How-To Library

Secure Agent Quick Start for Windows

Abstract

A Secure Agent is a lightweight program that runs all tasks that you configure in Informatica Intelligent Cloud Services℠ and processes your company's data locally and securely. A Secure Agent must be running to run tasks. This article provides instructions that you can follow to quickly install and configure a Secure Agent on Windows in the Spring 2020 and later versions of Informatica Intelligent Cloud Services.

Supported Versions

- Informatica Intelligent Cloud Services Spring 2020

Table of Contents

Overview

A Secure Agent is a lightweight program that runs all tasks and enables secure communication across the firewall between your organization and Informatica Intelligent Cloud Services. Each Secure Agent that you install is shared by the entire organization.

You can install a Secure Agent on any machine that has access to the data that you want to use with Informatica Intelligent Cloud Services. The Secure Agent must be up and running to run tasks and upload operational metadata to the cloud. So, install the Secure Agent on a machine that is always running, such as a production server.

For more information about Secure Agents, see "Runtime environments" in the Administrator help.

To set up a Secure Agent on Windows, complete the following steps:

1. Download and install the Secure Agent.
2. Configure a login for the Windows Secure Agent service.

Step 1. Download and install the Secure Agent

Check the system requirements, then download the installation program and install the Secure Agent.

Before you download and install the Secure Agent, verify that the following pre-requisites are met:

- The machine uses a supported operating system. For the list of supported operating systems for the Secure Agent, see the Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services on Informatica Network here.
- The machine has at least 5 GB of free disk space.
- The account you use to install the Secure Agent has access to all remote directories that contain flat source or target files.
- No other Secure Agent is installed on the machine. If another Secure Agent is installed on the machine, you must uninstall it first.

- If your organization uses a protective firewall, include the Informatica Intelligent Cloud Services domain name or IP address ranges in the list of approved domain names or IP addresses. You should also enable the port that the Secure Agent uses to connect to the internet, port 443 (HTTPS).
For more information, see this Knowledge Base article on Informatica Network.

To download and install the agent:

1. Open Administrator and select **Runtime Environments**.

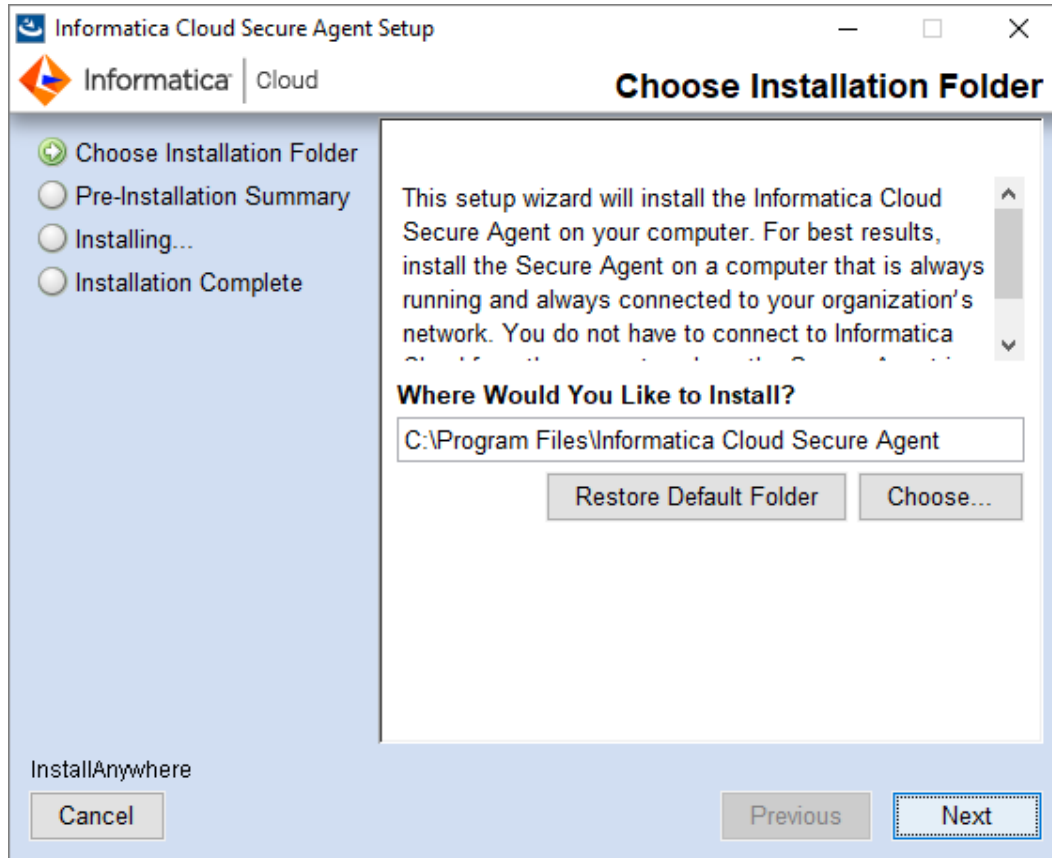2. On the **Runtime Environments** page, click **Download Secure Agent**.
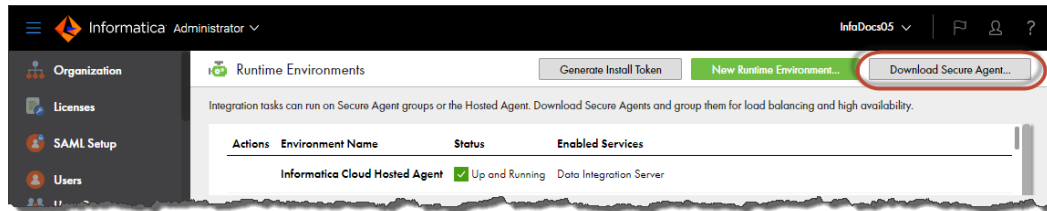
3. In the **Download the Secure Agent** dialog box, select the Windows 64-bit operating system platform and copy the install token.
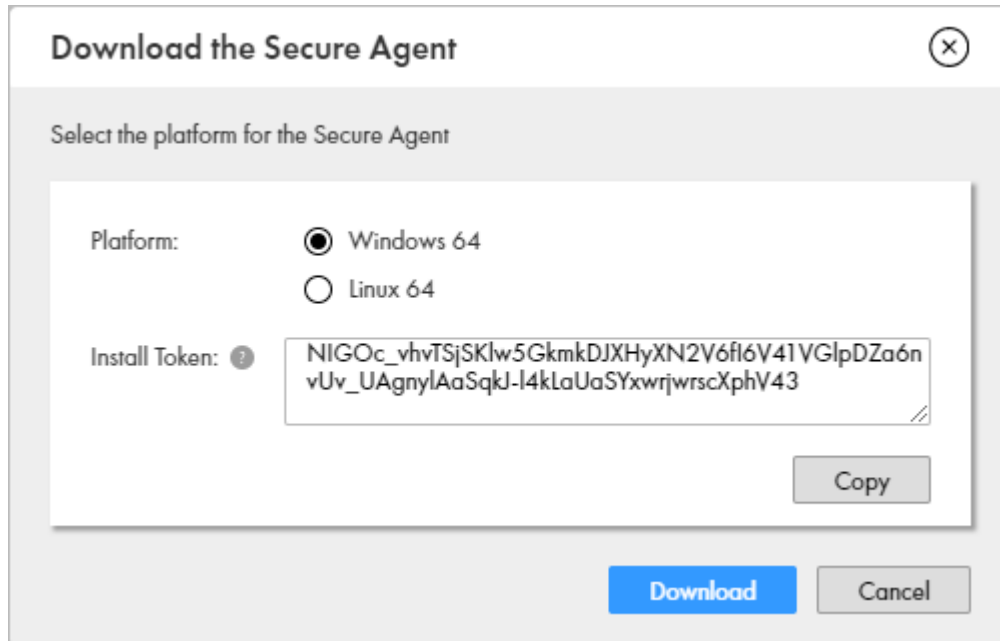
4. Click **Download**.

The installation program is downloaded to your machine. The name of the installation program is `agent64_install_ng_ext.exe`.

5. Run the installation program.

a. Specify the Secure Agent installation directory, and click **Next**.

b. Click **Install** to install the agent.

When the installation finishes, the Secure Agent Manager opens and prompts you to register the agent.

6. If you did not copy the install token when you downloaded the agent, click **Generate Install Token** on the **Runtime Environments** page in Administrator, and copy the token.

7. In the Secure Agent Manager, enter the following information, and then click **Register**:

Option	Description
User Name	User name that you use to access Informatica Intelligent Cloud Services.
Install Token	Token that you copied.

The Secure Agent Manager displays the status of the Secure Agent. It takes a minute for all of the services to start.

