SAP Data Services Agent Guide
## Content

1. SAP Data Services Agent for SAP Cloud Platform Integration .......................................................... 5
2. SAP Cloud Platform Integration architecture. ....................................................................................... 6
3. Planning and Preparation. ......................................................................................................................... 8
   3.1 Considerations for Using Multiple Agents. ...................................................................................... 9
   3.2 Linux user resource limits. ............................................................................................................... 10
4. Installing the SAP Data Services Agent. ............................................................................................... 11
5. Configuring the SAP Data Services Agent. .......................................................................................... 13
   5.1 Registering an Agent in the Web Interface. .................................................................................... 14
       About Agent Groups. ......................................................................................................................... 14
   5.2 Downloading the Agent Configuration File. .................................................................................. 15
   5.3 Configuring the Secure Agent Connection. .................................................................................... 16
       Reconfiguring the Agent Connection. ............................................................................................... 17
   5.4 Managing White-listed Directories. ................................................................................................. 17
   5.5 Connecting to Secure Web Services by Manually Adding Certificates. ........................................ 18
   5.6 Configuring SSL Support for SOAP Web Services. ..................................................................... 20
   5.7 Configuring the SuccessFactors Adapter. ..................................................................................... 21
   5.8 Configuring the OData Adapter. ...................................................................................................... 22
   5.9 Authenticating Client Certificates. .................................................................................................. 23
   5.10 Changing the Server Host Name. .................................................................................................. 24
   5.11 Updating the Agent Version. ......................................................................................................... 25
   5.12 Uninstalling the Agent. ................................................................................................................. 25
6. Importing Certificates. ........................................................................................................................... 27
7. Configuring SAP Business Suite Connectivity. .................................................................................... 29
   7.1 SAP Functions. ............................................................................................................................... 29
       Development versus Production Functions. ..................................................................................... 30
   7.2 Descriptions for SAP User Authorizations. .................................................................................... 31
       Open Hub: Administration for RFC Destination. ............................................................................. 34
       G_800S_GSE: Special Purpose Ledger Sets. ..................................................................................... 35
       S_BTCH_ADM: Background Processing. ......................................................................................... 35
       S_BTCHJOB: Batch Processing. ..................................................................................................... 35
       S_CTS_ADMI: Administration Functions in Change and Transport System. ..................................... 36
       S_DEVELOP: ABAP Workbench. ..................................................................................................... 36
       S_DSAUTH: SBOP Data Services - General Authorization. ............................................................ 37
A.3 Manually Uninstalling the Agent
1 SAP Data Services Agent for SAP Cloud Platform Integration

The SAP Data Services Agent provides secure connectivity to on-premise sources in your landscape. At design-time, the agent is used to provide metadata browsing functionality for on-premise sources to the web based user interface. At run-time, the agent will take care of the secure data transfer from the on-premise source to the targets in the cloud.

**Note**

While the SAP Data Services Agent is based on SAP Data Services technology, the two are not interchangeable. If you want to connect to SAP Cloud Platform Integration, you must use the SAP Data Services Agent.
2 SAP Cloud Platform Integration architecture

SAP Cloud Platform Integration for data services interacts with your local SAP landscape via the SAP Data Services Agent and secure HTTPS and RFC connections.

**Note**
Even when your data flows from the cloud to your on-premise landscape, there is no need to open the firewall to inbound traffic. The SAP Data Services Agent always initiates the request.
SuccessFactors BizX

When used with SuccessFactors BizX, the SAP Cloud Platform Integration architecture is slightly different:
3 Planning and Preparation

In order to securely transfer data from your on-premise sources to the cloud, you must install and configure the SAP Data Services Agent.

Before you begin the installation and configuration process, review the readiness checklist to ensure that you have all the required information and understand each step that you need to perform.

Readiness checklist

1. Review the agent system requirements and ensure that your host system meets the minimum requirements.
   - For a detailed list of supported environments and hardware requirements, consult the Product Availability Matrix (PAM). This information includes specific version and patch-level requirements for web application servers, web browsers, databases, and operating systems.
   - **Restriction**
     While the SAP Data Services Agent is based on SAP Data Services technology, the two are not interchangeable. Additionally, for Windows host systems, the agent cannot be installed on a host system where SAP Data Services or the Data Provisioning Agent for SAP HANA Smart Data Integration has already been installed. (This restriction does not apply to Linux host systems.)
   - If you are installing the agent on a Linux system, ensure that your host system has the following packages:
     - X Window
     - OpenGL libraries
     - libgtk-2_0-0
     - KornShell
     If any packages are missing, the dependent libraries can be found as operating system patches.

2. Ensure that you have the required installation information and resources.
   1. Download the agent installation package.
   2. Collect user account information required to run the installation program:
      - User name and password of the local user account that will run the SAP Data Services Agent service
      - **Note**
        While you must run the SAP Data Services Agent installation program with administrative privileges, the user account that will run the service does not require administrative privileges.
   3. Collect administrator account information for SAP Cloud Platform Integration:
      - User name and password for the SAP Cloud Platform Integration administrator account
   4. Register an agent in the SAP Cloud Platform Integration web interface and download the configuration file.
5. If you plan to use a proxy server, collect the necessary proxy information:
   ○ Host name and port for your proxy server
   ○ User name and password required by your proxy server (if required)

3. If you plan to read from or write to flat files, compile a list of the directories that will be accessed. Directories must be white-listed in the SAP Data Services Agent before you can access them in SAP Cloud Platform Integration.

4. If you plan to use web services (SOAP, RESTful or OData) that are secured with HTTPS, export the necessary certificates from the server hosting the web service.

5. If you plan to connect to SAP Business Suite applications, prepare your SAP systems:
   1. Install the required SAP function modules.
   2. Create an SAP user with the required authorizations or assign the authorizations to an existing user. The user you want to use to connect to the SAP Business Suite application requires the ZDSAUTH authorization. ZDSDEV may also be used to further restrict access.
   3. Configure an RFC connection, business extractors, and additional ABAP programs.
      For more information about the required functions and user authorizations, see “Configuring SAP Business Suite connectivity”.

6. If you plan to connect to a database, ensure that the correct connectivity drivers are installed on the host system for your Data Services agent. Refer to the Product Availability Matrix (PAM) for middleware version information. In all cases, the 64bit version of the driver is required.

7. Install the SAP Data Services Agent.
   During or after the installation process, configure the agent using the downloaded configuration file and other information that you have collected.

After completing the installation and configuration process, log in to the SAP Cloud Platform Integration web interface and see the Get Started tab for information about configuring projects and tasks.

Related Information

Considerations for Using Multiple Agents [page 9]
Linux user resource limits [page 10]
Configuring the SAP Data Services Agent [page 13]
Configuring SAP Business Suite Connectivity [page 29]
Installing the SAP Data Services Agent [page 11]
Connecting to Secure Web Services by Manually Adding Certificates [page 18]
Product Availability Matrix

3.1 Considerations for Using Multiple Agents

Depending on your requirements, you can use one or multiple agents to connect to SAP Cloud Platform Integration.

You might choose to use multiple agents for any of the following reasons:
- Large data load volumes - divide the load between multiple agents
- Fail-over support - if one agent host system is down or unreachable, your tasks will still run
- Separate agents for test and production tasks

**Restriction**

Windows host systems can support only one installed agent. Linux host systems can support multiple agents, but each agent must be run using a different operating system user.

When you use multiple agents, your datastores, projects, and other objects are not duplicated within SAP Cloud Platform Integration. Instead, you select the agent or agent group to use at run-time when you execute or schedule a task.

You can switch between agents freely as long as each agent is able to connect to the on-premise sources required in your task. For agents that use flat-file sources, each agent needs access to its own copy of the files, or you can use a network share to make them accessible to all agents.

**Tip**

When you edit a datastore connection, the agent that you choose is used only for metadata browsing. The agent specified in the datastore is not used when you execute a task at run-time.

### 3.2 Linux user resource limits

For installations on Linux host systems, it’s recommended that you use the following user resource limits. You can display these settings by running the `ulimit -a` command.

<table>
<thead>
<tr>
<th>User resource limit</th>
<th>Value</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>file (blocks)</td>
<td>unlimited</td>
<td></td>
</tr>
<tr>
<td>data (kilobytes)</td>
<td>unlimited</td>
<td></td>
</tr>
<tr>
<td>stack (kilobytes)</td>
<td>2048</td>
<td>2 MB</td>
</tr>
<tr>
<td>time (cpu-seconds)</td>
<td>unlimited</td>
<td></td>
</tr>
<tr>
<td>nofiles (descriptors)</td>
<td>1024</td>
<td></td>
</tr>
<tr>
<td>coredump (blocks)</td>
<td>unlimited</td>
<td></td>
</tr>
<tr>
<td>memory (kilobytes)</td>
<td>unlimited</td>
<td></td>
</tr>
<tr>
<td>lockedmem (kilobytes)</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>processes</td>
<td>7168</td>
<td></td>
</tr>
</tbody>
</table>
4 Installing the SAP Data Services Agent

The SAP Data Services Agent installation program is distributed in a self-extracting executable.

Procedure

1. Extract the installation package and start the installation program.
   - **Windows:** Run `DataServices-Agent-Installer.exe`. You must run the installation program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the `Run as administrator` option.
   - **Linux:** Run `DataServices-Agent-Installer.bin`. Do not install as root.

   After the package has been extracted, the installation program starts automatically.

2. Specify the location where you want to install the software.
   - On Windows platforms, the default installation location is `C:\Program Files\SAP\DataServicesAgent`.
   - On Linux platforms, the default installation location is `$HOME/DataServicesAgent`.

3. On Windows, specify the location where the agent should store log files and settings.
   
   The logs and settings path is referenced by the `<DS_COMMON_DIR>` environment variable. The default location is `C:\ProgramData\SAP\DataServicesAgent`.

