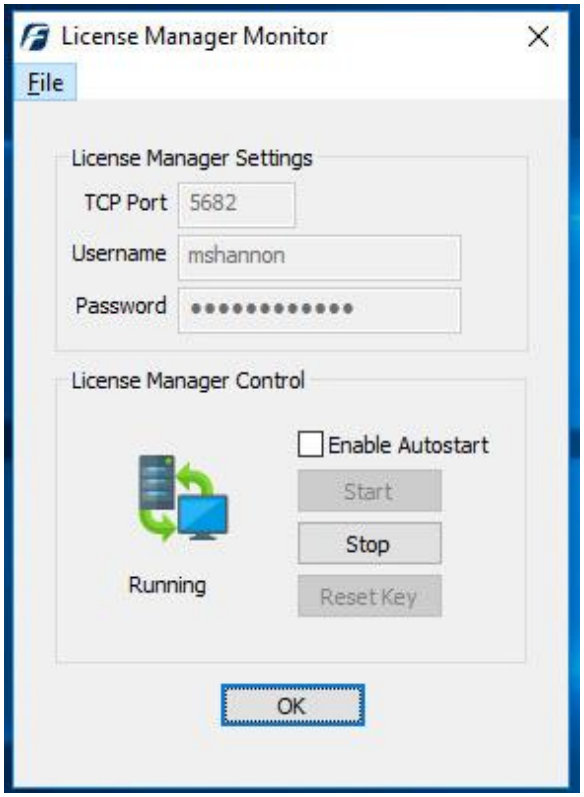
Mission Guide: Covert Deploy

Your Mission: Use F-Response to covertly connect to a remote Windows machine

Using F-Response to deploy and connect to a remote Windows machine and access one or more targets

Step 1: Open and start the F-Response License Manager Monitor (If you have not already done so)

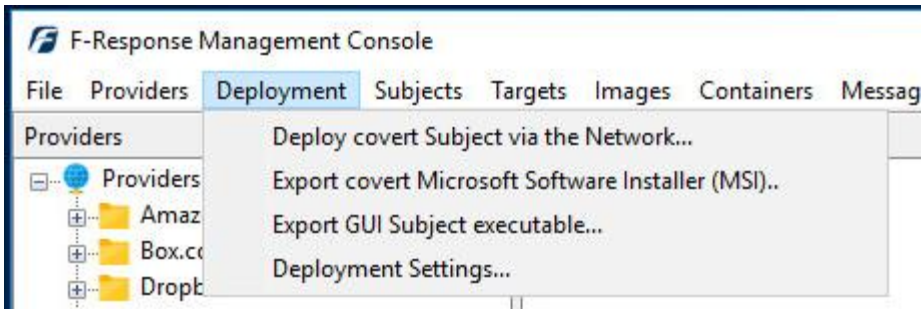
Open the F-Response License Manager Monitor and make sure you have input an F-Response specific username and password. These credentials are purely to control access to F-Response on the remote subject, they are NOT a domain account or system account. Once you have set the username and password be sure to press "Start" to start the License Manager Service.



