



Running UFM Server Software

Table of contents

[Running UFM Server Software in Management Mode](#)

[Running UFM Software in Monitoring Mode](#)

[Running UFM Software in High Availability Mode](#)

[HTTP/HTTPS Configuration](#)

[UFM Internal Web Server Configuration](#)

[User Authentication](#)

[UFM Authentication Server](#)

[Configurations of the UFM Authentication Server](#)

[Azure AD Authentication](#)

[Register UFM in Azure AD Portal](#)

[Enable Azure Authentication From UFM](#)

[Azure Authentication Login Page](#)

[Kerberos Authentication](#)

[Licensing](#)

[Showing UFM Processes Status](#)

List of Figures

Figure 0. Procedure Heading Icon Version 1 Modificationdate
1716899067970 Api V2

Figure 1. Monitoring Mode Icon Version 1 Modificationdate
1716899074913 Api V2

Figure 2. Image2023 7 26 7 16 15 Version 1 Modificationdate
1716899084347 Api V2

Figure 3. Azureauth2 Version 1 Modificationdate 1716899082930 Api V2

Figure 4. Azureauth3 Version 1 Modificationdate 1716899081533 Api V2

Figure 5. Azureauth4 Version 1 Modificationdate 1716899080893 Api V2

Figure 6. Azureauth5 Version 1 Modificationdate 1716899080280 Api V2

Figure 7. Azureauth6 Version 1 Modificationdate 1716899079460 Api V2

Figure 8. Image2023 7 26 7 28 25 Version 1 Modificationdate
1716899085627 Api V2

Figure 9. Image2023 7 26 7 27 55 Version 1 Modificationdate
1716899084787 Api V2

Figure 10. Azureauth9 Version 1 Modificationdate 1716899077050 Api
V2

Figure 11. MSFT Version 1 Modificationdate 1716899066270 Api V2

Figure 12. UFM STATUS1 Version 1 Modificationdate 1716899075660
Api V2

Figure 13. UFM STATUS2 Version 1 Modificationdate 1716899076253
Api V2

Before running UFM:

- Perform [Initial Configuration](#)
- Ensure that all ports used by the UFM server for internal and external communication are open and available. For the list of ports, see [Used Ports](#). You can run the UFM server software in the following modes:
- [Running UFM Server Software in Management Mode](#)
- [Running UFM Software in Monitoring Mode](#)
- [Running UFM Software in High Availability Mode](#)
- High Availability with failover to an external SM

i Note

In Management or High Availability mode, ensure that all Subnet Managers in the fabric are disabled *before* running UFM. Any remaining active Subnet Managers will prevent UFM from running.

Running UFM Server Software in Management Mode

After installing, run the UFM Server by invoking:

```
systemctl start ufm-enterprise.service
```

i Note

`/etc/init.d/ufmd` - Available for backward compatibility.

Log files are located under `/opt/ufm/files/log` (the links to log files are in `/opt/ufm/log`).

Running UFM Software in Monitoring Mode

Run UFM in Monitoring mode while running concurrent instances of Subnet Manager on NVIDIA switches. Monitoring and event management capabilities are enabled in this mode. UFM non-monitoring features such as provisioning and performance optimization are disabled in this mode.

The following table describes whether features are enabled or disabled in Monitoring mode.

Features Enabled/Disabled in Monitoring Mode


Feature	Enabled/Disabled in Monitoring Mode
Fabric Discovery	Enabled
Topology Map	Enabled
Fabric Dashboard	Enabled
Fabric Monitoring	Enabled
Alerts and Thresholds (inc. SNMP traps)	Enabled
Fabric Logical Model	Enabled
Subnet Manager and plugins	Disabled
Subnet Manager Configuration	Disabled
Automatic Fabric Partitioning	Disabled
Central Device Management	Disabled
Quality of Service	Disabled
Failover (High Availability mode)	Disabled
Traffic Aware Routing Algorithm	Disabled
Device Management	Disabled
Integration with Schedulers	Disabled
Unhealthy Ports	Disabled

In Monitoring mode, UFM periodically discovers the fabric and updates the topology maps and database.