4. Specify the user name and password for the local user account that will be used to run the job service.

   - **Note** For domain user accounts, specify the user name using the format `<DOMAIN>\<username>`. For local accounts, only the user name is required.

5. If you do not want to use the default ports, check **Specify port numbers used by installation**.
   
   Specify new port numbers as required.

   - **Note** If the installation program detects that the default ports are already in use, this option will be checked automatically.

6. Click **Install**.

   The installation progress is displayed. During the installation process, the installation program creates a log file at the following location:
   - On Windows platforms, `%DS_COMMON_DIR%\log\Install_<timestamp>.log`
   - On Linux platforms, `<install_dir>\log\install_<timestamp>.log`
Next Steps

After the installation process is complete, you can choose to configure the Agent immediately or at a later time.

Related Information

Configuring the SAP Data Services Agent [page 13]
5 Configuring the SAP Data Services Agent

Before you can use the SAP Data Services Agent to securely transfer your on-premise data with SAP Cloud Platform Integration, you must configure your instance of the agent.

1. Register the agent in the SAP Cloud Platform Integration web interface
2. Download the agent configuration file
3. Configure the secure agent connection

During initial configuration, or at a later time, you may need to change the software’s configuration to meet your requirements.

- Change the hostname of the SAP Cloud Platform Integration server
- Add or remove directories that may be accessed by the agent
- Change an adapter configuration
- Uninstall the agent from the host system

Related Information

- Registering an Agent in the Web Interface [page 14]
- Downloading the Agent Configuration File [page 15]
- Configuring the Secure Agent Connection [page 16]
- Managing White-listed Directories [page 17]
- Connecting to Secure Web Services by Manually Adding Certificates [page 18]
- Configuring SSL Support for SOAP Web Services [page 20]
- Configuring the SuccessFactors Adapter [page 21]
- Configuring the OData Adapter [page 22]
- Authenticating Client Certificates [page 23]
- Changing the Server Host Name [page 24]
- Updating the Agent Version [page 25]
- Uninstalling the Agent [page 25]
5.1 Registering an Agent in the Web Interface

Before you can configure a local SAP Data Services Agent instance, you must register the agent in the SAP Cloud Platform Integration interface.

Procedure

1. Log in to SAP Cloud Platform Integration as an administrator.
2. Go to the Agents area.
3. Click Create New Agent.
4. Specify the name, location, group, and optionally a description for the agent.

Next Steps

After registering the agent, you can choose to download the configuration file immediately. If you plan to configure the SAP Data Services Agent at a later time, you can download the configuration file later by returning to the Agents section.

Related Information

About Agent Groups [page 14]
Downloading the Agent Configuration File [page 15]
Configuring the Secure Agent Connection [page 16]

5.1.1 About Agent Groups

Agent groups are collections of agents (typically in the same location) that are logically grouped to enable high-availability solutions for your production tasks.

When you assign tasks to an agent group instead of an individual agent, SAP Cloud Platform Integration for data services can assign the task to any available agent in the group. You do not have to worry about whether a specific agent is available or not. Administrators can create and configure agent groups in the Agents area of the SAP Cloud Platform Integration for data services web UI.

Note

Agents created before version 1.0.6 will be automatically assigned to a default agent group, which is named after the organization.
Agent groups have the following restrictions:

- Every registered agent must belong to a group.
- A group must have at least one agent.
- An agent can only belong to one group at a time.
- An agent group must have at least one active, running agent in order to be selected to run a task.
- Actions which will result in an agent group being deleted (such as moving the last agent in the group) will not be allowed if the group has active schedules assigned to it.
- All agents in a group must be configured to have the same:
  - Shared location for file reader or file loader
  - Use proxy server setting and proxy server (if used)
  - SSL .pem file
  - PGP keys

5.2 Downloading the Agent Configuration File

When you configure the secure connection for an SAP Data Services Agent instance, you need to provide a configuration file from SAP Cloud Platform Integration.

Procedure

1. Log into SAP Cloud Platform Integration as an administrator.
2. Navigate to the Agents section.
3. Select the agent that you want to configure.
4. Choose Download Config File from Actions.

Related Information

Registering an Agent in the Web Interface [page 14]
Configuring the Secure Agent Connection [page 16]
5.3 Configuring the Secure Agent Connection

After installing the SAP Data Services Agent, you must configure the secure connection before the agent can be used with SAP Cloud Platform Integration.

**Prerequisites**

Before you begin, register the agent in the SAP Cloud Platform Integration web interface and download the configuration file.

**Procedure**

1. If you did not choose to start configuration immediately after installation, start the SAP Data Services Agent configuration program.
   - On Windows platforms, run `configureAgent.bat`.
   - On Linux platforms, run `configureAgent.sh`.

   **i Note**
   
   You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

   By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click Set up Agent.

3. Specify your SAP Cloud Platform Integration administrator user name and password and the location of the configuration file you downloaded.

4. If you are upgrading an existing agent or need to re-identify the agent instance with the cloud, select Upload the unique agent ID.
   
   The agent ID uniquely identifies the agent instance with the SAP Cloud Platform Integration server to ensure that messages from old or incorrect agents are not processed.

5. If the host system where the SAP Data Services Agent is installed is located behind a firewall, configure the agent to use a proxy.
   - Select Use proxy server.
   - Specify the address and port information for your proxy server.
   - If your proxy server requires authentication, select Proxy requires authentication and specify the user name and password.

6. Click Upload.

   The configuration program connects to SAP Cloud Platform Integration, uploads security certificates, and verifies that the configuration was successful. If there are no errors, the status of the agent in the SAP Cloud Platform Integration interface changes to indicate that the agent is registered correctly.
If you are done configuring the SAP Data Services Agent, click Exit to close the configuration program.

**Note**
When you change the agent configuration, the SAP Data Services Agent service must be restarted for the changes to take effect. You can choose to automatically restart the service when closing the configuration program, or to manually restart the service at a later time.

**Related Information**
- Reconfiguring the Agent Connection [page 17]
- Registering an Agent in the Web Interface [page 14]
- Downloading the Agent Configuration File [page 15]

### 5.3.1 Reconfiguring the Agent Connection

If you need to change the username and password used by the SAP Data Services Agent or your proxy information has changed, you can update the agent configuration.

To reconfigure the agent, run the SAP Data Services Agent configuration program.

**Note**
If you want to change the registration of the agent in SAP Cloud Platform Integration, you must uninstall and reinstall the SAP Data Services Agent on the host system.

### 5.4 Managing White-listed Directories

To read from and write to flat files in SAP Cloud Platform Integration, you must authorize the SAP Data Services Agent to access directories on the host system.

**Procedure**

1. Start the SAP Data Services Agent configuration program.
   - On Windows platforms, run `configureAgent.bat`.
   - On Linux platforms, run `configureAgent.sh`. 
You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click Configure Directories. The list of directories that the SAP Data Services Agent may access is displayed.

3. Configure the accessible directories.
   - To add a new directory to the list, click Add and browse to the directory that you want to add.
   - To remove a directory from the list, select the directory and click Remove.

4. If you are done configuring the SAP Data Services Agent, click Exit to close the configuration program.

When you change the directory configuration, the SAP Data Services Agent service must be restarted for the changes to take effect. You can choose to automatically restart the service when closing the configuration program, or to manually restart the service at a later time.

5.5 Connecting to Secure Web Services by Manually Adding Certificates

To connect to web services (SOAP, RESTful or OData) that are secured with HTTPS, add your custom certificates to the trusted certificates directory on the server hosting your Data Services agent.

Context

The manual process described here can be done automatically using the Import Certificates dialog in the Data Services Agent Configuration tool.
Procedure

1. Obtain a signed certificate from the server where the web service is hosted.
   Export the certificate from the tools or settings of your web browser. The certificate must be saved with the file extension .cer and start with -----BEGIN CERTIFICATE-----.
   For Restful and SOAP web services, export the certificate in base-64 encoded X.509 (.cer) file format. For OData, export the certificate in either base-64 encoded X.509 (.cer) or DER encoded binary X.509 (.cer) file format.
2. Save your .cer file in the trusted_certs directory.
   The directory is located at <LINK_DIR>\ssl\trusted_certs.
3. Run <LINK_DIR>\bin\SetupJavaKeystore.bat
   Running this command regenerates the keystore based on all certificates located in the trusted certificates directory.

   **Note**
   You must run the command from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

4. Check if the file dsod.pem exists in the directory <DS_COMMON_DIR>\conf and then do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
   | If the dsod.pem file exists... | 1. Stop the Data Services Agent.  
                                 | 2. Rename the dsod.pem file. For example rename to dsod.pem.bak.  
                                 | 3. Start the Data Services Agent.                                      |
   | If the dsod.pem file does not exist... | No action necessary                             |

   The Agent will scan the trusted_certs directory for all .cer files and add your .cer to the list of trusted certificates.

   **Note**
   You must use a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

Related Information

Importing Certificates [page 27]
Importing Certificates [page 27]
5.6 Configuring SSL Support for SOAP Web Services

To configure SSL support for SOAP web services, you must enable the SERVER_CERT parameter.

Prerequisites

Ensure you have imported a signed certificate from the server where the web service is hosted. If needed, you can import the certificate by one of the following methods: Importing Certificates [page 27] or Connecting to Secure Web Services by Manually Adding Certificates [page 18]:

Procedure

1. Open LINK_DIR\ext\webservice-c\axis2.xml in a text editor.
2. Locate the commented SERVER_CERT element in the XML:

   <!--<parameter name="SERVER_CERT">/path/to/ca/certificate</parameter> -->

3. Remove the comment tags <!-- --> around the SERVER_CERT element.
4. In the SERVER_CERT parameter, enter the full path (including the certificate file name) to the CA certificate stored in the trusted_certs directory.