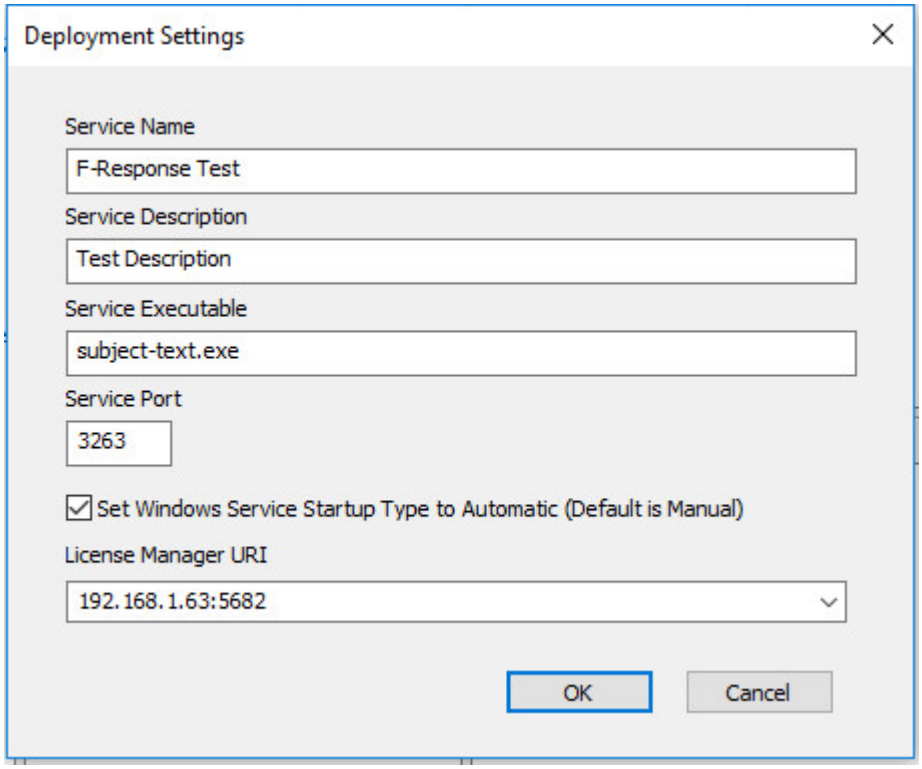
F-Response License Manager Monitor

Step 2: Confirm the Deployment Settings

Open the F-Response Management Console and go to Deployment->Deployment Settings.



Deployment Settings



Deployment Settings Dialog

Many of the options will be pre-populated for you, however you are welcome to adjust them to meet your needs.

Service Name: When F-Response is deployed to the remote machine this is the name of the Windows service that will be created.

Service Description: When F-Response is deployed to the remote machine this is the service description that will be assigned.

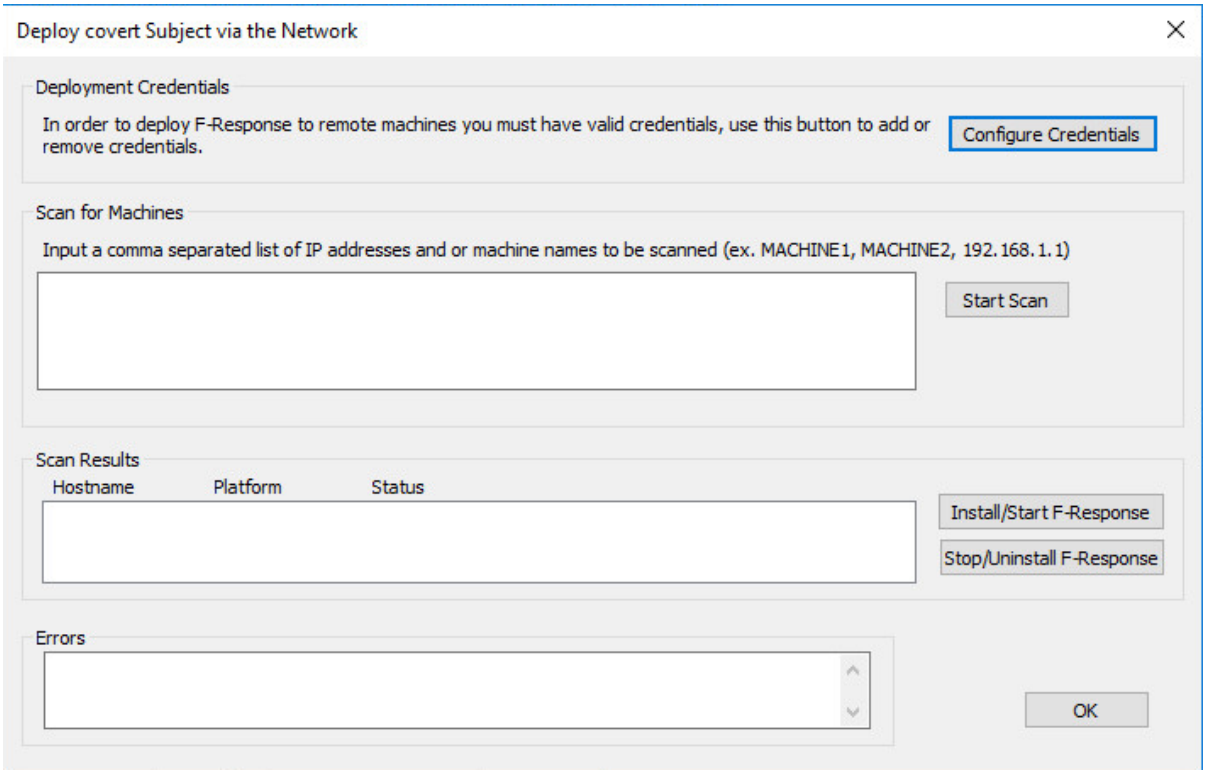
Service Executable: When F-Response is deployed to the remote machine this is the executable name that will be assigned.

