

# Upgrading Cloudera Flow Management

Date published: 2019-06-26

Date modified: 2022-05-12



# Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

# Contents

|  |          |
|--|----------|
| <b>Before you upgrade.....</b>                                   | <b>4</b> |
| <b>Upgrading to CFM 2.1.4 from CFM 2.x.....</b>                  | <b>5</b> |
| <b>Upgrading to CFM 2.1.4 from CFM 1.1.0.....</b>                | <b>6</b> |
| Turn off TLS regeneration.....                                   | 6        |
| Back up NiFi keystore and truststore settings.....               | 7        |
| Back up NiFi Registry keystore and truststore settings.....      | 8        |
| Upgrading to CFM 2.1.4.....                                      | 9        |
| Restore NiFi keystore and truststore settings.....               | 10       |
| Restore your NiFi Registry keystore and truststore settings..... | 11       |
| Turn off identity mapping.....                                   | 12       |
| Additional post-upgrade steps for some upgrade scenarios.....    | 13       |
| Enable Auto-TLS for CFM.....                                     | 13       |
| Create a Ranger user for the Initial Admin Identity.....         | 14       |
| Manually integrate with Atlas.....                               | 15       |
| Integrate with Atlas when Auto-TLS is enabled.....               | 16       |
| Start your NiFi and NiFi Registry services.....                  | 16       |

# Before you upgrade

Before beginning your CFM upgrade, it is crucial that you review the migration and upgrade options, upgrade paths, and your CDP Private Cloud Base cluster requirements to ensure that you understand the pre-requisites.

## CFM migration and upgrade options

You have two options for moving to CFM 2.1.4.

- Upgrade refers to a full in-place upgrade of CFM to CDP Private Cloud Base.
- Data migration refers to moving existing HDF cluster workloads to a new installation of CDP Private Cloud Base. For migration information see the *Migration Guide*.



### Note:

Review the *Upgrade Paths* document for detailed information on the upgrade and migration options appropriate for your use case.

## Upgrade paths

You can upgrade to CFM 2.1.4 from the following previous version:

- CFM 2.1.3
- CFM 2.1.2
- CFM 2.1.1
- CFM 1.1.0 on CDH 6.x

## Supported CDP Private Cloud Base cluster versions

CFM 2.1.4 runs on the following CDP Private Cloud Base cluster versions:

- 7.1.7
- 7.1.7 SP1
- 7.1.7 SP2
- 7.1.8



### Important:

You cannot run CFM 2.1.4 on CDH 5.x or 6.x clusters. To upgrade your underlying cluster, see the CDP upgrade documentation appropriate for your use case.

- *Getting Started with CDP Upgrade and Migration*
- *In-Place Upgrade of CDH to CDP Private Cloud Base*
- *In-Place Upgrade of CDP Private Cloud Base*

## Related Information

[Upgrade Paths](#)

[Migration Guide](#)

[Getting Started with CDP Upgrade and Migration](#)

[In-Place Upgrade from CDH to CDP Private Cloud Base](#)

[In-Place Upgrade of CDP Private Cloud Base](#)

## Upgrading to CFM 2.1.4 from CFM 2.x

This section describes the steps of the upgrade process from CFM 2.x to CFM 2.1.4. To upgrade to CFM 2.1.4, you must stop the CFM services, update the CSD files, restart the SCM Server, activate the new CFM parcel, and then restart your CFM services.

### Before you begin

- You have upgrade Cloudera Manager and CDP Private Cloud Base if needed.



**Important:** CFM 2.1.4 requires at least CDP Private Cloud Base 7.1.7.

- You have reviewed *Upgrade Paths* to be sure you are performing the right upgrade for your use case.
- You have reviewed the following information in *Before you upgrade* are sure that you have met the pre-requisites.
  - CFM migration and upgrade options
  - Upgrade paths
  - Supported CDP Private Cloud Base cluster versions

### Procedure

- Stop the NiFi and NiFi Registry services, in this order.
- Delete the old CSD files.
- Download the new CSD files.