   <parameter name="SERVER_CERT"><LINK_DIR>\ssl\trusted_certs\<file_name.crt></parameter>

   For example:

   <parameter name="SERVER_CERT"> C:\ProgramData\SAP BusinessObjects\Data Services\ssl\trusted_certs\<file_name.crt></parameter>

Related Information

Importing Certificates [page 27]
Connecting to Secure Web Services by Manually Adding Certificates [page 18]
5.7 Configuring the SuccessFactors Adapter

To read from and write to a SuccessFactors instance, you must configure the SuccessFactors adapter in the SAP Data Services Agent.

Procedure

1. Start the SAP Data Services Agent configuration program.
   - On Windows platforms, run `configureAgent.bat`.
   - On Linux platforms, run `configureAgent.sh`.

   **i Note**
   You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

   By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click Configure Adapters.
   The adapter configuration page is displayed.

3. Configure the SuccessFactors adapter as required for your instance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter Retry Count</td>
<td>The number of times the agent should attempt to start the adapter.</td>
</tr>
<tr>
<td>Adapter Retry Interval</td>
<td>The amount of time the agent should wait between attempts to start the adapter, in milliseconds.</td>
</tr>
<tr>
<td>Trace Mode</td>
<td>Enables or disables trace logging for the adapter.</td>
</tr>
<tr>
<td>Additional Java Launcher Options</td>
<td>Additional options to use when starting the adapter instance.</td>
</tr>
</tbody>
</table>

4. Click Save to save your configuration changes.

5. If you are done configuring the SAP Data Services Agent, click Exit to close the configuration program.

   **i Note**
   When you change the agent configuration, the SAP Data Services Agent service must be restarted for the changes to take effect. You can choose to automatically restart the service when closing the configuration program, or to manually restart the service at a later time.
5.8 Configuring the OData Adapter

To read from and write to an OData instance, you must configure the OData adapter in the SAP Data Services Agent.

Procedure

1. Start the SAP Data Services Agent configuration program.
   ○ On Windows platforms, run `configureAgent.bat`.
   ○ On Linux platforms, run `configureAgent.sh`.

2. Click Configure Adapters.
   The adapter configuration page is displayed.

3. Configure the OData adapter as required for your instance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter Retry Count</td>
<td>The number of times the agent should attempt to start the adapter.</td>
</tr>
<tr>
<td>Adapter Retry Interval</td>
<td>The amount of time the agent should wait between attempts to start the adapter, in milliseconds.</td>
</tr>
<tr>
<td>Trace Mode</td>
<td>Enables or disables trace logging for the adapter.</td>
</tr>
<tr>
<td>Additional Java Launcher Options</td>
<td>Additional options to use when starting the adapter instance.</td>
</tr>
<tr>
<td></td>
<td>The proxy can be disabled by removing the default proxy line from this field.</td>
</tr>
<tr>
<td></td>
<td>Additionally, to support a client authentication certificate, from the Agent Configuration Tool, copy the line of generated output from the Configure Client Authentication tab that provides the keystore and password. For example, <code>Djavax.net.ssl.keyStore=&quot;C:\Program Files\SAP\DataServicesAgent\ssl\client_certs\&lt;keystoreName&gt;.jks&quot; -Djavax.net.ssl.keyStorePassword=&lt;*****&gt;</code></td>
</tr>
</tbody>
</table>

4. Click Save to save your configuration changes.

5. If you are done configuring the SAP Data Services Agent, click Exit to close the configuration program.

   When you change the agent configuration, the SAP Data Services Agent service must be restarted for the changes to take effect. You can choose to automatically restart the service when closing the configuration program, or to manually restart the service at a later time.
Related Information

Authenticating Client Certificates [page 23]

5.9 Authenticating Client Certificates

You must generate a Java keystore output in order to authenticate a client certificate to be sent to the server.

Prerequisites

1. Obtain the signed client certificate.
2. Obtain the private key associated with the client certificate
3. Extract and download the end-entity, intermediate, and root chain certificates from the signed client certificate:
   1. In the certificate, select the certificate path.
   2. Select View Certificate.
   3. Choose Copy to File.
   4. Select Base-64 encoded X.509(.CER).
   5. Repeat steps a-c to download each of the three chain certificates.

Context

A client certificate is sent from the client to the server at the start of a session and is used by the server to authenticate the client. Follow these steps to generate and import the Java keystore that is used to verify the client.

Procedure

1. Launch the Agent Configuration Tool.
2. Select Configure Client Authentication on the left-hand side menu.
3. Create a name for the Java keystore in the Keystore field. The generated Java keystore will be stored under this file name.
4. Create a password for the Java keystore in the Password field.
5. Upload the Private Key associated with the client certificate.
6. Upload the End-Entity Certificate.
8. Upload the Root Certificate.
9. Click Generate and Import.

The Java keystore file will be generated under %LINK_DIR%\ssl\client_certs. It will also copy the intermediate and root certificate that you downloaded from the chain certificate to %LINK_DIR%\ssl \trusted_certs and import the certificates into the trustStore. You can now use the generated output in the Configure Adapter tab of the Agent Configuration Tool to authenticate a client certificate.

Related Information

Configuring the OData Adapter [page 22]

5.10  Changing the Server Host Name

If your agent connects to an instance of SAP Cloud Platform Integration that is not hosted in the SAP HANA cloud, you may need to update the server host name if it changes.

Procedure

1. Start the SAP Data Services Agent configuration program.
   ○ On Windows platforms, run configureAgent.bat.
   ○ On Linux platforms, run configureAgent.sh.

   **Note**
   You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

   By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click Set up Agent.

3. Select Update the SAP HANA Cloud Platform Integration server host name and enter the new host name for the instance.

4. Click Update to save your changes to the agent configuration.

5. If you are done configuring the SAP Data Services Agent, click Exit to close the configuration program.

   **Note**
   When you change the server host name, the SAP Data Services Agent service must be restarted for the changes to take effect. You can choose to automatically restart the service when closing the configuration program, or to manually restart the service at a later time.
5.11 Updating the Agent Version

If you need to promote and run tasks created in a newer version of SAP Cloud Platform Integration, you must update the SAP Data Services Agent to the new version.

To update the version of the agent installed on your host system, run the standard SAP Data Services Agent installation program. When the installation program detects that an older version of the agent is already installed on the host system, it automatically updates the existing installation instead of performing a new installation.

Related Information

Installing the SAP Data Services Agent [page 11]

5.12 Uninstalling the Agent

If you need to remove the SAP Data Services Agent from the host system, you can use a script to uninstall the agent.

Procedure

1. Close any open files, windows, or command prompts in the %LINK_DIR% or %DS_COMMON_DIR% folders.

   By default, %LINK_DIR% and %DS_COMMON_DIR% are located at the following locations:
   - On Windows platforms, C:\Program Files\SAP\DataServicesAgent and C:\ProgramData\SAP\DataServicesAgent
   - On Linux platforms, $HOME/DataServicesAgent

   If you don’t close open files in these locations, the uninstallation script may be unable to remove all agent files, and manual cleanup may be required.

2. Start the uninstallation process.

   - On Windows platforms, run uninstall.bat.

   You can also start the uninstallation process from Programs and Features in the Windows Control Panel. Select the SAP Data Services Agent and click Uninstall.

   - On Linux platforms, run uninstall.sh.
You must run the uninstallation script from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

By default, the uninstallation script is located in the directory where the SAP Data Services Agent was installed on the host system.

Results

The uninstallation script stops and removes the SAP Data Services Agent service, and removes all SAP Data Services Agent files from the host system.

Next Steps

After uninstallation, uninstall.bat or uninstall.sh and uninstall.log will be left in the %LINK_DIR% folder. If you want to remove all traces of the agent, you can manually remove these files after the uninstallation script has finished.

Related Information

Stopping the Internal Database [page 66]
Manually Uninstalling the Agent [page 66]
6 Importing Certificates

You may need to import new or updated certificates for secure communication between the Data Services Agent and other servers such as those hosting web services or OData.

Context

The Data Services Agent configuration tool eliminates the manual steps associated with updating the Data Services Agent keystore.

Procedure

1. If the SAP Data Services Agent configuration program is not already open, open it.
   - On Windows platforms, run `configureAgent.bat`.
   - On Linux platforms, run `configureAgent.sh`.

   **i Note**
   You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the *Run as administrator* option.

   By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click *Import Certificates*.

3. Specify the certificates you want to import by one of three methods:

<table>
<thead>
<tr>
<th>Method</th>
<th>General use case</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a certificate file</td>
<td>SAP Cloud Platform Integration server</td>
<td>Browse to the location of the updated or new certificate.</td>
</tr>
</tbody>
</table>

   **i Note**
   This is unusual. When needed, updated certificates are included in support package or patch releases.

   Proxy server
Download certificates from an http server
As needed, also specify the proxy server host and port as well as proxy user and password.

<table>
<thead>
<tr>
<th>Method</th>
<th>General use case</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download certificates from an http server</td>
<td>Web service</td>
<td>http://&lt;serverabcd&gt;:&lt;8080&gt;</td>
</tr>
<tr>
<td>As needed, also specify the proxy server host and port as well as proxy user and password.</td>
<td>Proxy server</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **Import**.

After the import is complete, the **SAP Data Services Agent** service automatically restarts.

**Related Information**

Troubleshooting [page 64]
7 Configuring SAP Business Suite Connectivity

If you want to use SAP Cloud Platform Integration to connect to your SAP Business Suite applications, you must configure user authorizations and functions on the SAP application.

SAP Functions [page 29]
The SAP Data Services Agent functions have a naming convention that includes a prefix.

Descriptions for SAP User Authorizations [page 31]
To access and integrate SAP Business Suite data, ensure that you have specific authorizations that support SAP Data Services Agent operations.

Authenticating with Secure Network Communications (SNC) [page 51]
Enabling SNC provides a secure connection between SAP systems and the SAP Data Services Agent.

Considerations for Running ABAP Programs [page 52]
When you use ABAP transforms in an SAP Cloud Platform Integration data flow, there are additional configuration options that you need to consider.