Service Port: This is the default TCP port that F-Response will use when listening on the remote machine.

License Manager URI: This is the IP or Hostname plus Port that F-Response will attempt to use to locate your license manager (see step 1). Most of the time it will be easy to determine what to select here, however keep in mind the address you select must be accessible to the remote machine.

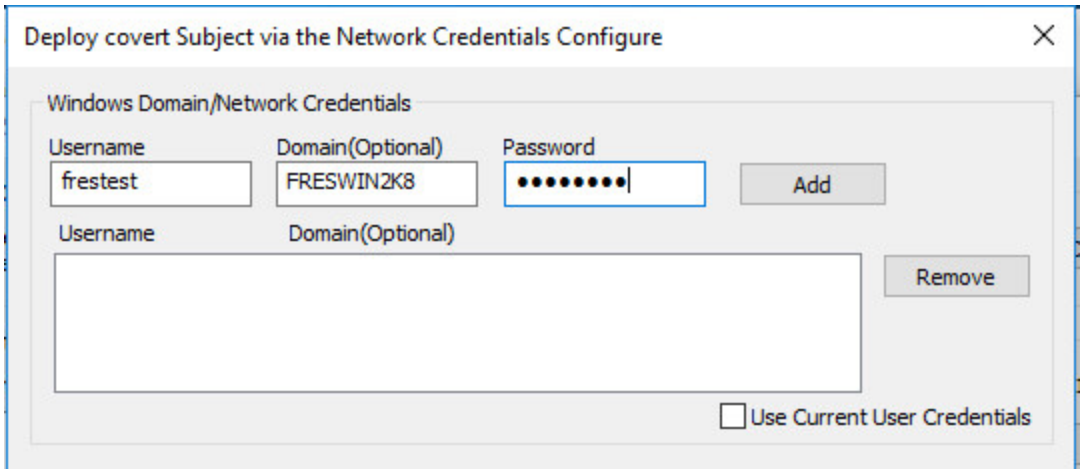
Step 3: Begin the deployment process by adding credentials

Open the Deployment->Deploy covert Subject via the Network… dialog to begin the deployment process.



Deploy covert Subject via the Network…

Now that we've opened the dialog the first order of business is to configure credentials to use for deployment. Keep in mind that unlike previous versions of F-Response, starting in version 7, F-Response stores the deployment credentials encrypted in the examiner's registry. Press Configure Credentials to get started.

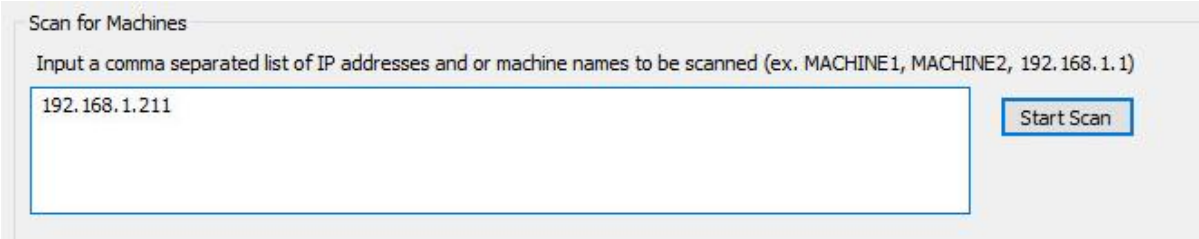


Adding Windows Deployment Credentials

You will want to input one or more Username/Domain/Password combinations to use for deployment. Please keep in mind that some credentials will not work properly even when they are accurate due to Microsoft Workgroup and Domain policies. If you are having issues with credentials, please see the Troubleshooting section at the end of this document.