For Monitoring mode, connect UFM to the fabric using port ib0 only. The fabric must have a subnet manager (SM) running on it (on another UFM, HBSM, or switch SM).

 **Note**

When UFM is running in Monitoring mode, the internal OpenSM is not sensitive to changes in OpenSM configuration (opensm.conf).

 **Note**

When running in Monitoring mode, the following parameters are automatically

overwritten in the `/opt/ufm/files/conf/opensm/opensm_mon.conf` file on startup:

- `event_plugin_name osmufmpi`
- `event_plugin_options --vendinfo -m 0`

Any other configuration is not valid for Monitoring mode.

To run in Monitoring mode:



1. In the `/opt/ufm/conf/gv.cfg` configuration file:

- Set **monitoring_mode** to `yes`
- If required, change **mon_mode_discovery_period** (the default is 60 seconds)

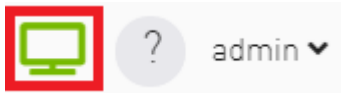
- Set **reset_mode** to no_reset

We recommend this setting when running multiple instances of UFM so that each port counter is not reset by different UFM instances. For more information, see [Resetting Physical Port Counters](#).

2. Restart the UFM Server.

The Running mode is set to Monitoring, and the frequency of fabric discovery is updated according to the setting of **mon_mode_discovery_period**.

Note that a monitor icon will appear at the top of the navigation bar indicating that monitoring mode is enabled:



Running UFM Software in High Availability Mode

On the Master server, run the UFM Server by invoking:

```
ufm_ha_cluster start
```

You can specify additional command options for the ufmha service.

ufm_ha_cluster Command Options

Command	Description
start	Starts UFM HA cluster.
stop	Stops UFM HA cluster.
failover	Initiates failover (change mastership from local server to remote server).
takeover	Initiates takeover (change mastership from remote server to local server).
status	Shows current HA cluster status.
cleanup	Cleans the HA configurations on this node.
help	Displays help text.

HTTP/HTTPS Configuration

By default, UFM is configured to work with the secured HTTPS protocol.

After installation, the user can change the the Web Server configuration to communicate in secure (HTTPS) or non-secure (HTTP) protocol.

For changing the communication protocol, use the following parameter under the [Server] section in the `gv.cfg` file:

- `ws_protocol = https`

Changes will take effect after restarting UFM.

For further information, please refer to the [Launching a UFM Web UI Session](#) available in the [UFM Quick Start Guide](#).

UFM Internal Web Server Configuration

UFM uses Apache as the main Web Server for client external access. The UFM uses an internal web server process to where the Apache forwards the incoming requests.

By default, the internal web server listens to the local host interface (127.0.0.1) on port 8000.

For changing the listening local interface or port, use the following parameters under the [Server] section in the `gv.cfg` file:

- `rest_interface = 127.0.0.1`
- `rest_port = 8000`

Changes will take effect after restarting UFM.

User Authentication

UFM User Authentication is based on standard Apache User Authentication. Each Web Service client application must authenticate against the UFM server to gain access to the system.

The UFM software comes with one predefined user:

- Username: admin
- Password: 123456

You can add, delete, or update users via [User Management Tab](#).

UFM Authentication Server

The UFM Authentication Server, a centralized HTTP server, is responsible for managing various authentication methods supported by UFM.

Configurations of the UFM Authentication Server

The UFM Authentication Server is designed to be configurable and is initially turned off by default. This means that existing authentication methods are managed either by the native Apache functionality (such as Basic, Session, and Client Certificate authentication) or at the UFM level (including Token-Based authentication and Proxy Authentication).

Enabling the UFM Authentication Server provides a centralized service that oversees all supported authentication methods within a single service, consolidating them under a unified authentication API.

Apache utilizes the authentication server's APIs to determine a user's authentication status.

To enable the UFM Authentication Server, refer to [Enabling UFM Authentication Server](#).

All activities of the UFM Authentication Server are logged in the `authentication_service.log` file, located at `/opt/ufm/files/log`.