Set Up the Communication between BW and Agent [page 55]
You must configure the RFC destination including the Program ID to enable loading data from SAP Cloud Platform Integration to SAP BW.

Related Information

7.1 SAP Functions

The SAP Data Services Agent functions have a naming convention that includes a prefix.

The prefix of /SAPDS/ or /BODS/ is included with the corresponding SAP function names. The prefix depends on the version of the SAP NetWeaver in use.

To extract data from an SAP Business Suite system, ensure that you run an SAP NetWeaver support package that includes the required function modules.

Related Information

Development versus Production Functions [page 30]
7.1.1 Development versus Production Functions

The SAP Data Services Agent functions are intended for use in either a development or production environment.

Additionally, user permissions differ between development and production environments.

Depending on the SAP NetWeaver version, the namespace for the Data Services Agent is `/SAPDS/` or `/BODS/`. For example, the fully qualified name of the AUTH_IMPORT function is either `/SAPDS/AUTH_IMPORT` or `/BODS/AUTH_IMPORT`.

Development-only functions

Use the following functions only in a development environment:

- AUTH_IMPORT
- EXTRACTOR_IMPORT
- FUNCTION_GET
- IDOC_IMPORT
- RFC_ABAP_INSTALL_RUN
- TABLE_IMPORT
- TREE_IMPORT
- TREE_IMPORT40
- UPLOAD

Production functions

Use the following functions only in a production environment:

- ABAP_RUN
- BW_QUERY
- COLUMN_SEARCH
- DATA_PROFILE
- EXTRACTOR.Navigate
- EXTRACTOR_SEARCH
- FILE_ROW_COUNT
- GET_VERSION
- IDOC_SEARCH
- JOB_LOG
- JOB_RUN
- JOB_STATUS
- MODEL_NAVIGATE
- READ_TEXT
- RFC_READ_EXTRACTOR
To access and integrate SAP Business Suite data, ensure that you have specific authorizations that support SAP Data Services Agent operations. Determine the required authorizations based on factors that include the following dependencies:

- Mode of transportation
- ABAP mode
- Source system version

As part of your planning process, determine your required authorizations and then request that they be included in the profile associated with your SAP user.

Tip
For improved security, avoid using wildcards, generic, or blank values for authorization fields, especially in a production environment. Instead use specific values that are appropriate to your business applications.

The following table helps you determine the required authorizations based on your specific needs.

<table>
<thead>
<tr>
<th>In order to....</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process batch jobs</td>
<td>S_BTCH_JOB: Batch Processing [page 35]</td>
</tr>
<tr>
<td>Perform the following actions:</td>
<td>S_DEVELOP: ABAP Workbench [page 36]</td>
</tr>
<tr>
<td>• perform a column search</td>
<td></td>
</tr>
<tr>
<td>• run generated programs on the SAP server</td>
<td></td>
</tr>
<tr>
<td>• import a table</td>
<td></td>
</tr>
<tr>
<td>• search for a table</td>
<td></td>
</tr>
<tr>
<td>Execute remote functions on an SAP server</td>
<td>S_RFC: Authorization Check for RFC Access [page 40]</td>
</tr>
<tr>
<td>Access table data in an SAP system</td>
<td>S_TABU_DIS: Table Maintenance [page 46]</td>
</tr>
<tr>
<td>In order to</td>
<td>Authorization</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access specific transactions</td>
<td>S_TCODE: Authorization Check for Transaction Start [page 46]</td>
</tr>
<tr>
<td>Execute functions in the Data Warehousing Workbench</td>
<td></td>
</tr>
<tr>
<td>Access ERP hierarchies</td>
<td>G_800S_GSE: Special Purpose Ledger Sets [page 35]</td>
</tr>
<tr>
<td>Check background processing privileges</td>
<td>S_BTCH_ADM: Background Processing [page 35]</td>
</tr>
<tr>
<td>Perform CTS operations</td>
<td>S_CTS_ADM: Administration Functions in Change and Transport System [page 36]</td>
</tr>
<tr>
<td>Work with IDocs</td>
<td>S_IDOCDEFT: Access to IDoc Development [page 39]</td>
</tr>
<tr>
<td>Stream using RFC</td>
<td>S_RFC_ADM: Administration for RFC Destination [page 40]</td>
</tr>
<tr>
<td>Check DataSource access privileges</td>
<td>S_RO_OSOA: SAP DataSource Authorizations [page 40]</td>
</tr>
<tr>
<td>Load to BW</td>
<td>S_RS_ADMWB: Administrator Workbench - Objects [page 41]</td>
</tr>
<tr>
<td>Access an InfoCube</td>
<td>S_RS_ICUBE: Data Warehousing Workbench - InfoCube [page 41]</td>
</tr>
<tr>
<td>Access a DataStore Object</td>
<td>S_RS_ODSO: Data Warehousing Workbench - DataStore Object [page 42]</td>
</tr>
<tr>
<td>Read SAP texts</td>
<td>S_SCRP_TXT: SAPscript [page 42]</td>
</tr>
<tr>
<td>Access the SAP Data Services Agent functions</td>
<td>S_SDAUTH: SBOP Data Services - General Authorization [page 43]</td>
</tr>
<tr>
<td></td>
<td>S_DSAUTH: SBOP Data Services - General Authorization [page 37]</td>
</tr>
<tr>
<td></td>
<td>ZDSAUTH: SBOP Data Services - General Authorization [page 48]</td>
</tr>
<tr>
<td>SAP Data Services Agent-specific equivalent of the SAP S_DEVELOP authorization object</td>
<td>S_DSDEV: SBOP Data Services Authorization Object for Development [page 44]</td>
</tr>
<tr>
<td></td>
<td>S_DSDEV: SBOP Data Services Authorization Object for Development [page 38]</td>
</tr>
<tr>
<td></td>
<td>ZDSDEV: SBOP Data Services Authorization Object for Development [page 49]</td>
</tr>
<tr>
<td>In order to....</td>
<td>Authorization</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
</tr>
</tbody>
</table>
| Execute programs | S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 45]  
S_DSPGMCHK: SBOP Data Services Authorization Object for Program Names [page 39]  
ZPGMCHK: SBOP Data Services Authorization Object for Program Names [page 49] |
| Define whether the SAP system should be treated as a development or production system | S_SDSS: Data Services Authorization Object for Functions [page 45]  
S_SDS: Data Services Authorization Object for Functions [page 42]  
ZDSDEV: SBOP Data Services Authorization Object for Development [page 49] |
| Access the Transport Organizer | S_TRANSPRT: Transport Organizer [page 47] |
| Establish a connection to the SAP server | S_USER_GRP: User Master Maintenance [page 47] |
| Import an authorization profile | S_USER_PRO: User Master Maintenance [page 48] |
| Use the Open Hub interface | Open Hub: Administration for RFC Destination [page 34] |
| Browse metadata in an SAP BW source datastore | Browse Metadata for an SAP BW Source Datastore [page 51] |

### Related Information

Open Hub: Administration for RFC Destination [page 34]  
G_800S_GSE: Special Purpose Ledger Sets [page 35]  
S_BTCHADM: Background Processing [page 35]  
S_BTCHJOB: Batch Processing [page 35]  
S_CTS_ADM: Administration Functions in Change and Transport System [page 36]  
S_DEVELOP: ABAP Workbench [page 36]  
S_DSAUTH: SBOP Data Services - General Authorization [page 37]  
S_DSDEV: SBOP Data Services Authorization Object for Development [page 38]  
S_DSPGMCHK: SBOP Data Services Authorization Object for Program Names [page 39]  
S_IDOCDEFT: Access to IDoc Development [page 39]  
S_RFC: Authorization Check for RFC Access [page 40]  
S_RFCADM: Administration for RFC Destination [page 40]  
S_RO_OSOA: SAP DataSource Authorizations [page 40]  
S_RS_ADMWB: Administrator Workbench - Objects [page 41]  
S_RS_ICUBE: Data Warehousing Workbench - InfoCube [page 41]
7.2.1 Open Hub: Administration for RFC Destination

The S_BI_WHM_RFC profile contains the necessary authorizations to use the Open Hub interface in SAP Data Services Agent.

Additionally, SAP Data Services Agent needs the S_RFC_ADM authorization to work with the Open Hub interface.

**Purpose:** This object includes authorization checks for accessing individual administration functions in transaction SM59.

**Use:** DEV, PROD

**Text (Description):** Administration for RFC Destination

**Class:** Cross-application Authorization Objects

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
<tr>
<td>RFCTYPE</td>
<td>T</td>
</tr>
<tr>
<td>RFCDEST</td>
<td>List of RFC destinations the user is allowed to access</td>
</tr>
<tr>
<td>ICF_VALUE</td>
<td>Authorizations for destination in transaction SM59</td>
</tr>
</tbody>
</table>

**Related Information**

S_RFC_ADM: Administration for RFC Destination [page 40]
7.2.2 G_800S_GSE: Special Purpose Ledger Sets

The G_800S_GSE authorization allows SAP Data Services Agent to access ERP hierarchies.

**Use:** DEV, PROD

**Text (Description):** Special Purpose Ledger Sets: Set

**Class:** Financial Accounting

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization group</td>
<td>Not used</td>
</tr>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
</tbody>
</table>

7.2.3 S_BTCH_ADM: Background Processing

The S_BTCH_ADM authorization checks background processing privileges.

**Use:** DEV, PROD

**Text (Description):** Background Processing: Background Administrator

**Class:** Basis

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background administrator ID</td>
<td>Y</td>
</tr>
</tbody>
</table>

7.2.4 S_BTCH_JOB: Batch Processing

The S_BTCH_JOB authorization checks privileges for releasing batch jobs.

**Use:** DEV, PROD

**Text (Description):** Batch processing

**Class:** Basis

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job operation</td>
<td>RELE</td>
</tr>
<tr>
<td>Summary of jobs for a group</td>
<td>Not used</td>
</tr>
</tbody>
</table>
7.2.5  S_CTS_ADMI: Administration Functions in Change and Transport System

The S_CTS_ADMI authorization allows SAP Data Services Agent to perform CTS operations.

