Outpost24

Vulnerability Management made easy

Authenticated Scanning Using SMB

Configuration Guide

Version: 1.3

2018-07-27

Table of Contents

1 AUTHENTICATED SCANNING 4

1.1 WINDOWS 7 4
1.2 WINDOWS 8.1 9
1.3 WINDOWS 10 13
1.4 WINDOWS 2008 R2 SERVER 16
1.5 WINDOWS 2012 R2 SERVER 22
1.6 WINDOWS 2016 SERVER 27
1.7 CORE INSTALLATION 32

2 AUTHENTICATED SCANNING USING OUTSCAN/HIAB 35

2.1 PER TARGET 35
2.2 PER TARGET GROUP 37
2.3 PER SCAN POLICY 38

About This Guide

The main purpose of this document is to provide users a comprehensive overview of Windows configuration required to succeed with authenticated scans using OUTSCAN or HIAB. This document has been elaborated under the assumption the reader has access to the OUTSCAN/HIAB account and Portal Interface.

For support information, visit https://www.outpost24.com/support.

1 Authenticated Scanning

This guide will provide you with the technical procedure to succeed with authenticated scanning for Windows targets when using OUTSCAN or HIAB.
This document covers procedure for:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows 2016 Server

Note: *When performing authenticated scanning against windows hosts, the scanner creates and starts a service called O24 Auth on the target machine.*

This service is used to execute commands on the target and send the results back to the scanner.

Do not remove the service during scanning, it will stop and remove itself after it is done.

1.1 Windows 7

To succeed with authenticated scanning using SMB for Windows 7 targets, follow the procedure below.

Caution

The following steps are only applicable for Windows 7 Pro or higher, ***NOT*** *Windows 7 Home.*

Step 1 - Enable Remote Registry

To enable Remote Registry (optional, can also be configured within the scanner):

1. Press the **Windows Start Button** and open **Run Prompt** by entering *Run* in the search field.
2. Type *services.msc* in the **Run Prompt** and press **OK**. This will open **Services.** Under Services (Local) find Remote Registry >> right click and select **Properties**.
   Note*: If Remote Registry is already enabled on your device, go to Step 2.*

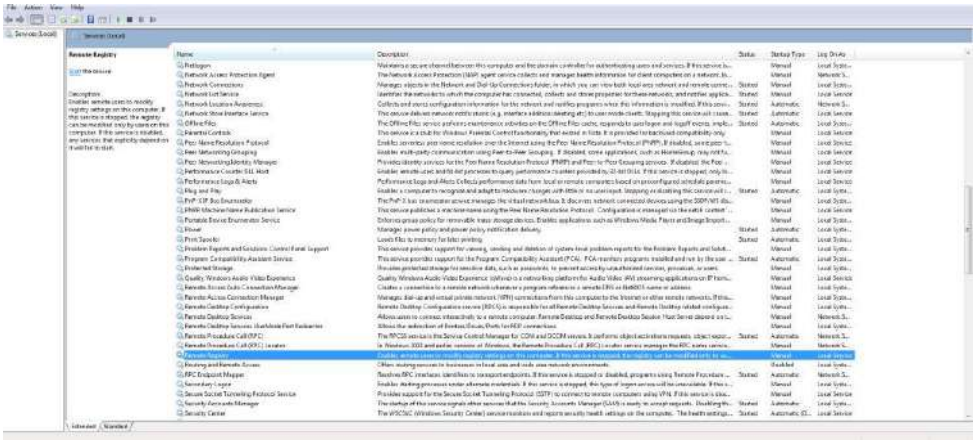


Figure 1 Services (Local) >> Remote Registry

3. In **Remote Registry Properties (Local Computer)**, change the *Startup Type* to **Automatic** and start the service.

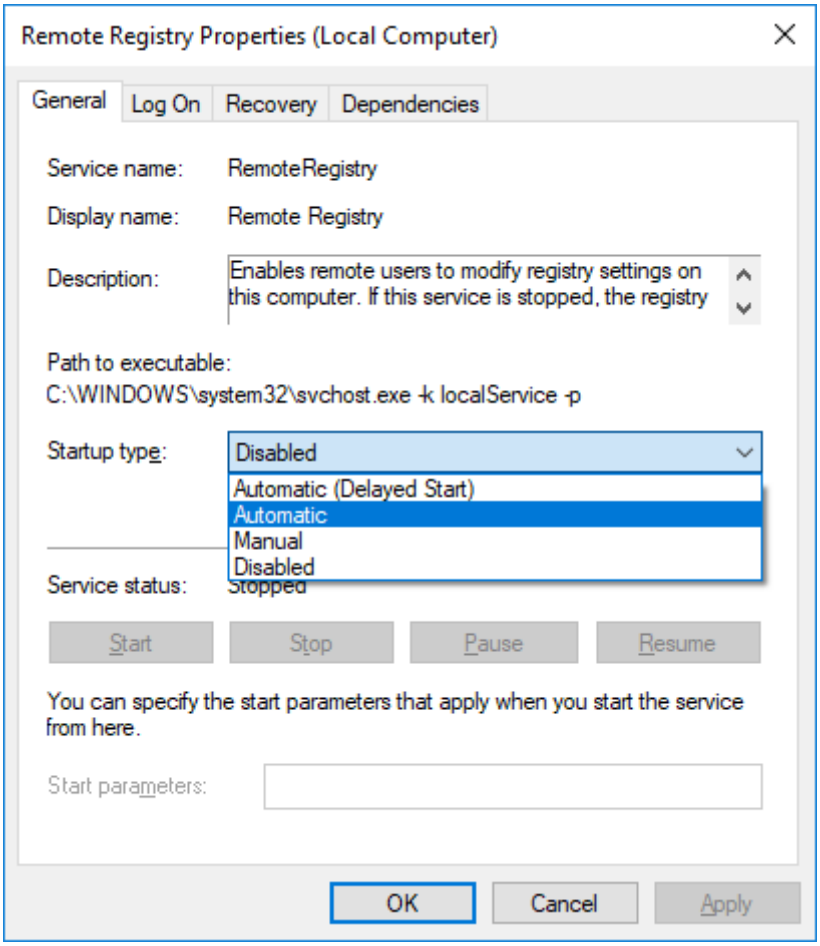


Figure 2 Remote Registry Properties

Step 2 - File and Printer Sharing

To turn on File and Printer Sharing:

1. Access **Network and Sharing Center** by pressing **Windows Start Button** and enter **Network and Sharing Center** into the search field.
2. In Network and Sharing Center, go to **Change advanced sharing settings**, located on the left-hand side.
3. In your current profile, Private/Guest or Public, check the box for **Turn on file and printer sharing** and click **Save Changes**.

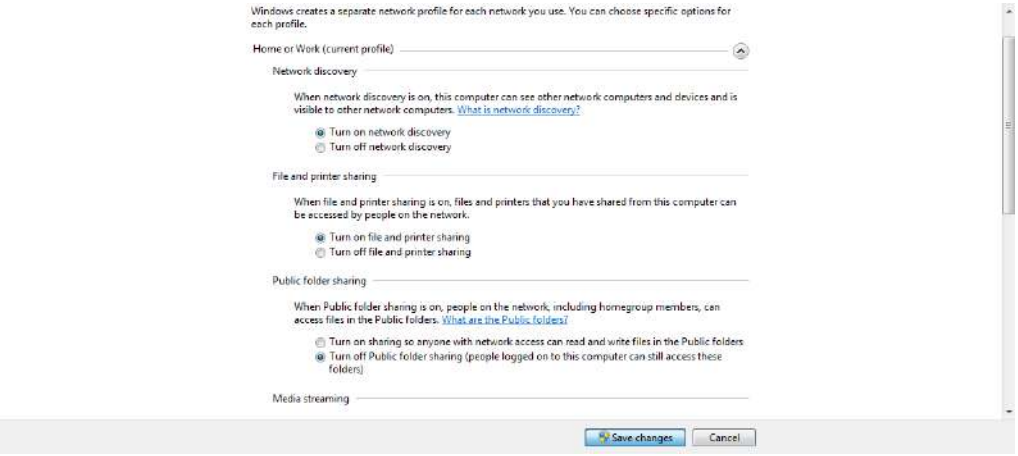


Figure 3 Network and Sharing Center >> Change Advanced Sharing Settings >> Turn on File and Printer Sharing

Step 3 - Administrator Rights

To succeed with the authentication, the account in use needs to either be a *Domain User Account* or a *local user* part of the **Administrator Group**.

Domain User Account: Make sure that the domain user account is a member of the *Administrators* group, this user will run with full administrator access on therefore User Account Control (UAC) does not need to be disabled.

Local User: Make sure that the local account is included in the Administrators Group:

1. Access **Microsoft Management Console** by pressing **Windows Start Button** and enter **mmc** into the search field.
2. Click **Local Users and Groups**, located on the left-hand side.
3. If you cannot see **Local Users and Groups**, click the **File Menu** and choose **Add/Remove Snap-in**.
4. Click **Local Users and Groups >> Add >> Local Computer >> Finish >> Ok**
5. Enter the **Groups** folder and double click the **Administrators** group.
6. If the account is not listed under **Members**, click **Add** >> Enter the name of the already created account that you wish to add >> click **Check Names** >> click **Ok** >> click **Ok**

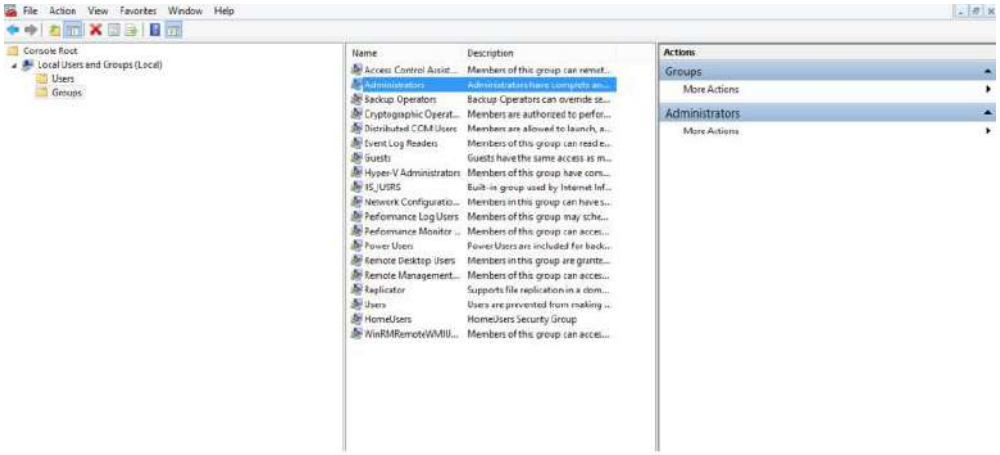
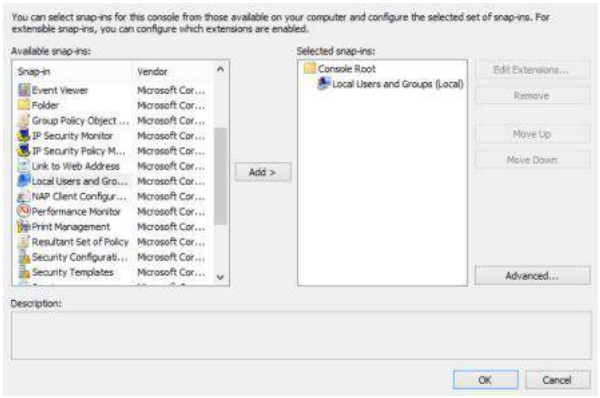


Figure 4 Microsoft Management Console



File >> Add/Remove Snap-In >> Local Users and Groups >> Groups >> Administrator >> Members

***Note**: The following step are not recommended, if possible use the domain user account.*

Make sure that the Windows User Account Control (UAC) is disabled.

