PUBLIC

SAP Cloud Integration for data services 1.0.11

2023-11-01

SAP Data Services Agent Guide

THE BEST RUN SAP

Content

1 SAP Data Services Agent

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.

> **i** 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 Integration for data services, you must use the SAP Data Services Agent.

2 Upgrade Recommendations for SAP Data Services Agent

We strongly recommend you use a version of the SAP Data Services Agent that is within **four (4)** releases of the latest release of SAP Cloud Integration for data services.

Example:

Current release = (n)	2311	Recommended
Release (n-1)	2309	Recommended
Release (n-2)	2306	Recommended
Release (n-3)	2303	Recommended
Release (n-4)	2211	Not recommended
Release (n-5)	2209	Not recommended
Release (n-6)	2206	Not recommended
Release (n-7)	2203	Not recommended

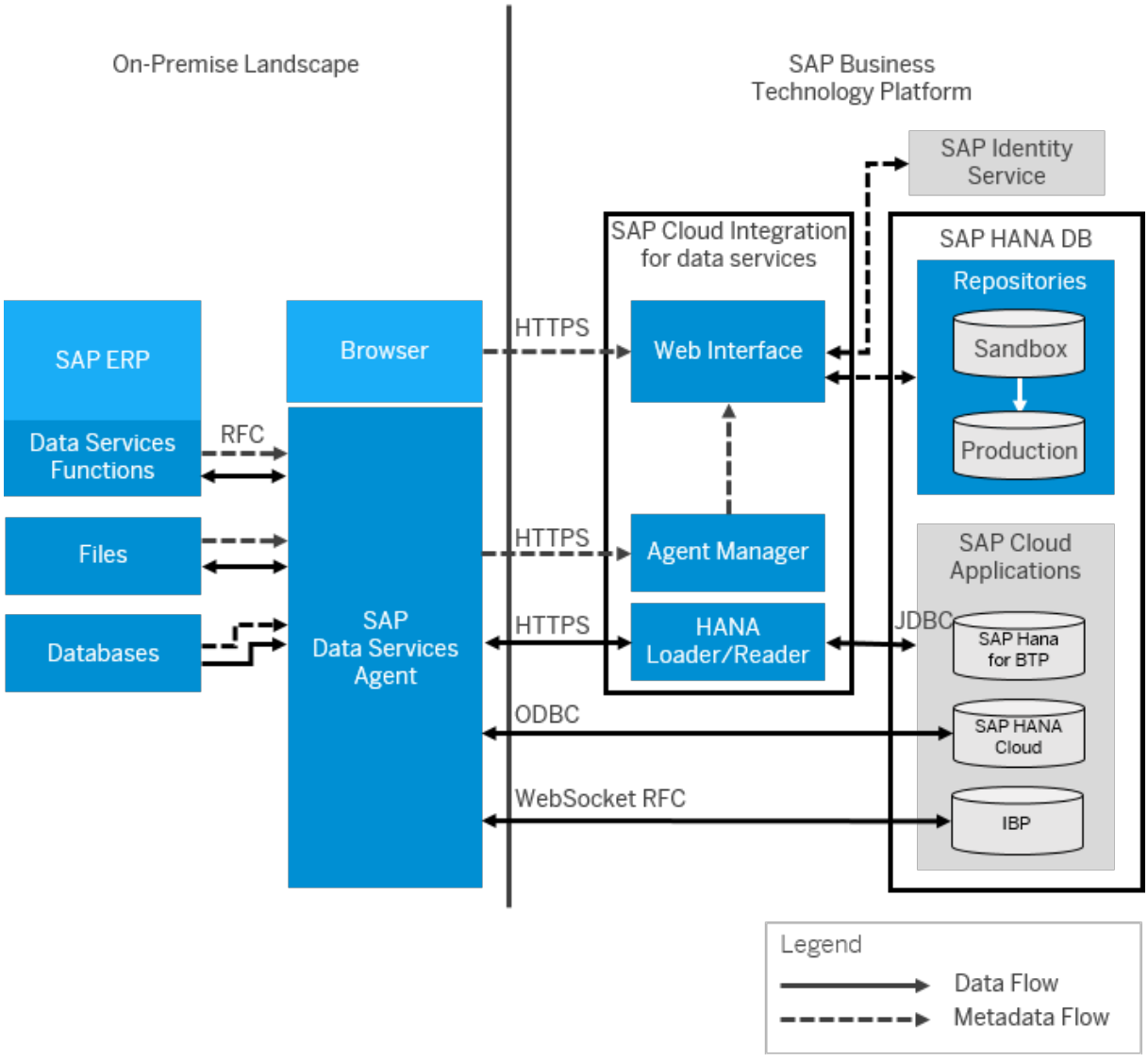
With each new release of SAP Cloud Integration for data services, the minimum recommended version increases by one version.

