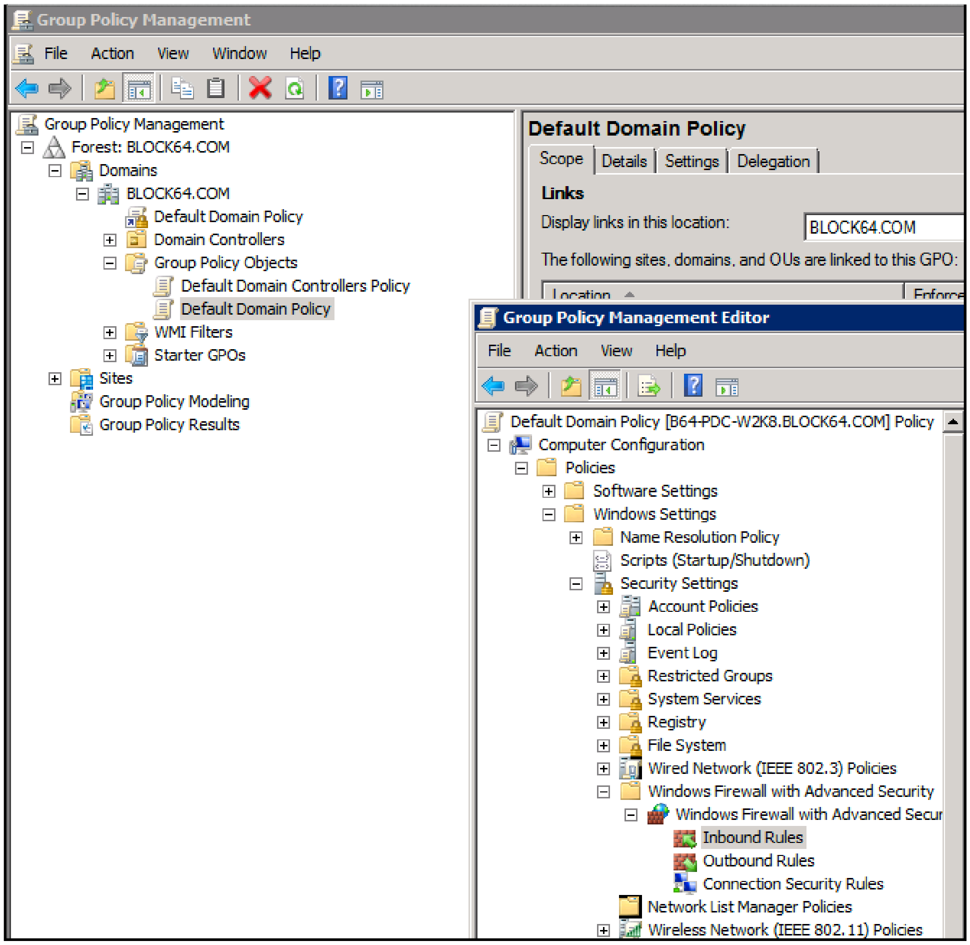
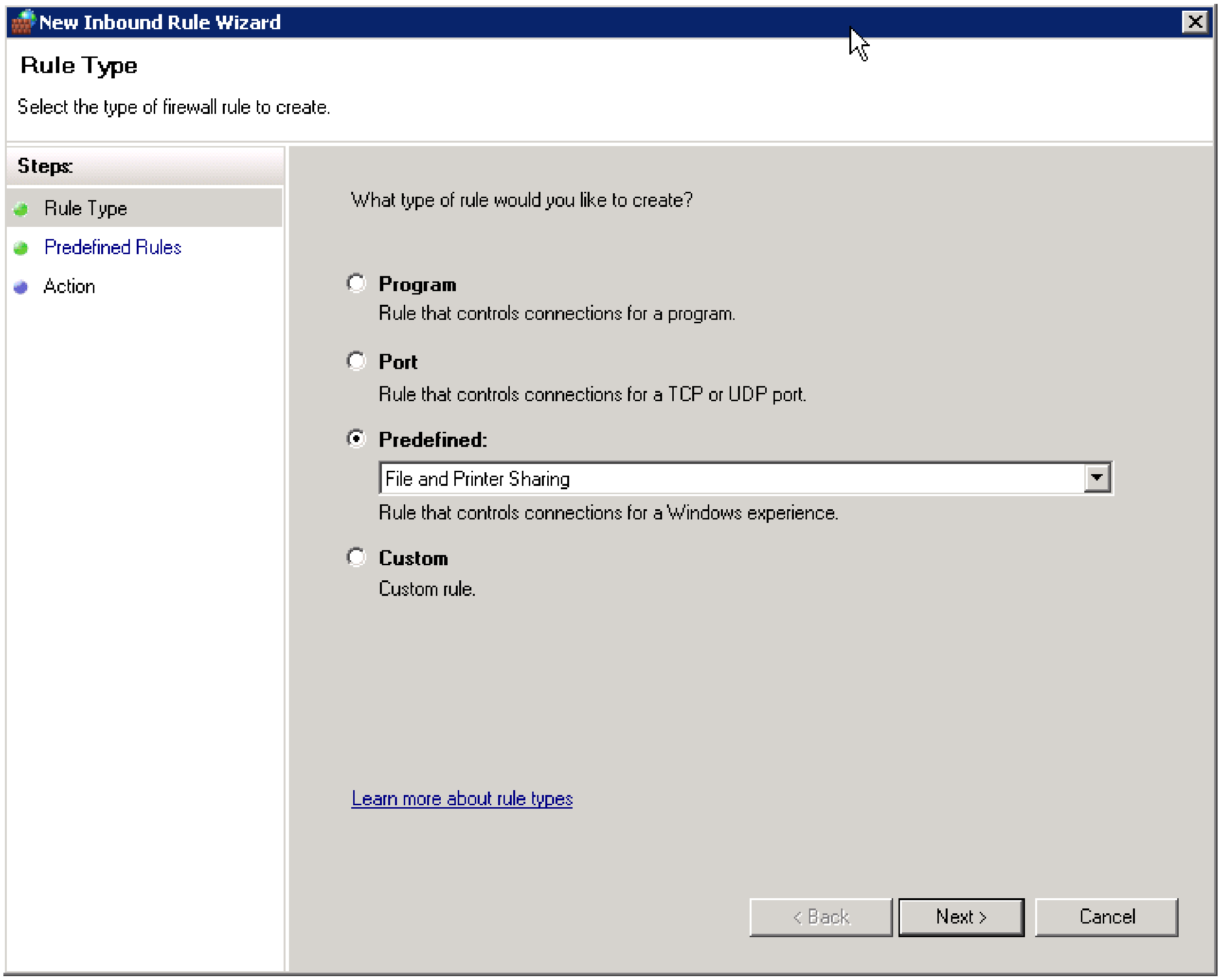