1. Access the **Run Prompt** through **Windows Start Menu** by entering *Run* into the search field.
2. Type *regedit* in the **Run Prompt** and click **OK**, this will open the **Registry Editor**.
3. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system*
4. Right click the **System Folder**, choose **New >> DWORD (32-bit) Value** and name the DWORD LocalAccountTokenFilterPolicy
5. Right click the newly created DWORD and choose **Modify**, in the Edit Window set **Value Data** to 1.
6. If **User Account Control** is disabled, *EnableLUA* must be set to 0 in *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System*

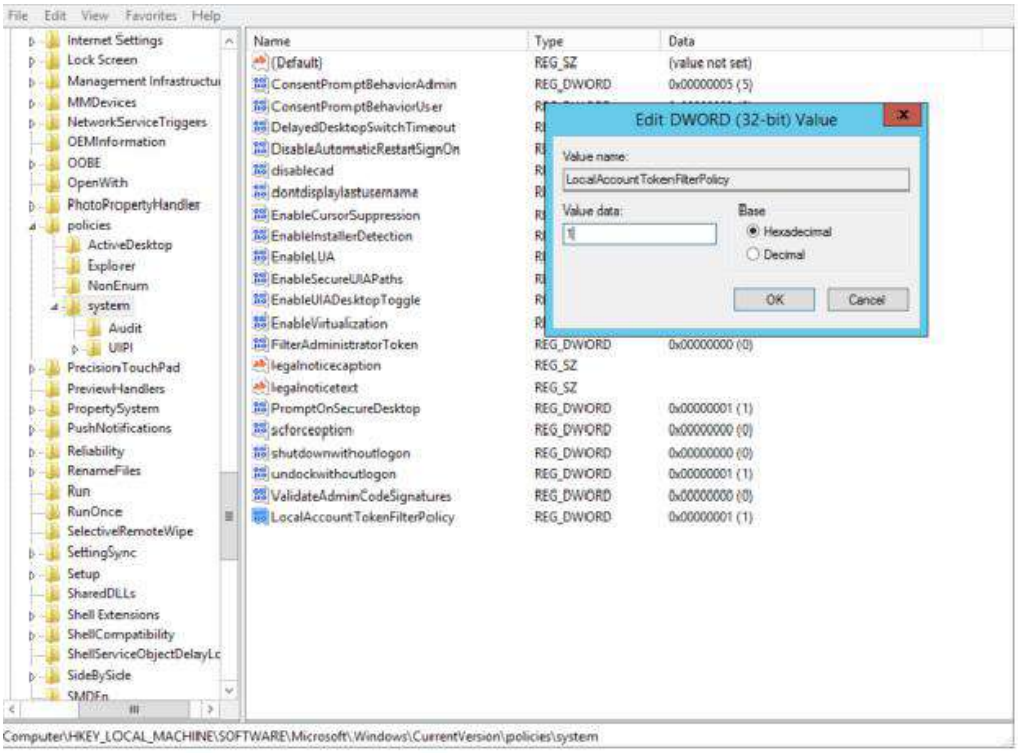


Figure 5 Remote Registry

Step 4 - Memory Leak in the Remote Registry Service

To resolve the Memory Leak in the Remote Registry Service:

1. Open the **Run Prompt** by typing *Run* in the Windows Start search field.
2. Type *regedit.exe* and press enter.
3. Locate the following registry sub key: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\RemoteRegistry*
4. In the details pane, on the right-hand side, double-click **DisableIdleStop.**
5. Change the value to 00000001.

1.2 Windows 8.1

To succeed with authenticated scanning using SMB for Windows 8.1 targets, follow the steps below.

***Note**: The following steps are only applicable for Windows 8.1 Pro or higher, NOT Windows 8.1 Home.*

Step 1 - Enable Remote Registry

To enable Remote Registry (Optional, can also be configured within the scanner):

1. Click the **Windows Start Button** and open **Run Prompt** by entering *Run* in the search field.
2. Type *services.msc* in the **Run Prompt** and press **OK** - this will open **Services**.
3. Under **Services (Local)** find **Remote Registry** >> Right Click and select **Properties**.
   ***Note:** If Remote Registry is already enabled on your device, skip to Step 2.*
4. In **Remote Registry Properties (Local Computer)**, change the Startup Type to Automatic and start the service.

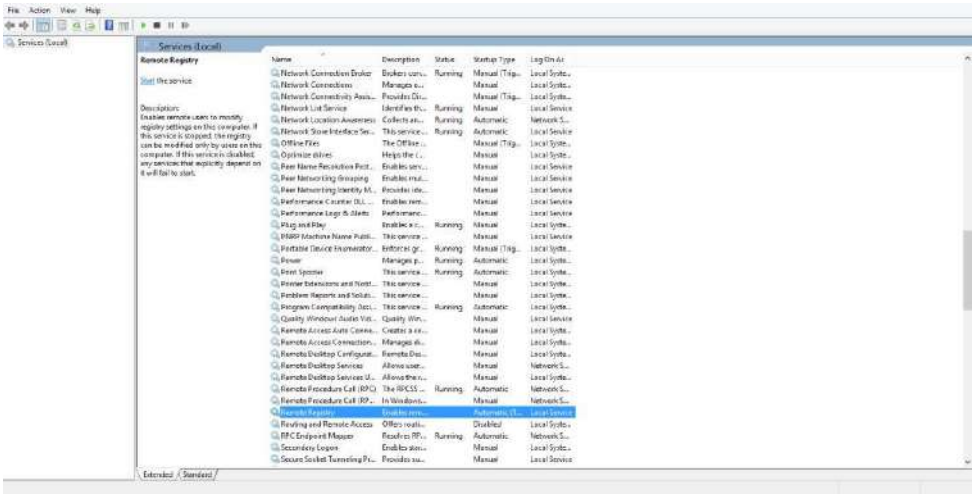


Figure 6 Services (Local) >> Remote Registry

Step 2 - File and Printer Sharing

To turn on File and Printer Sharing:

1. Access **Network and Sharing Center** by entering *Network and Sharing Center* in the **Start Screen**
2. In **Network and Sharing Center**, access **Change advanced sharing settings**, located on the left-hand side.
3. In your current profile, **Private/Guest** or **Public**, check the box for **Turn ON file and printer sharing** and click **Save Changes**.

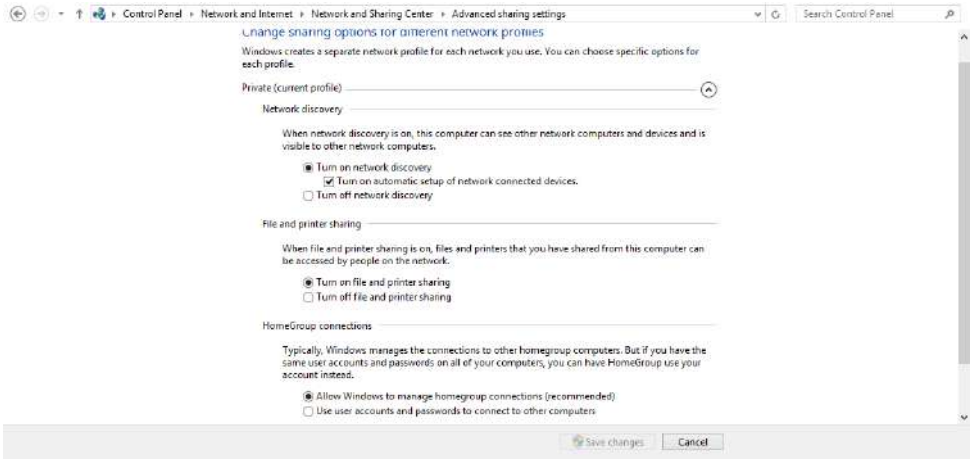


Figure 7 Network and Sharing Center >> Change Advanced Sharing Settings >> Turn on File and Printer Sharing

Step 3 - Administrator Rights

To succeed with the authentication, the account in use needs to either be a Domain User Account or a local user part of the **Administrator Group**.

Domain User Account - Make sure that the domain user account is a member of the Administrators group, this user will run with full administrator access on therefore User Account Control (UAC) does not need to be disabled.

Local User - To make sure that the local account is included in the Administrators Group:

1. Access **Microsoft Management Console** by pressing **Windows Start Button** and enter *mmc* into the search field.
2. Click **Local Users and Groups** on the left-hand side.
3. *If you don't see **Local Users and Groups** click the **File Menu** and choose **Add/Remove Snap-in.***
4. *Click **Local Users and Groups >> Add.***
5. *Click **Local Computer >> Finish >> Ok**.*
6. Enter the **Groups** folder and double click the **Administrators** group. If the account is not listed under **Members**, click **Add** >> Enter the name of the already created account that you wish to add >> click **Check Names** >> click **Ok** >> click **Ok.**

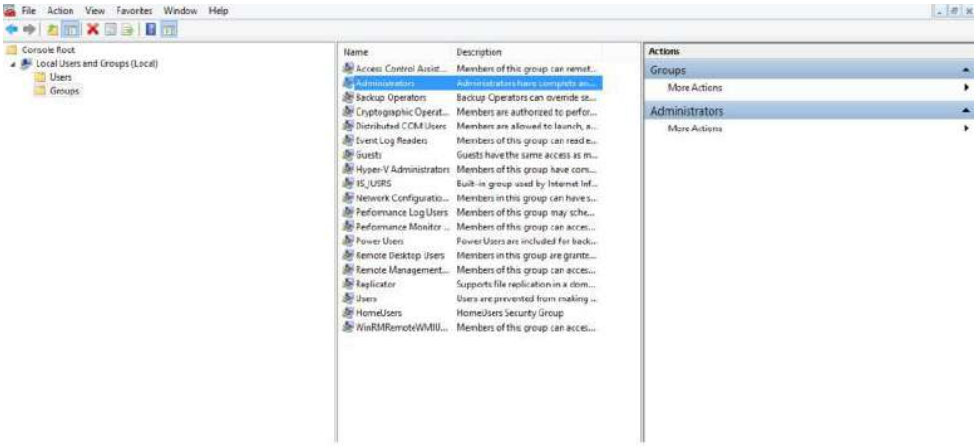
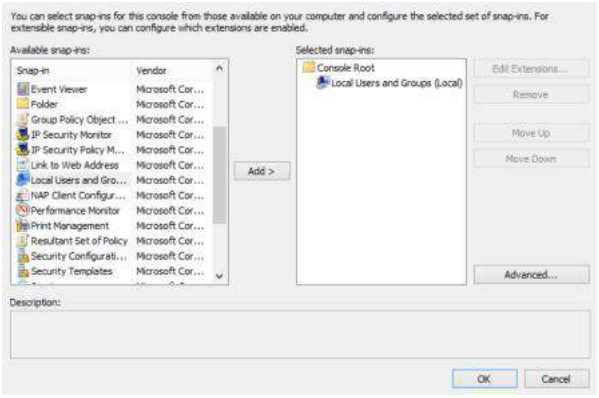


Figure 8 Microsoft Management Console



- *File >> Add/Remove Snap-In >> Local Users and Groups >> Groups >> Administrator >> Members*

Make sure that the Windows User Account Control (UAC) is disabled.

1. Access the **Run Prompt** through **Windows Start Menu** by entering *Run* into the search field.
2. Type *regedit* in the **Run Prompt** and click OK, this will open the **Registry Editor**
3. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system.*
4. Right click the System Folder, choose **New >> DWORD (32-bit) Value** and name the DWORD *LocalAccountTokenFilterPolicy.*
5. Right click the newly created DWORD and choose **Modify**, in the Edit Window set **Value Data** to “1”.

