CDGC – Configuration

User Guide

Secure Agent Configuration

By

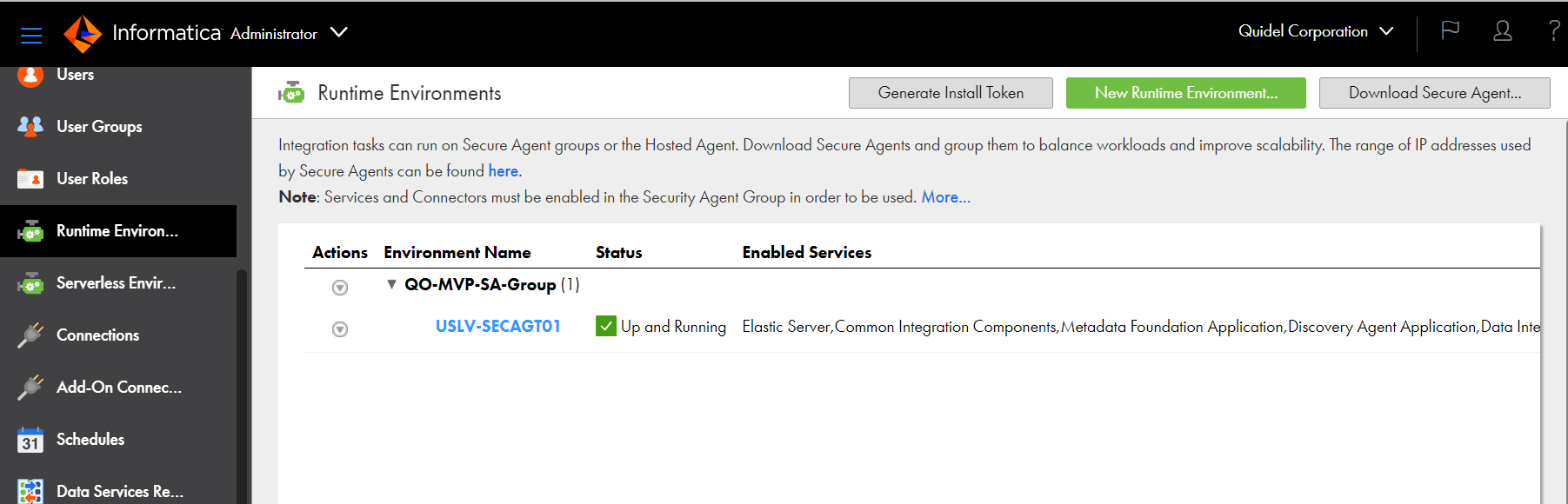
Aswini Arasu

Table of Contents

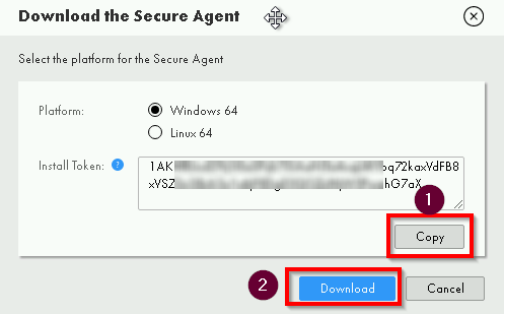
Steps to Configure [Secure Agent 3](#_Toc131459361)

# Instructions/Steps

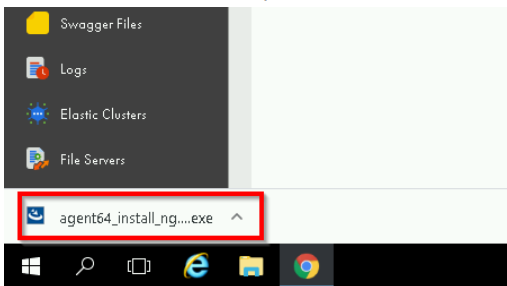
1. Log in to the Administrator service using the admin user, click the Runtime Environments menu from the navigation bar on the left. And then click the Download Secure Agent button as highlighted.