In addition, please be aware that in order to receive the most current features, functionality, and fixes, you must use the latest release of the Agent. Updates and hot fixes to releases prior to the current release will not be provided.

For additional release information, see the Product Availability Matrix (PAM).

3 SAP Cloud Integration for data services Architecture

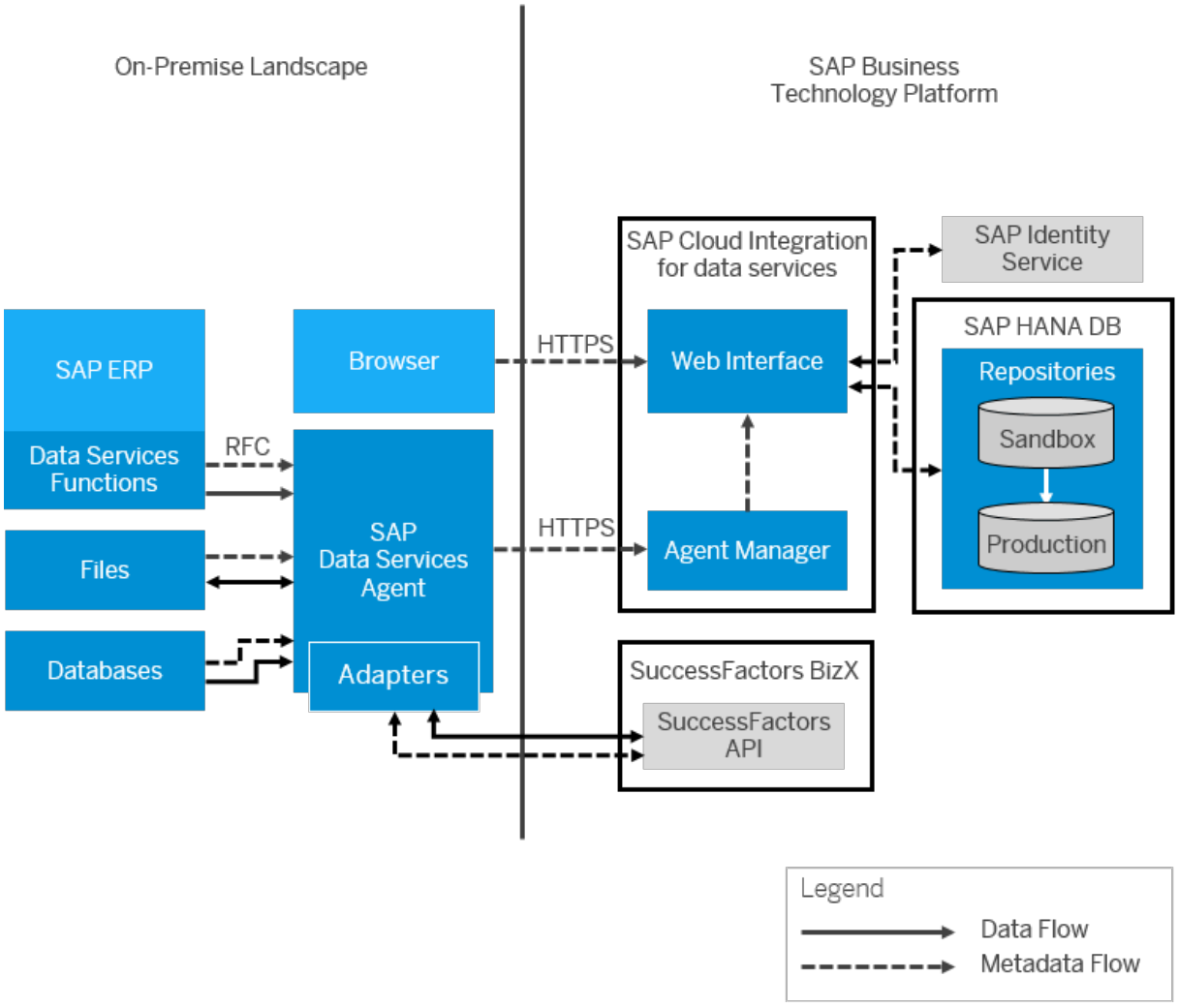
SAP Cloud Integration for data services interacts with your local SAP landscape via the SAP Data Services Agent and secure HTTPS and RFC connections.