Use: DEV

Text (Description): Administration Functions in Change and Transport System

Class: Basis: Administration

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Tasks for Change and Transport PROJ System</td>
<td>PROJ</td>
</tr>
</tbody>
</table>

7.2.6  S_DEVELOP: ABAP Workbench

SAP Data Services Agent uses the S_DEVELOP authorization in several ways.

Purpose: This implementation of S_DEVELOP allows SAP Data Services Agent to perform a column search.

Use: DEV, PROD

Text (Description): ABAP Workbench

Class: Basis - Development Environment

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>List of packages for tables that a user is allowed to access</td>
</tr>
<tr>
<td>Object type</td>
<td>TABL</td>
</tr>
<tr>
<td>Object name</td>
<td>List of tables that a user is allowed to access</td>
</tr>
<tr>
<td>Authorization group</td>
<td>ABAP/4 program</td>
</tr>
<tr>
<td>Authorization group ABAP/4 program</td>
<td>Not used</td>
</tr>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
</tbody>
</table>

Purpose: The S_DEVELOP authorization allows SAP Data Services Agent to run generated programs on the SAP server.

Use: DEV

Text (Description): ABAP Workbench

Class: Basis - Development Environment

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>$TMP</td>
</tr>
<tr>
<td>Object type</td>
<td>PROG</td>
</tr>
</tbody>
</table>
### Purpose
This implementation allows SAP Data Services Agent to import a table or to search for a table.

**Use:** DEV, PROD (table search)

**Text (Description):** ABAP Workbench

**Class:** Basis - Development Environment

### 7.2.7 S_DSAUTH: SBOP Data Services - General Authorization

The S_DSAUTH authorization gives a user access to SAP Data Services Agent functions.

**Use:** DEV, PROD

**Text (Description):** SBOP Data Services - general authorization

**Class:** SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT: Activity</td>
<td>16 (Execute)</td>
</tr>
</tbody>
</table>

**Note**
In some SAP NetWeaver versions, this authorization object is named ZDSAUTH or S_SDSAUTH. The objects are identical except for the name.

### Related Information

- S_DSAUTH: SBOP Data Services - General Authorization [page 43]
- ZDSAUTH: SBOP Data Services - General Authorization [page 48]
- ZDSAUTH: SBOP Data Services - General Authorization [page 48]
7.2.8 S_DSDDEV: SBOP Data Services Authorization Object for Development

S_DSDDEV is the general authorization object that is the SAP Data Services Agent-specific equivalent of the SAP S_DEVELOP authorization object.

Use: DEV, PROD

Text (Description): SBOP Data Services Authorization Object for development

Class: SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>List of packages for tables that a user is allowed to access</td>
</tr>
<tr>
<td>Object type</td>
<td>VIEW, TABL, and TTYP</td>
</tr>
<tr>
<td>Object name</td>
<td>DD objects that a user is allowed to access</td>
</tr>
<tr>
<td>Authorization group</td>
<td>Not used</td>
</tr>
<tr>
<td>ABAP/4 program</td>
<td></td>
</tr>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
</tbody>
</table>

**i Note**

In some SAP NetWeaver versions, this authorization object is named S_SDSDEV or ZDSDEV. The objects are identical except for the name.

**Related Information**

S_SDSDEV: SBOP Data Services Authorization Object for Development [page 44]
S_SDSDEV: SBOP Data Services Authorization Object for Development [page 44]
ZDSDEV: SBOP Data Services Authorization Object for Development [page 49]
ZDSDEV: SBOP Data Services Authorization Object for Development [page 49]
S_SDSDEV: SBOP Data Services Authorization Object for Development [page 44]
ZDSDEV: SBOP Data Services Authorization Object for Development [page 49]
7.2.9  S_DSPGMCHK: SBOP Data Services Authorization Object for Program Names

The S_DSPGMCHK authorization determines which programs may execute in a production environment.

**Use:** PROD

**Text (Description):** SBOP Data Services Authorization Object for program names

**Class:** SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT: Activity</td>
<td>16 (Execute)</td>
</tr>
<tr>
<td>PROGRAM: ABAP program name</td>
<td>Program names that are allowed to be executed in a production environment</td>
</tr>
</tbody>
</table>

**Note**

In some SAP NetWeaver versions, this authorization object is named S_SDSPGMCK or ZPGMCHK. The objects are identical except for the name.

**Related Information**

- S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 45]
- S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 45]
- ZPGMCHK: SBOP Data Services Authorization Object for Program Names [page 49]
- ZPGMCHK: SBOP Data Services Authorization Object for Program Names [page 49]
- S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 45]
- ZPGMCHK: SBOP Data Services Authorization Object for Program Names [page 49]

7.2.10  S_IDOCDEFT: Access to IDoc Development

The S_IDOCDEFT authorization allows SAP Data Services Agent to work with IDocs.

**Use:** DEV, PROD

**Text (Description):** WFEDI: S_IDOCDEFT - Access to IDoc Development

**Class:** Basis - Central Functions

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
<tr>
<td>Extension</td>
<td>Not used</td>
</tr>
<tr>
<td>Basic type</td>
<td>Not used</td>
</tr>
</tbody>
</table>
7.2.11 S_RFC: Authorization Check for RFC Access

The S_RFC authorization allows users to execute remote functions on an SAP server.

**Use:** DEV, PROD

**Text (Description):** Authorization check for RFC access

**Class:** Cross-application authorization object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction code</td>
<td>WE30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>16</td>
</tr>
<tr>
<td>Name of RFC to be protected</td>
<td>BAPI, CADR, RFC1, SCAT, SDIF, SLST, SUNI, SUTL, SDTX, SYST, /BODS/BODS, RSAB, SDIFRUNTIME, and any other required function group</td>
</tr>
<tr>
<td>Type of RFC object to be protected</td>
<td>FUGR</td>
</tr>
</tbody>
</table>

7.2.12 S_RFC_ADM: Administration for RFC Destination

The S_RFC_ADM authorization is required for RFC streaming.

**Use:** DEV, PROD

**Text (Description):** Administration for RFC Destination

**Class:** Cross-application

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
<tr>
<td>Type of Entry in RFCDES</td>
<td>Not used</td>
</tr>
<tr>
<td>Logical Destination (Specified in Function Call)</td>
<td>RFC destination</td>
</tr>
<tr>
<td>Internet Communication Framework Values</td>
<td>Not used</td>
</tr>
</tbody>
</table>

7.2.13 S_RO_OSOA: SAP DataSource Authorizations

The S_RO_OSOA authorization checks DataSource access privileges.

**Use:** DEV, PROD

**Text (Description):** SAP DataSource Authorizations
Class: BW Service API

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
<tr>
<td>DataSource (OSOA/OSOD)</td>
<td>DataSource for data extraction</td>
</tr>
<tr>
<td>Application Component of a DataSource (OSOA/OSOD)</td>
<td>Not used</td>
</tr>
<tr>
<td>Subobject for DataSource</td>
<td>DATA</td>
</tr>
</tbody>
</table>

7.2.14 S_RS_ADMWB: Administrator Workbench - Objects

The S_RS_ADMWB authorization is used for BW loading.

Use: DEV, PROD

Text (Description): Administrator Workbench - Objects

Class: Business Warehouse

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Workbench object</td>
<td>WORKBENCH, SOURCESYS, APPLCOMP, INFOAREA, INFOOBJECT, INFOPACKAG, ODSOBJECT</td>
</tr>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
</tbody>
</table>

7.2.15 S_RS_ICUBE: Data Warehousing Workbench - InfoCube

The S_RS_ICUBE authorization allows SAP Data Services Agent to access an InfoCube.

Use: DEV, PROD

Class: Business Information Warehouse

Text (Description): Data Warehousing Workbench - InfoCube

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfoArea</td>
<td>List of InfoAreas that a user is allowed to access</td>
</tr>
<tr>
<td>InfoCube</td>
<td>List of InfoCubes that a user is allowed to access</td>
</tr>
<tr>
<td>InfoCube Subobject</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
</tbody>
</table>
7.2.16 S_RS_ODSO: Data Warehousing Workbench - DataStore Object

The S_RS_ODSO authorization allows SAP Data Services Agent to access a DataStore Object.

**Use:** DEV, PROD

**Text (Description):** Data Warehousing Workbench - DataStore Object

**Class:** Business Information Warehouse

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfoArea</td>
<td>List of InfoAreas that a user is allowed to access</td>
</tr>
<tr>
<td>DataStore Object</td>
<td>List of DataStore Objects that a user is allowed to access</td>
</tr>
<tr>
<td>Subobject for ODS Object</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
</tbody>
</table>

7.2.17 S_SCRP_TXT: SAPscript

The S_SCRP_TXT authorization allows SAP Data Services Agent to read SAP texts.

**Use:** DEV, PROD

**Text (Description):** SAPscript: Standard text

**Class:** SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language Key</td>
<td>List of language keys that a user is allowed to access</td>
</tr>
<tr>
<td>Text ID</td>
<td>List of text IDs that a user is allowed to access</td>
</tr>
<tr>
<td>Name</td>
<td>List of text names that a user is allowed to access</td>
</tr>
<tr>
<td>Activity</td>
<td>SHOW</td>
</tr>
</tbody>
</table>

7.2.18 S_SDS: Data Services Authorization Object for Functions

The S_SDS authorization enables you to define whether the SAP system should be treated as a development or a production system from the perspective of SAP Data Services Agent.

**Use:** DEV, PROD

**Text (Description):** Data Services Authorization Object for functions

**Class:** SBOP Data Services Authorization Object
### Field Values

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT</td>
<td>Not used</td>
</tr>
<tr>
<td>ZSYSTYPE</td>
<td>D: Development system</td>
</tr>
<tr>
<td></td>
<td>Any other value: Production system</td>
</tr>
</tbody>
</table>

**Note**

In some SAP NetWeaver versions, this authorization object is named ZSDS or S_SDSS. The objects are identical except for the name.

