

# HowTo: Non Admin User

Wednesday, August 19, 2020 1:03 PM

[http://liwiki.ds.idsu.net/index.php?title=Running\\_as\\_a\\_Non-Administrator](http://liwiki.ds.idsu.net/index.php?title=Running_as_a_Non-Administrator)

Contents

[hide]

## [1 General Notes](#)

### [1.1 GeoPerformance / AriesoGEO components](#)

#### [1.1.1 Problem Identification Wizard](#)

#### [1.2 Running Service](#)

#### [1.3 Running Scheduled Task](#)

#### [1.4 URL Reservations](#)

## [2 Types of Admin](#)

## [3 GEO Loader Chain](#)

### [3.1 Setup steps performed by Administrator](#)

### [3.2 Folder Permissions](#)

### [3.3 GeoMonitor Service](#)

### [3.4 MongoDB Service](#)

### [3.5 FTPFileTransferer](#)

### [3.6 MapLoader.exe](#)

### [3.7 Zabbix Monitoring](#)

## [4 GEO Data Feeds Services](#)

### [4.1 ariesoGEO Data Feeds REST Service](#)

### [4.2 ariesoGEO Data Feeds Writer Service](#)

## [5 GeoWeb](#)

## [6 Small Cell Planing Module \(SCM\)](#)

## [7 GeoAuthenticationService](#)

## [8 Deploying lightning and pegasus under a non admin account](#)

### [8.1 GeoMonitoring \(Zabbix\)](#)

### [8.2 Setting Modify permissions on KafkaDataLoader input directories](#)

### [8.3 Removing a previous administrator account](#)

## [9 Deploying RabbitMQ as non-admin](#)

## General Notes

- The Administrator account should only be used for installation/configuration, including starting and stopping services. The Non-Admin account should be used for any routine running.
- Non-administrator users/groups should **NOT** be given *Full Control* permissions to folders. They should be given *Modify* permissions only. This allows them to read/write/modify files in those folders, but prevents them from doing actions such as further modifying folder permissions.

## GeoPerformance / AriesoGEO components

### *Problem Identification Wizard*

To run/update problem identification need grants:

- [For user which credentials was specified to run Task] Running Scheduled Task
- [For user which runs GEO] For files: "GeoConfig.xml", "GeoConfig.xml.bak", "GeoConfig.xml.new" in "C:\ProgramData\ariesoGEO\" folder. Required rights: Read, Write, Modify, Read & Execute.

When you want to schedule "Problem Identification" then you need grant permissions for the user/group which will be used for running task:

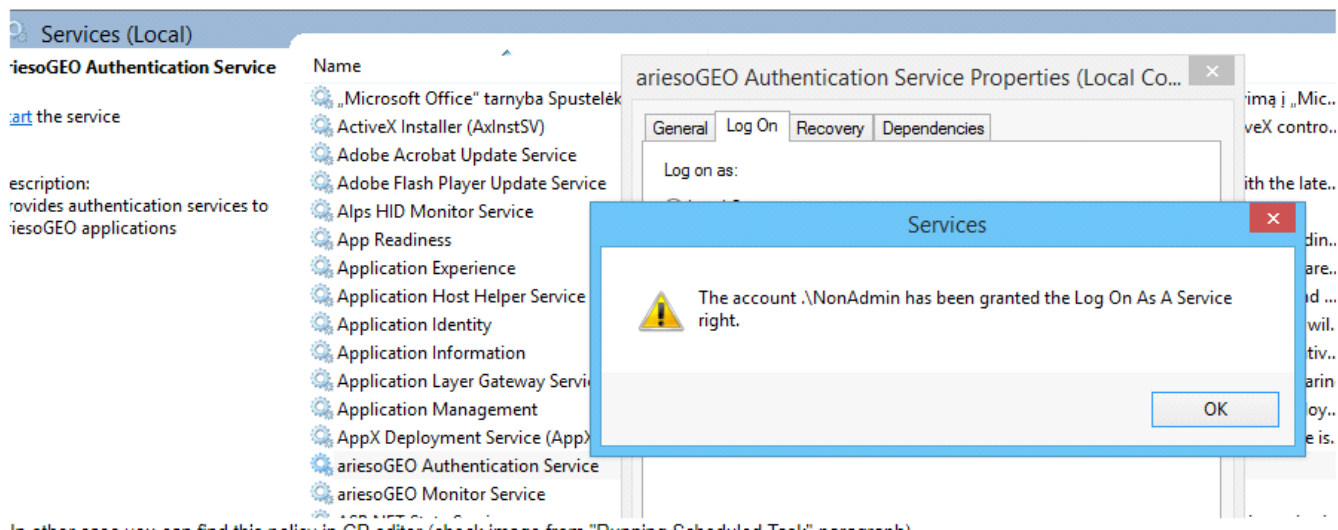
```
.\subinacl.exe /onlyfile "C:\ProgramData\ariesoGEO\GeoConfig.xml" /grant=NonAdmin=RXECW
.\subinacl.exe /onlyfile "C:\ProgramData\ariesoGEO\GeoConfig.xml.bak"
/grant=NonAdmin=RXECW
.\subinacl.exe /onlyfile "C:\ProgramData\ariesoGEO\GeoConfig.xml.new"
/grant=NonAdmin=RXECW
```