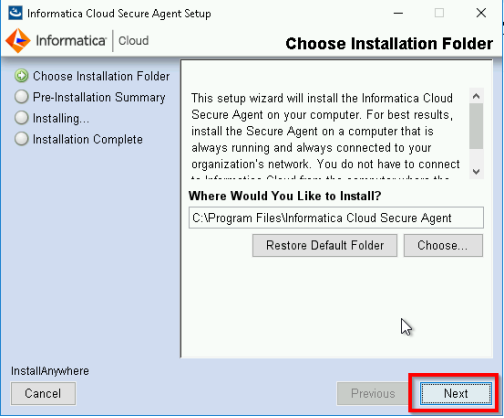
1. Select the platform as Windows 64/Linux 64. Click the Copy button and keep the Install Token at hand for the Secure Agent registration later. Click the Download button to download the binary for installation.



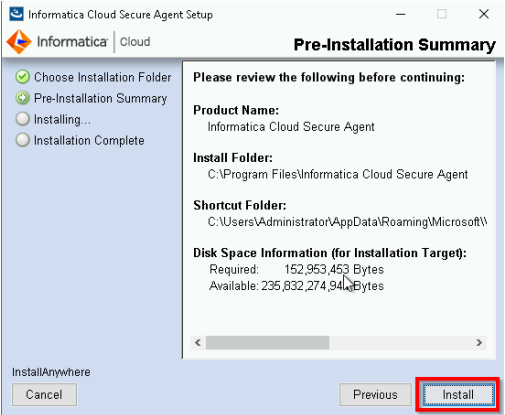
1. Once the download is complete, click the installer to start the installation.

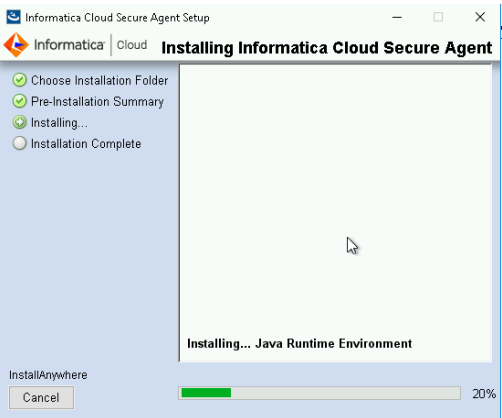


1. Use the default folder or choose another location if desired, and click the Next button.

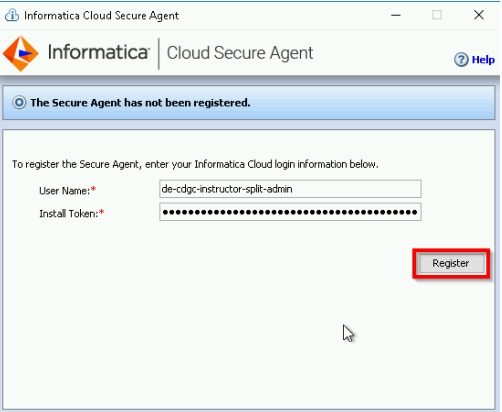


1. Confirm all details are correct and click the Install button. Wait until the installation is done.

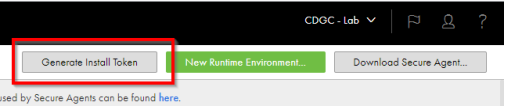




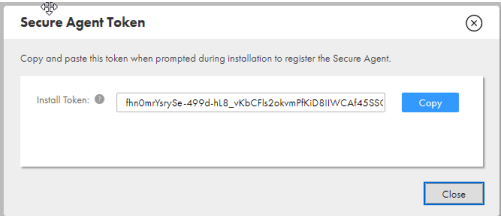
1. Fill in the user name that is used for logging in to IDMC, install the token that was copied earlier, and click the Register button. Note the Secure Agent will be registered to the IDMC organization under which the user is created. If you have a sub-organization and want to install and register a Secure Agent, ensure the admin user of that sub-organization is used to generate the install token for this registration.



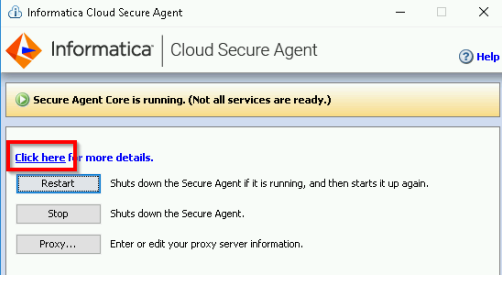
1. The install token is valid for 24 hours. If it is expired, you can generate a new one by clicking this button.