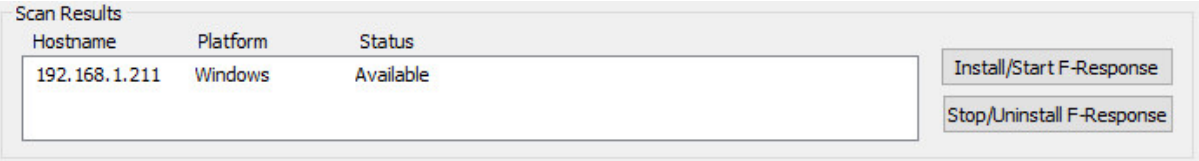
Step 4: Scan for one or more remote machines

After adding at least one credential you will be able to use the Scan input to add one or more comma delineated hostnames or IP addresses. Once you've added them you must press the Start Scan button to begin the scanning process.



Scan for Machines

The results will appear below in the Scan Results section of the dialog. Provided your credentials were successful and the machine was available on the network you should see the following response. If not, please check your credentials and try again, failing that we recommend you consult the Troubleshooting section at the end of this document.



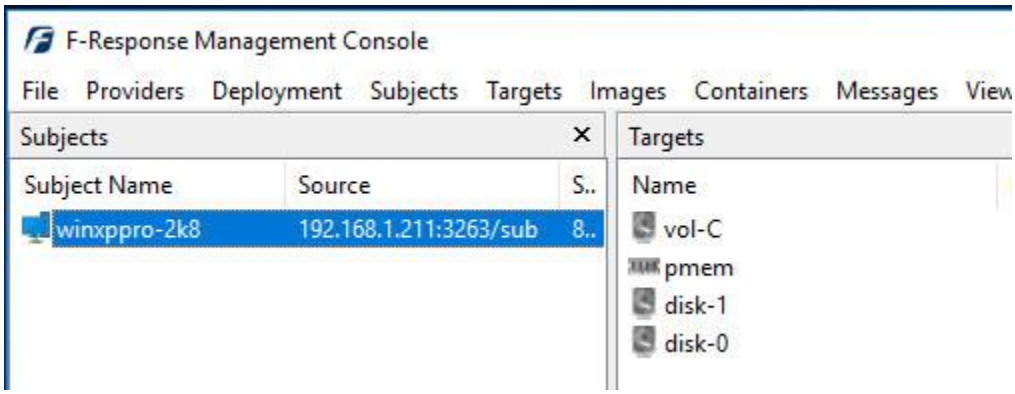
Scan Results

Select the hostname(s) and press Install/Start F-Response to begin the deployment process.

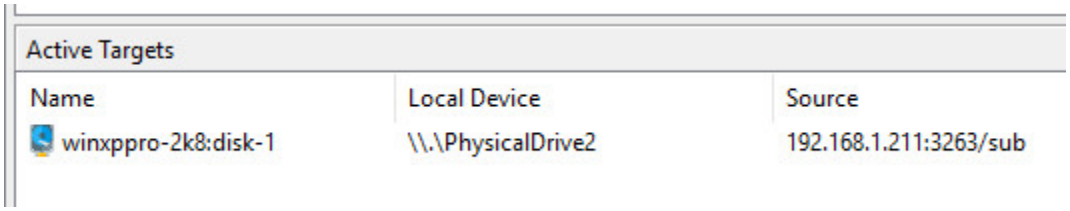
Step 5: List the available targets and attach one or more to your local machine

After successfully deploying F-Response to one or more remote machines you should see those machines in the Subjects panel (use the View->Subjects menu to show the Subjects panel if it is hidden). Hovering over any subject will give you the version of F-Response deployed and the operating system of the subject. Double-Click on any subject or use the Targets->Scan for Targets menu item to get a listing of targets in the Targets panel.

Mounting one or more targets is a simple matter of either double-clicking on the target or selecting the target and using the Targets->Attach Target menu item. Once attached additional target details will appear in the Active Targets panel.