> **i 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 Integration for data services architecture is slightly different:



4 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.
   - Review Upgrade Recommendations for SAP Data Services Agent [page 6] for important information about the releases of SAP Data Services Agent you should use.
   - 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 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
     - libncurses (if using SUSE 15.0 or higher)

       > **i Note**
       >
       > If you are installing the agent from release 2311 or later, libncurses**6** is required due to an SQL Anywhere dependency upgrade. For an agent from release 2309 or earlier, libncurses**5** is required.

     If any packages are missing, the dependent libraries can be found as operating system patches.

     > **i Note**
     >
     > MS SQL support on Linux will use the pre-configured DataDirect ODBC driver that is bundled with SAP Cloud Integration for data services.

- Use the following command to install libcrypt.so.1:
  `zypper install libcrypt1-32bit`
- Use the following command to install liblzma.so.5 lib:
  `sudo zypper install liblzma5-32bit`

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

      > **i 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 Integration for data services:
      - User name and password for the SAP Cloud Integration for data services administrator account
   4. Register an agent in the SAP Cloud Integration for data services 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)
   6. Ensure that you can access the URL that hosts the data center that communicates with the agent.

      > **i Note**
      >
      > You may need your IT administrator to add the datastore or data center URL to the allowlist to obtain access.

   7. Ensure that any necessary certificates are imported to your agent. See Importing Certificates [page 38] for more information.
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 allowlisted in the SAP Data Services Agent before you can access them in SAP Cloud Integration for data services.
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 64-bit version of the driver is required.
7. If you plan to run on Microsoft Windows, ensure that Microsoft Visual C++ 2019 is installed.
8. 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 Integration for data services web interface and see the *Get Started* tab for information about configuring projects and tasks.

Related Information

Considerations for Using Multiple Agents [page 11]
Linux user resource limits [page 12]
Configuring the SAP Data Services Agent [page 22]
Configuring SAP Business Suite Connectivity [page 40]
Installing the SAP Data Services Agent [page 13]
Connecting to Secure Web Services by Manually Adding Certificates [page 29]
Product Availability Matrix
Configuring SAP Business Suite Connectivity [page 40]

4.1 Considerations for Using Multiple Agents

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

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 Integration for data services. 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.

> **! Restriction**
>
> A one-to-one correlation exists between the agent configuration file that you download and install and the machine that you install it on. You cannot reuse an agent configuration file on multiple machines or on multiple users on Linux. If you are moving the agent from one machine to another machine, for example, you must first delete the agent entry for the old computer before installing the agent on the new computer. Do this within SAP Cloud Integration for data services, at the Agents tab.