6. If **User Account Control** is disabled, **EnableLUA** must be set to “0” in *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.*

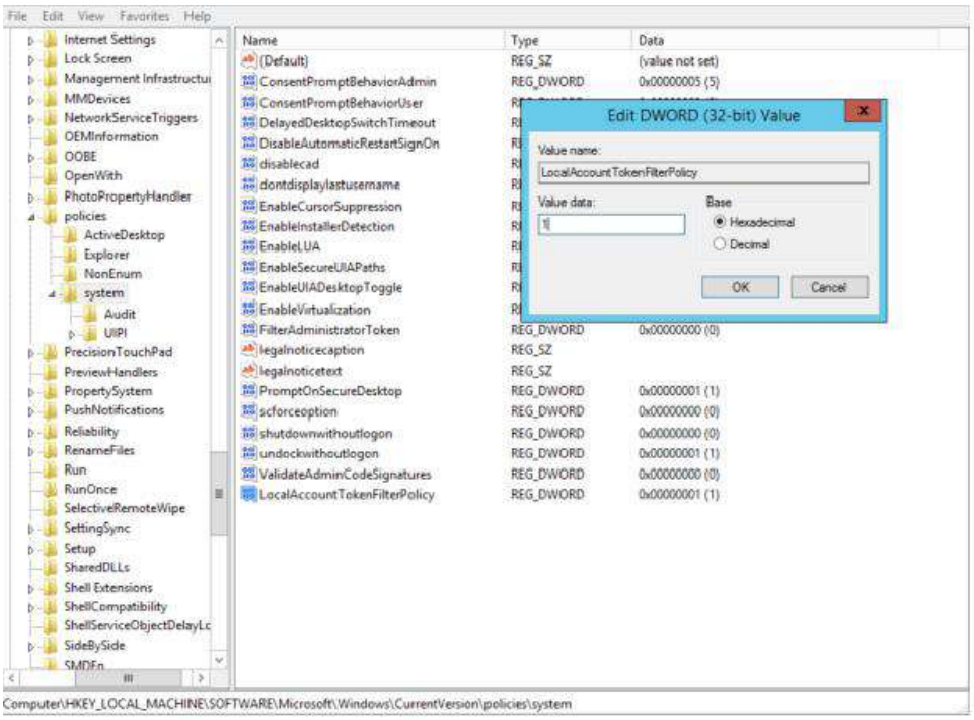


Figure 9 Remote Registry

Step 4 - Memory Leak in the Remote Registry Service

To resolve the Memory Leak in the Remote Registry Service:

1. Open the **Run Prompt** by typing *Run* in the Windows Start search field.
2. Type *regedit.exe* and press enter.
3. Locate the following registry sub key: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\RemoteRegistry.*
4. In the details pane, on the right-hand side, double-click **DisableIdleStop.**
5. Change the value to *00000001.*

1.3 Windows 10

To succeed with authenticated scanning using SMB for Windows 10 targets, follow the steps given below:

***Note**: The following steps are only applicable for Windows 10 Pro or higher, NOT Windows 10 Home.*

Step 1 - Enable Remote Registry

To enable Remote Registry (*Optional*, can also be configured within the scanner)

1. Click the **Windows Start Button** and open **Run Prompt** by entering *Run* in the search field..
2. Type *services.msc* in the Run Prompt and press OK - this will open **Services**
3. Under **Services (Local)** find **Remote Registry** >> Right Click and select **Properties.**
   ***Note:** If Remote Registry is already enabled on your device, skip to Step 2*
4. In **Remote Registry Properties (Local Computer)**, change the Startup Type to Automatic and start the service.

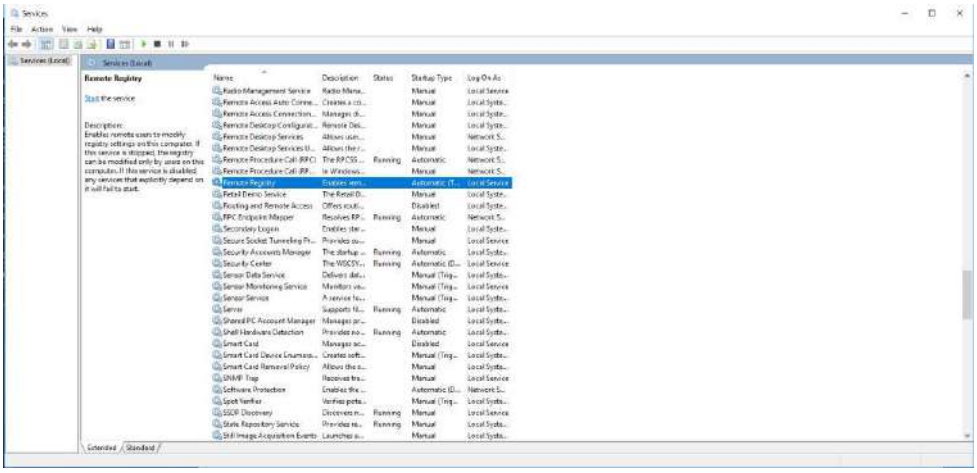


Figure 10 Services (Local) >> Remote Registry

Step 2 - File and Printer Sharing

To turn ON File and Printer Sharing:

1. Access **Network and Sharing Center** by clicking the **Windows Start Button** and enter *Network and Sharing Center* into the search field.
2. In **Network and Sharing Center**, access **Change advanced sharing settings**, located on the left-hand side.
3. In your current profile, Private/Guest or Public, check the box for **Turn ON file and printer sharing** and click **Save Changes.**

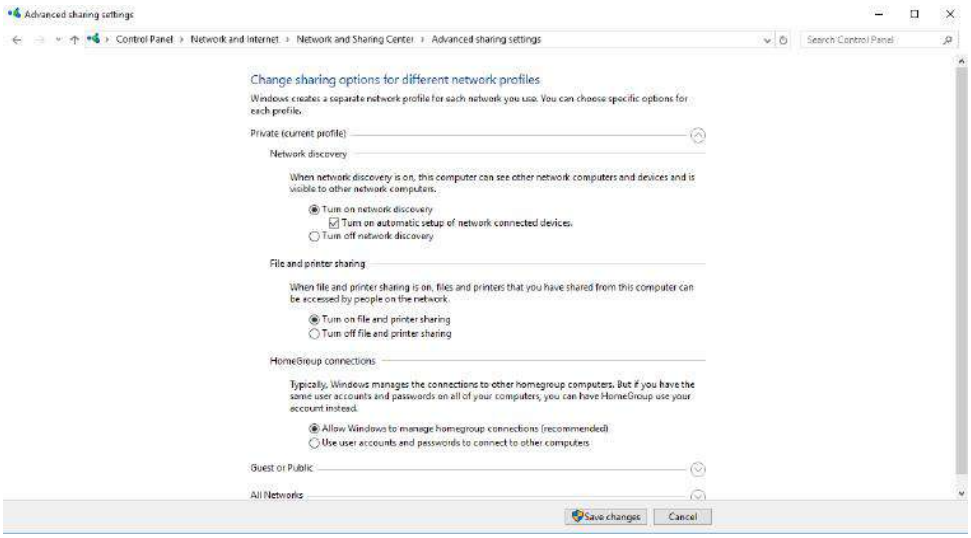


Figure 11 Network and Sharing Center >> Change Advanced Sharing Settings >> Turn on File and Printer Sharing

Step 3 - Administrator Rights

To succeed with authentication, the account in use needs to either be a **Domain User Account** or a local user part of the **Administrator Group**.

Domain User Account: Make sure that the domain user account is a member of the Administrators group, this user will run with full administrator access on therefore User Account Control (UAC) does not need to be disabled.

Local User: Make sure that the local account is included in the Administrators Group:

1. Access Microsoft Management Console by pressing Windows Start Button and enter *mmc* into the search field.
2. Click **Local Users and Groups** on the left-hand side.
3. *If you don't see **Local Users and Groups** click the **File** Menu and choose **Add/Remove Snap-in.***
4. *Click **Local Users and Groups >> Add.***
5. *Click **Local Computer >> Finish >> Ok**.*
6. Enter the **Groups** folder and double click the **Administrators** group.
7. If the account is not listed under Members, click **Add** >> Enter the name of the already created account that you wish to add >> click **Check Names** >> click **Ok** >> click **Ok**.

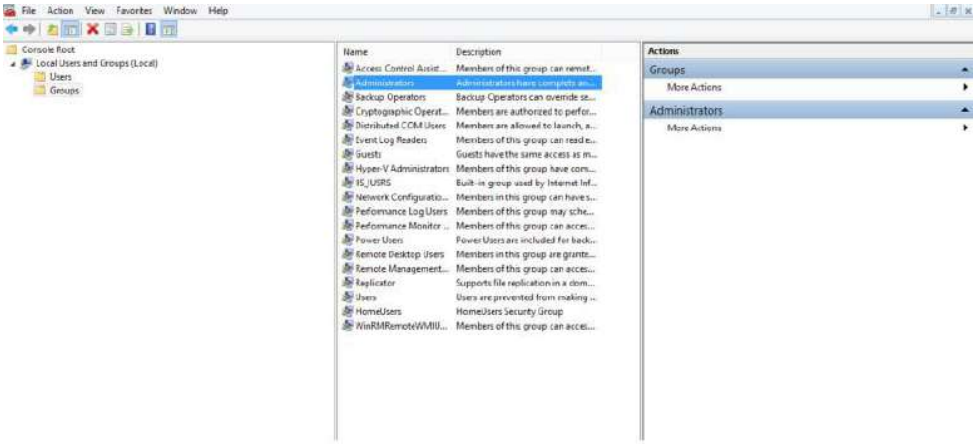
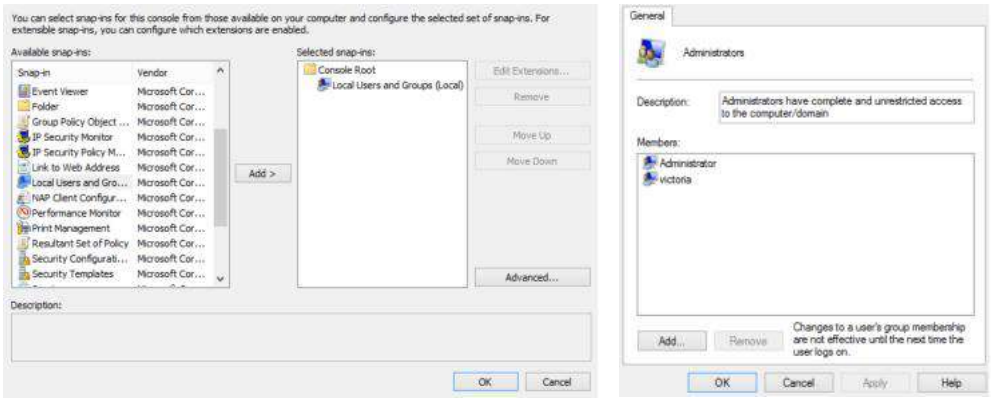


Figure 12 Microsoft Management Console



File >> Add/Remove Snap-In >> Local Users and Groups >> Groups >> Administrator >> Members

***Note**: The following step are not recommended, if possible use the domain user account.*

Make sure that the Windows User Account Control (UAC) is disabled.