The default CSD location is `/opt/cloudera/csd`, but you can configure that location from Cloudera Manager Administration | Settings | Local Descriptor Repository Path.

Ensure that you maintain the appropriate file ownership and access attributes and SELinux permissions if needed.

- Download the new CFM parcel and .sha checksums file appropriate for your operating system.

The default parcel location is `/opt/cloudera/parcel-repo/`.

Ensure that you maintain the appropriate file ownership and access attributes and SELinux permissions if needed.

- Restart the `cloudera-scm-server` service:

```
service cloudera-scm-server restart
```

- In Cloudera Manager, from the **Parcels** page, distribute and activate the CFM 2.1.4 parcel.  
After clicking Activate, the Activate CFM <version> on <cluster-name> pop-up displays. Click Activate Only, and then OK.
- Restart Cloudera Management Service.
- Restart NiFi and NiFi Registry and deploy the client configurations.
- Optionally, to clean up, remove the previous parcels from the host.
  - From the Parcel menu, go to the older CFM parcel.
  - Select Remove From Host.
  - Select Delete.
- From the Ranger UI, NiFi service controller policy:
  - Add the `nifi` user to the policy with READ permissions.
  - Verify the `nifi` group is set in the policy.

### Related Information

[Upgrade Paths](#)

[Before you upgrade](#)

## Upgrading to CFM 2.1.4 from CFM 1.1.0

This section describes the steps of the upgrade process from CFM 1.1.0 on CDH to CFM 2.1.4 on CDP Private Cloud Base.

Before starting your CFM upgrade, it is crucial that you review the migration and upgrade options, upgrade paths, and your CDP Private Cloud Base cluster requirements to ensure that you understand and fulfill the prerequisites.

### Upgrade paths

If you have CFM 1.0.x, first you need to upgrade to CFM 1.1.0.

If you have CFM 1.1.0 running on CDH 6.x, you can upgrade to CFM 2.1.5. For other upgrade scenarios, see the *Upgrade paths* documentation.

### Supported CDP Private Cloud Base cluster versions

CFM 2.1.4 runs on the following CDP Private Cloud Base cluster versions:

- 7.1.7
- 7.1.7 SP1
- 7.1.7 SP2
- 7.1.8

## Turn off TLS regeneration

The NiFi CA is not installed as part of CFM 2.1.4. You must turn off NiFi CFM upgrade edits CA Force Regenerate before proceeding with your upgrade.

### Before you begin

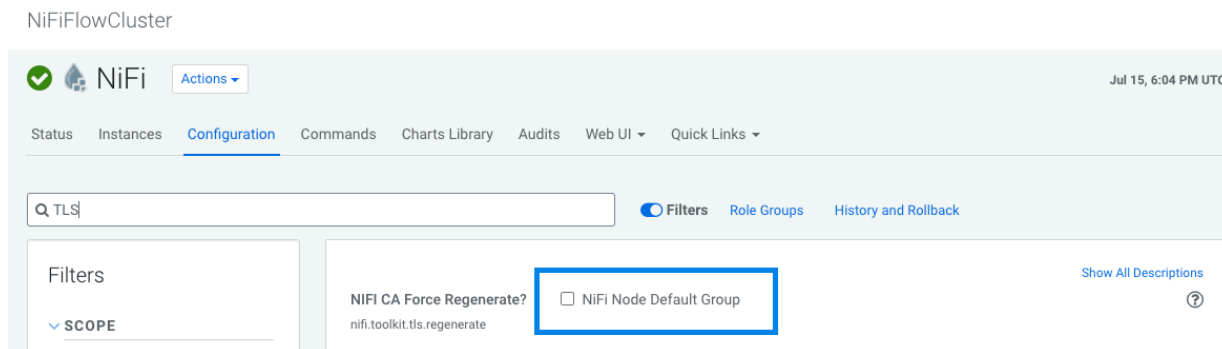
You have reviewed the following *Before you upgrade* information and are sure that you are performing the right upgrade for your use case.