4.2 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.

User resource limit	Value	Comments
file (blocks)	unlimited	
data (kilobytes)	unlimited	
stack (kilobytes)	2048	2 MB
time (cpu-seconds)	unlimited	
nofiles (descriptors)	65536	
coredump (blocks)	unlimited	
memory (kilobytes)	unlimited	
lockedmem (kilobytes)	4	
processes	7168	

5 Installing the SAP Data Services Agent

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

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 path where you want to install the software.
   - On Windows platforms, the default installation path is `C:\Program Files\SAP\DataServicesAgent`.
   - On Linux platforms, the default installation path is `$HOME/DataServicesAgent`.
3. On Windows, specify the path where the agent should store log files and settings. To prevent issues when upgrading or applying patches, this path must be different than the installation path entered in the previous step.

   The logs and settings path is referenced by the `<DS_COMMON_DIR>` environment variable. The default path 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.

   > **i 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.

   > **i 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 displays. During the installation process, the installation program creates a log file as follows:
   - On Windows platforms, `%DS_COMMON_DIR%\log\Install_<timestamp>.log`
   - On Linux platforms, `<install_dir>\log\Install_<timestamp>.log`

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 22]

6 Setting Up a WebSocket RFC Connection

Use a WebSocket RFC-enabled connection to connect SAP Cloud Integration for data services and SAP Integrated Business Planning.

There are two types of authentication for WebSocket RFC communication to an IBP datastore:

- Certificate-based authentication using an X.509 certificate
- Password authentication

Related Information

Connecting to SAP IBP Using Certificate-Based Authentication [page 15]
Connecting to SAP IBP Using Password Authentication [page 18]
Additional Information [page 21]

6.1 Connecting to SAP IBP Using Certificate-Based Authentication

X.509 certificate-based authentication requires a Personal Security Environment (PSE) file.

1. Create a Personal Security Environment with a PSE File [page 16]
   A personal security environment (PSE) is required to establish a WebSocket RFC connection. Use the X.509 certificate to authenticate via certificate to WebSocket RFC connections.
2. Add the Server Certificate to the PSE [page 18]
   A server certificate is required to encrypt information and provide identity assurance in your PSE.

Related Information

Personal Security Environment (PSE)

6.1.1 Create a Personal Security Environment with a PSE File

A personal security environment (PSE) is required to establish a WebSocket RFC connection. Use the X.509 certificate to authenticate via certificate to WebSocket RFC connections.

Prerequisites:

- Install or upgrade your agent to Patch 38 or higher.
- Generate the client certificate in a P12 format with a private key and save it in the <SECUDIR> folder. The client certificate must be available before setting it up with the PSE file.

> **i Note**
>
> To provide a high degree of security, the certificate in P12 format should be generated by the connection owner using any certificate generator or generated and signed by a third-party certificate authority (CA) listed in SAP Note 2871840. The private key of this certificate should be kept in a secure location and maintained by the connection owner.

A PSE is a secure container that stores the public-key information of a user or component. Creating a PSE is mandatory to successfully authenticate and connect to a WebSocket RFC connection. The location of this secure PSE container is defined by the agent during installation.

> **i Note**
>
> - Personal Security Environment (PSE) files are loaded and generated from the SECUDIR variable and they should not be moved or renamed. If moved, the PSE file will not work.
> - The PSE file must be generated in the same machine as the agent. Again, it should not be shared, moved, or renamed. If tasks are run against an agent group, generate a PSE file for each agent machine within that group.
> - If you alter an existing PSE file, functionality such as testing connections, browsing, and importing require you to restart the agent to establish a WebSocket RFC connection. Job execution and job run-time do not require you to restart the agent.

> **⚠ Caution**
>
> When a certificate used for a PSE expires, you must recreate the PSE from a new certificate.

