Knowledge Base Article 219

How to use a domain user account for NSI Remote WMI Agent v10

Date: March 10th, 2011

Problem:

You don't want to execute the Remote WMI service as Local System and want to use a domain user account with privileges.

1. Table of Contents

2. Create a domain user

Create a domain user that belongs to the domain users group.

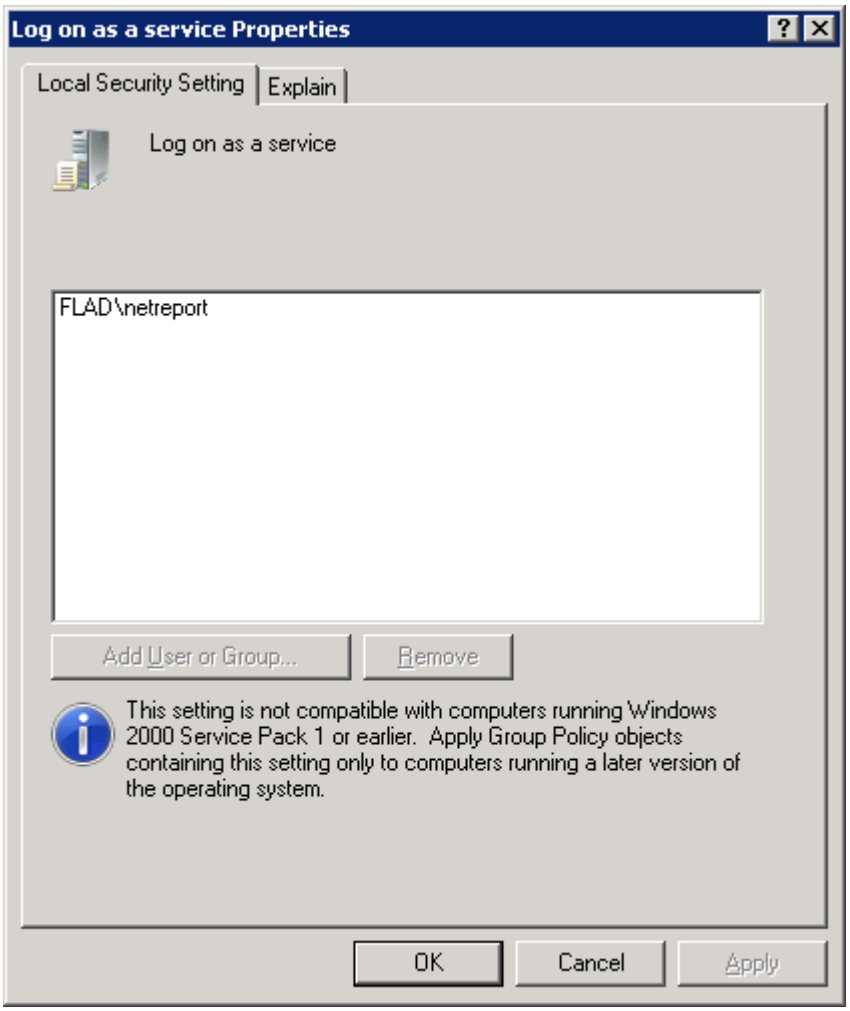
In the remainder of the document:

- Domain user is FLA\netreport.
- Settings have to be realized on the Windows machines which run the Remote WMI Agent.

3. Grant user privileges to execute the service

From **Administrative Tools**, start the Local **Security Policy**.
Then, in **Local Policies / User Rights Assignment**, add this user to entries below:

- Log on as a service

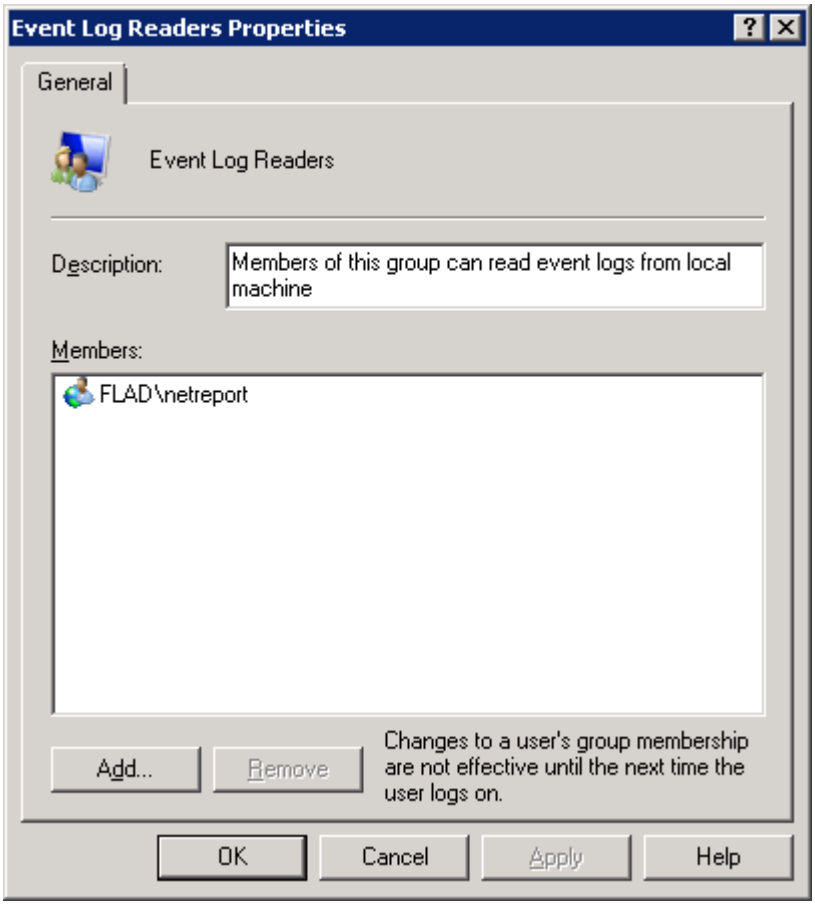


Contact us: E-mail: support@clickndecide.com **Tel:** +33 (0)4 67 84 48 00
Headquarters: Click&DECiDE 130, rue du Baptistou - 34980 St Gély du Fesc, France.
To contact your nearest Click&DECiDE partner, click here.

4. Grand WMI rights to this user

4.1. Windows 2008

Add this user to the local group “Event Log Readers” on each Windows 2008 machine you want to spy.



4.2. Windows 2003

1. Get the SID of the domain user.
A solution is to copy the text below in a file named `get_sid.vbs` on the domain controller.

```
Set objWMIService = GetObject("winmgmts://./root/cimv2")
Set objAccount = objWMIService.Get ("Win32_UserAccount.Name='netreport',Domain='FLAD'")
wscript.echo objAccount.SID
```

WARNING: Do not forget to replace the user Netreport and the domain name FLAD.

Then execute in a DOS box the following command > `cscript get_sid.vbs`

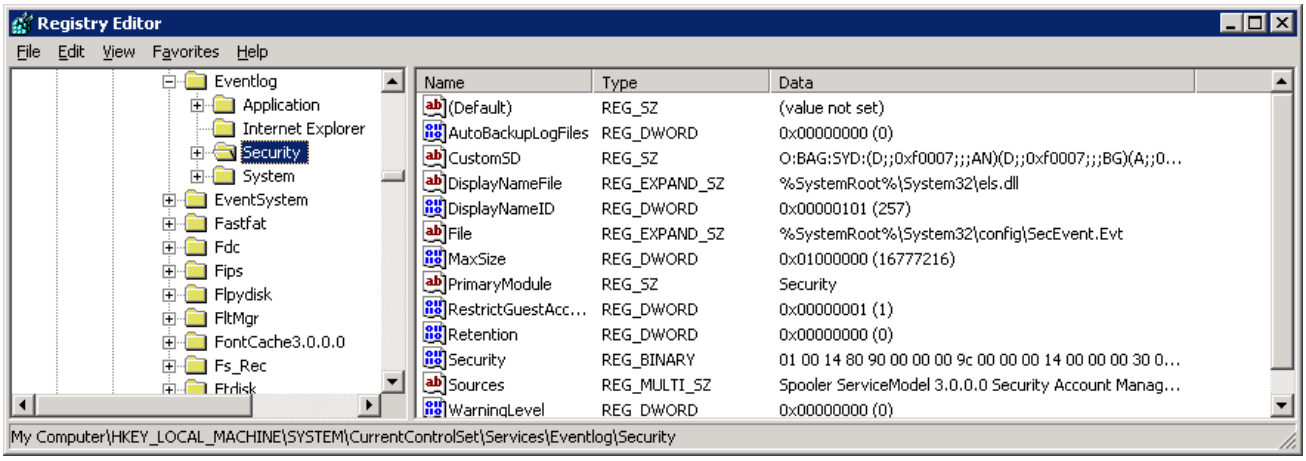
The SID should be displayed: `S-1-5-21-1817572523-641405561-3590760785-1106` per example.

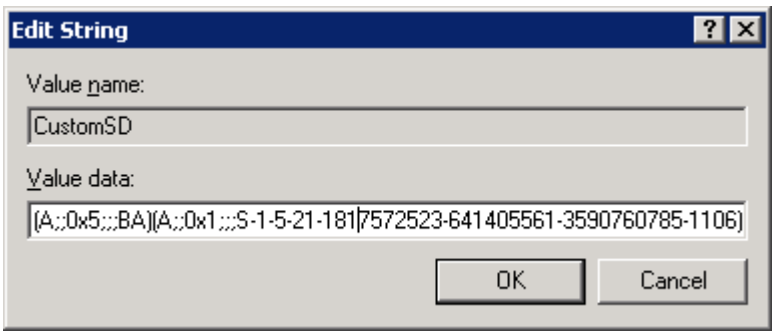
2. Then in the registry, edit the entry `CustomSD` at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security`

Add `(A;;0x1;;;S-1-5-21-1817572523-641405561-3590760785-1106)` at the end of the value.