Fig 1.1: Location of Domain GPO for Inbound Firewall Rules

5. You can add the following predefined rules here:
    - File and Printer Sharing
    - Remote Administrator
    - WMI (Windows Management Instrumentation)

   If you do not have those predefined rules, your Active Directory functional level may be Windows 2003 or older. If so, we would strongly recommend elevating your AD functional level to at least Windows 2008 or above (https://support.microsoft.com/en-us/help/322692/how-to-raise-active-directory-domain-and-forest-functional-levels)… but if that is not a possibility, let us know and we'll work with you to enable the individual firewall rules.



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:**
File and Printer Sharing
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Learn more about rule types

Fig 1.2: Rule Settings for “File and Printer Sharing” Inbound Firewall Rule

Appendix 1.3: Allowing Remote Registry Access via Group Policy

Supplementary Reading: Microsoft KB314837 - *“How to Manage Remote Access to the Registry”* (http://support.microsoft.com/kb/314837)

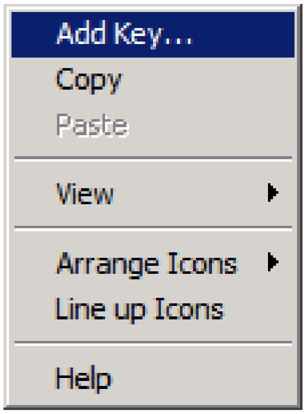
In some environments, or in cases where a special set of credentials has been prepared for the BlockBox by the Windows Domain Administrator at your site, we may encounter difficulties connecting to the Windows Registry remotely. This method of connecting to the registry is really only used as a last resort. The following steps may not be necessary. If you’re not sure - ask the tech who provided you with this software. They’ll know!