Azure AD Authentication

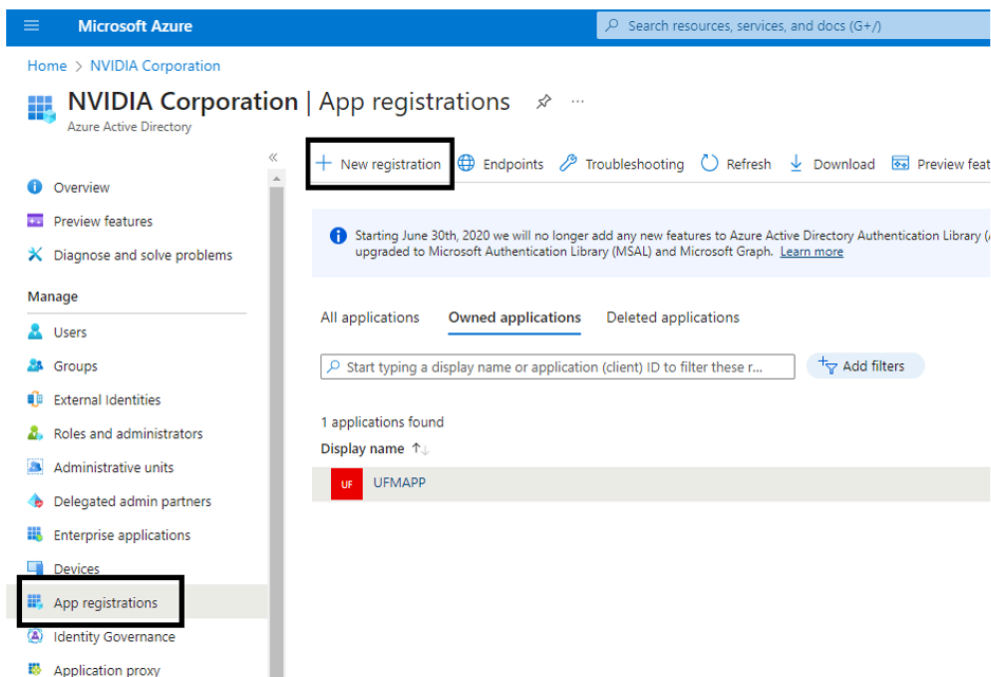
Microsoft Azure Authentication is a service provided by Microsoft Azure, the cloud computing platform of Microsoft. It is designed to provide secure access control and authentication for applications and services hosted on Azure.

UFM supports Authentication using Azure Active Directory, and to do so, you need to follow the following steps:

Register UFM in Azure AD Portal

To log in via Azure, UFM must be registered in the Azure portal using the following steps:

1. Log in to [Azure Portal](#), then click "**Azure Active Directory**" in the side menu.
2. If you have access to more than one tenant, select your account in the upper right. Set your session to the Azure AD tenant you wish to use.
3. Under "**Manage**" in the side menu, click App Registrations > New Registration.



4. Provide the application details:

1. **Name:** Enter a descriptive name.
2. **Supported account types:** Account types that are allowed to login and use the registered application.

3. **Redirect URL:** select the app type **Web**, and Add the following redirect URL `https:// /auth/login`

Home > NVIDIA Corporation | App registrations >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?

Accounts in this organizational directory only (NVIDIA Corporation only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

[Register](#)

Then, click **Register**. The app's **Overview** page opens.