Contact us: E-mail: support@clickndecide.com **Tel:** +33 (0)4 67 84 48 00
Headquarters: Click&DECiDE 130, rue du Baptistou - 34980 St Gély du Fesc, France.
To contact your nearest Click&DECiDE partner, click here.

WARNING: Do not forget to replace the SID with your value.



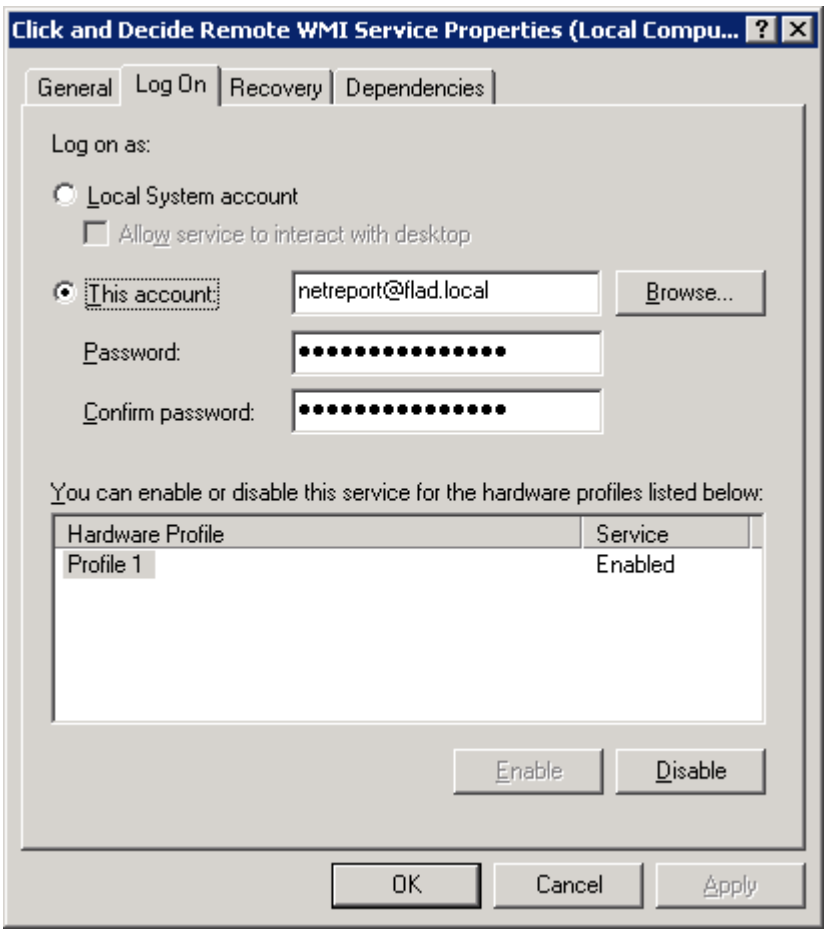


Contact us: E-mail: support@clickndecide.com **Tel:** +33 (0)4 67 84 48 00
Headquarters: Click&DECiDE 130, rue du Baptistou - 34980 St Gély du Fesc, France.
To contact your nearest Click&DECiDE partner, click here.