- CFM migration and upgrade options
- Upgrade paths
- Supported CDP Private Cloud Base cluster versions

### Procedure

1. From Cloudera Manager, click the Clusters tab in the left-hand navigation
2. Click NiFi in the list of services to display the NiFi service page.
3. Select the Configuration tab.

#### 4. Deselect the TLS regeneration check-box.



#### 5. Repeat these steps for NiFi Registry.

### What to do next

Once you have turned off TLS regeneration, backup your keystore and truststore values for NiFi and NiFi Registry, and then proceed with the upgrade to CFM 2.1.4.

Once you have completed the upgrade, Cloudera recommends that you use Auto-TLS for your CDP Private Cloud Base cluster.

## Back up NiFi keystore and truststore settings

If your CFM installation from which you are upgrading is TLS enabled, use the Encrypt Config tools to backup your NiFi keystore and truststore settings. You will set these values in Cloudera Manager once you complete the upgrade.

### Disposition: / Status:

Regarding last sentence "You will set these values in CM once you complete the upgrade." Really? I don't believe we've actually told people how to do this, have we?

### Before you begin

- You have turned off TLS regeneration.
- If JAVA\_HOME is not set, you should set it before proceeding. The default path is /usr/java/default.

### Procedure

#### 1. Locate the encrypt-config.sh script from the NiFi Toolkit.

The default location is /opt/cloudera/parcels. You can find your location by running:

```
find /opt/cloudera/parcels -name 'encrypt-config.sh'
```



#### Note:

If you have installed more than one CFM parcel, you may have more than one script. In this case, ensure that you have the script from CFM 1.1.0.

#### 2. Find the latest NiFi process directory:

```
find /var/run/cloudera-scm-agent/process/ -name nifi.properties | grep "NIFI_NODE"
```

#### 3. Run encrypt-config.sh:

```
<path_to_encrypt-config.sh>
```

```
-c
-b <path_to_nifi_proc_dir>/bootstrap.conf
-n <path_to_nifi_proc_dir>/nifi.properties
```

For example:

```
/opt/cloudera/parcels/CFM-1.1.0.0/encrypt-config.sh
-c
-b /run/cloudera-scm-agent/182-NIFI_NODE.../bootstrap.conf
-n /run/cloudera-scm-agent/182-NIFI_NODE.../nifi.properties
```

4. Back up the `encrypt-config.sh` output.

## Results

The `encrypt-config.sh` output will be similar to:

```
keystore=/var/lib/nifi/cert/keystore.jks
keystorePasswd=/TLVwnnFESyIwn2YrBGiVWrANNhiSk
keyPasswd=/TLVwnnFESyIwn2YrBGiVWrANNhiSk
truststore=/var/lib/nifi/cert/truststore.jks
truststorePasswd=4wIWsnHpkVa5MR8P353s3ruMDGj1UL
```

## What to do next

Once you have completed this step for NiFi, do the same for NiFi Registry.

## Back up NiFi Registry keystore and truststore settings

If your CFM installation from which you are upgrading is TLS enabled, use the Encrypt Config tools to backup your NiFi Registry keystore and truststore settings. You will set these values in Cloudera Manager once you complete the upgrade.

### Before you begin

If `JAVA_HOME` is not set, you should set it before proceeding. The default path is `/usr/java/default`.

### Procedure

1. Locate the `encrypt-config.sh` script from the NiFi Toolkit.

The default location is `/opt/cloudera/parcels`. You can find your location by running:

```
find /opt/cloudera/parcels -name 'encrypt-config.sh'
```



#### Note:

If you have installed more than one CFM parcel, you may have more than one script. In this case, ensure that you have the script from CFM 1.1.0.