1. Access the **Run Prompt** through **Windows Start Menu** by entering *Run* into the search field.
2. Type *regedit* in the **Run Prompt** and click **OK**, this will open the **Registry Editor.**
3. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system.*
4. Right click the System Folder, choose **New >> DWORD (32-bit) Value** and name the DWORD *LocalAccountTokenFilterPolicy.*
5. Right click the newly created DWORD and choose **Modify**, in the Edit Window set **Value Data** to **1**.
6. If **User Account Control** is disabled, **EnableLUA** must be set to *0* in *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.*

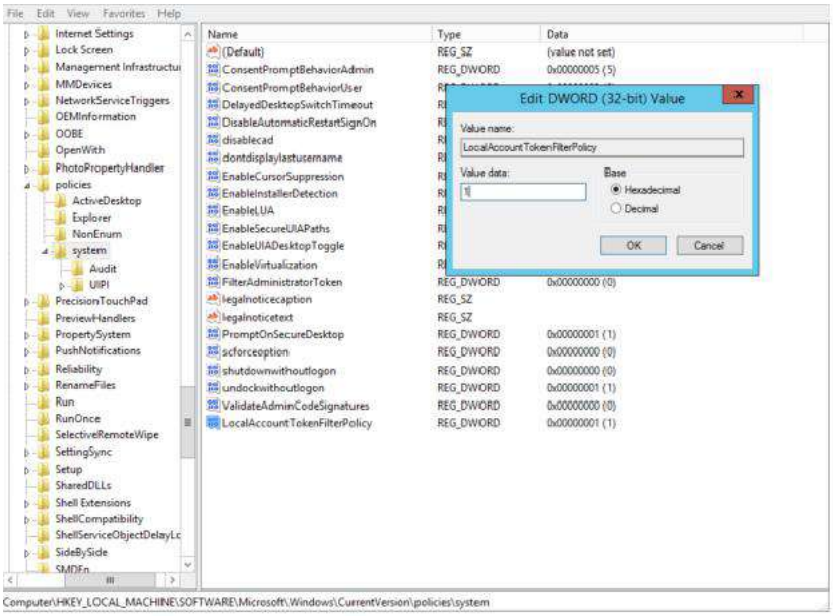


Figure 13 Remote Registry

Step 4 - Memory Leak in the Remote Registry Service

To resolve the Memory Leak in the Remote Registry Service:

1. Open the **Run Prompt** by typing *Run* in the Windows Start search field.
2. Type *regedit.exe* and press enter.
3. Locate the following registry sub key: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\RemoteRegistry.*
4. In the details pane, on the right-hand side, double-click **DisableIdleStop.**
5. Change the value to *00000001.*

1.4 Windows 2008 R2 Server

To succeed with authenticated scanning using SMB for Windows 2008 R2 Server

targets, follow the steps given below.

Step 1 - Enable Remote Registry

To enable Remote Registry (Optional, can also be configured within the scanner)

1. Press the Windows Start Button and open Run Prompt by entering *Run* in the search field.
2. Type *services.msc* in the Run Prompt and press OK, this will open Services.
3. Under Services (Local) find Remote Registry >> Right Click and select **Properties.**
   Note: *If Remote Registry is already enabled on your device, skip to Step 2*
4. In Remote Registry Properties (Local Computer), change the Startup Type to Automatic and start the service.

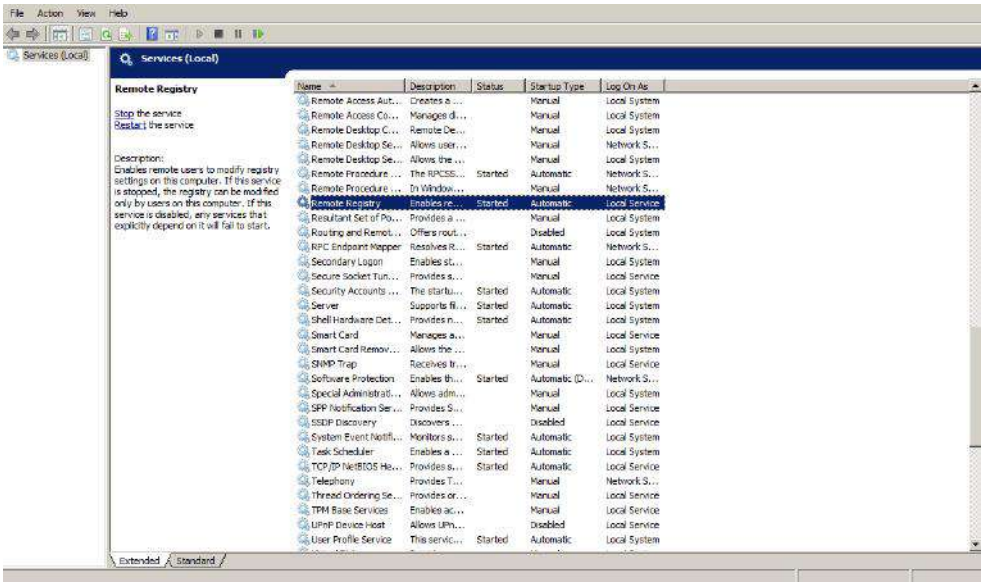


Figure 14 Services (Local) >> Remote Registry

Step 2 - File and Printer Sharing

Turn ON File and Printer Sharing

1. Access **Network and Sharing Center** by accessing **Windows Start Button** and enter *Network and Sharing Center* into the search field.
2. In **Network and Sharing Center**, access **Change advanced sharing settings**, located on the left-hand side.
3. In your current profile, Private/Guest or Public, check the box for **Turn ON file and printer sharing** and click **Save Changes**.

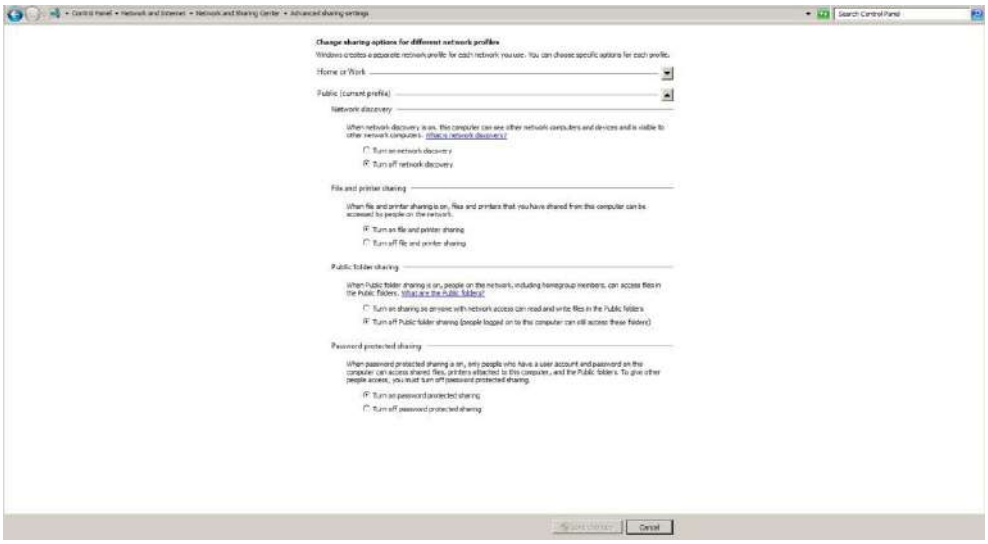


Figure 15 Network and Sharing Center >> Change Advanced Sharing Settings >> Turn on File and Printer Sharing

Step 3 - Administrator Rights

To succeed with the Authentication, the account in use needs to either be a **Domain User Account** or a local user part of the **Administrator Group**.

Domain User Account - Make sure that the domain user account is a member of the Administrators group, this user will run with full administrator access on therefore User Account Control (UAC) does not need to be disabled.

Local User - Make sure that the local account is included in the Administrators Group:

1. Access **Microsoft Management Console** by pressing **Windows Start Button** and enter *mmc* into the search field.
2. Click **Local Users and Groups** on the left-hand side.
3. *If you don't see **Local Users and Groups** click the **File** Menu and choose **Add/Remove Snap-in.***
4. *Click **Local Users and Groups >> Add.***
5. *Click **Local Computer >> Finish >> Ok** .*
6. Enter the **Groups** folder and double click the **Administrators** group .
7. If the account is not listed under **Members**, click **Add** >> Enter the name of the already created account that you wish to add >> click **Check Names** >> click **Ok** >> click **Ok.**

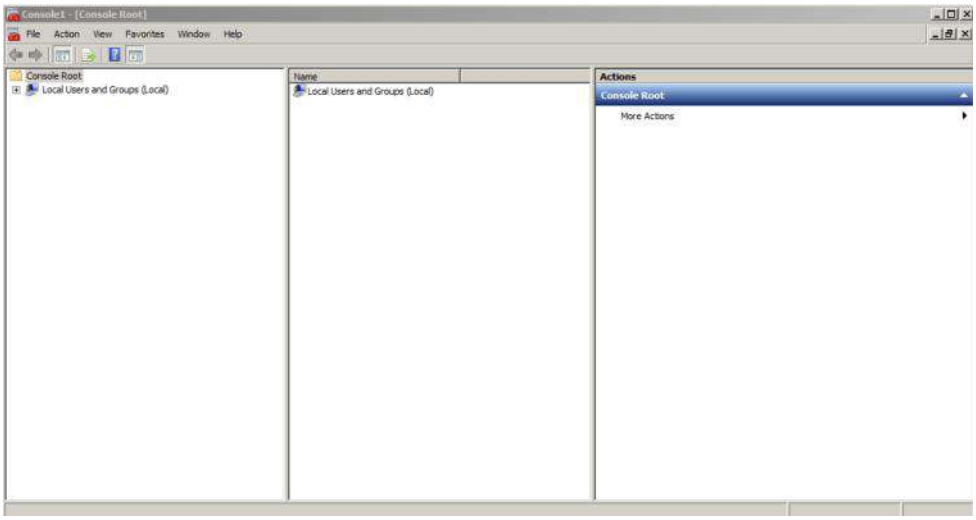
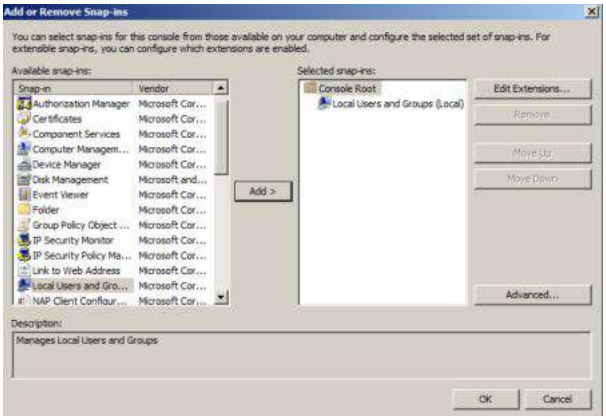


Figure 16 Microsoft Management Console



- *File >> Add/Remove Snap-In >> Local Users and Groups >> Groups >> Administrator >> Members*

***Note**: The following step are not recommended, if possible use the domain user account.*

Make sure that the Windows User Account Control (UAC) is disabled.