When all of the services have started, the message, "The Secure Agent and all services are up and running," appears in the Secure Agent Manager.
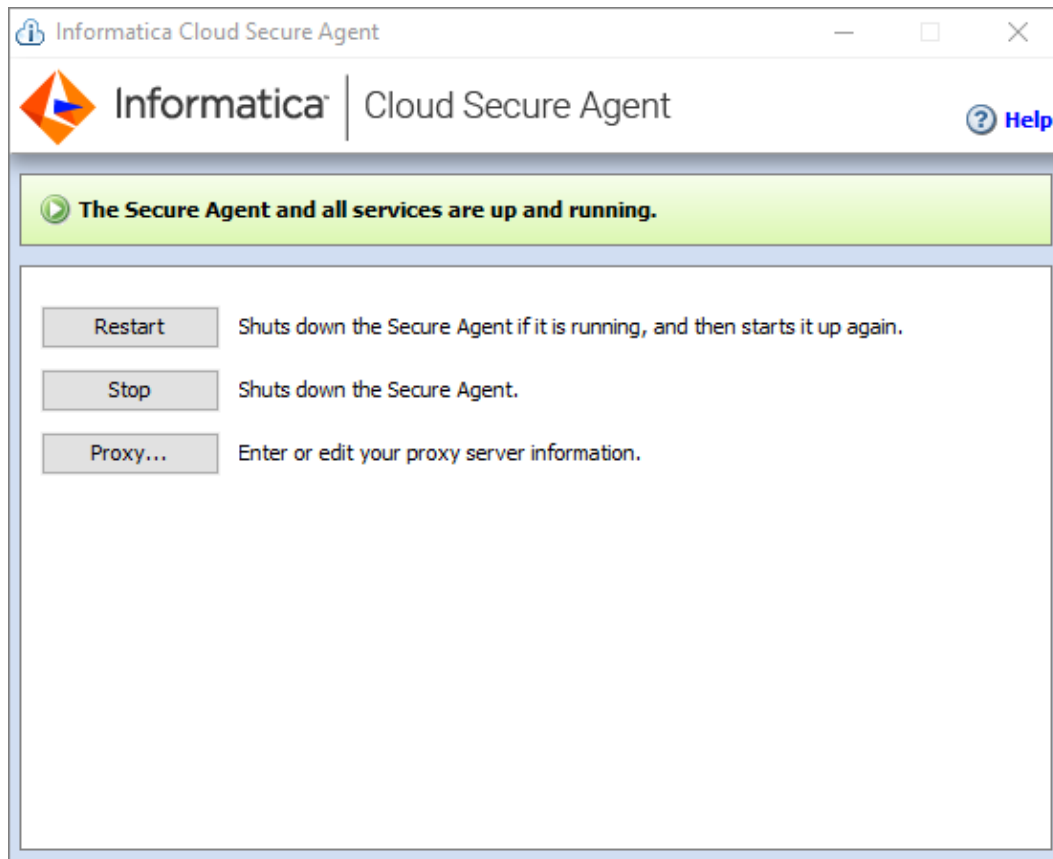
8. If your organization uses an outgoing proxy server to connect to the internet, click **Proxy**.

a. Select **Use a proxy server**.

b. Enter the following information and click **OK**:

Field	Description
Proxy Host	Required. Host name of the outgoing proxy server that the Secure Agent uses.
Proxy Port	Required. Port number of the outgoing proxy server.
User Name	User name to connect to the outgoing proxy server.
Password	Password to connect to the outgoing proxy server.

The Secure Agent Manager restarts the Secure Agent to apply the settings.

9. Close the Secure Agent Manager.

The Secure Agent Manager minimizes to the taskbar and continues to run as a service until stopped.

# Step 2. Configure a login for a Windows Secure Agent service

Configure a network login for the Secure Agent service. The Secure Agent can access the network with the privileges and permissions associated with the login.

Configure a login for the Secure Agent machine to allow the Secure Agent to access directories to configure and run tasks. When you configure connections, configure tasks, and run tasks that use Flat File or FTP/SFTP connection types, the Secure Agent might require read and write permissions on the related directories.

For example, to browse to a directory to configure a Flat File or FTP/SFTP connection, the Secure Agent might require permission to access the directory. Without a Secure Agent login with the appropriate permissions, Informatica Intelligent Cloud Services cannot display the directory in the **Browse for Directory** dialog box.

1. Go to the **Services** window from the Windows Administrative tools.
2. In the **Services** window, right-click the Informatica Cloud Secure Agent service and choose **Properties**.
3. In the **Properties** dialog box, click the **Log On** tab.
4. To configure a login, select **This Account**.
5. Enter an account and password.