### Related Information

S_SDSS: Data Services Authorization Object for Functions [page 45]  
S_SDSS: Data Services Authorization Object for Functions [page 45]  
ZSDS: Data Services Authorization Object for Functions [page 50]  
ZSDS: Data Services Authorization Object for Functions [page 50]  
ZSDS: Data Services Authorization Object for Functions [page 50]  
S_SDSS: Data Services Authorization Object for Functions [page 45]

### 7.2.19 S_SDAUTH: SBOP Data Services - General Authorization

The S_SDAUTH authorization gives a user access to the SAP Data Services Agent functions.

**Use:** DEV, PROD

**Text (Description):** SBOP Data Services - general authorization

**Class:** SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT: Activity</td>
<td>16 (Execute)</td>
</tr>
</tbody>
</table>

**Note**

In some SAP NetWeaver versions, this authorization object is named ZDAUTH or S_DSAUTH. The objects are identical except for the name.

### Related Information

S_DSAUTH: SBOP Data Services - General Authorization [page 37]
7.2.20 S_SDSDEV: SBOP Data Services Authorization Object for Development

S_SDSDEV is the general authorization object that is SAP Data Services Agent-specific equivalent of the SAP S_DEVELOP authorization object.

**Use:** DEV, PROD

**Text (Description):** SBOP Data Services Authorization Object for development

**Class:** SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>List of packages for tables that a user is allowed to access</td>
</tr>
<tr>
<td>Object type</td>
<td>VIEW, TABL, and TTYP</td>
</tr>
<tr>
<td>Object name</td>
<td>DD objects that a user is allowed to access</td>
</tr>
<tr>
<td>Authorization group ABAP/4 program</td>
<td>Not used</td>
</tr>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
</tbody>
</table>

**Note**

In some SAP NetWeaver versions, this authorization object is named S_DSDEV or ZDSDEV. The objects are identical except for the name.

**Related Information**

S_DSDEV: SBOP Data Services Authorization Object for Development [page 38]
ZDSDEV: SBOP Data Services Authorization Object for Development [page 49]
S_DSDEV: SBOP Data Services Authorization Object for Development [page 49]
ZDSDEV: SBOP Data Services Authorization Object for Development [page 38]
S_DSDEV: SBOP Data Services Authorization Object for Development [page 49]
ZDSDEV: SBOP Data Services Authorization Object for Development [page 49]
7.2.21 S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names

The S_SDSPGMCK authorization determines which programs may execute in a production environment.

Use: PROD

Text (Description): SBOP Data Services Authorization Object for program names

Class: SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT: Activity</td>
<td>16 (Execute)</td>
</tr>
<tr>
<td>PROGRAM: ABAP program name</td>
<td>Program names that are allowed to be executed in a production environment</td>
</tr>
</tbody>
</table>

**Note**

In some SAP NetWeaver versions, this authorization object is named S_DSPGMCHK or ZPGMCHK. The objects are identical except for the name.

**Related Information**

S_DSPGMCHK: SBOP Data Services Authorization Object for Program Names [page 39]
ZPGMCHK: SBOP Data Services Authorization Object for Program Names [page 49]
S_DSPGMCHK: SBOP Data Services Authorization Object for Program Names [page 39]
ZPGMCHK: SBOP Data Services Authorization Object for Program Names [page 49]

7.2.22 S_SDSS: Data Services Authorization Object for Functions

The S_SDSS authorization lets you to define whether the SAP system should be treated as a development or a production system from the perspective of the SAP Data Services Agent.

Use: DEV, PROD

Text (Description): Data Services Authorization Object for functions

Class: SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT</td>
<td>Not used</td>
</tr>
<tr>
<td>ZSYSTYPE</td>
<td>D: Development system</td>
</tr>
</tbody>
</table>
### Related Information

- **S_SDS**: Data Services Authorization Object for Functions [page 42]
- **ZSDS**: Data Services Authorization Object for Functions [page 50]
- **S_SDS**: Data Services Authorization Object for Functions [page 42]
- **ZSDS**: Data Services Authorization Object for Functions [page 50]
- **S_SDS**: Data Services Authorization Object for Functions [page 42]

### 7.2.23 S_TABU_DIS: Table Maintenance

The S_TABU_DIS authorization allows SAP Data Services Agent to access table data in an SAP system.

**Use:** DEV, PROD

**Text (Description):** Table Maintenance (via standard tools such as SM30)

**Class:** Basis

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
<tr>
<td>Authorization group</td>
<td>Table groups that a user is allowed to access</td>
</tr>
</tbody>
</table>

### 7.2.24 S_TCODE: Authorization Check for Transaction Start

SAP Data Services Agent uses the S_TCODE authorization in several ways.

**Purpose:** This authorization grants the user access to specific transactions.

**Text (Description):** Authorization check for transaction start

**Class:** Cross-application authorization object
Purpose: This authorization allows SAP Data Services Agent to execute functions in the Data Warehousing Workbench.

Use: DEV, PROD

Text (Description): Transaction Code Check at Transaction Start

Class: Cross-application Authorization Objects

In addition, you should have access to the contents of the following tables:

- RSDAREA
- RSDAREAT
- RSDCUBE
- RSDCUBET
- RSDODSO
- RSDODSOT

### 7.2.25 S_TRANSPRT: Transport Organizer

The S_TRANSPRT authorization allows SAP Data Services Agent to access the Transport Organizer.

Use: DEV

Text (Description): Transport Organizer

Class: Basis - Development Environment

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Type (Change and Transport System)</td>
<td>DTRA</td>
</tr>
<tr>
<td>Activity</td>
<td>01</td>
</tr>
</tbody>
</table>

### 7.2.26 S_USER_GRP: User Master Maintenance

The S_USER_GRP authorization allows SAP Data Services Agent to establish a connection to the SAP server.

Use: DEV, PROD

Text (Description): User Master Maintenance: User Groups

Class: Basis: Administration
7.2.27 S_USER_PRO: User Master Maintenance

The S_USER_PRO authorization allows SAP Data Services Agent to import an authorization profile.

**Use:** DEV

**Text (Description):** User Master Maintenance: Authorization Profile

**Class:** Basis: Administration

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth. profile in user master maintenance</td>
<td>Authorization Profile to be imported</td>
</tr>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
</tbody>
</table>

7.2.28 ZDSAUTH: SBOP Data Services - General Authorization

The ZDSAUTH authorization gives a user access to SAP Data Services Agent functions.

**Use:** DEV, PROD

**Text (Description):** SBOP Data Services - general authorization

**Class:** SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT: Activity</td>
<td>16 (Execute)</td>
</tr>
</tbody>
</table>

**Note**

In some SAP NetWeaver versions, this authorization object is named S_SDAUTH or S_DSAUTH. The objects are identical except for the name.

**Related Information**

S_DSAUTH: SBOP Data Services - General Authorization [page 37]  
S_SDAUTH: SBOP Data Services - General Authorization [page 43]  
S_DSAUTH: SBOP Data Services - General Authorization [page 37]  
S_SDAUTH: SBOP Data Services - General Authorization [page 43]  
S_DSAUTH: SBOP Data Services - General Authorization [page 37]  
S_SDAUTH: SBOP Data Services - General Authorization [page 43]
7.2.29  ZDSDEV: SBOP Data Services Authorization Object for Development

ZDSDEV is the general authorization object that is the SAP Data Services Agent-specific equivalent of the SAP S_DEVELOP authorization object.

Use: DEV, PROD

Text (Description): SBOP Data Services Authorization Object for development

Class: SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>List of packages for tables that a user is allowed to access</td>
</tr>
<tr>
<td>Object type</td>
<td>VIEW, TABL, and TTYP</td>
</tr>
<tr>
<td>Object name</td>
<td>DD objects that a user is allowed to access</td>
</tr>
<tr>
<td>Authorization group ABAP/4 program</td>
<td>Not used</td>
</tr>
<tr>
<td>Activity</td>
<td>03</td>
</tr>
</tbody>
</table>

Note

In some SAP NetWeaver versions, this authorization object is named S_DSDEV or S_SDSDEV. The objects are identical except for the name.

Related Information

S_SDSDEV: SBOP Data Services Authorization Object for Development [page 44]
S_DSDEV: SBOP Data Services Authorization Object for Development [page 38]
S_SDSDEV: SBOP Data Services Authorization Object for Development [page 44]
S_DSDEV: SBOP Data Services Authorization Object for Development [page 38]
S_SDSDEV: SBOP Data Services Authorization Object for Development [page 44]

7.2.30  ZPGMCHK: SBOP Data Services Authorization Object for Program Names

ZPGMCHK authorization determines which programs may execute in a production environment.

Use: PROD
Text (Description): SBOP Data Services Authorization Object for program names

Class: SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT: Activity</td>
<td>16 (Execute)</td>
</tr>
<tr>
<td>PROGRAM: ABAP program name</td>
<td>Program names that are allowed to be executed in a production environment</td>
</tr>
</tbody>
</table>

Note
In some SAP NetWeaver versions, this authorization object is named S_DSPGMCHK or S_SDSPGMCK. The objects are identical except for the name.

Related Information

S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 45]
S_DSPGMCHK: SBOP Data Services Authorization Object for Program Names [page 39]
S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 45]
S_DSPGMCHK: SBOP Data Services Authorization Object for Program Names [page 39]
S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 39]
S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 45]

7.2.31 ZSDS: Data Services Authorization Object for Functions

The ZSDS authorization lets you to define whether the SAP system should be treated as a development or a production system from the perspective of SAP Data Services Agent.