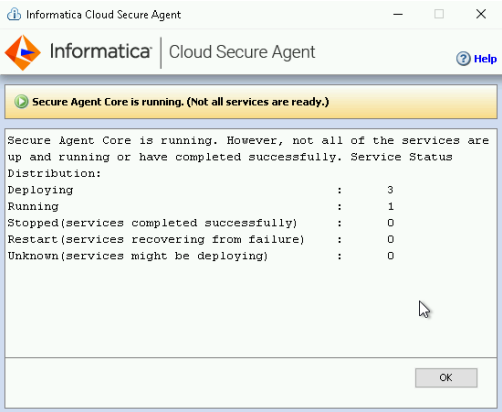
1. And copy the install token for the registration.



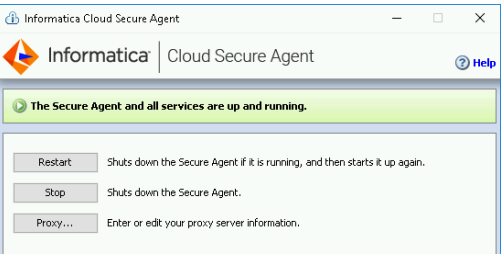
1. Once the registration credential is accepted, you can monitor the Secure Agent status. At this stage, the Secure Agent is communicating with the IDMC services for initialization, and getting everything synchronized may take a while. In the meantime, you can click the ‘Click here’ hyperlink to find more details.



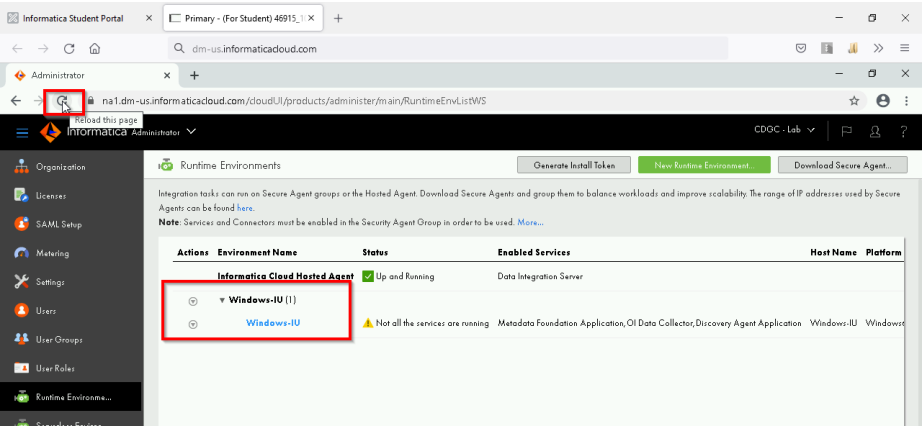
1. Here it shows three services are being deployed, and one service is in the running state.



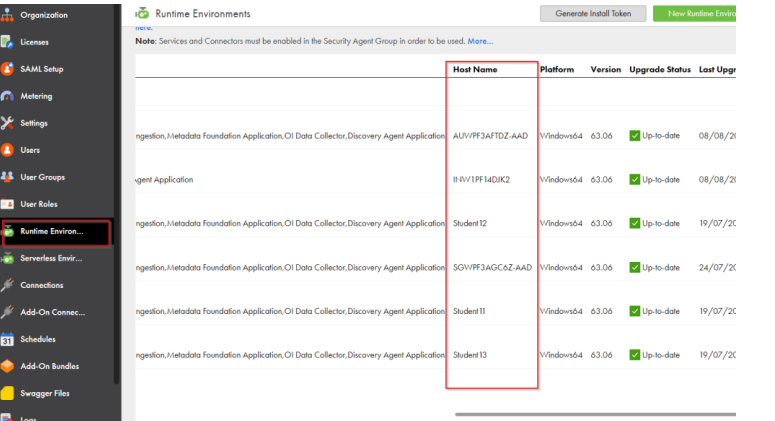
1. Once the service deployment is done, the Secure Agent and all services should be up and running.