2. Find the latest NiFi Registry process directory:

```
find /var/run/cloudera-scm-agent/process/ -name nifi-registry.properties
| grep "NIFI_REGISTRY_SERVER"
```



### 3. Run `encrypt-config.sh`:

```
${ENCRYPT_CONFIG_PATH}
--nifiRegistry
--decrypt
-r ${NIFIREG_PROC_DIR}/nifi-registry.properties
-b ${NIFIREG_PROC_DIR}/bootstrap.conf
```

### 4. Back up the `encrypt-config.sh` output.

## Results

The `encrypt-config.sh` output will be similar to:

```
nifi.registry.security.keystore=/var/lib/nifiregistry/cert/keystore.jks
nifi.registry.security.keystorePasswd=5BNrrLRmcrgi+qqlBNpEpoIzyOALo
nifi.registry.security.truststore=/var/lib/nifiregistry/cert/truststore.jks
nifi.registry.security.truststorePasswd=qKdbQ9Q0a0uX/XAphhLjR4d2zxRHQ3
```



#### Note:

`nifi.registry.security.keystorePasswd` is the same as `keyPassword`.

## What to do next

Once you have completed this step for NiFi Registry, you may proceed with the upgrade to CFM 2.1.4.

## Upgrading to CFM 2.1.4

To upgrade from CFM 1.1.0 to CFM 2.1.4, you must stop the CFM services, update the CSD files, restart the SCM Server, and activate the new CFM parcel.

### About this task

If you must upgrade from CFM version 1.0.x, you should first upgrade to CFM 1.1.0. See the *Upgrade documentation* for CFM 1.1.0 for more information.

### Before you begin

Before you begin the CFM upgrade, ensure that you have completed the steps to:

- Turn off TLS regeneration.
- Back up your keystore and truststore settings for NiFi and NiFi Registry.

### Procedure

1. Stop NiFi, NiFi Registry, and NiFi CA Service in this order.
2. Delete the old CSD files.
3. Download the new CSD files.

The default CSD location is `/opt/cloudera/csd`, but you can configure that location from Cloudera Manager Administration | Settings | Local Descriptor Repository Path.

Ensure that you maintain the appropriate file ownership and access attributes and SELinux permissions if needed.

4. Download the new CFM parcel and .sha checksum file appropriate for your operating system.

The default parcel location is `/opt/cloudera/parcel-repo/`.

Ensure that you maintain the appropriate file ownership and access attributes and SELinux permissions if needed.

5. Restart the cloudera-scm-server service:

```
service cloudera-scm-server restart
```

6. In Cloudera Manager, from the **Parcels** page, distribute and activate the CFM parcel to which you want to upgrade.

After clicking Activate, the Activate CFM <version-number> on <cluster-name> pop-up displays. Click Activate Only, and then OK.

7. Optionally, to clean up, remove the older parcels from the host.

- a) From the Parcel menu, go to the older CFM parcel.
- b) Select Remove From Host.
- c) Select Delete.

**Important:**

Do not start the NiFi and NiFi Registry services yet. Complete the post-upgrade steps before you start any services.

**What to do next**

Once you have completed the upgrade, perform the following additional tasks:

- Set the keystore and truststore settings with the values from your backup.
- Turn off identity mapping for both NiFi and NiFi Registry.
- Start the NiFi and NiFi Registry.

**Note:**

Do not start the NiFi CA service, as this is no longer supported as part of CFM 2.1.4.

- Optionally, you can remove the NiFi CA service.

**Related Information**

[Upgrading CFM 1.0.1](#)

## Restore NiFi keystore and truststore settings

Learn how to restore your NiFi keystore and truststore settings from the backup you made prior to upgrade.

**Before you begin**

- You have completed your upgrade to CFM 2.1.4.
- You have the NiFi keystore and truststore settings that you backed up before beginning your upgrade.

**Procedure**

1. From Cloudera Manager, click the Clusters tab in the left-hand navigation
2. Click NiFi in the list of services to display the NiFi service page.
3. Select the Configuration tab.

- Use the search bar to find the Keystore configuration options and update the following three with the values from your backup.