Use: DEV, PROD

Text (Description): Data Services Authorization Object for functions

Class: SBOP Data Services Authorization Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTVT</td>
<td>Not used</td>
</tr>
<tr>
<td>ZSYSTYPE</td>
<td>D: Development system</td>
</tr>
<tr>
<td></td>
<td>Any other value: Production system</td>
</tr>
</tbody>
</table>

Note
In some SAP NetWeaver versions, this authorization object is named S_SDSS or S_SDS. The objects are identical except for the name.
Related Information

S_SDSS: Data Services Authorization Object for Functions [page 45]
S_SDS: Data Services Authorization Object for Functions [page 42]
S_SDSS: Data Services Authorization Object for Functions [page 45]
S_SDS: Data Services Authorization Object for Functions [page 42]
S_SDSS: Data Services Authorization Object for Functions [page 45]
S_SDS: Data Services Authorization Object for Functions [page 42]

7.2.32 Browse Metadata for an SAP BW Source Datastore

To browse metadata for an SAP BW source datastore, access the contents of several tables.

Use the following tables to browse metadata for an SAP BW source datastore:

- RSDAREA
- RSDAREAT
- RSDCUBE
- RSDCUBET
- RSDODSO
- RSDODSOT

If you do not have access to these tables, request access from your administrator.

7.3 Authenticating with Secure Network Communications (SNC)

Enabling SNC provides a secure connection between SAP systems and the SAP Data Services Agent.

Prerequisites

Secure Network Communications (SNC) must be configured on the SAP system.

Procedure

1. Open the Datastores tab and add or select the datastore for which you want to enable SNC.
2. In the Authentication option, select SNC.
Considerations for Running ABAP Programs

When you use ABAP transforms in an SAP Cloud Platform Integration data flow, there are additional configuration options that you need to consider.

In all cases where you use an ABAP transform in SAP Cloud Platform Integration, data is sent via RFC from the SAP application server to the SAP Data Services Agent. In order to send the data via RFC, you must first configure the RFC destination in the SAP application server.

For more information, see “Configuring the RFC destination”.

ABAP Query transform

When you use an ABAP Query transform in an SAP Cloud Platform Integration data flow, it can be used in two ways:

- **Generate and Execute**
  
  This is the recommended execution mode for sandbox and SAP application development environments.

  The ABAP created by the data flow resides on the same host system as the SAP Data Services Agent and is submitted to the SAP system using the /BODS/RFC_ABAP_INSTALL_AND_RUN function. You should use this option if the data flow changes each time that it is executed.

- **Execute pre-loaded**
  
  This is the recommended execution mode for production environments.

  The ABAP resides on the SAP application server and is submitted using SAP Data Services RFC function modules. You should use this option if the data flow does not change each time that it is executed. In many production environments, the security policy prohibits the execution of auto-generated code. In this case, the ABAP programs need to be transported to the SAP system manually. The SAP BASIS administrator can review the ABAP programs prior to uploading, and can add additional security checks. For more information, see “Uploading ABAP programs to the SAP system”.

Related Information

SAP NetWeaver Security Guide
Custom ABAP transform

When you use a Custom ABAP transform in an SAP Cloud Platform Integration data flow, the generated ABAP program will contain the custom ABAP FORM. In the datastore, if the ABAP execution mode is set to *Execute pre-loaded*, the generated ABAP program needs to be installed on the SAP server.

Related Information

Configuring the RFC Destination [page 53]
Manually Uploading ABAP Programs to the SAP System [page 54]

7.4.1 Configuring the RFC Destination

Before you can extract from SAP Business Suite application sources in an SAP Cloud Platform Integration data flow, you must register the RFC destination in the SAP application server.

In the SAP application server, use transaction *SM59* to configure an RFC destination with the following settings:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RFC Destination</strong></td>
<td>SAPDS</td>
</tr>
<tr>
<td><strong>Connection Type</strong></td>
<td>T (TCP/IP connection)</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>User-defined description of the RFC destination</td>
</tr>
</tbody>
</table>

**Technical Settings tab**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activation Type</strong></td>
<td>Registered Server Program</td>
</tr>
<tr>
<td><strong>Program ID</strong></td>
<td>&lt;must always be empty&gt;</td>
</tr>
</tbody>
</table>

**i Note**

If you attempt to test the connection with these settings, it is normal for the test to fail due to a connection timeout. No listener is active unless an SAP Cloud Platform Integration task is currently running.
7.4.2 Manually Uploading ABAP Programs to the SAP System

When you use the *Execute pre-loaded datastore* option in an ABAP query transform, you must manually upload the ABAP program to the SAP system.

**Prerequisites**

Before you can run the task in *Execute pre-loaded* mode, you must first run the task in *Generate and Execute* mode on a development system to generate the ABAP program.

**Context**

To upload the ABAP program to the SAP system:

- **Note**
  The manual process described here can be done automatically using the *Generate and view ABAP report* dialog in the data flow editor in the SAP Cloud Platform Integration user interface.

**Procedure**

1. Locate the generated ABAP file on the SAP Data Services Agent host system.
2. Copy the contents of the ABAP file.
3. Run transaction *SE38* in the SAP system.
4. Create a new program with the name shown as defined in the R3 data flow.
5. Paste the contents of the generated ABAP file into the new program.
### 7.5 Set Up the Communication between BW and Agent

You must configure the RFC destination including the Program ID to enable loading data from SAP Cloud Platform Integration to SAP BW.

**Procedure**

1. From the SAP Data Warehousing Workbench window, go to **Modeling** ➔ **Source Systems** ➔ **External System**.
2. Right-click **External System** to create a new one.
3. Give the system a name and a description.
4. Click the check mark button, and the **RFC Destination** window appears.
5. In the **Technical Settings** tab, select **Registered Server Program**.
6. Enter the **Program ID**.

△ **Caution**

If you have multiple BW systems, make sure the **Program ID** values are exactly the same.

The Program ID value is case sensitive.

7. Save the RFC destination.

ℹ️ **Note**

**Connection Test** is not available in this case.
SAP Cloud Platform Integration uses PGP to encrypt or decrypt sensitive data that is stored in files. PGP provides privacy and security.

By encrypting the files, only the intended receiver will be able to see the actual content. The optional digital signature verifies the sender's identity. It is recommended that you use PGP to protect all sensitive data.

PGP keys are managed through the Data Services Agent Configuration program. Within an SAP Cloud Platform Integration organization, a single key pair is shared between all agents. Additionally any external (third-party) public keys must be imported on all systems hosting an SAP Data Services Agent.

The following keys are used to read files from an external source:

<table>
<thead>
<tr>
<th>Key</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization public key</td>
<td>Used by external third-party to encrypt data</td>
</tr>
<tr>
<td>Organization private key</td>
<td>Used to decrypt the data from the external third-party</td>
</tr>
<tr>
<td>External third-party public key</td>
<td>Imported and then used to verify the digital signature</td>
</tr>
</tbody>
</table>

The following keys are used to load files to an external source:

<table>
<thead>
<tr>
<th>Key</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>External third-party public key</td>
<td>Used by SAP Cloud Platform Integration to encrypt data</td>
</tr>
<tr>
<td>Organization private key</td>
<td>Used when generating the optional digital signature.</td>
</tr>
<tr>
<td>Organization public key</td>
<td>Exported from SAP Cloud Platform Integration. Sent to third party to use to verify the digital signature</td>
</tr>
</tbody>
</table>

Related Information

Generating a PGP Key Pair [page 57]
Moving your Organization Key Pair [page 58]
Importing an External Public Key [page 59]
Exporting your Public Key [page 60]
Reading from PGP-protected Source Files [page 60]
Loading into PGP-protected Target Files [page 62]
8.1 Generating a PGP Key Pair

Within an SAP Cloud Platform Integration organization, generate a single PGP key pair.

Context

The key pair contains a public key and a private key. The organization public key can be sent to third-parties who can use it to encrypt data. SAP Cloud Platform Integration can decrypt the data using the organization private key.

Procedure

1. If the SAP Data Services Agent configuration program is not already running, start it.
   ○ On Windows platforms, run `configureAgent.bat`.
   ○ On Linux platforms, run `configureAgent.sh`.

   **Note**
   You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the **Run as administrator** option.

   By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click **Configure PGP**.
3. Click **Generate a key pair for your organization**.
   a. Select the key size, hash algorithm, and symmetric algorithm appropriate for your requirements.
   b. Enter a user ID.
      The user ID is the name bound to the public key. It can be an email address, name, or other identifying information.

4. Click **Apply**.

Results

A PGP key pair is generated and saved to the host system where your SAP Data Services Agent is installed.
Related Information

SAP Note 1887289

8.2 Moving your Organization Key Pair

If your organization has multiple agents, all agents must share the same key pair. The file containing the organization’s PGP key pair must be stored locally on each system that hosts an SAP Data Services Agent.

Prerequisites

A PGP key pair has been generated for the organization.

Context

After the organization’s key pair has been generated, it must be exported to a known location and then imported to each system which hosts an SAP Data Services Agent.

Procedure

1. If the SAP Data Services Agent configuration program is not already running, start it.
   - On Windows platforms, run `configureAgent.bat`.
   - On Linux platforms, run `configureAgent.sh`.

   **Note**
   You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

   By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click Configure PGP.

3. Click Export your organization’s key pair.

4. Type or browse to the desired location and type a passphrase.
   
   Take note of this information as it will be required later when you import the key pair.

5. Click Apply.
6. From a system which hosts a different SAP Data Services Agent, start the SAP Data Services Agent configuration program as described in Step 1.

7. Click *Import your organization’s key pair*.

8. Enter the location and passphrase you created in Step 4 when you exported the key pair from the system where it was generated.

9. Click *Apply*.

10. Repeat steps 6 - 9 for each system which hosts an SAP Data Services Agent.

### 8.3 Importing an External Public Key

Import an external (third-party) public key to use when encrypting data you are loading to a file.

#### Context

**i Note**

The external (third-party) public key must be imported to the server hosting the SAP Data Services agent used in the task.