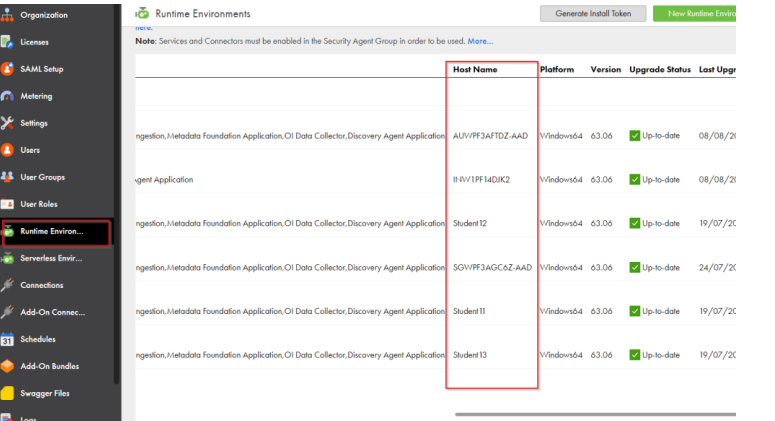
1. Toggle back to the IDMC Administrator UI, and refresh the page. You should find the new Secure Agent has been created. By default, a Secure Agent Group (with the same name as the Secure Agent) is created for the newly created Secure Agent. Click the Secure Agent hyperlink, which will navigate to the details page.



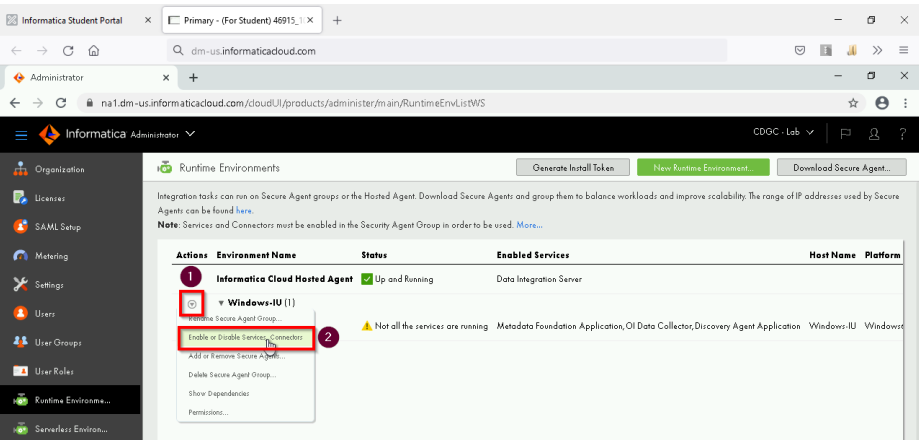
1. By default, when a new Secure Agent is registered, the IDMC platform creates a Runtime Environment with the hostname. In a shared environment, if the existing Runtime Environment has used the hostname of the new Secure Agent, the IDMC platform will not create a new Runtime Environment. Instead, it will simply re-use the existing Runtime Environment, and the name might be changed from the default hostname. In this case, you can scroll the Runtime Environment page to the right and find the value under the Host Name. Then, you can locate the Runtime Environment and rename it to the expected name.