**Note:**

The `nifi.security.keystorePasswd` value should be the same as the `keyPassword` value.

|   |  |  |
|---|--|--|
| NiFi Node TLS/SSL Server<br>JKS Keystore File Location<br><small>nifi.security.keystore</small>       | NiFi Node Default Group                      |  |
|   | <input type="text" value="{{CM_AUTO_TLS}}"/> |  |
| NiFi Node TLS/SSL Server<br>JKS Keystore File Password<br><small>nifi.security.keystorePasswd</small> | NiFi Node Default Group                      |  |
|   | <input type="password" value="....."/>       |  |
| NiFi Node TLS/SSL Server<br>JKS Keystore Key Password<br><small>nifi.security.keyPasswd</small>       | NiFi Node Default Group                      |  |
|   | <input type="password" value="....."/>       |  |

- Use the search bar to find the Truststore configuration options and update the following two with the values from your backup.

|   |  |  |
|---|--|--|
| NiFi Node TLS/SSL Client<br>Trust Store File<br><small>nifi.security.truststore</small>           | NiFi Node Default Group                      |  |
|   | <input type="text" value="{{CM_AUTO_TLS}}"/> |  |
| NiFi Node TLS/SSL Client<br>Trust Store Password<br><small>nifi.security.truststorePasswd</small> | NiFi Node Default Group                      |  |
|   | <input type="password" value="....."/>       |  |

**What to do next**

Once you have completed this step for the NiFi service, do the same for NiFi Registry.

## Restore your NiFi Registry keystore and truststore settings

Learn how to restore your NiFi Registry keystore and truststore settings from the backup you made prior to upgrade.

**Before you begin**

- You have completed your upgrade to CFM 2.1.4.
- You have the NiFi Registry keystore and truststore settings that you backed up before beginning your upgrade.

**Procedure**

- From Cloudera Manager, click the Clusters tab in the left-hand navigation
- Click NiFi Registry in the list of services to display the NiFi Registry service page.
- Select the Configuration tab.

- Use the search bar to find the Keystore configuration options and update the following three with the values from your backup.

**Note:**

The `nifi.registry.security.keystorePasswd` value should be the same as the `keyPassword` value.

|  |  |   |
|--|--|---|
| NiFi Registry TLS/SSL Server                         | NiFi Registry Default Group                  | ? |
| JKS Keystore File Location                           | <input type="text" value="{{CM_AUTO_TLS}}"/> |   |
| <small>nifi.registry.security.keystore</small>       |  |   |
| NiFi Registry TLS/SSL Server                         | NiFi Registry Default Group                  | ? |
| JKS Keystore File Password                           | <input type="password" value="....."/>       |   |
| <small>nifi.registry.security.keystorePasswd</small> |  |   |
| NiFi Registry TLS/SSL Server                         | NiFi Registry Default Group                  | ? |
| JKS Keystore Key Password                            | <input type="password" value="....."/>       |   |
| <small>nifi.registry.security.keyPasswd</small>      |  |   |

- Use the search bar to find the Truststore configuration options and update the following two with the values from your backup.

|  |  |   |
|--|--|---|
| NiFi Registry TLS/SSL Client                             | NiFi Registry Default Group                  | ? |
| Trust Store File   | <input type="text" value="{{CM_AUTO_TLS}}"/> |   |
| <small>nifi.registry.security.truststore</small>         |  |   |
| NiFi Registry TLS/SSL Client                             | NiFi Registry Default Group                  | ? |
| Trust Store Password                                     | <input type="password" value="....."/>       |   |
| <small>nifi.registry.security.truststorePassword</small> |  |   |

**What to do next**

Once you have restored NiFi and NiFi Registry keystore and truststore settings, turn off identity mapping.

## Turn off identity mapping

Describes the steps to turn off identity mapping.

**About this task**

If you enable auto-TLS, you must ensure that identity mapping is turned off.

**Procedure**

- From Cloudera Manager, click the Clusters tab in the left-hand navigation.
- Click NiFi in the list of services to display the NiFi service page.
- Select the Configuration tab.
- Use the search bar to find the Identity Mapping configuration options and remove the values for the following parameters:
  - Identity Mapping - DN Pattern (`nifi.security.identity.mapping.pattern.dn`)
  - Identity Mapping - DN Value (`nifi.security.identity.mapping.value.dn`)

5. Repeat these steps for NiFi Registry. The NiFi Registry Identity Mapping configuration options are:

- Identity Mapping - DN Pattern (`nifi.registry.security.identity.mapping.pattern.dn`)
- Identity Mapping - DN Value (`nifi.registry.security.identity.mapping.value.dn`)