1. Access the **Run Prompt** through **Windows Start Menu** by entering *Run* in the search field.
2. Type *regedit* in the **Run Prompt** and click **OK**, this will open the **Registry Editor..**
3. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system*
4. Right click the System Folder, choose **New >> DWORD (32-bit) Value** and name the DWORD *LocalAccountTokenFilterPolicy.*
5. Right click the newly created DWORD and choose **Modify**, in the Edit Window set **Value Data** to *1.*
6. If UAC is disabled, **EnableLUA** must be set to *0* in *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.*

Step 4 - Inbound File and Printer Sharing Exception

Allow Inbound File and Printer Sharing Exception

1. Access **Windows Start Menu** and open the **Run Prompt** by entering *Run* in the search field.
2. Type *gpedit.msc* in the **Run Prompt** and click OK, this will open the **Group Policy Object Editor.**
3. Navigate to **Local Computer Policy >> Computer Configuration >> Administrative Templates >> Network >> Network Connections >> Windows Firewall >> Standard Profile**.
4. Under **Standard Profile** enable **Windows Firewall**: **Allow inbound file and printer sharing exception** by right clicking the entry >> **Edit** >> check **Enabled** >> click **Ok.**

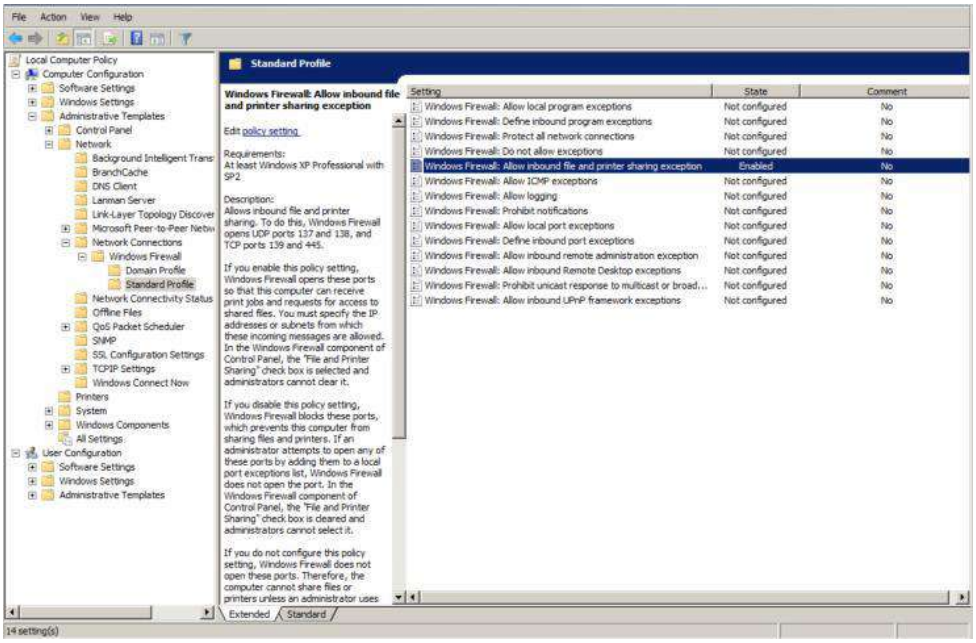


Figure 17 Standard Profile

1.5 Windows 2012 R2 Server

To succeed with authenticated scanning using SMB for Windows 2012 R2 Server targets, follow the steps given below:

Step 1 - Enable Remote Registry

To enable Remote Registry (optional, can also be configured within the scanner)

1. Access the Run Prompt through Windows Start Menu by entering *Run* into the search field.
2. Type *services.msc* in the Run Prompt and press OK, this will open Services.
3. Under Services (Local) find **Remote Registry >>** Right Click and select **Properties.**
4. If Remote Registry is already enabled on your device, skip to **Step 2.**
5. In Remote Registry Properties (Local Computer) change the Startup Type to Automatic and start the service.

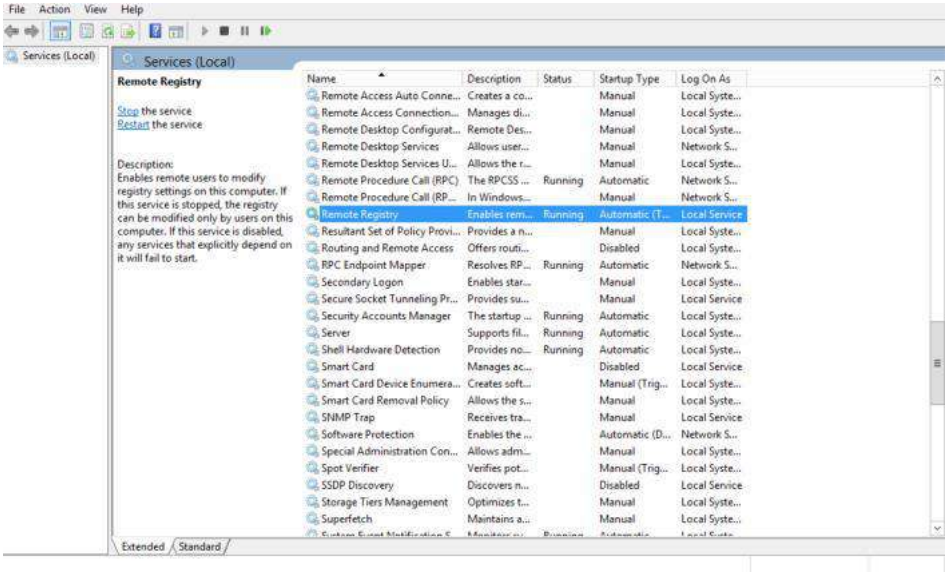


Figure 18 Services (Local) >> Remote Registry

Step 2 - File and Printer Sharing

To turn on File and Printer Sharing:

1. Access Network and Sharing Center by pressing the Windows Start button and enter **Network and Sharing Center** into the search field.
2. In Network and Sharing Center, access **Change advanced sharing settings** which are located on the left-hand side.
3. In your current profile, Private/Guest or Public, check the box for **Turn on file and printer sharing** and click **Save Changes**.

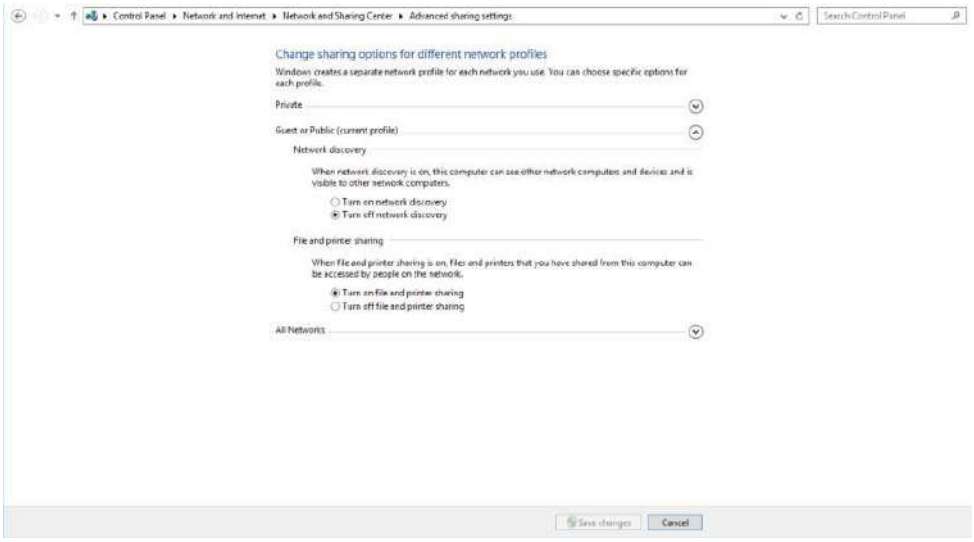


Figure 19 Network and Sharing Center >> Change Advanced Sharing Settings >> Turn on File and Printer Sharing

Step 3 - Administrator Rights

To succeed with authentication, the account in use needs to either be a Domain User Account or a local user part of the Administrator Group.

Domain User Account - Make sure that the domain user account is a member of the Administrators group, this user will run with full administrator access on therefore User Account Control (UAC) does not need to be disabled.

Local User - Make sure that the local account is included in the Administrators Group:

1. Access **Microsoft Management Console** by pressing Windows Start button and enter *mmc* into the search field.
2. Click **Local Users and Groups** on the left-hand side.
3. *If you don't see **Local Users and Groups** click the **File Menu** and choose **Add/Remove Snap-in.***
4. *Click **Local Users and Groups >> Add.***
5. *Click **Local Computer >> Finish >> Ok** .*
6. Enter the Groups folder and double click the **Administrators group.**
   If the account is not listed under Members, click **Add >>** Enter the name of the already created account that you wish to add >> click **Check Names >>** click **Ok >>** click **Ok**

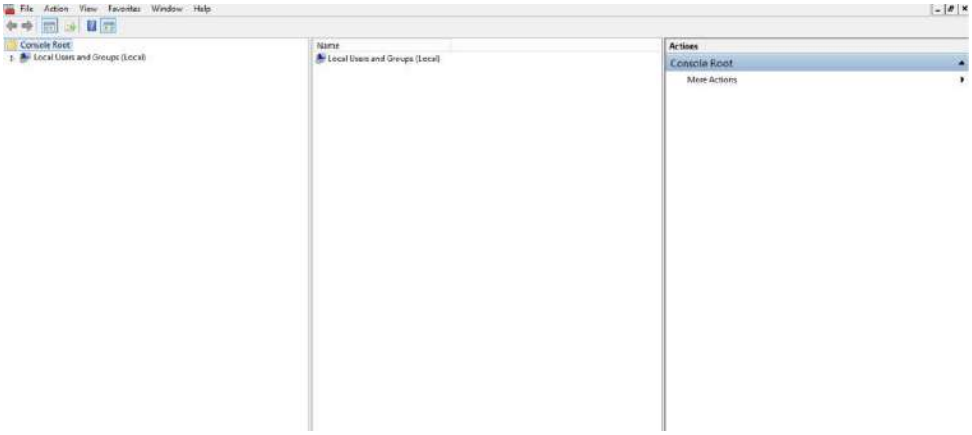
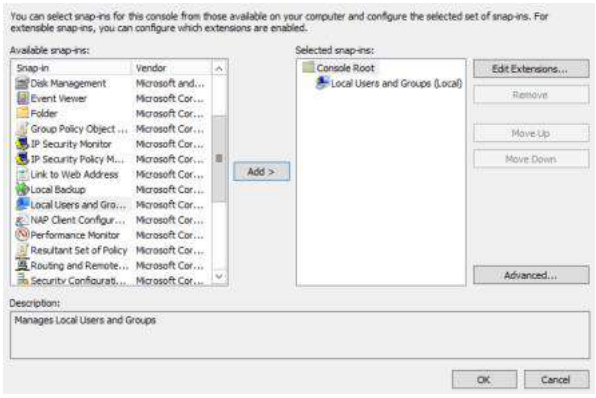
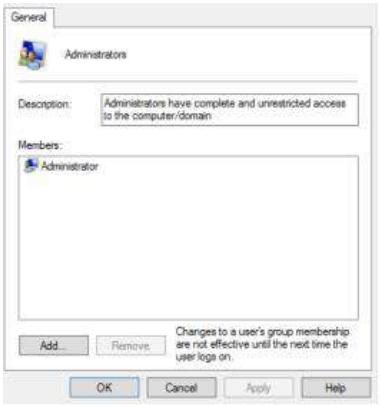


Figure 20 Microsoft Management Console





- *File >> Add/Remove Snap-In >> Local Users and Groups >> Groups >> Administrator >> Members*

***Note**: The following step are not recommended, if possible use the domain user account.*

Make sure that Windows User Account Control (UAC) is disabled.
Access the Run Prompt through Windows Start Menu by entering “Run” into the search field

1. Type *regedit* in the Run Prompt and click **OK**, this will open the Registry Editor.
2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system.*
3. Right click the System Folder, choose **New >> DWORD (32-bit) Value** and name the DWORD *LocalAccountTokenFilterPolicy.*
4. Right click the newly created DWORD and choose **Modify**, in the Edit Window set **Value Data** to *1.*
5. If User Account Control is disabled, **EnableLUA** must be set to *0* in *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.*