5. Under **Manage** in the side menu, click **Certificates & Secrets** > New client secret.

Add a client secret

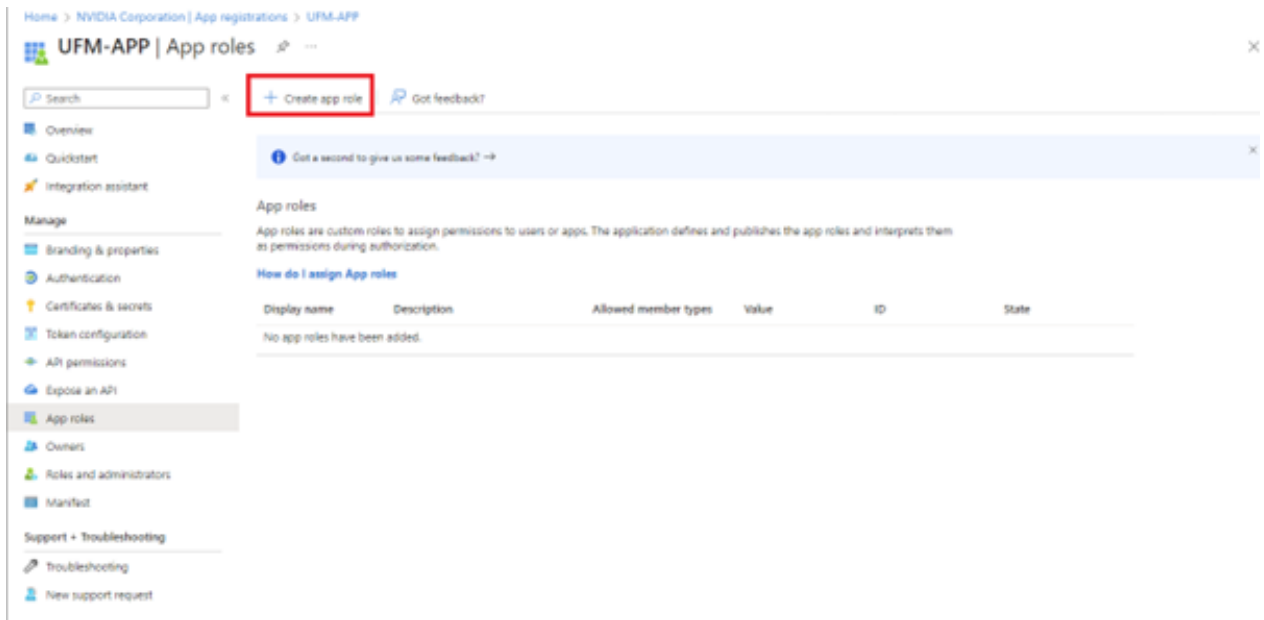


Description	<input type="text" value="UFM_APP_sec"/>
Expires	<input type="text" value="Recommended: 180 days (6 months)"/> ▼

Provide a description for the client secret and set an expiration time, then click **"Add."**

6. Copy the client secret key value which will be needed to configure the UFM with Azure AD (Please note that the value of the generated secret will be hidden and will not be able to be copied/read after you leave the page.

Under **"Manage"** in the side menu, click App roles > Create app role.



7. Provide the role details. Please note that the role value must be a valid UFM role; otherwise, the login will fail.

Create app role ✕

Display name * ⓘ

System_Admin ✓

Allowed member types * ⓘ

Users/Groups
 Applications
 Both (Users/Groups + Applications)

Value * ⓘ

System_Admin ✓

Description * ⓘ

System_Admin

Do you want to enable this app role? ⓘ

8. Assign the created role to the user. Follow the below steps:

App roles

App roles are custom roles to assign permissions to users or apps. The application determines permissions during authorization.

[How do I assign App roles](#) 1

Display name	Description	Allowed member ty...	Value
System_Admin	System_Admin	Users/Groups,Applicat...	Syste

Assigning app roles ✕

App roles for Users/Groups

Assign app roles with 'User' allowed member types in **Enterprise** applications or in Microsoft Graph APIs.

[Learn more about how to assign App roles for Users/Groups](#)

App roles for applications

Assign app roles with 'Applications' allowed member types in API permissions blade.

Properties


UF Name ⓘ Copy to clipboard
UFM-APP


Application ID ⓘ
0d5e6cda-9144-47a2-b685-...


Object ID ⓘ
dd2a68d5-a3e0-45e3-9c1c-...

Getting Started

3

**1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)

**2. Provision User Accounts**
You'll need to create user accounts in the application
[Learn more](#)

**3. Self service**
Enable users to request access to the application using their Azure AD credentials
[Get started](#)

+ Add user/group 4 Edit assignment Remove Update credentials | Columns | Got feedback?

i The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this. →

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registration](#).

First 200 shown, to search all users & gro...

Display Name	Object Type	Role assigned
No application assignments found		

Home > UFM-APP | App roles > UFM-APP | Users and groups >

Add Assignment ...

NVIDIA Corporation

Users and groups

1 user selected.