To set up the X.509 certificate, perform these steps:

1. Open the command line:
   - CMD as administrator on Windows

     > **⚠ Caution**
     >
     > It is important that you do this as an Administrator. Creating the file as a non-Administrator user will produce an unusable file.

   - Terminal on Linux
2. Go to the `<agent_installation_folder>/bin` directory.
3. Create a PSE file using information from the P12:

> **Note**
>
> - If your SAP Integrated Business Planning datastore has different configurations for Sandbox and Production, the PSE files should have different names between the two environments.
> - You should use the same PSE file name within the same agents in the same group, so a task that is sent to the agents in the same group will refer to the same PSE file name defined in the datastore.

For example:

```
sapgenpse import_p12 –p <PSE_NAME> <P12_File>
```

- Encryption password: P12 file password
- PSE PIN/passphrase: Choose a new password for the PSE file.

> **Note**
>
> If switching from Basic Authentication to X.509, the PSE file is overridden and a new password needs to be created.

4. Grant user access to the PSE file using the following command:

```
sapgenpse seclogin -p <PSE_NAME.pse> -x <PIN> -O [<NT_Domain>\]<user_ID>
```

- -p: Personal Security Environment filename. Same filename as used previously.
- -x: Password to encode and decode. Same password as used previously.
- -o: User with management access to the Agent

By default, the path for Windows and Linux are:

- Windows:
  %DS_COMMON_DIR%\ssl\sec
- Linux:
  <agent_installation_folder>/ssl/sec

5. Upload the public certificate to IBP.

- (optional) Extract the public client certificate from the PSE file.

```
sapgenpse export_own_cert -o <public_client_certificate.crt> -p <PSE_Name>
-x <PIN>
```

- Open the `<public_client_certificate.crt>` and remove the “BEGIN CERTIFICATE” and “END CERTIFICATE” tags before uploading it to IBP because the IBP system does not accept BEGIN and END tags in the certificate.
- Ensure that the client certificate is signed by one of the certificate authorities listed in 2871840.
- Create/edit a communication arrangement and make sure the certificate is uploaded in the communication user. For more information, see the "Using Basic Authentication" section of Defining the Communication Arrangement.

6. Add the certificate to PSE. See Add the Server Certificate to the PSE [page 18].

Task overview: Connecting to SAP IBP Using Certificate-Based Authentication [page 15]

Next task: Add the Server Certificate to the PSE [page 18]

6.1.2 Add the Server Certificate to the PSE

A server certificate is required to encrypt information and provide identity assurance in your PSE.

To add a server certificate to your PSE, perform the following steps:

1. Download the certificate from the IBP server.
2. Open the command line:
   - CMD as an administrator on Windows

     > ⚠ Caution
     >
     > It is important that you do this as an Administrator. Creating the file as a non-Administrator user will produce an unusable file.

   - Terminal on Linux
3. Navigate to the `SECUDIR` folder.
4. Go to `<agent_installation_folder>\bin`.
5. Run `sapgenpse` to add the certificate to the PSE file:

```
sapgenpse maintain_pk -a <path>/<certificate>.crt -p <file>.pse -x <PIN>
```

To complete the WebSocket RFC setup, define the communication arrangements in the SAP Integrated Business Planning UI. For more information, see “Defining the Communication Arrangement” in the *SAP Cloud Integration Guide* available on the SAP Help Portal.

Task overview: Connecting to SAP IBP Using Certificate-Based Authentication [page 15]

Previous task: Create a Personal Security Environment with a PSE File [page 16]

6.2 Connecting to SAP IBP Using Password Authentication

Authentication by password requires a username, a password, and a Personal Security Environment (PSE) file.

1. Create a Personal Security Environment with a PSE File [page 19]
2. Add the Server Certificate to the PSE [page 20]
   A server certificate is required to encrypt information and provide identity assurance in your PSE.