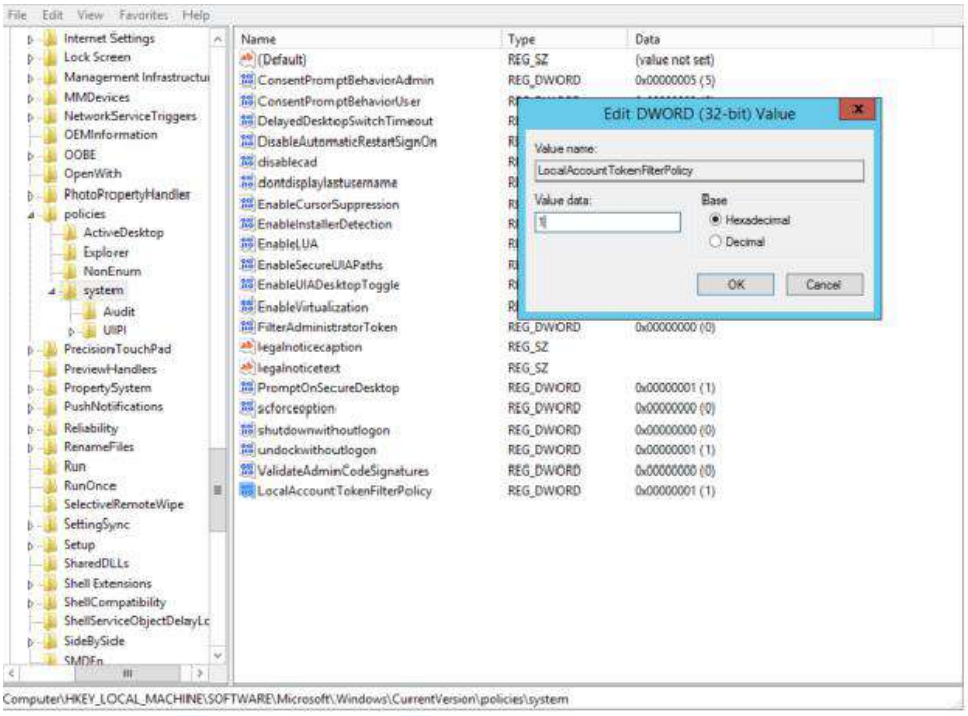


Figure 21 Remote Registry

Step 4

Allow Inbound File and Printer Sharing Exception

1. Access Windows Start Menu and open the Run Prompt by entering *Run* in the search field.
2. Type *gpedit.msc* in the Run Prompt and click **OK**, this will open the **Group Policy Object Editor.**
3. Navigate to Local Computer **Policy >> Computer Configuration >> Administrative Templates >> Network >> Network Connections >> Windows Firewall >> Standard Profile** .
4. Under Standard Profile enable Windows Firewall: Allow inbound file and printer sharing exception by right clicking the entry >> **Edit >>** check **Enabled >>** click **Ok**.

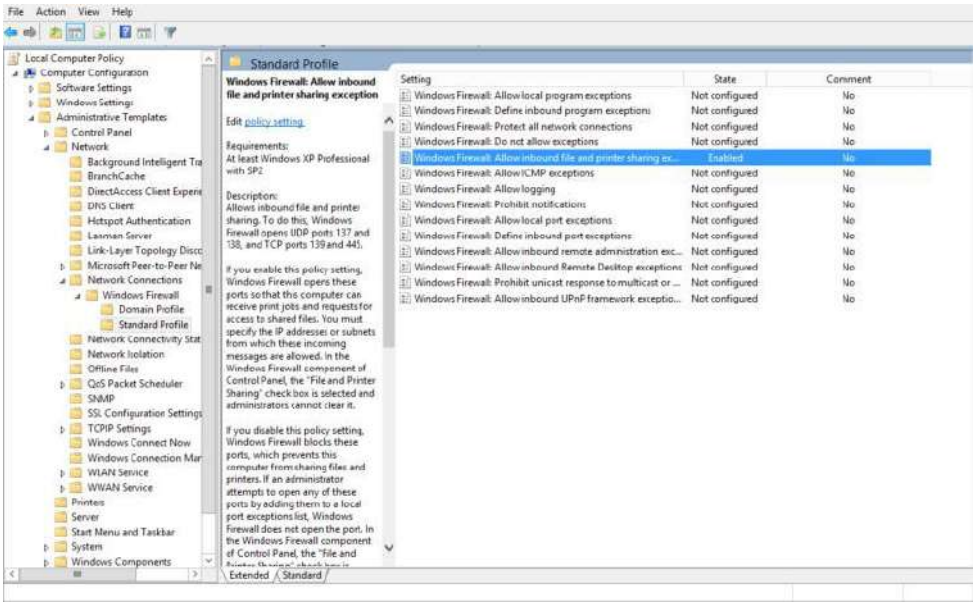


Figure 22 Local Computer Policy >> Computer Configuration >> Administrative Templates >> Network >> Network Connections >> Windows Firewall >> Standard Profile >> Windows Firewall: Allow Inbound File and Printer >> Sharing Exception

Step 5 - Remote Registry Service

To resolve the Memory Leak in the Remote Registry Service:

1. Open the Run Prompt by searching for **Run** in the Windows Start search field.
2. Type *regedit.exe* and press enter.
3. Locate the following registry sub key: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\RemoteRegistry.*
4. In the details pane, on the right-hand side, double-click *DisableIdleStop.*
5. Change the value to *00000001.*

1.6 Windows 2016 Server

To succeed with authenticated scanning using SMB for Windows 2016 Server targets, follow the procedure given below.

Step 1 - Enable Remote Registry

Enable Remote Registry (optional, can also be configured within the scanner)

1. Press the Windows Start Button and open Run Prompt by entering *Run* in the search field.
2. Type *services.msc* in the Run Prompt and press **OK**, this will open Services.
3. Under Services (Local) find **Remote Registry >>** Right Click and select **Properties.**
4. If Remote Registry is already enabled on your device, skip to Step 2.
5. In Remote Registry Properties (Local Computer) change the **Startup Type** to **Automatic** and start the service.

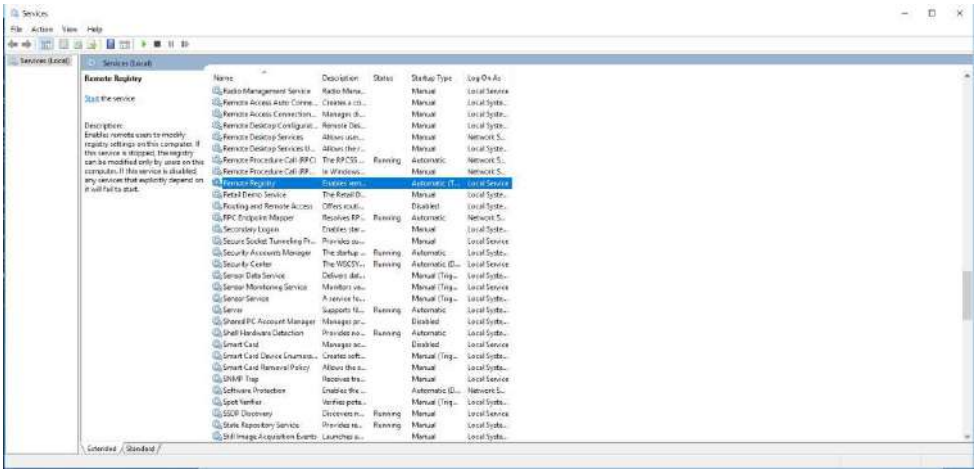


Figure 23 Services (Local) >> Remote Registry

Step 2 - File and Printer Sharing

To turn on the File and Printer Sharing:

1. Access **Network and Sharing Center** by pressing the **Windows Start Button** and enter *Network and Sharing Center* into the search field.
2. In Network and Sharing Center, access Change advanced sharing settings which are located on the left-hand side.
3. In your current profile, Private/Guest or Public, check the box for **Turn on file and printer sharing** and click **Save Changes.**

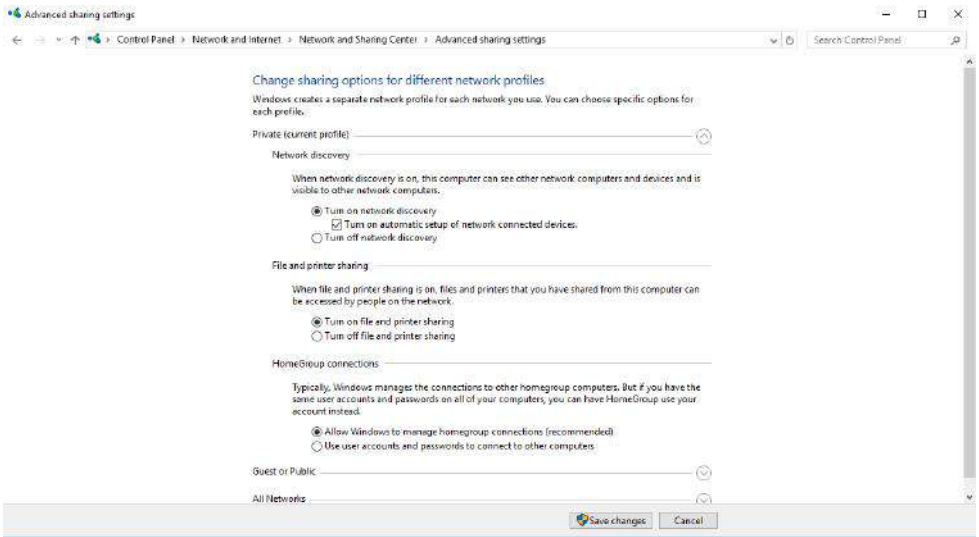


Figure 24 Network and Sharing Center >> Change Advanced Sharing Settings >> Turn on File and Printer Sharing

Step 3 - Administrator Rights

To succeed with the authentication, the account in use needs to be either a **Domain User Account** or a local user part of the **Administrator Group**.

Domain User Account - Make sure that the domain user account is a member of the Administrators group, this user will run with full administrator access on therefore User Account Control (UAC) does not need to be disabled.

Local User - Make sure that the local account is included in the Administrators Group:

1. Access **Microsoft Management Console** by pressing **Windows Start Button** and enter *mmc* into the search field.
2. Click **Local Users and Groups** on the left-hand side.
3. If you don't see Local Users and Groups click the File Menu and choose Add/Remove Snap-in.
4. Click **Local Users and Groups >> Add**.
5. Click **Local Computer >> Finish >> Ok**.
6. Enter the **Groups** folder and double click the **Administrators** group
7. If the account is not listed under **Members**, click **Add** >> Enter the name of the already created account that you wish to add >> click **Check Names** >> click **Ok** >> click **Ok**

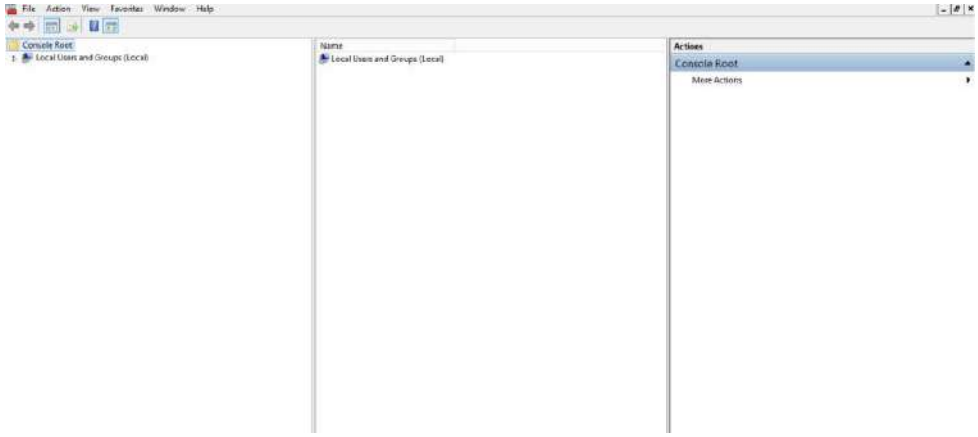
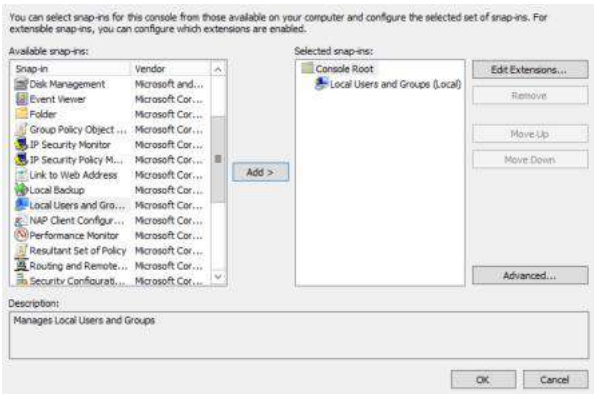
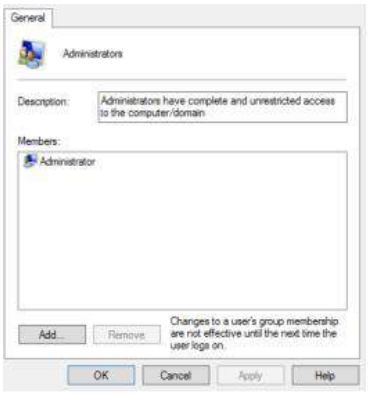


Figure 25 Microsoft Management Console



File >> Add/Remove Snap-In >> Local Users and Groups



Groups >> Administrator >> Members

***Note**: The following steps are not recommended, if possible use the domain user account.*

Make sure that Windows User Account Control (UAC) is disabled.