Subject and Targets

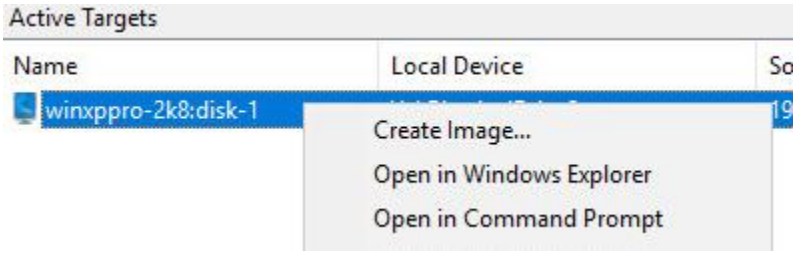


Active Targets

The remaining steps in this mission guide go over making an image of the newly attached device using the F-Response Imaging capability. This is completely optional, at this point you have a full read-only locally attached disk that you can interact with, analyze, etc. using any of the forensic, incident response, or e-discovery tools you have at your disposal.

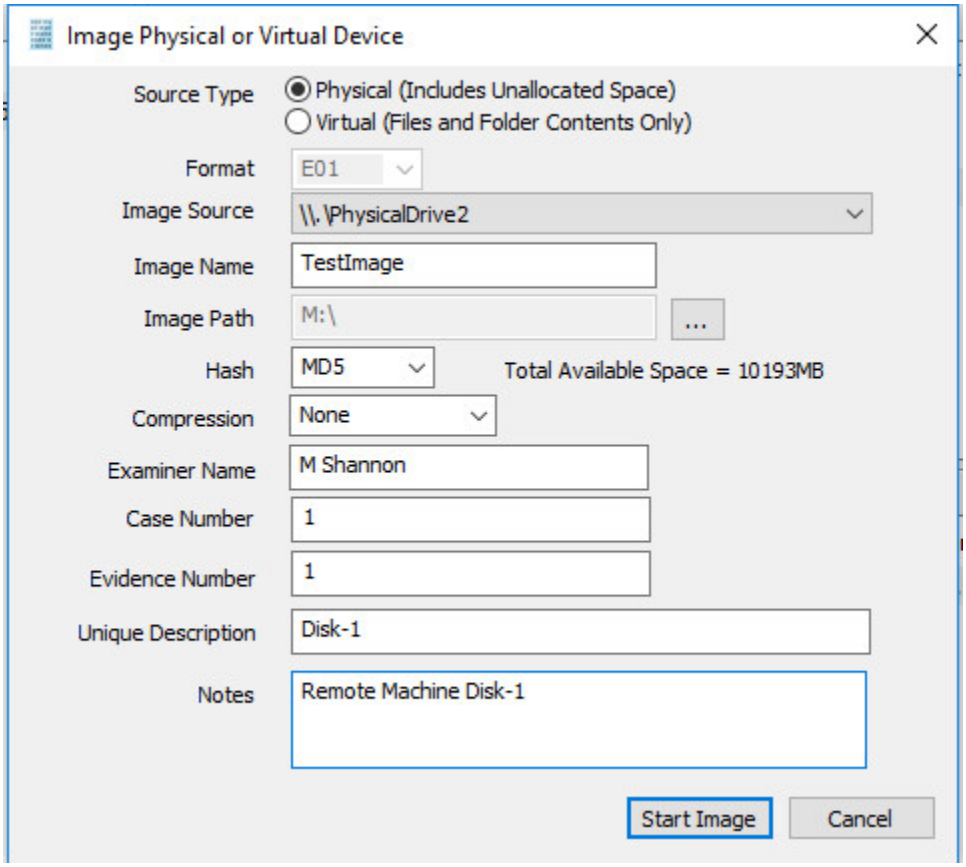
Step 6: Create Image of attached device (optional)

Select the newly attached target and right click on it in the Local Device column. Use the "Create Image…" option to open the "Image" dialog to begin imaging the device.



Start Imaging Process…

Step 7: Complete Imaging Options…



We'll work through this window from the top down. First, the **Source Type** is set to **Physical** (by default) to be able to create an image of the connected Physical device data.

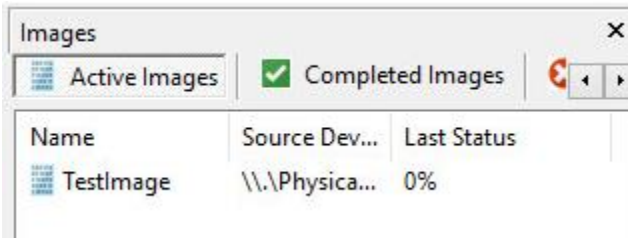
For **Image Path** we need to choose our destination drive—this must be a physical drive attached to our examiner machine (we cannot image to a network share).