In many cases, this can be fixed via Group Policy Objects (GPO) by following these instructions:

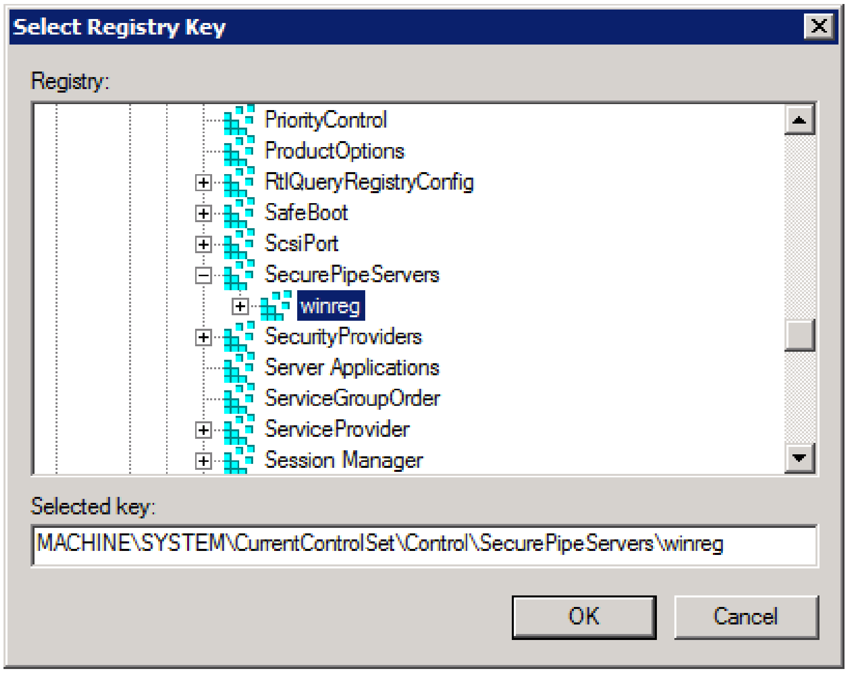
On a domain controller, Start > Administrative Tools > Group Policy Editor > Either edit an existing policy or create a new one (Remember it's a computer policy you need to link it to something with computers in it, if you link it to a users OU nothing will happen).

Navigate to Local Computer Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Registry

In the right hand pane, right click and Select ‘**Add Key’**:



You will then want to navigate to MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg, click it, and then click ok:

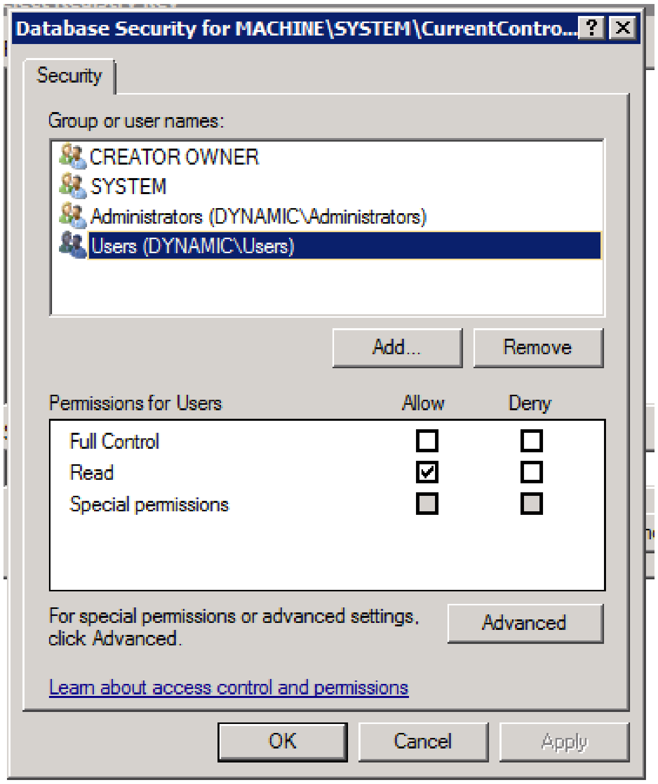


Selected key: MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

At this point, you need to add the appropriate permissions. Below are the recommended settings:

Administrator Group: Read Access

Users Group: Read Access


Database Security for MACHINE\SYSTEM\CurrentContro...