1. Access the **Run Prompt** through **Windows Start Menu** by entering “Run” into the search field.
2. Type *regedit* in the **Run Prompt** and click OK, this will open the **Registry Editor.**
3. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system.
4. Right click the System Folder, choose **New** >> **DWORD (32-bit) Value** and name the DWORD *LocalAccountTokenFilterPolicy.*
5. Right click the newly created DWORD and choose **Modify**, in the Edit Window set **Value Data** to *1.*
6. If **User Account Control** is disabled, EnableLUA must be set to 0 in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

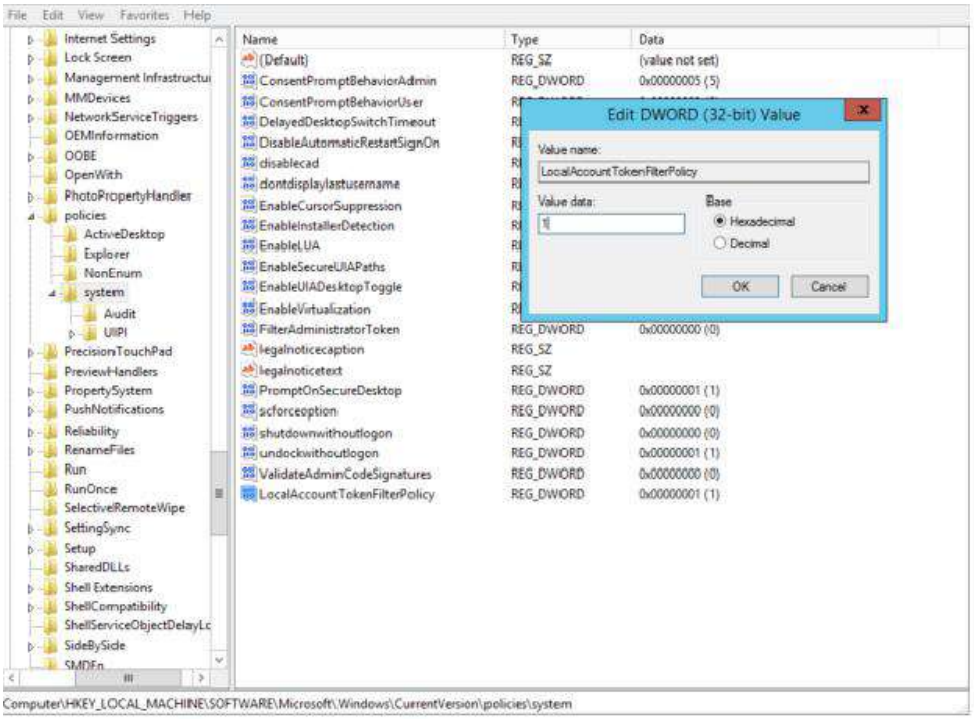


Figure 26 Remote Registry

Step 4 - File and Printer Sharing Exception

Allow Inbound File and Printer Sharing Exception

1. Access **Windows Start Menu** and open the **Run Prompt** by entering "*Run*" in the search field.
2. Type *gpedit.msc* in the **Run Prompt** and click **OK**, this will open the **Group Policy Object Editor.**
3. Navigate to **Local Computer Policy >> Computer Configuration >> Administrative Templates >> Network >> Network Connections >> Windows Firewall >> Standard Profile** .
4. Under Standard Profile enable Windows Firewall: Allow inbound file and printer sharing exception by right clicking the entry >> **Edit** >> check Enabled >> click **Ok**.

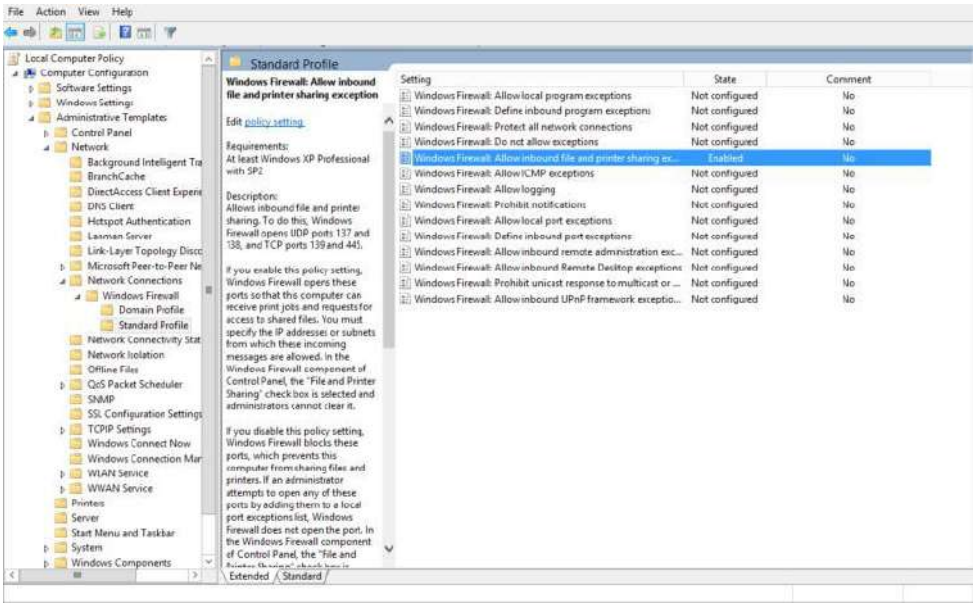


Figure 27 Local Computer Policy >> Computer Configuration >> Administrative Templates >> Network >> Network Connections >> Windows Firewall >> Standard Profile >> Windows Firewall: Allow Inbound File and Printer >> Sharing Exception

Step 5 - Memory Leak in the Remote Registry Service

To resolve the Memory Leak in the Remote Registry Service:

1. Open the **Run Prompt** by searching for “Run” in the Windows Start search field.
2. Type *regedit.exe* and press enter.
3. Locate the following registry sub key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\RemoteRegistry.
4. In the details pane, on the right-hand side, double-click **DisableIdleStop.**
5. Change the value to *00000001.*

1.7 Core Installation

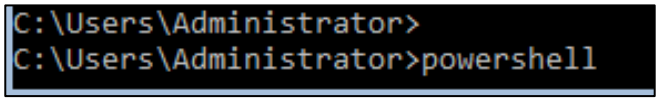
To succeed with authenticated scanning using SMB for Core Installations of Windows, there are five steps that you need to follow.

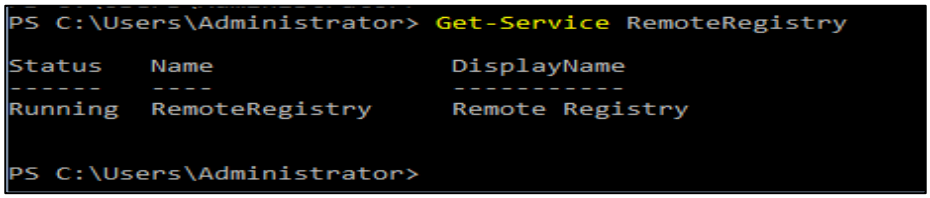
Step 1 - Enable Remote Registry

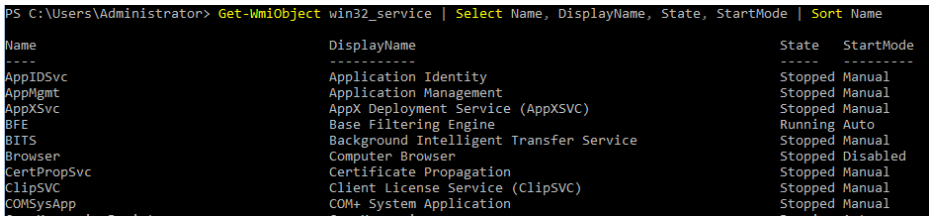
Enable Remote Registry (*optional,* can also be configured within the scanner)

1. Start **powershell** by typing *powershell* in **CMD.**
2. In **powershell**, write *Get-Service RemoteRegistry* to verify the status of the service.
3. If the service is not running, write *Run-Service RemoteRegistry.*
4. To set the service to run automatically, write *Set-Service RemoteRegistry –startuptype automatic.*
5. If you wish to view information and status of all your services, write Get-WmiObject win32_service | Select Name, DisplayName, State, StartMode | Sort Name.

The service should now be running







Step 2 - File and Printer Sharing

To turn on the File and Printer Sharing :

1. Start **powershell** by typing *powershell* in **CMD.**
2. In **powershell**, write “netsh advfirewall firewall set rule group= ”File and Printer Sharing” new enable=Yes” to turn on File and Printer Sharing..

```
PS C:\Users\Administrator> netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes

Updated 16 rule(s).
Ok.
```

Step 3 - Administrator Rights

For the authentication to succeed the account in use needs to either be the **built in Administrator** or a part of the **Administrator Group**.

Built in Administrator

To active the built-in administrator account:

1. In **CMD** Run the command “net user administrator /active: yes”

```
C:\Windows\system32>net user administrator /active:yes
The command completed successfully.

C:\Windows\system32>
```

Local User

1. Make sure the local account is included in the Administrators Group:
2. Start powershell by typing *powershell* in CMD
3. In powershell, run the command *net localgroup administrator* to list the uses within the administrator group
4. If the user is not included run the command *net localgroup administrators “<username>” /add* to add the user

```
PS C:\Users\Administrator> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
The command completed successfully.
```

Step 4 - File and Printer Sharing

Allow Inbound File and Printer Sharing Exception

1. In CMD run the command REG add “HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\FileAndPrint ” /v Enabled /t REG_DWORD /d 1 /f

```
C:\Users\Administrator>REG add "HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\FileAndPrint" /v
 Enabled /t REG_DWORD /d 1 /f
The operation completed successfully.
```

Step 5 - Memory Leak in the Remote Registry

Resolving the Memory Leak in the Remote Registry Service

1. Start **powershell** by typing *powershell* in **CMD.**
2. In **powershell**, write *regedit* to access the **Registry Editor..**
3. Locate the following registry sub key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\RemoteRegistry.
4. In the details pane, on the right-hand side, double-click **DisableIdleStop.**
5. Change the value to *00000001.*

2 Authenticated Scanning using OUTSCAN/HIAB

It is possible to set up authenticated scanning in three different ways, these are applicable for both OUTSCAN and HIAB.