## Running Service

To run any service non admin user has to have these grants in Group Policy:

- Log on as a service

This policy is mostly added automatically (if you have rights to modify GP) when you try to run/Lon on service as a user which yet does not have that right. So popup will appear and you need click OK:

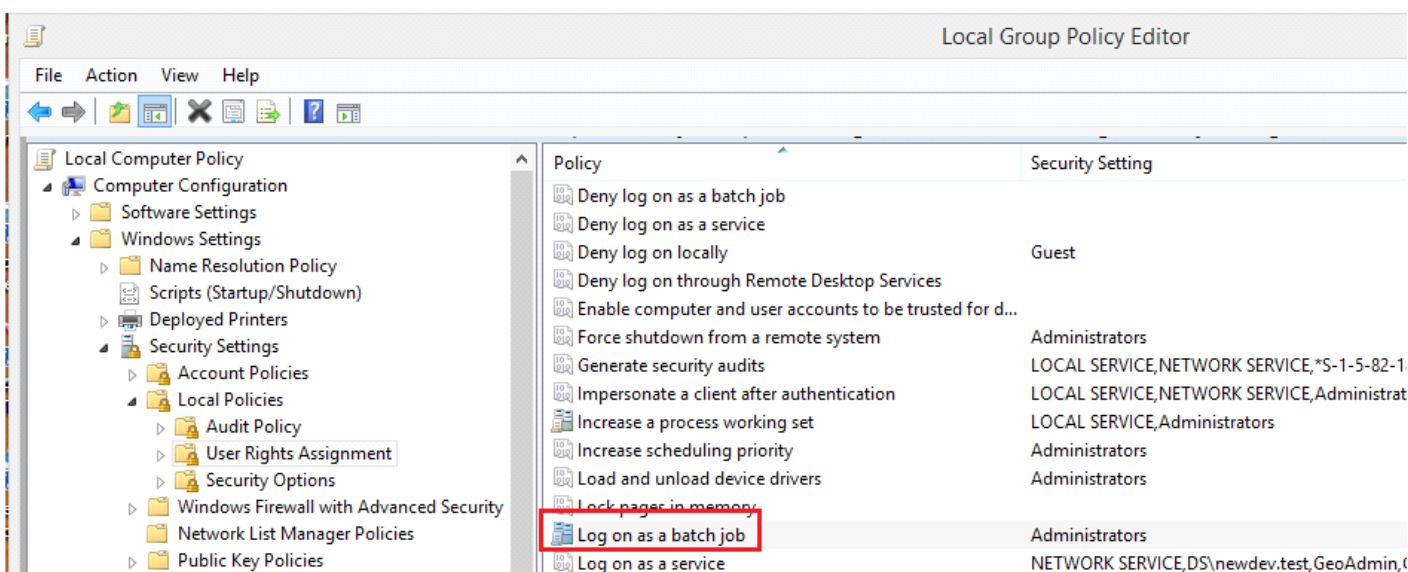


In other case you can find this policy in GP editor (check image from "Running Scheduled Task" paragraph).