#### Procedure

1. If the SAP Data Services Agent configuration program is not already running, start it.
   - On Windows platforms, run `configureAgent.bat`.
   - On Linux platforms, run `configureAgent.sh`.
   
   **i Note**
   
   You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the *Run as administrator* option.

   By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click *Configure PGP*.

3. Click *Import an external (third-party) public key*.

4. Type or browse to the location of the external (third-party) public key.

5. Click *Apply*. 
8.4 Exporting your Public Key

Export your organization's public key so it can be used when encrypting the source data.

Procedure

1. If the SAP Data Services Agent configuration program is not already running, start it.
   - On Windows platforms, run `configureAgent.bat`.
   - On Linux platforms, run `configureAgent.sh`.

   **Note**
   You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

   By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click Configure PGP.
3. Click Export your organization's public key.
4. Type or browse to a location where your public key can be accessed as required.
5. Click Apply.

8.5 Reading from PGP-protected Source Files

In order to read and decrypt a PGP-protected source file, your organization's public key must be used to encrypt the source file.

Additionally, to decrypt a file which contains a digital signature to verify the authenticity of the data's origin and integrity, you must have the external (third-party) key from the owner of the source file.

Prerequisites

As needed for your situation, from the Data Services Agent Configuration program, make sure that the following prerequisites are met:
Table 2: Prerequisites to decrypt a source file

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>A PGP key pair exists for your organization.</td>
<td>Generating a PGP Key Pair [page 57]</td>
</tr>
<tr>
<td>The organization key pair is imported to the system hosting your agent.</td>
<td>If the key pair was generated on the system hosting your agent, you do not need to import it. If the key pair was generated on a different system in your organization, then you must move it to the system that hosts your agent. Moving your Organization Key Pair [page 58]</td>
</tr>
<tr>
<td>The owner of the source file has your public key.</td>
<td>Export your public key and send it to the owner of the source file. Exporting your Public Key [page 60]</td>
</tr>
<tr>
<td>The owner of the source file has encrypted the file using your public key.</td>
<td></td>
</tr>
</tbody>
</table>

Additionally, if the source file contains a digital signature, make sure you have met the following prerequisites:

Table 3: Prerequisites to verify a digital signature

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>You have received the external (third-party) public key from the owner of the source file.</td>
<td></td>
</tr>
<tr>
<td>You have imported the external (third-party) public key to the system which hosts your agent.</td>
<td>Importing an External Public Key [page 59]</td>
</tr>
</tbody>
</table>

**Context**

First use the Data Services Agent Configuration program to meet the prerequisites. Then, use the SAP Cloud Platform Integration user interface to create and run the task to read and decrypt the source file.

**Procedure**

1. In the SAP Cloud Platform Integration user interface, create a task and data flow to read the encrypted source data.
2. In the data flow, select the transform that reads the source data.
3. In the **Transform Details** do the following:
   a. From the **File Options** tab, in the **Selected input information**, in the **PGP Protected** field, select **yes**.
b. If the file contains a digital signature, in the **PGP Signature** field, select **yes**.

Next Steps

Validate and run the task as usual.

### 8.6 Loading into PGP-protected Target Files

In order to load data to a PGP-protected target file, the public key of the external third-party that will receive the file must be used to encrypt the source file.

Additionally, to encrypt a file with your digital signature to verify the authenticity of the data’s origin and integrity, you must use your organization’s public key.

### Prerequisites

As needed for your situation, from the Data Services Agent Configuration program, make sure that the following prerequisites are met:

Table 4: Prerequisites to encrypt a file to load to a target

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ You have received the public key of the external third-party that will receive the target.</td>
<td>Make sure to get the user ID of the key. The user ID can be an email address, name, or other identifying information.</td>
</tr>
<tr>
<td>❑ You have imported the external third-party public key.</td>
<td>Importing an External Public Key [page 59]</td>
</tr>
</tbody>
</table>

Additionally, to generate your digital signature, make sure you have met the following prerequisites:

Table 5: Prerequisites to generate a digital signature

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ A PGP key pair exists for your organization.</td>
<td>Generating a PGP Key Pair [page 57]</td>
</tr>
<tr>
<td>❑ The organization key pair is imported to the server hosting your agent.</td>
<td>If the key pair was not generated on the server hosting your agent, you must move it to the server. Moving your Organization Key Pair [page 58]</td>
</tr>
<tr>
<td>❑ You have exported your organization’s public key.</td>
<td>Exporting your Public Key [page 60]</td>
</tr>
<tr>
<td>Prerequisite</td>
<td>More information</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>❑ You have sent your public key to the external third-party that owns the target.</td>
<td></td>
</tr>
</tbody>
</table>

**Context**

First use the Data Services Agent Configuration program to meet the prerequisites. Then, use the SAP Cloud Platform Integration user interface to create and run the task that creates the PGP-encrypted target file.

**Procedure**

1. In the SAP Cloud Platform Integration user interface, create a task to load a target file.
2. Create a data flow. In the **Set Up** step, in the **Encrypt with PGP** field, select **yes** and type the user ID of the external third-party public key.
3. If you want to include a digital signature, in the **Include Digital Signature** field, select **yes**.

**Next Steps**

**Next steps:**

Validate and run the task as usual.
A Troubleshooting

Errors may occur during the installation, configuration, or operation of the SAP Data Services Agent. For more information, see the log files or other available information resources.

Log file locations

If you encounter issues with the SAP Data Services Agent during the installation or configuration processes, you can check the log files created on the host system for more information.

<table>
<thead>
<tr>
<th>Log file</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation log</td>
<td>Install_&lt;timestamp&gt;.log</td>
</tr>
<tr>
<td>Configuration log</td>
<td>Config_&lt;timestamp&gt;.log</td>
</tr>
</tbody>
</table>

- On Windows platforms, the log files are created under %DS_COMMON_DIR%\log. For example, C:\Program Files\SAP\DataServicesAgent\log.
- On Linux platforms, the log files are created under <install_dir>/log. For example, $HOME/DataServicesAgent/log.

Additional troubleshooting information

For more information about troubleshooting common issues regarding SAP Cloud Platform Integration and the SAP Data Services Agent, see SAP Note 1800845 on the SAP Service Marketplace.

Related Information

- Collect Agent Diagnostic Information [page 64]
- Stopping the Internal Database [page 66]
- Manually Uninstalling the Agent [page 66]
- SAP Note 1800845: Data Services Agent Installer Troubleshooting Tips

A.1 Collect Agent Diagnostic Information

The Agent diagnostic tool checks for common issues that cause the Data Services Agent to go offline or that prevent the agent service from starting. You can attach the information gathered with this tool to SAP Support.
tickets for efficient resolution of agent issues. The location of the zip file to attach is noted at the end of the results in the Output pane.

Prerequisites

Before running the agent diagnostics tool, make sure that you have registered the Data Services Agent with your SAP Cloud Platform Integration server.

Context

Types of information that is collected for analysis includes:

- System-related information including operating system, IP addresses, processors, JVM memory and system space statistics
- Network diagnostics to check communication between the Data Services Agent and SAP Cloud Platform Integration server
- TCP/IP port information
- Security certificate information

Procedure

1. Start the SAP Data Services Agent configuration program.
   ○ On Windows platforms, run `configureAgent.bat`.
   ○ On Linux platforms, run `configureAgent.sh`.

   **Note**
   You must run the configuration program from a user account that has administrative privileges. On Windows platforms that have User Account Control (UAC) enabled, you can also choose the Run as administrator option.

   By default, the configuration program is located in the directory where you installed the SAP Data Services Agent.

2. Click Run Agent Diagnostics.

3. Click Run.
   The information collected displays in the Output pane and a zip file is created and stored on the system hosting your Data Services Agent. The last entry in the Output pane contains the path to the zip file.

Next Steps

Attach the zip file to your SAP Support ticket.
Related Information

Configuring the SAP Data Services Agent [page 13]

A.2 Stopping the Internal Database

If the internal database is still running when you try to uninstall the SAP Data Services Agent, the uninstallation script may be unable to delete some files.

If the script fails to delete some files, first stop the internal database:

```
dbstop -y dsod_agent_repo
```

By default, `dbstop` is located in `%LINK_DIR%\sqla`.

After stopping the internal database, you can manually delete any remaining files and folders left in the following locations:

- `%LINK_DIR%`
- `%DS_COMMON_DIR%`
- `%DS_USER_DIR%`

A.3 Manually Uninstalling the Agent

If you encounter errors while uninstalling the SAP Data Services Agent, or have removed the uninstallation script, you can manually uninstall the software.

Procedure

1. Close any open files, windows, or command prompts in the `%LINK_DIR%` or `%DS_COMMON_DIR%` folders.

   By default, `%LINK_DIR%` and `%DS_COMMON_DIR%` are located at the following locations:
   - On Windows platforms, `C:\Program Files\SAP\DataServicesAgent` and `C:\ProgramData\SAP\DataServicesAgent`
   - On Linux platforms, `$HOME/DataServicesAgent`

   If you don’t close open files, windows, or command prompts in these locations, you may be unable to remove all agent files.

2. From the Services window, stop the **SAP Data Services Agent** service.

3. Delete the Windows service.

   `sc.exe delete DSOD_JOBSERVICE`
4. Delete the `dsod_agent_repo` ODBC data source.
   By default, the data source is located in `ODBC Data Sources > System DSN`.

5. Uninstall the internal database driver.
   ```
   regsvr32 /u "%LINK_DIR%\sqla\dbodbc12DSAgent.dll"
   ```

6. Delete the installed files and folders under `%LINK_DIR%`, `%DS_COMMON_DIR%`, and `%DS_USER_DIR%`.

7. Remove the `%LINK_DIR%`, `%DS_COMMON_DIR%`, and `%DS_USER_DIR%` system environment variables.

**Next Steps**

To remove the `SAP Data Services Agent` entry from `Programs and Features` in the Windows Control Panel, remove the registry key `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SAPDataServicesAgent`. 
Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP’s gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP’s gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.