Select a role *

System_Admin

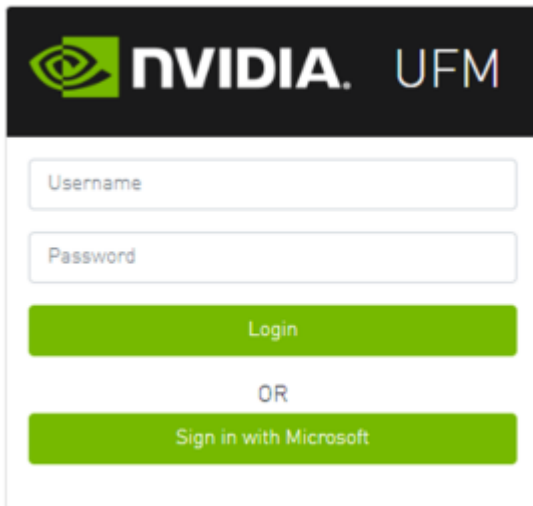
9. Click on "**Overview**" in the side menu to view the application information, such as tenant ID, client ID, and other details.

Enable Azure Authentication From UFM

Azure authentication is disabled by default. To enable it, please refer to [Enabling Azure AD Authentication](#).

Azure Authentication Login Page

After enabling and configuring Azure AD authentication, an additional button will appear on the primary UFM login page labeled 'Sign In with Microsoft,' which will lead to the main Microsoft sign-in page:

The image shows a login interface for NVIDIA UFM. At the top, there is a black header with the NVIDIA logo and the text 'NVIDIA. UFM'. Below the header, there are two input fields: 'Username' and 'Password'. Underneath these fields is a green button labeled 'Login'. Below the 'Login' button is the text 'OR' in a smaller font. At the bottom, there is another green button labeled 'Sign in with Microsoft'.

Kerberos Authentication

Kerberos is a network authentication protocol designed to provide strong authentication for client-server applications by using secret-key cryptography.

The Kerberos protocol works on the basis of tickets, it helps ensure that communication between various entities in a network is secure. It uses symmetric-key cryptography, which means both the client and servers share secret keys for encrypting and decrypting communication.

To enable Kerberos Authentication, refer to [Enabling Kerberos Authentication](#).

Setting Up Kerberos Server Machine

To set up a system as a Kerberos server, perform the following:

1. Install the required packages:

```
#Redhat
sudo yum install krb5-libs krb5-server
# Ubuntu
sudo apt-get install krb5-kdc krb5-admin-server
```

2. Edit the Kerberos configuration file `'/etc/krb5.conf'` to reflect your realm, domain and other settings:


```
[libdefaults]
    default_realm = YOUR-REALM

[realms]
    YOUR-REALM = {
        kdc = your-kdc-server
        admin_server = your-admin-server
    }

[domain_realm]
    your-domain = YOUR-REALM
    your-domain = YOUR-REALM
```

3. Use the `kdb5_util` command to create the Kerberos database:

```
kdb5_util create -r YOUR-REALM -s
```

4. Add administrative principals:

```
Kadmin.local addprinc -randkey HTTP/YOUR-HOST-NAME@YOUR-REALM
```

5. Start KDC and Kadmin services:

```
sudo systemctl start krb5kdc kadmin
sudo systemctl enable krb5kdc kadmin
```

6. Generate a keytab file. The keytab file contains the secret key for a principal and is used to authenticate the service.

```
kadmin.local ktadd -k /path/to/your-keytab-file HTTP/YOUR-HOST-
NAME@YOUR-REALM
```

Replace `/path/to/your-keytab-file` with the actual path where you want to store the keytab file.

Setting Up Kerberos Client Machine

Follow the below steps to set up a system as a Kerberos client.