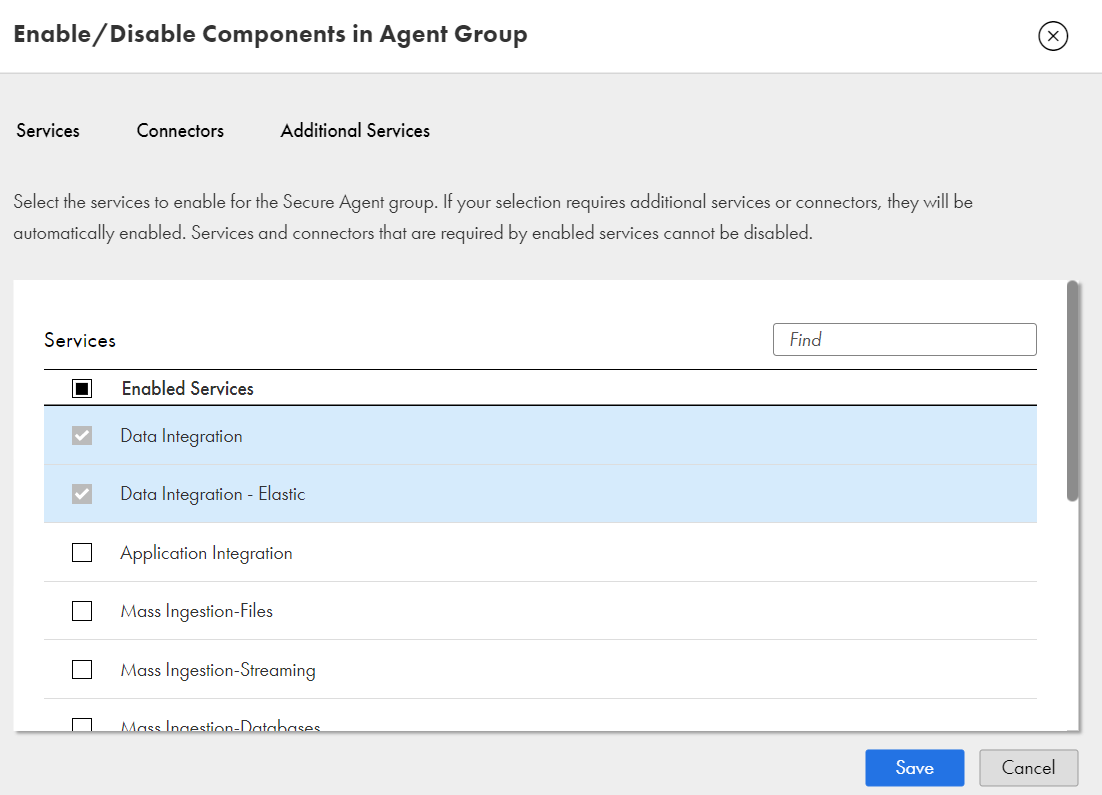
1. Here is the details page for this Secure Agent. Confirm all the default services are up and running. Click the Close button to return to the Runtime Environments overview page.