### Running Scheduled Task

To run scheduled reports non admin user has to have these grants in Group Policy:

- Log on as a batch job:



If you do not have this grant then you will get error like this:

Task Scheduler failed to start - Additional Data: Error Value: 2147943785

Check <https://social.technet.microsoft.com/Forums/en-US/68019b24-78a5-4db0-a150-ada921930924/task-scheduler-failed-to-start-additional-data-error-value-2147943785?forum=winservergen> for more details.

### URL Reservations

Some of our applications require the ability to open specific ports. When running as an administrator this was transparent however when running as a non-administrator a port needs to be specifically reserved for that user to use.

As noted for specific applications, below, this is done using this command (run from an admin command prompt):

```
netsh http add urlacl url=http://+:PORT/ user=DOMAIN\USERNAME
```

Once this port is registered for that user, no other user is able to use it. On upgrading, or if you want to change the user that's running our services, then you need to remove the existing reservation, then add it again for the new user.

To view the current URL Reservation setting for a specific port:

```
netsh http show urlacl url=http://+:PORT/
```

To remove the reservation:

```
netsh http delete urlacl url=http://+:PORT/
```

## Types of Admin

NOTE: Through these instructions it is important to keep a clear distinction between the two types of Admin used:

**Windows-Level Administrator:** A Windows user who is defined as being a member of the **Administrators** group in *Computer Management > Users and Groups: Properties > Member Of*

This is a user with total access to all parts of Windows, (including GEO), and in a large corporate network, all parts of that network too. It is an operating system feature and not created by Viavi.

**Geo-Level Admin:** A Windows user who is defined as a being member of the **GeoAdminGroup** group in *Computer Management > Users and Groups: Properties > Member Of*

This is a user granted access to various high-level functions in GEO, including the GEO Administrator Console, various Loader Chain and DB elements, and unencrypted IMSI/IMEI (SPI) Data. This is controlled through the **RoleManager.config** file, and is purely a function of the GEO platform, having no bearing on Windows or other software.

Any given Windows user may be either, both or neither. Going forward, the aim is for a customer to only require Windows-Level Administrator access to install and first-time configure GEO.

## GEO Loader Chain

### Setup steps performed by Administrator

When Geo Performance is installed the following files need to be configured by the Administrator or Administrator level privilege

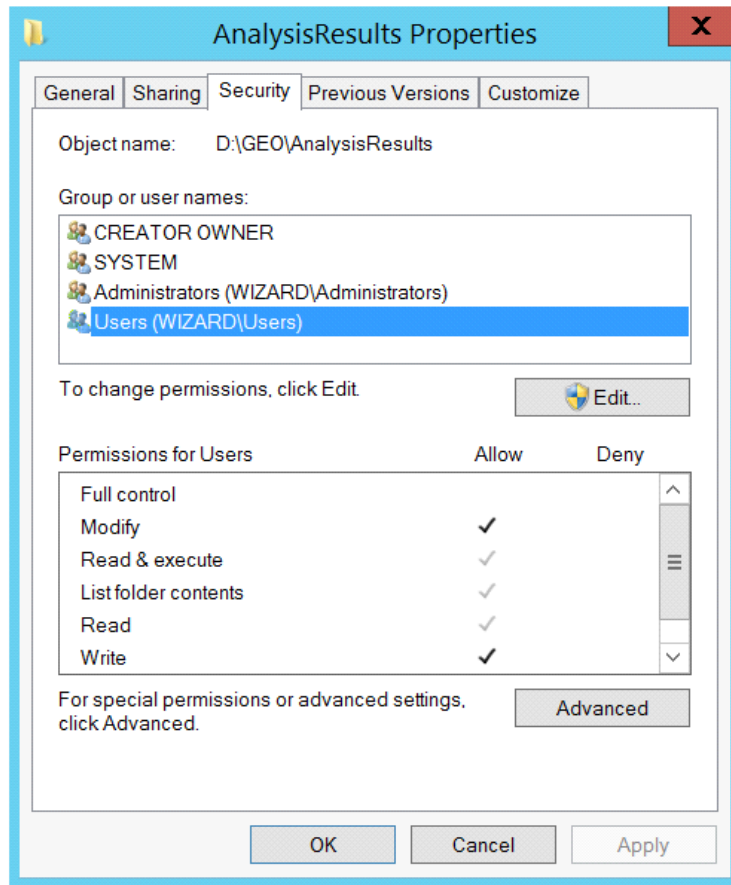
- mongod.cfg for mongo
- regexp.xml document used by file archiver
- GeoDataLoader.config and GeoMonitor.config