1. Install the required packages. When installing the UFM, the following packages will be installed as dependencies:

```
#Redhat
krb5-libs krb5-workstation mod_auth_gssapi
# Ubuntu
krb5-config krb5-user libapache2-mod-auth-gssapi
```

2. Configure the `/etc/krb5.conf` file to reflect your realm, domain, local names map and other settings:

```
[libdefaults]
    default_realm = YOUR-REALM

[realms]
    YOUR-REALM = {
        kdc = your-kdc-server
        admin_server = your-admin-server
        auth_to_local_names = {
            your-principle-name = your-local-user
        }
    }

[domain_realm]
    your-domain = YOUR-REALM
    your-domain = YOUR-REALM
```

3. Copy the keytab file from the Kerberos server to the machine where your service runs (the client). It is important to ensure that it is kept confidential. Please ensure that the keytab file exists and that Apache has the necessary read permissions to access the keytab file; otherwise, Kerberos authentication will not function properly.
4. Obtain a Kerberos ticket-granting ticket (TGT):

```
kinit -k -t /path/to/your-keytab-file HTTP/YOUR-HOST-NAME@YOUR-REALM
```

5. Enable Kerberos Authentication from UFM. Kerberos authentication is disabled by default. To enable it, please refer to [Enabling Kerberos Authentication](#).
6. Test the Kerberos Authentication. You can use curl to test whether the user can authenticate to UFM REST APIs using Kerberos.

```
curl --negotiate -i -u : -k 'https://ufmc-eos01/ufmRestKrb/app/tokens'
```

Licensing

UFM license is subscription-based featuring the following subscription options:

- 1-year subscription
- 3-year subscription
- 5-year subscription
- Evaluation 30-day trial license

Note

UFM will continue to support old license types, but they are no longer available to obtain.

2 months before the expiration of your subscription license, UFM will warn you that your license will expire soon. After the subscription expires, UFM will continue to work with the expired license for two months beyond its expiration.

During this extra two-month period, UFM will generate a critical alarm indicating that the UFM license has expired and that you need to renew your subscription. Failing to do so within that 2-month period activates UFM Limited Mode. Limited mode blocks all REST APIs and access to the UFM web UI.

UFM enables functionality based on the license that was purchased and installed. This license determines the functionality and the maximum allowed number of nodes in the fabric.

To renew your UFM subscription, purchase a new license and install the new license file by downloading the license file to a temp directory on the UFM master server and then copying the license file to `/opt/ufm/files/licenses/` directory.

Note

UFM may not detect new license files if downloaded directly to `/opt/ufm/files/licenses`. If UFM does not detect the new license file, a UFM restart may be required.

If several licenses are installed on the server (more than one license file exists under `/opt/ufm/files/licenses/`), UFM uses only the strongest license and takes into consideration the expiration date, and the managed device limits on it, regardless of any other licenses that may exist on the server.

For instructions on how to view your license, please refer to the [UFM Quick Start Guide](#).

Showing UFM Processes Status

This functionality allows users to view the current status of main processes handled by the UFM.

- To view the main UFM processes, run the script `show_ufm_status.sh` under the `/opt/ufm/scripts`. Example: `/opt/ufm/scripts/show_ufm_status.sh`
- To view the UFM main and child processes, run the script `show_ufm_status.sh` with `-e` (extended_processes).
Example: `/opt/ufm/scripts/show_ufm_status.sh -e`

```
[root@r-ufm77 gvm_github]# /opt/ufm/scripts/show_ufm_status.sh
=====
                        UFM Main Processes
=====
ModelMain      Process is : [ Running ]
Opensm         Process is : [ Running ]
SHARP          Process is : [ Running ]
Unhealthy Ports Process is : [ Running ]
Daily Report   Process is : [ Running ]
UFM Health     Process is : [ Running ]
UFM Telemetry  Process is : [ Running ]

-----

[root@r-ufm77 gvm_github]# /opt/ufm/scripts/show_ufm_status.sh -e
=====
                        UFM Main Processes
=====
ModelMain      Process is : [ Running ]
Opensm         Process is : [ Running ]
SHARP          Process is : [ Running ]
Unhealthy Ports Process is : [ Running ]
Daily Report   Process is : [ Running ]
UFM Health     Process is : [ Running ]
UFM Telemetry  Process is : [ Running ]

-----
                        UFM ModelMain Child Processes
=====
SMClientConsumer Process is : [ Running ]
SMTrapHandler    Process is : [ Running ]
SysinfoJsonAgent Process is : [ Running ]
Telemetry Agent  Process is : [ Running ]
Telemetry History Process is : [ Running ]
```

© Copyright 2024, NVIDIA. PDF Generated on 06/06/2024