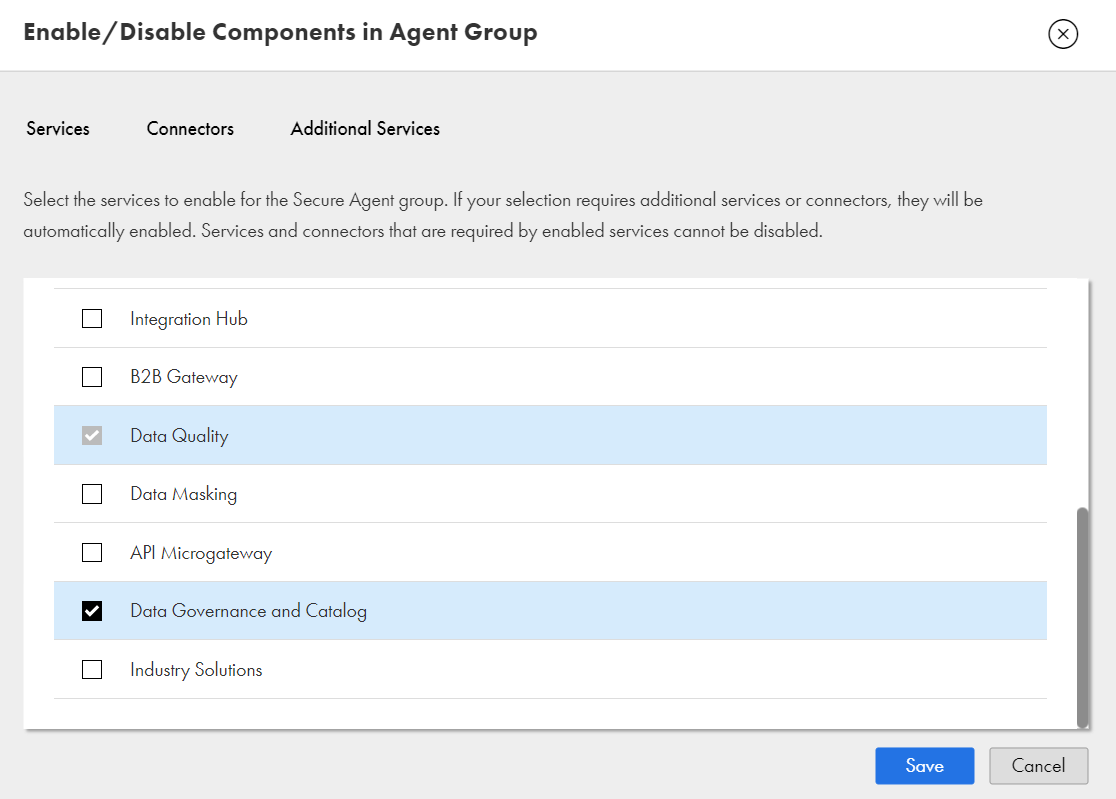


1. On this overview page, hover the mouse over the drop-down icon and click the ‘Enable or Disable Services Connectors.’ This is to enable the Data Integration Service for the Secure Agent. The CDGC services need this DIS component in the Secure Agent to extract metadata from the sources for ingestion into the CDGC catalog.

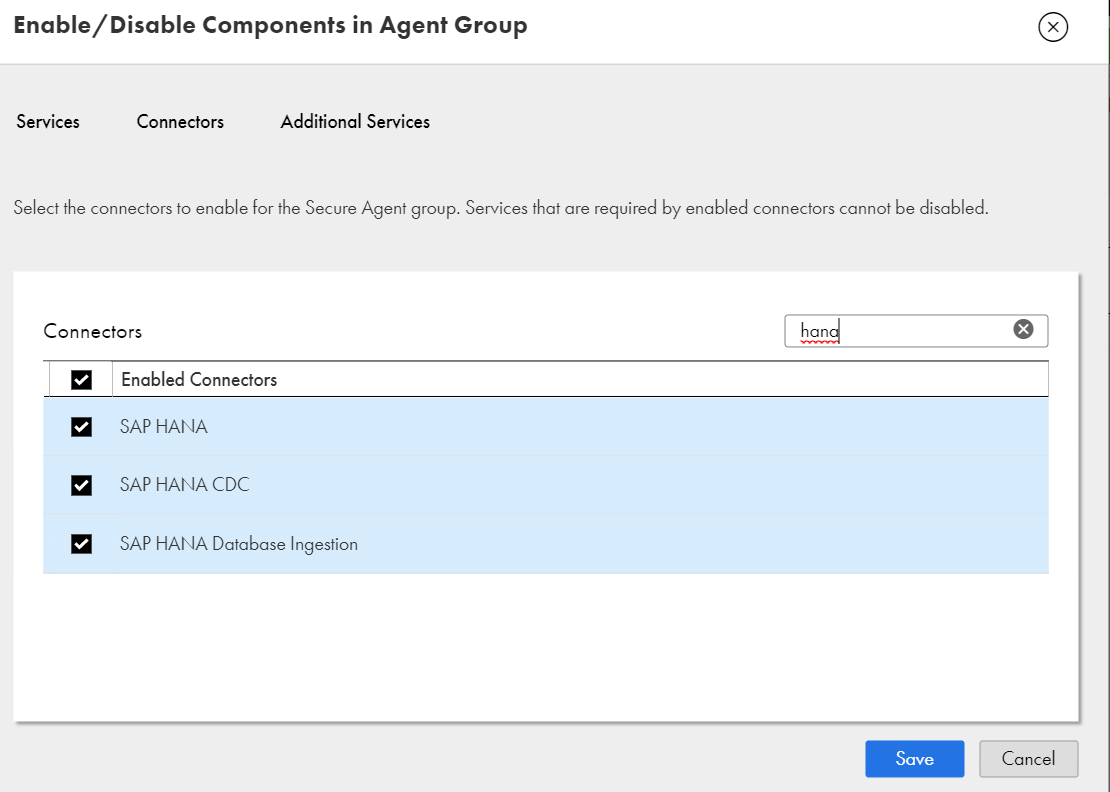


1. Select the Data Integration, Data Integration-Elastic, Data Quality and Data Governance and catalog services and save the change. The Data Quality service is needed in the Data Quality rule execution lab.