### Folder Permissions

1. Add *Modify* permissions to the Non-Admin user on *C:\ariesoGEO Logs*
2. Find all directories defined in the *GeoMonitor.Config* and *GeoDataLoader.Config* files, and Add *Modify* permissions to the Non-Admin user on each top-level directory found
3. Run setgeoconfig in dos and check what this value is set to 'AnalysisResultsDirectory', eg

AnalysisResultsDirectory=D:\GEO\AnalysisResults

So D:\GEO\AnalysisResults folder needs to be set for non Admin accounts to have Modify, Read and Write (user group)



## GeoMonitor Service

**NOTE: These steps must be carried out (as Administrator) every time Geo is upgraded.**

Requires [Running as a Non-Administrator - Running Service](#).

To Allow running GeoMonitor as a Non-Admin user:

- Download the 'subinac1' tool from <https://www.microsoft.com/en-us/download/details.aspx?id=23510>
  - (Added a copy of this installer to the Release Build folder - customer generally does not have/allow internet access on these machines.)
- Install it. Then run the following commands using an Administrator command-prompt under 'C:\Program Files (x86)\Windows Resource Kits\Tools\':
- Allow the Non-Admin user to get a handle of GeoMonitoringService, by assigning *GENERIC\_READ* right to 'SCMManager':

```
subinac1 /service scmmanager /grant=<Non-Admin user name>=R
```

(I had an error, saying 'scmanager - OpenService Error : 1060 The specified service does not exist as an installed service.' It all worked despite the error.)

- Allow to change shutdown timeout for the 'ariesoGEOMonitorService' service, by assigning it *SERVICE\_CHANGE\_CONFIG* (C), *SERVICE\_START* (T) and *SERVICE\_STOP* (O) rights:

```
subinac1 /service ariesoGEOMonitorService /grant=<Non-Admin user name>=CTO
```

Change Log On of the 'ariesoGEOMonitorService' to use the Non-Admin user (see details under 'ariesoGEO Data Feeds REST Service' below)

- MongoDB
- ```
subinac1 /service MongoDB /grant=<Non-Admin user name>=CTO
```

Start the 'ariesoGEOMonitorService' as normal

(More in-depth details on the **subinac1** tool here: <https://support.microsoft.com/en-gb/help/288129/how-to-grant-users-rights-to-manage-services-in-windows-2000>)

## MongoDB Service

1. Give *Modify* permissions to the Non-Admin user on C:\ariesoGEO Logs.
2. Ensure the 'Normal' and 'Error' directories exist under C:\ariesoGEO Logs. If not - create them, otherwise MongoDB service will fail to start with an 1053 error.
3. Ensure your MongoDB's database directory exists (as defined in the C:\Program Files\Arieso\Shared\MongoDB\mongod.cfg file, under the 'dbPath' entry).

4. Give *Modify* permissions to the Non-Admin user on your MongoDB's database folder.
5. Change the Log On of the MongoDB Windows Service to use the Non-Admin user.
6. Start the MongoDB Windows Service.

If [LTE - Per eNodeB Metrics](#) is used, you will need to give the *EnodebListLoader.exe* process (which normally runs by GeoMonitor) access to the eNodeB-List file: Give 'Modify' permissions to the Non-Admin user on the directory containing the eNodeB-List (by default - `C:\ProgramData\ariesoGEO\eNodeBList\`)

## FTPFileTransferer

For a Non-Admin controlled Loader to successfully import cell trace files into the Loader Chain from a remote FTP Server it must be granted access to that source FTP server. It needs Read **and** Write access, to allow the DeleteRemote functionality to work.