2.1 Per Target

In **Manage Targets** it is possible to set SMB authentication per target. To access these settings please right click on the desired target and choose **Edit**.

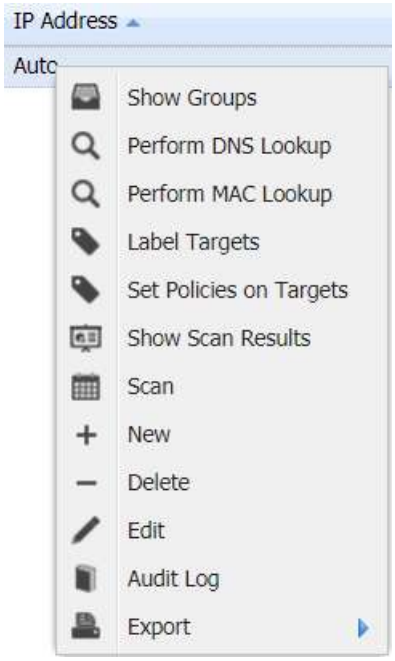


Figure 28 Options

This action will toggle a new window in which you can navigate to the **Authentication** tab. Here you can choose SMB in the drop-down menu and enter the credentials that will be in use, and also if the scanner is allowed to **Enable Remote Registry** by checking the box for this. On the right-hand side of the **Credentials Grid** there is a **Test** button, using this will test the credentials against the target and verify if the authentication was successful or not.

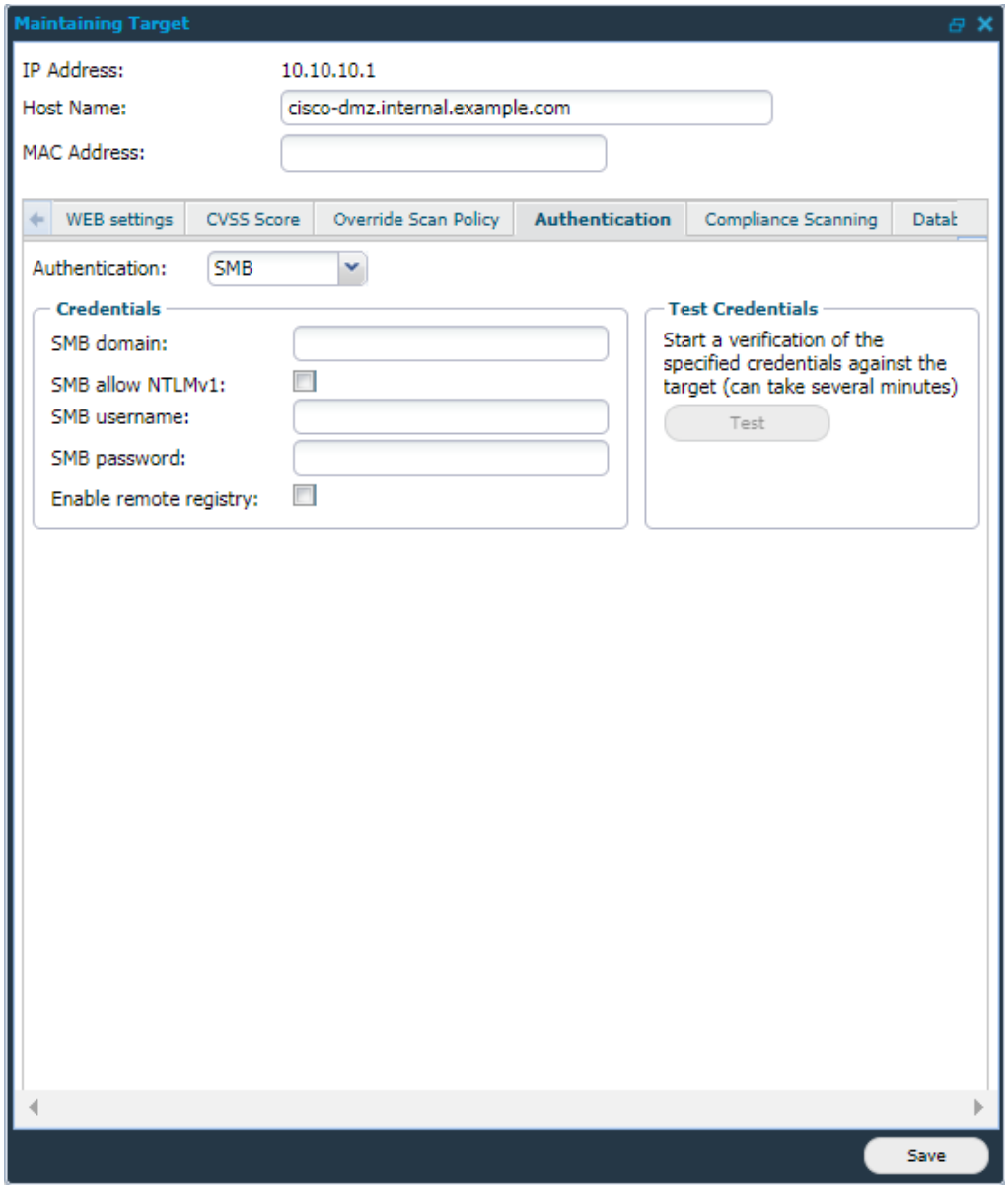


Figure 29 Maintaining Target - Authentication

2.2 Per Target Group

In **Manage Targets** it is possible to set SMB authentication for a Target Group. To access these settings please right click on the desired target group and choose **Set Target Authentication**.

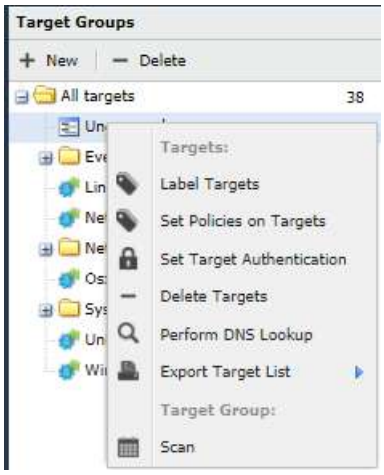


Figure 30 Target Groups

This action will toggle a new window where you are allowed to choose SMB in the drop-down menu and enter the credentials that will be in use for all targets in this group. You may also decide if the scanner should be allowed to **Enable Remote Registry** by checking the box for this. On the right-hand side of the **Credentials Grid** there is a **Test** button, using this will test the credentials against the target and verify if the authentication was successful or not.

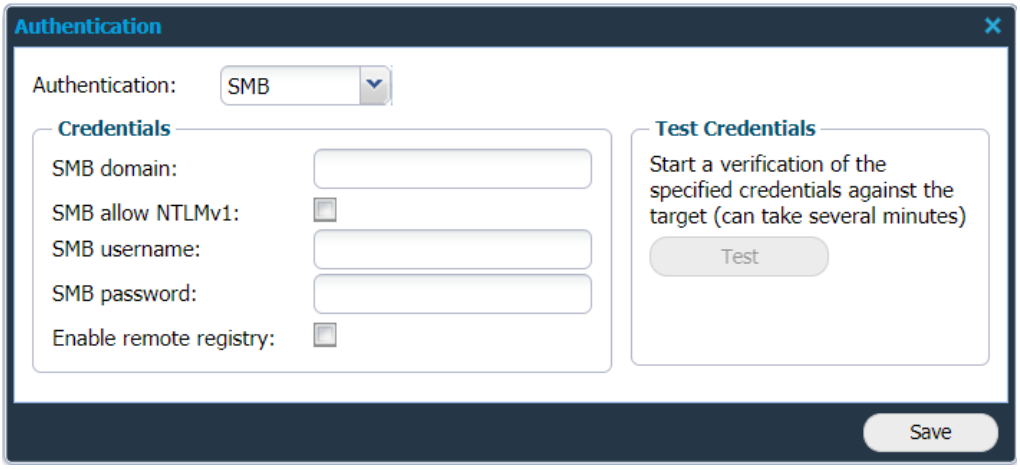


Figure 31 Authentication

2.3 Per Scan Policy

When creating a **Scan Policy** in **Scan Scheduling** it is possible to set SMB authentication. To access these settings, navigate to the **Scan Policy Tab** in **Scan Scheduling** and choose to either **edit** an existing Scan Policy or create a **new** policy.

In the **Maintaining Scanning Policy** window, there is a **SMB** tab in which you are allowed to enter the credentials that will be in use. You may also decide if the scanner is allowed to **Enable Remote Registry** by checking the box for this.

Below the credentials grid there is a **Test Credentials** button, using this against a provided target will test the credentials and verify if the authentication was successful or not.

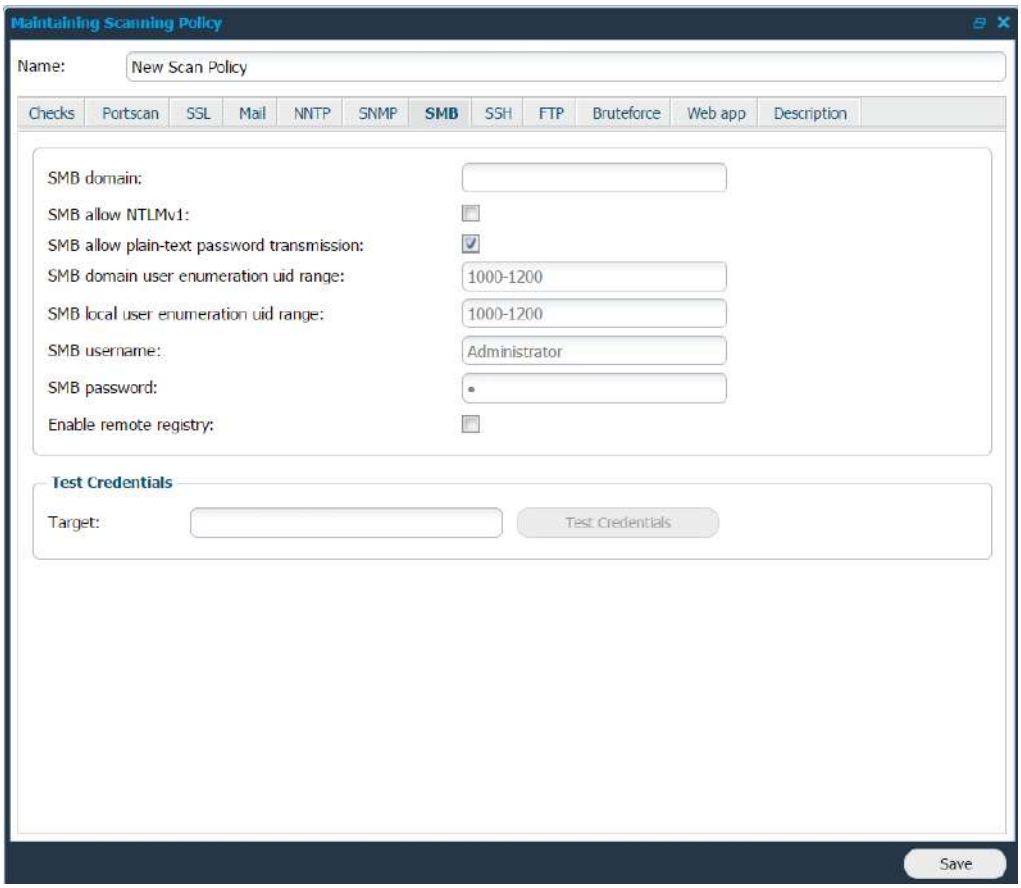


Figure 32 Maintaining Scanning Policy