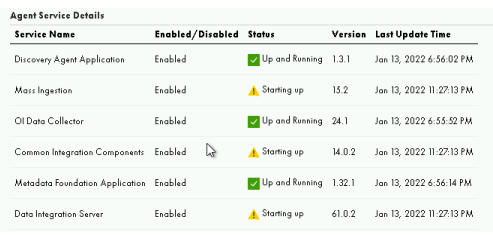




1. Select the Connectors and enable the



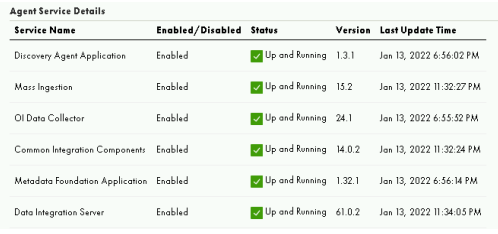
1. Now you will see a few more services are enabled for the Secure Agent and in the ‘Starting Up’ state



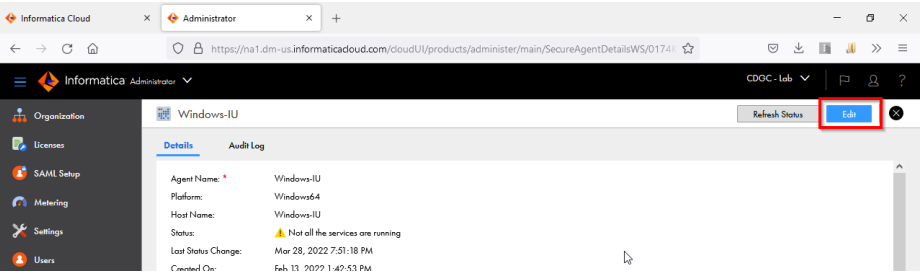
1. Allow some time for these services to be up and running. In the meantime, you can click this button to refresh the status.



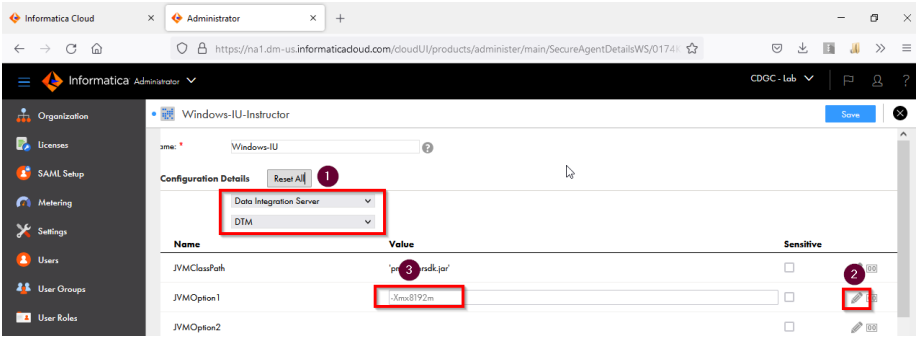
1. After a few minutes, all these services should be in the ‘Up and Running’ state.



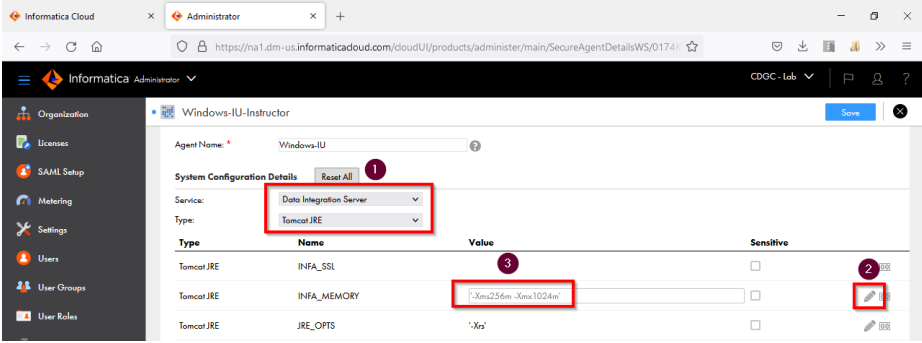
1. You may want to increase Secure Agent’s memory setting when multiple services are enabled. Open the Secure Agent and click the Edit button.



1. Set the JVMOption1 value to '-Xmx8192m' under the DTM type of the Data Integration Server service:



1. Set the INFA\_MEMORY value to '-Xms256m -Xmx1024m' under the Tomcat JRE type of the Data Integration Server service:



1. Click the Save button and allow some time for Secure Agent to restart.
2. This concludes steps to configure secure agent.