   Use an account with the required privileges and permissions for the network security defined for the domain. By default, the account format is <domain name>\<user name>.
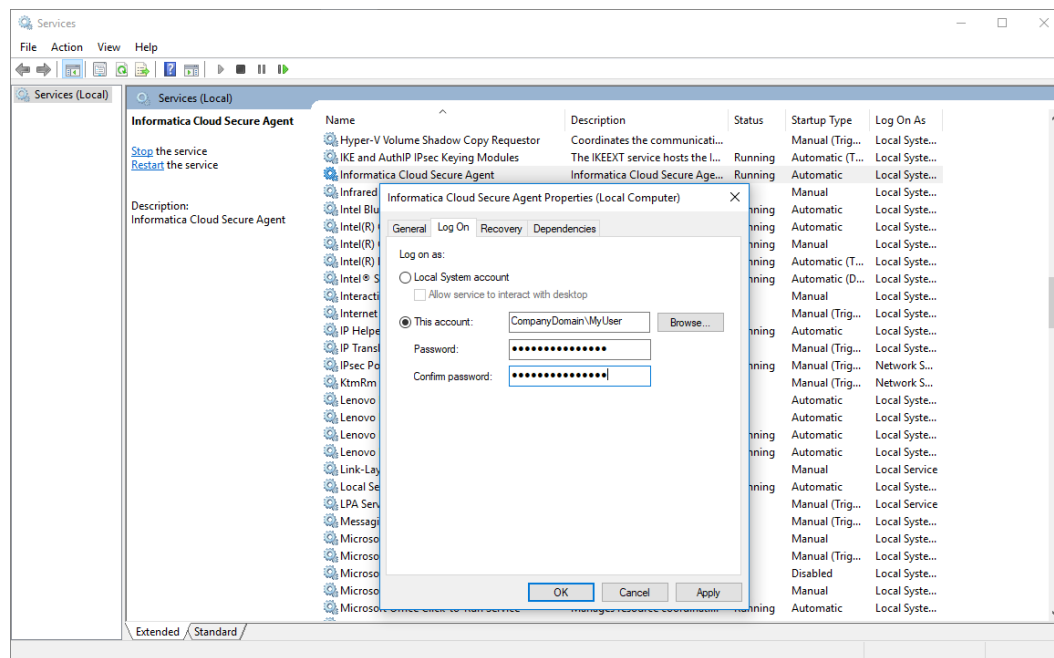
6. Click **OK**.

7. In the **Services** window, restart the Secure Agent service for the changes to take effect:
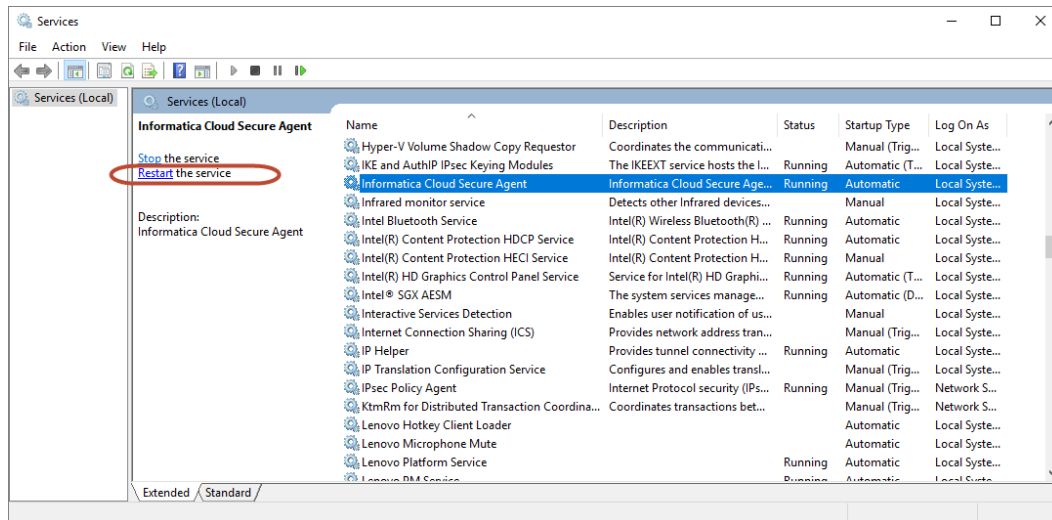
Next steps

After you install the Secure Agent, you can perform the following tasks:

- You can edit the Secure Agent name, update Secure Agent configuration properties, and add custom configuration properties to change or optimize Secure Agent behavior.

- By default, the Secure Agent is assigned to its own Secure Agent group. You can rename the Secure Agent group, if desired.

- If you have the appropriate license, you can add multiple Secure Agents to a single Secure Agent group to balance the workload across machines and improve scalability for connections and tasks.

- If you have the appropriate license, you can enable and disable services for a Secure Agent to reduce the potential demand on a Secure Agent group.

- If you have the appropriate license, you can share Secure Agent groups with your sub-organizations.

For more information, see "Secure Agent installation" in the Administrator help or this video.

Author

Lori Troy
Principal Technical Writer