Next we can choose a **Hash** format and the **Compression** level if you wish to compress the resulting image file. The remaining fields are specific to your case and can be filled out accordingly. These fields will be included in the resulting log file for the image.

Once you have all your information entered simply click the **Start Image** button to begin the process.

Step 8: Review the Image

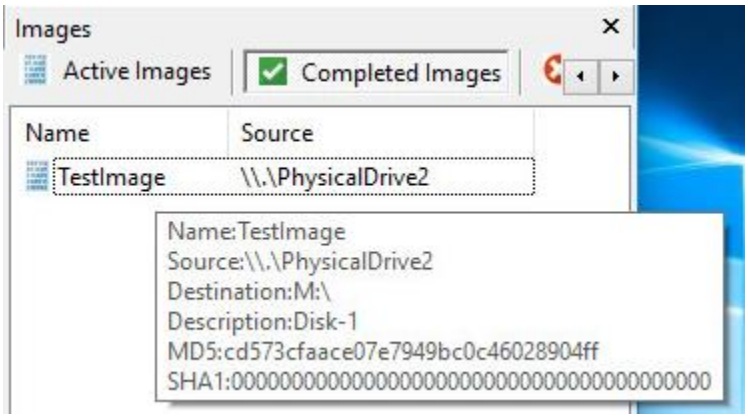
Once started the dialog will close and you'll be able to monitor the image using the Active Images panel (Use View->Images to display the Images panel if it is hidden). When the Image completes you will see it move to Completed Images.



Imaging started and running…

Step 9: Review the Completed Image

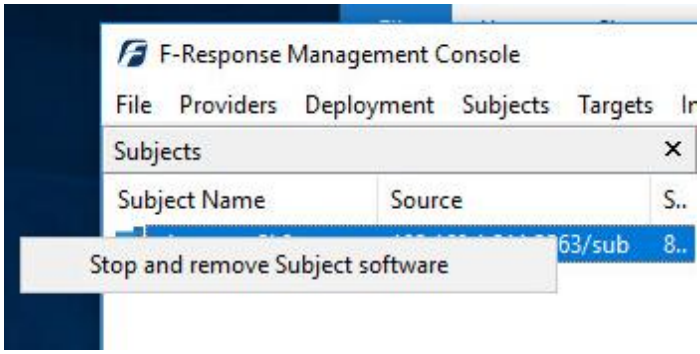
Right click on the completed image to access the Image Path, Log, and File List. These logs and listings contain details about the image, the image itself, and a file listing of files collected.



Reviewing the completed image.

Step 10: Removing F-Response from the remote machine

When you are finished using F-Response on the remote machine it can be readily removed using the Subject menu. First disconnect any active targets by either double-clicking on them, or using the Target->Detach Target menu item. Once all targets are detached, simply select the subject machine in the Subjects panel and right-click to select the "Stop and Remove Subject Software" to stop and remove all F-Response software from the remote machine.



Stopping and removing F-Response from the remote machine.

Troubleshooting

I can deploy F-Response, but when I try to start it I get an error telling me it could not connect to License Server?

Check if your license manager is bound to the correct local IP address on your analyst machine.

When I attempt to deploy F-Response using the console I cannot, even though I have valid credentials?

This is typically the case when attempting to connect to Windows machines that are not part of a Domain.

Your target machine is most likely a Windows machine not running in "Classic" mode for credential authentication. To switch the target machine to Classic you must open the Local Security Policy Administration Tool under Control Panel, Administrative Tools. You will then select Local Policies->Security Options and change the value of "Network Access: Sharing and Security Model for Local Accounts" to "Classic – Local Users authenticate as themselves". This is only necessary when using the Console to deploy F-Response to computers that are not part of a Windows Domain. If the target machine is a Windows 7 or newer Windows OS and not joined to a Domain (ie. Workgroup Member) then a key will need to be added to the registry of the target machine. You can manually create and add it the registry by following these steps:

To create your registry key, copy the following information into Notepad:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000001

Save this file as LocalAccountTokenFilterPolicy.reg, and then copy it to your target machine. Double click this file on the target machine to populate the registry with this key.

To remove follow the same steps as above this time with the following information:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000000