### Example

The screenshot shows the NiFi Configuration page. The search bar contains "identity map". The left sidebar shows a filter for "SCOPE" with counts: NiFi (Service-Wide) 0, Gateway 0, and NiFi Node 7. The main content area shows two configuration items:

| Configuration Item  | Value  |
|---|--|
| Identity Mapping - DN Pattern<br><code>nifi.security.identity.mapping.pattern.dn</code> | NiFi Node Default Group<br><code>^CN=(.*?), .+&amp;</code> |
| Identity Mapping - DN Value<br><code>nifi.security.identity.mapping.value.dn</code>     | NiFi Node Default Group<br><code>\$1</code>                |

### What to do next

Once you have turned off identity mapping, review the additional post-upgrade steps for any additional requirements that pertain to your CFM 2.1.4 deployment scenario.

## Additional post-upgrade steps for some upgrade scenarios

Depending on the type of CFM 1.1.0 installation you are upgrading, there are some additional post-upgrade steps you must take. You should review the following information for anything pertaining to your upgrade scenario.

### Enable Auto-TLS for CFM

Provides steps to enable Auto-TLS for CFM.

#### About this task

You should perform these steps if you are upgrading from a CFM 1.1.0 installation where:

- TLS is enabled for CFM 1.1.0; AND
- Auto-TLS is enabled on the CDH cluster.

#### Before you begin

- You have turned off identity mapping.

#### Procedure

1. Launch the API Explorer from the Cloudera Manager Support menu at the bottom of the left navigation pane.

2. Run the `configureAutoTlsServices` API call.

**POST** `/clusters/{clusterName}/commands/configureAutoTlsServices` Configures all services in a cluster to use Auto-TLS.

**Implementation Notes**  
Configures all services in a cluster to use Auto-TLS

**Response Class (Status 201)**  
Success

**Model** **Model Schema**

```
{
  "id": 12345,
  "name": "...",
  "startTime": "...",
  "endTime": "...",
  "active": true,
  "success": true,
  "resultMessage": "...",
  "resultDataUrl": "...",
  "clusterRef": {
    "clusterName": "...",
    "clusterId": "..."
  }
}
```

**Response Content Type** application/json

**Headers**

| Header | Description | Type | Other |
|--------|-------------|------|-------|
|        |             |      |       |

**Parameters**

| Parameter          | Value      | Description              | Parameter Type | Data Type |
|--------------------|------------|--------------------------|----------------|-----------|
| <b>clusterName</b> | (required) | The name of the cluster. | path           | string    |

[Try it out!](#)

3. Edit the `users.xml`, to remove the users associated with the NiFi nodes.

Repeat these steps for NiFi Registry.

4. Edit the `authorizations.xml` file.

In the `/proxy` policy, remove the users corresponding to the NiFi nodes and replace them with:

```
<group identifier="nifi"/>
```

Repeat these steps for NiFi Registry/

5. Review the other policies related to the NiFi nodes, to similarly edit any other references to the NiFi nodes.

### Related Tasks

[Create a Ranger user for the Initial Admin Identity](#)

[Manually integrate with Atlas](#)

[Integrate with Atlas when Auto-TLS is enabled](#)

## Create a Ranger user for the Initial Admin Identity

In some upgrade scenarios, you must manually create a Ranger user for the Initial Admin Identity and add it to the `nifi` group.

### About this task

You should perform these steps if you are upgrading from a CFM 1.1.0 installation where:

- CFM has Kerberos and TLS enabled; AND
- The CDP Private Cloud Base cluster does not have Auto-TLS enabled; AND
- You want Ranger as part of your CFM 2.1.4 on CDP Private Cloud Base 7.1.x deployment.

### Before you begin

Ranger is running on your CDP Private Cloud Base 7.1.x cluster.

### Procedure

1. Create a Ranger user with the same user name as your NiFi Initial Admin Identity.
2. Assign this user to the Ranger group `nifi`.
3. Create a Ranger user with the same username as your NiFi Registry Initial Admin Identity.
4. Assign this user to the Ranger group `nifiregistry`.