Security

Group or user names:

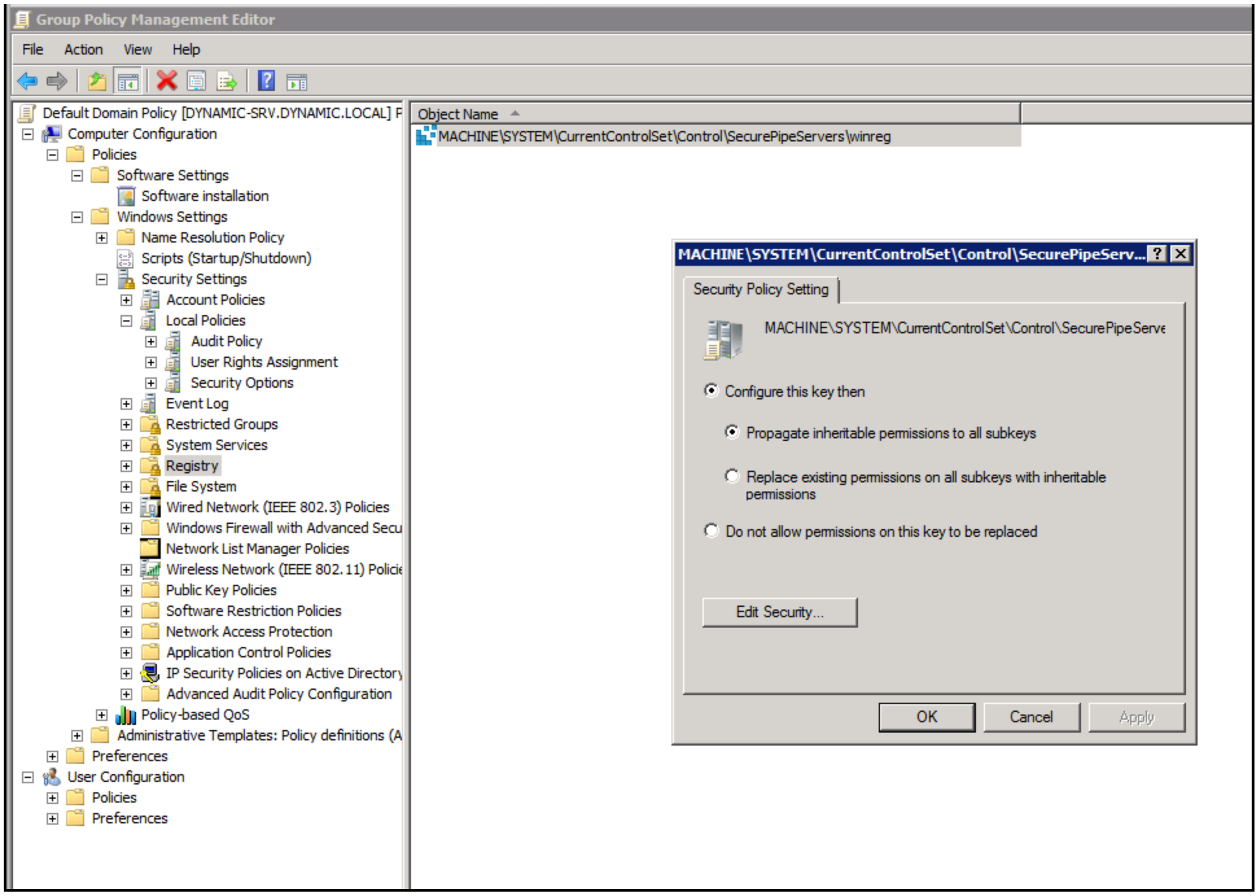
- CREATOR OWNER
- SYSTEM
- Administrators (DYNAMIC\Administrators)
- Users (DYNAMIC\Users)

Permissions for Users	Allow	Deny
Full Control	□	□
Read	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

Use the default setting of ‘Configure the key then > Propogate inheritable permissions to all subkeys’, and click ‘**OK’**.


Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [DYNAMIC-SRV.DYNAMIC.LOCAL] F
Computer Configuration
Policies
Software Settings
Software installation
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Policie
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (A
Preferences
User Configuration
Policies
Preferences
Object Name
MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServ...
Security Policy Setting
Edit Security...
OK
Cancel
Apply

MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServe

● Configure this key then

● Propagate inheritable permissions to all subkeys

○ Replace existing permissions on all subkeys with inheritable permissions

○ Do not allow permissions on this key to be replaced

After their next reboot, each client should have the appropriate permissions set.

Appendix 1.4: Enabling Necessary Services using Group Policy

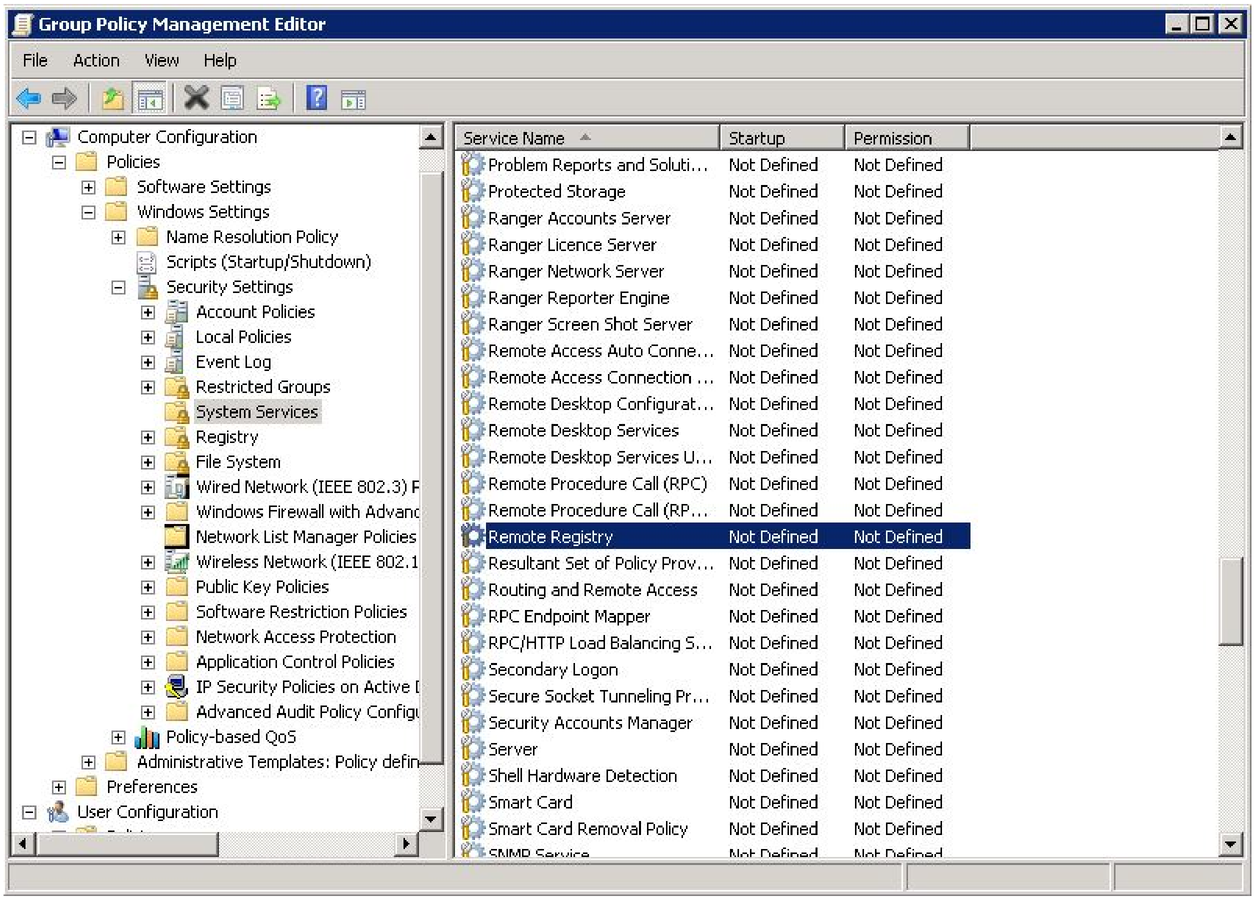
Please note these steps are likely unnecessary if the furnished credentials have both Local & Domain Administrative privileges.