5. Install Remote WMI Agent Service

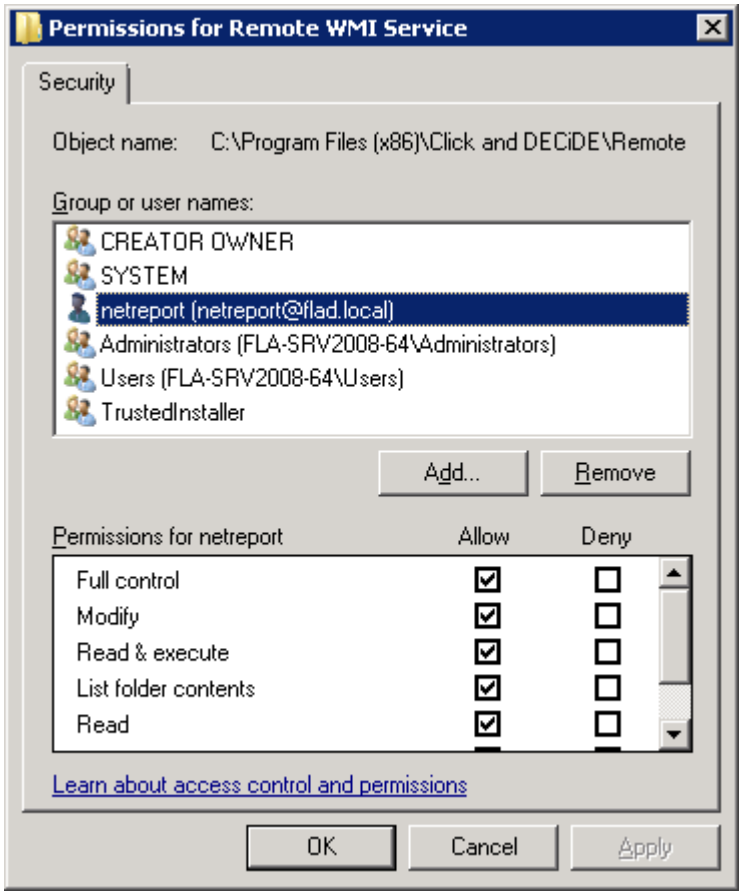
5.1. Version before 10.2.2

Run the standard setup of the Remote WMI Agent Service and then set the service to start with the user logon you want.



Grant full control for your domain user to the installation directory:

Contact us: E-mail: support@clickndecide.com **Tel:** +33 (0)4 67 84 48 00
Headquarters: Click&DECiDE 130, rue du Baptistou - 34980 St Gély du Fesc, France.
To contact your nearest Click&DECiDE partner, click here.



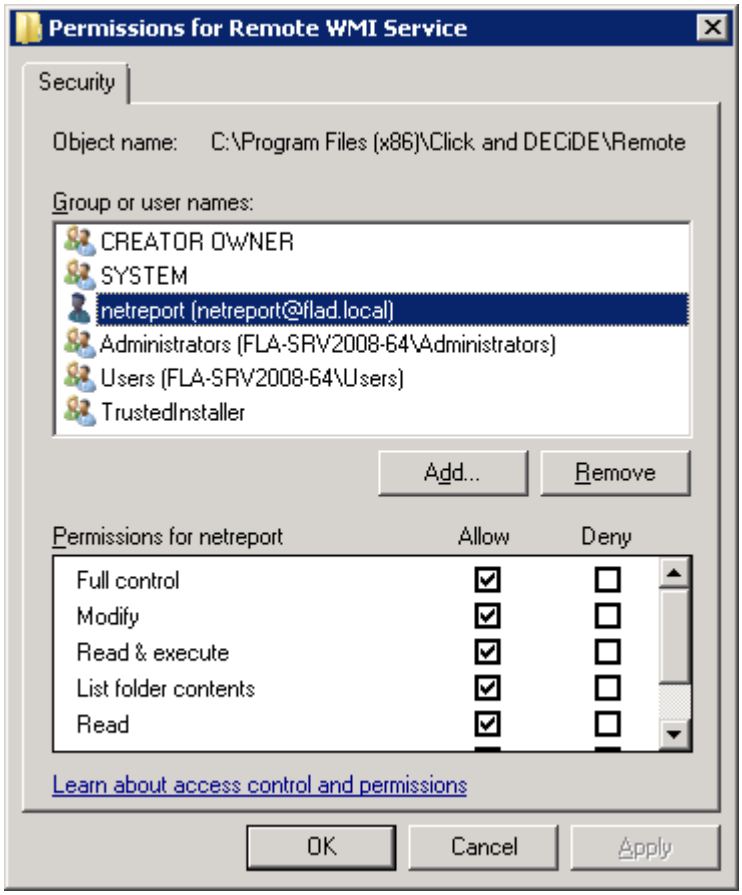
The service needs to be restarted.

5.2. For version 10.2.2 and upper, you can run the following command lines:

```
setup.exe /V"/qn NRRWMI_SVCUID=<domain>\<user> NRRWMI_SVCPWD=<password>
NRRWMI_SERVER=<nsi_server> NRRWMI_PORT=<port_number>"
```

WARNING: in version 10.2.2 and 10.2.3 the directory right is missing in the installation process. So, grant full control for your domain user to the installation directory as below. This has been fixed from 10.2.4 version.

Contact us: E-mail: support@clickndecide.com **Tel:** +33 (0)4 67 84 48 00
Headquarters: Click&DECiDE 130, rue du Baptistou - 34980 St Gély du Fesc, France.
To contact your nearest Click&DECiDE partner, click here.



The service needs to be started:

```
NET START NRRemoteWmiSvc
```


Contact us: E-mail: support@clickndecide.com **Tel:** +33 (0)4 67 84 48 00
Headquarters: Click&DECiDE 130, rue du Baptistou - 34980 St Gély du Fesc, France.
To contact your nearest Click&DECiDE partner, click here.