### Related Tasks

[Enable Auto-TLS for CFM](#)

[Manually integrate with Atlas](#)

[Integrate with Atlas when Auto-TLS is enabled](#)

## Manually integrate with Atlas

Provides steps to manually integrate with Atlas by creating the `ReportLineageToAtlas` reporting task.

### About this task

If you are upgrading from a CFM 1.1.0 installation where:

- CFM does not have TLS enabled; AND
- The CDP Private Cloud Base cluster does not have Auto-TLS enabled; AND
- You do not want to enable Auto-TLS; AND
- You want Atlas as part of CFM 2.1.4 on your CDP Private Cloud Base 7.1.x deployment.

### Procedure

1. Start NiFi.
  - a) From Cloudera Manager, click the Clusters tab in the left-hand navigation.
  - b) Click NiFi in the list of services to display the NiFi service page.
  - c) Click the Actions drop-down, and then click Start.
2. From the Global Menu located in NiFi's upper right corner, select Controller Services and click the Reporting Tasks tab.
3. Click the Add (+) icon to launch the Add Reporting Task dialog.
4. Select `ReportLineageToAtlas` and click Add.
5. Click the Edit icon to launch the Configure Reporting Task dialog. The following properties are required:
  - Atlas URLs – a comma-separated list of Atlas Server URLs. Once you have started reporting, you cannot modify an existing Reporting Task to add a new Atlas Server. When you need to add a new Atlas Server, you must create a new reporting task.
  - Atlas Authentication Method – Specifies how to authenticate the Reporting Task to the Atlas Server. Basic authentication is the default.
  - NiFi URL for Atlas – Specifies the NiFi cluster URL
  - Lineage Strategy – Specifies the level of granularity for your NiFi dataflow reporting to Atlas. Once you have started reporting, you should not switch between simple and complete lineage reporting strategies.
  - Provenance Record Start Position – Specifies where in the Provenance Events stream the Reporting Task should start.
  - Provenance Record Batch Size – Specifies how many records you want to send in a single batch
  - Create Atlas Configuration File – If enabled, the `atlas-application-properties` file and the Atlas Configuration Directory are automatically created when the Reporting Task starts.
  - Kafka Security Protocol – Specifies the protocol used to communicate with Kafka brokers to send Atlas hook notification messages. This value should match Kafka's `security.protocol` property value.

### Related Tasks

[Enable Auto-TLS for CFM](#)

[Create a Ranger user for the Initial Admin Identity](#)  
[Integrate with Atlas when Auto-TLS is enabled](#)

## Integrate with Atlas when Auto-TLS is enabled

Provides manual steps to integrate with Atlas when Auto-TLS is enabled on your CDP Data Center cluster.

### About this task

You must perform these steps if:

- You want CFM 2.1.4 to integrate with Atlas; AND
- The CDP Private Cloud Base 7.1.x cluster has Auto-TLS enabled

### Procedure

1. Start NiFi.
  - a) From Cloudera Manager, click the Clusters tab in the left-hand navigation.
  - b) Click NiFi in the list of services to display the NiFi service page.
  - c) Click the Actions drop-down, and then click Start.
2. Select the Atlas Dependency checkbox.
3. Restart NiFi.
4. Click Create required NiFi objects from the Actions drop-down.

### Related Tasks

[Enable Auto-TLS for CFM](#)  
[Create a Ranger user for the Initial Admin Identity](#)  
[Manually integrate with Atlas](#)

## Start your NiFi and NiFi Registry services

Provides steps to start your NiFi and NiFi Registry services.

### About this task

The final upgrade step is to start your NiFi and NiFi Registry services if you have not already done so.

### Before you begin

You have completed all applicable post-upgrade steps. If you have not completed these steps, your services may fail to start.

### Procedure

1. From Cloudera Manager, click the Clusters tab in the left-hand navigation.
2. Click NiFi in the list of services to display the NiFi service page.
3. Click the Actions drop-down, and then click Start.
4. Repeat these steps for NiFi Registry.