The remote inventory features of the BlockBox allow the inventory of Windows-based machines without the installation of any agent. However, they *do* require the enablement of some services that allow remote inventory on the endpoints in question. The good news is that the Group Policy Editor will allow your administrator to enable these services programmatically across your endpoints. The services we would like to enable are as follows:

- Remote Procedure Call (RPC)
- Remote Registry
- Windows Management Instrumentation

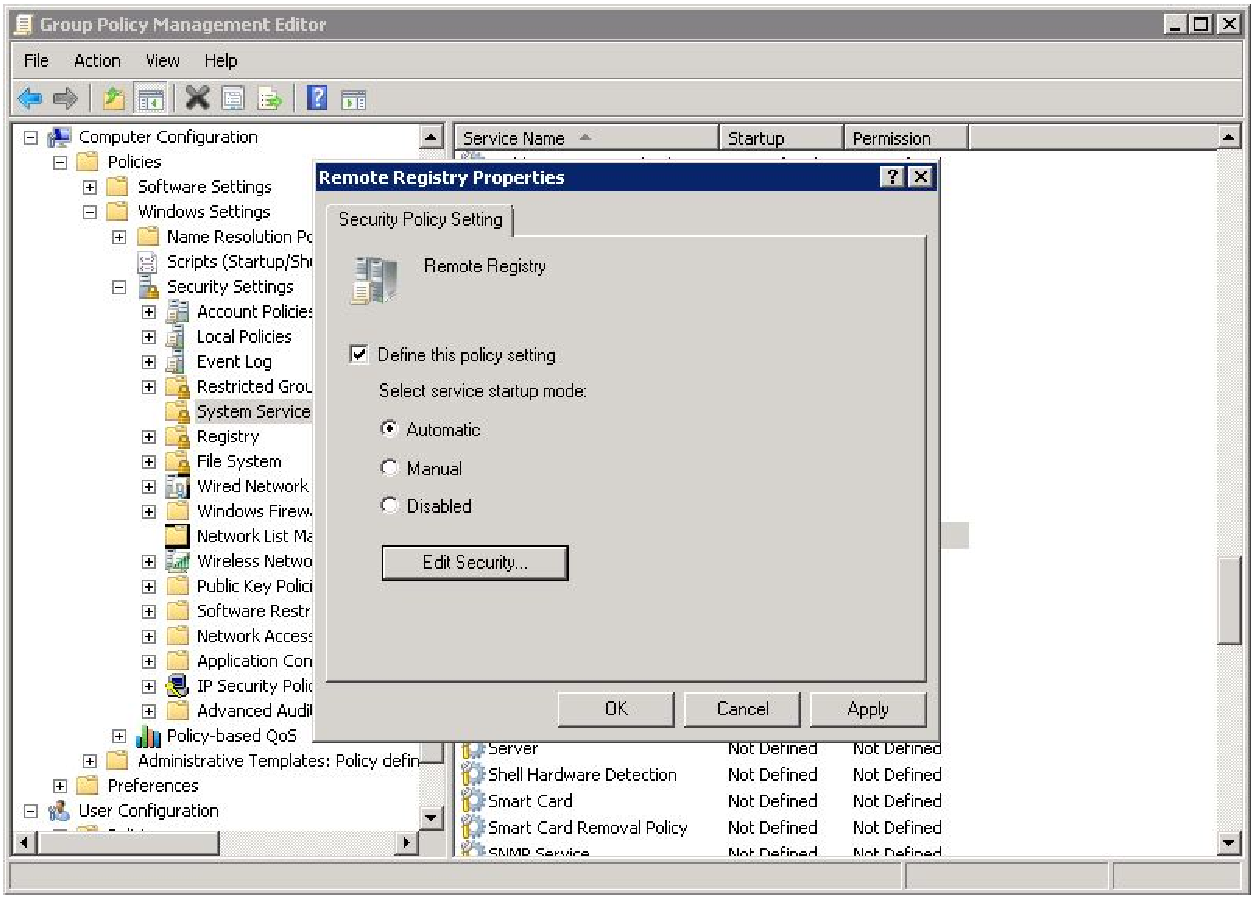
To enable each of these services, it’s just a matter of a couple of clicks -

1. On a domain controller, Start > Administrative Tools > Group Policy Editor > Either edit an existing policy or create a new one (Remember it's a computer policy you need to link it to something with computers in it, if you link it to a users OU nothing will happen).
2. Navigate to, Local Computer Policy > Computer Configuration > Policies > Windows Settings > Security Settings > System Services.
3. In the right hand pane locate "Remote Registry".