- On the Source FTP machine, create a new Non-Admin user.
- On the Source FTP machine, use the Administrative Tools > Internet Information Services Manager to Edit Permissions for the FTP Home folder, adding Modify access to the new Non-Admin user of that machine.
- On the Loader machine, change the appropriate values in the FtpFileTransferer Config file (typically `ftptrans.config`):
  - `<Username>` </Username> - This should NOT be Administrator - set it to the Non-Admin account created on the FTP machine.
  - `<Password>` </Password> - Set to the matching password for the Non-Admin account.

## MapLoader.exe

For a Non-Admin user to run the MapLoader.exe, the input folder and output folder should be under the Geo subfolders which should have access rights.

## Zabbix Monitoring

The ZabbixAgent service requires the ability to create performance counters therefore the non-admin user must be added to the *Performance Monitor Users* Windows group. Go to *Computer Management* -> *Groups* and add the non-admin user into this group. Arieso GeoMonitoring Plugins Runner and Arieso GeoMonitoring Proxy services need no specific changes for non-administrators.

Additionally the folder that *NonLightningMonitoring* is copied to requires **Modify** permissions.

## GEO Data Feeds Services

### ariesoGEO Data Feeds REST Service

- If [Authentication](#) is used, ensure that the user who's credentials are used is a member of the group specified by the relevant 'ActiveDirectoryGroup' entry in the 'RoleManager.config' file. For example, if your 'RoleManager.config' file contains `Domain="Local"` and `ActiveDirectoryGroup="Users"`, you will need to verify that the user is a member of the "Users" group on the machine hosting the *ariesoGEOAuthenticationService*.

Before starting the service, set up the following:

- Run the following command from an admin command prompt, swapping the Port number (3579 is the default) and the DOMAIN and USERNAME params accordingly

```
netsh http add urlacl url=http://+:3579/ user=DOMAIN\USERNAME
```

- Give *Modify* permissions to the `C:\ariesoGEO Logs` folder to allow log file content to be written
- Start the service as normal - the log files should indicate whether it has started successfully

If you are running the service as installed by the *ariesoGeoDataFeedsRestServiceInstaller\_x64* installer:

- Open the Windows -> Services dialog
- Right-click on the *ariesoGEO Data Feeds REST Service* service
- On the *Log On* tab, set the account to be the non-administrator username and password
- Start the service as normal - the log files should indicate whether it has started successfully

### ariesoGEO Data Feeds Writer Service

This service is only provided by the *ariesoGeoDataFeedsRestServiceInstaller\_x64* installer.

Before starting the service, set up the following:

- Run the following command from an admin command prompt, swapping the Port number (3575 is the default) and the DOMAIN and USERNAME params accordingly

```
netsh http add urlacl url=http://+:3575/ user=DOMAIN\USERNAME
```

- Give *Modify* permissions to the `C:\ariesoGEO Logs` folder to allow log file content to be written
- Open the Windows -> Services dialog
- Right-click on the *ariesoGEO Data Feeds Writer Service* service
- On the *Log On* tab, set the account to be the non-administrator username and password
- Start the service as normal - the log files should indicate whether it has started successfully

## GeoWeb

Requires [Running as a Non-Administrator - Running Scheduled Task](#).

The Non-Admin Account running the *ariesoGeoMonitorService* will need Modify permission on:

- `\WebAnalysisResults`
- `\AnalysisResults`

(This is easiest done by ensuring they exist in the Loader folder and so inherit permissions. The SetGeoConfig options for the paths should be set accordingly.)