Group Policy Management Editor
File
Action
View
Help
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
File System
Wired Network (IEEE 802.3) P
Windows Firewall with Advanc
Network List Manager Policies
Wireless Network (IEEE 802.1
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Configu
Policy-based QoS
Administrative Templates: Policy defin
Preferences
User Configuration

Service Name	Startup	Permission
Problem Reports and Soluti...	Not Defined	Not Defined
Protected Storage	Not Defined	Not Defined
Ranger Accounts Server	Not Defined	Not Defined
Ranger Licence Server	Not Defined	Not Defined
Ranger Network Server	Not Defined	Not Defined
Ranger Reporter Engine	Not Defined	Not Defined
Ranger Screen Shot Server	Not Defined	Not Defined
Remote Access Auto Conne...	Not Defined	Not Defined
Remote Access Connection ...	Not Defined	Not Defined
Remote Desktop Configurat...	Not Defined	Not Defined
Remote Desktop Services	Not Defined	Not Defined
Remote Desktop Services U...	Not Defined	Not Defined
Remote Procedure Call (RPC)	Not Defined	Not Defined
Remote Procedure Call (RP...	Not Defined	Not Defined
Remote Registry	Not Defined	Not Defined
Resultant Set of Policy Prov...	Not Defined	Not Defined
Routing and Remote Access	Not Defined	Not Defined
RPC Endpoint Mapper	Not Defined	Not Defined
RPC/HTTP Load Balancing S...	Not Defined	Not Defined
Secondary Logon	Not Defined	Not Defined
Secure Socket Tunneling Pr...	Not Defined	Not Defined
Security Accounts Manager	Not Defined	Not Defined
Server	Not Defined	Not Defined
Shell Hardware Detection	Not Defined	Not Defined
Smart Card	Not Defined	Not Defined
Smart Card Removal Policy	Not Defined	Not Defined
SNMP Service	Not Defined	Not Defined

Define the policy, and set the startup type to automatic.



Remote Registry Properties

Security Policy Setting

Remote Registry

☑ Define this policy setting

Select service startup mode:

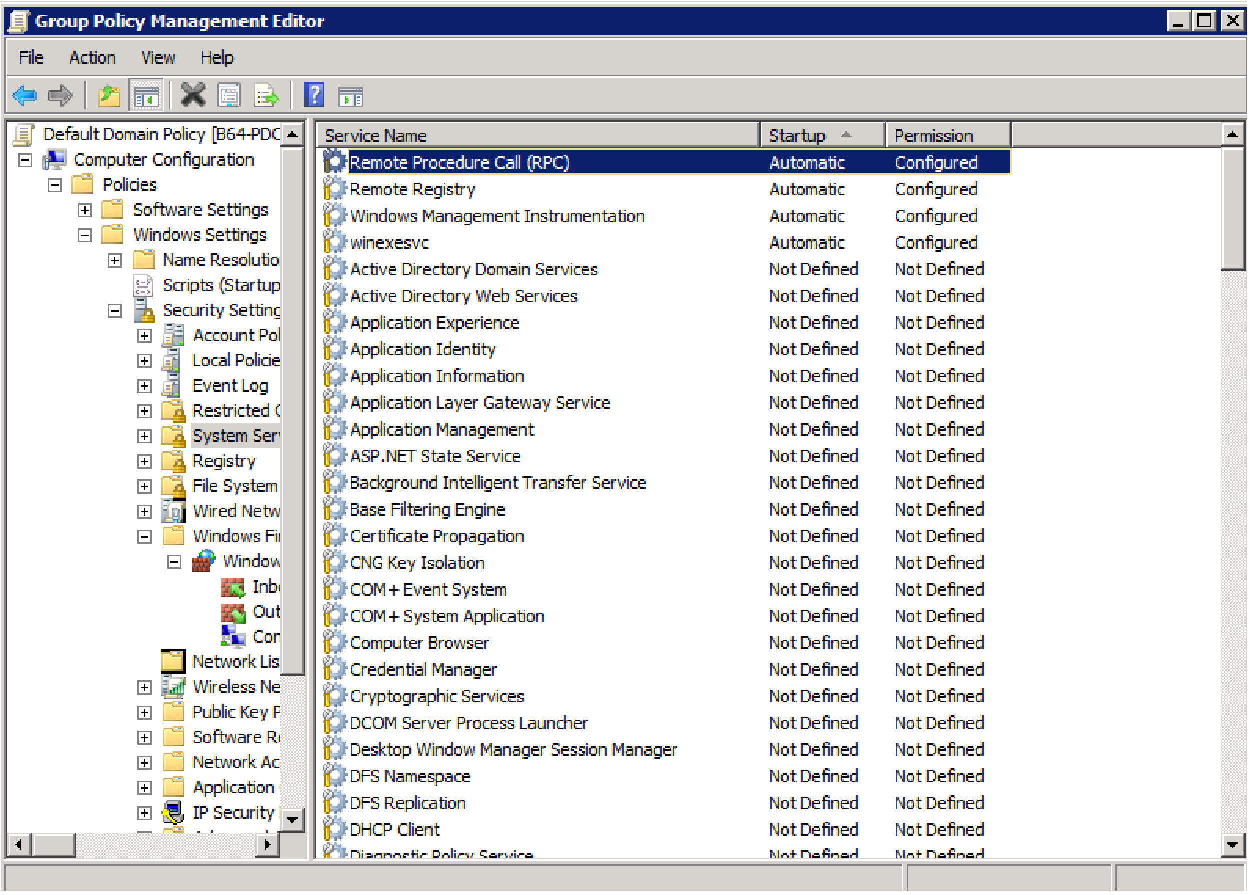
● Automatic

○ Manual

○ Disabled

Service Name	Startup	Permission
Server	Not Defined	Not Defined
Shell Hardware Detection	Not Defined	Not Defined
Smart Card	Not Defined	Not Defined
Smart Card Removal Policy	Not Defined	Not Defined
SNMP Service	Not Defined	Not Defined

Repeat Step 3 for the Remote Procedure Call (RPC) and Windows Management Instrumentation services. These services would typically be started anyhow, but this step ensures they haven't been stopped, which might interfere with the Windows inventory. When done, your list of services should look something like this:



Default Domain Policy [B64-PDC
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolutio
      - Scripts (Startup
      - Security Setting
        - Account Pol
        - Local Policie
        - Event Log
        - Restricted (
        - System Ser
        - Registry
        - File System
        - Wired Netw
        - Windows Fi
          - Window
            - Inb
            - Out
            - Cor
        - Network Lis
        - Wireless Ne
        - Public Key F
        - Software R
        - Network Ac
        - Application
        - IP Security

Service Name	Startup	Permission
Remote Procedure Call (RPC)	Automatic	Configured
Remote Registry	Automatic	Configured
Windows Management Instrumentation	Automatic	Configured
winexesvc	Automatic	Configured
Active Directory Domain Services	Not Defined	Not Defined
Active Directory Web Services	Not Defined	Not Defined
Application Experience	Not Defined	Not Defined
Application Identity	Not Defined	Not Defined
Application Information	Not Defined	Not Defined
Application Layer Gateway Service	Not Defined	Not Defined
Application Management	Not Defined	Not Defined
ASP.NET State Service	Not Defined	Not Defined
Background Intelligent Transfer Service	Not Defined	Not Defined
Base Filtering Engine	Not Defined	Not Defined
Certificate Propagation	Not Defined	Not Defined
CNG Key Isolation	Not Defined	Not Defined
COM+ Event System	Not Defined	Not Defined
COM+ System Application	Not Defined	Not Defined
Computer Browser	Not Defined	Not Defined
Credential Manager	Not Defined	Not Defined
Cryptographic Services	Not Defined	Not Defined
DCOM Server Process Launcher	Not Defined	Not Defined
Desktop Window Manager Session Manager	Not Defined	Not Defined
DFS Namespace	Not Defined	Not Defined
DFS Replication	Not Defined	Not Defined
DHCP Client	Not Defined	Not Defined
Diagnostic Policy Service	Not Defined	Not Defined

After their next reboot, all your clients will have the service running.