The Non-Admin Account running the ariesoGeoMonitorService must be granted permissions on the GeoWeb http namespace:

Open a Command Window on the machine hosting the GeoWeb site (typically the App Server) and run the following, as Windows-Level Administrator. Note the different port numbers, each must be enabled (GeoWebDataServer and the Desktop and Web GeoResultsCaches):

```
netsh http add urlacl url=http://+:9002/ user=<DOMAIN>\<USERNAME>
netsh http add urlacl url=http://+:9003/ user=<DOMAIN>\<USERNAME>
netsh http add urlacl url=http://+:9007/ user=<DOMAIN>\<USERNAME>
```

e.g:

```
netsh http add urlacl url=http://+:9002/ user=GEOL7-APP1\GeoNonAdmin
netsh http add urlacl url=http://+:9003/ user=GEOL7-APP1\GeoNonAdmin
netsh http add urlacl url=http://+:9007/ user=GEOL7-APP1\GeoNonAdmin
```

The following is displayed is successful:

URL reservation successfully added

Upon ariesoGeoMonitorService restart, Publish to Web should now work under a Non-Admin Monitor Service.

### Small Cell Planing Module (SCM)

1. Give Modify permissions to the Non-Admin user on C:\ariesoGEO Logs.
2. Ensure the 'Normal' and 'Error' directories exist under C:\ariesoGEO Logs. If not - create them, otherwise MongoDB service will fail to start with an 1053 error.
3. The Non-Admin Account must be granted permissions on the SCM http namespace:

Open a Command Window on the machine hosting the SCM site (typically the App Server) and run the following, as Windows-Level Administrator. Note port must be specified which will be used for SCM site (mostly we use port "8080"):

```
netsh http add urlacl url=http://+:<USED_PORT>/ user=<NonAdminUser>
```

Example:

```
netsh http add urlacl url=http://+:8080/ user=DS\newdev.test
```

### GeoAuthenticationService

The GeoAuthenticationService is required by DataFeeds, but not GEOperformance or the Loader Chain: See more here: [Authentication Setup for Data Feeds](#)

Similar to above, the GeoAuthenticationService requires the Non-Admin User to be granted permission on the http server:

```
netsh http add urlacl url=http://+:7655/GeoAuthenticationService/
user=<DOMAIN>\<USERNAME>
```

### Deploying lightning and pegasus under a non admin account

To deploy as a non-admin local user set the ServiceUserGroup in the cluster configuration to "Users", as per the following example

```
$ConfigurationData =
@{
    AllNodes =
    @(
        @{ NodeName = "*";
            AdminUser = 'Administrator';
            AdminPassword = 'Network123!';
            ServiceUser = 'hadoop';
            ServiceUserGroup = "Users";
            ServicePassword = 'Network123!';
        }
        @{ NodeName = "127.44.18.101"; Group = "Thor";}
    )
}
```

NOTE: If the ServiceUserGroup is not specified, the user group defaults to "Administrators". NOTE: Domain users are not created as part of the deployment steps and must be setup ahead of deployment.

### GeoMonitoring (Zabbix)

The 3 services associated with GeoMonitoring (ZabbixAgent, ariesoGEO Lightning Monitoring, ariesoGEO Lightning Monitoring Proxy) will also all be started using the ServiceUser. The ZabbixAgent service requires the user to be in the *Performance Monitor Users* Windows group. This is automatically done by the deployment scripts and should require no special action, however it's noted here for reference.

If deploying with a domain user, the user will not be automatically added to the Performance Monitor Users group. This must be done via group policy or manually on the loaders.

### Setting Modify permissions on KafkaDataLoader input directories

Each cluster node that is assigned an Application Role of "KafkaDataLoader", should be given *Modify* permissions on any input directory defined in the cluster configuration's 'KafkaDataLoaderInputDirectory':

```
KafkaDataLoaderInputDirectory="D: \Loader\input", "D: \Test\AnotherInput";
```

This will be done automatically as part of a Lightning deployment, as long as the input directories exist on each relevant node. If the input directories don't exist when Lightning is deployed, you will have to grant the *Modify* permissions manually.

### Removing a previous administrator account

If you have previously deployed using an administrator account you will need to remove the user before you redeploy otherwise the user will still retain administrator privileges.

Run:

```
DeploymentScripts\RemoveServiceUser.ps1
```

NOTE: This will not remove a domain level user.