Related Information

Personal Security Environment (PSE)

6.2.1 Create a Personal Security Environment with a PSE File

Prerequisite: Install or upgrade your agent to Patch 38 or higher.A personal security environment (PSE) is required to establish a WebSocket RFC connection.

A personal security environment (PSE) is required to establish a WebSocket RFCA PSE is a secure container where the public-key information of a user or component is stored. Creating a PSE is mandatory to successfully authenticate and connect to a WebSocket RFC connection. The location of this secure PSE container is defined by the agent during installation.

> **i Note**
>
> - Personal Security Environment (PSE) files are loaded and generated from the SECUDIR variable and they should not be moved or renamed. If moved, the PSE file will not work.
> - The PSE file must be generated in the same machine as the agent. It cannot be shared, moved, or renamed. If tasks are run against an agent group, generate a PSE file for each agent machine within that group.
> - If you alter an existing PSE file, functionality such as testing connections, browsing, and importing require you to restart the agent to establish a WebSocket RFC connection. Job execution and job runtime do not require you to restart the agent.

1. Open the command line:
   - CMD as an administrator on Windows.

     > **⚠ Caution**
     >
     > It is important that you do this as an Administrator. Creating the file as a non-Administrator user will produce an unusable file.

   - Terminal on Linux
2. Go to the `<agent_installation_folder>/bin` directory.
3. Run `sapgenpse` to generate the PSE file.

   ```
   sapgenpse get_pse -p <PSE_Name.pse> -x <PIN> <DN>
   ```

   > **i Note**
   >
   > The PSE file will be generated in the SECUDIR location.

   - -p: Personal Security Environment filename
     For example, `ibp_no_password.pse`
   - -x: Password to encode and decode
     - DN: The distinguished name.
       This must be unique per PSE file.
     - CN = <Common_Name>
       This must be unique per PSE file.
     - OU = <Organizational_Unit>
     - O = <Organization>
     - C = <Country>

For example, "CN=iNumber, O=SAP, C=BR"

4. Grant user access to the PSE file using the following command:

```
sapgenpse seclogin -p <PSE_NAME.pse> -x <PIN> -O [<NT_Domain>\]<user_ID>
```

   - -p: Personal Security Environment filename. Same filename as used previously.
   - -x: Password to encode and decode. Same password as used previously.
   - -o: User with management access to the Agent

   By default, the path for Windows and Linux are:
   - Windows:
     %DS_COMMON_DIR%\ssl\sec
   - Linux:
     <agent_installation_folder>/ssl/sec
5. Add the certificate to the PSE. See Add the Server Certificate to the PSE [page 20].

Parent topic: Connecting to SAP IBP Using Password Authentication [page 18]

Next task: Add the Server Certificate to the PSE [page 20]

Related Information

Personal Security Environment (PSE)

6.2.2 Add the Server Certificate to the PSE

A server certificate is required to encrypt information and provide identity assurance in your PSE.

To add a server certificate to your PSE, perform the following steps:

1. Download the certificate from the IBP server.
2. Open the command line:
   - CMD as an administrator on Windows

     > ⚠ Caution
     >
     > It is important that you do this as an Administrator. Creating the file as a non-Administrator user will produce an unusable file.

   - Terminal on Linux
3. Navigate to the `SECUDIR` folder.
4. Go to `<agent_installation_folder>\bin`.
5. Run `sapgenpse` to add the certificate to the PSE file:

```
sapgenpse maintain_pk -a <path>/<certificate>.crt -p <file>.pse -x <PIN>
```

To complete the WebSocket RFC setup, define the communication arrangements in the SAP Integrated Business Planning UI. For more information, see “Defining the Communication Arrangement” in the *SAP Cloud Integration Guide* available on the SAP Help Portal.

Task overview: Connecting to SAP IBP Using Password Authentication [page 18]

Previous: Create a Personal Security Environment with a PSE File [page 19]

6.3 Additional Information

Helpful information about your WebSocket RFC connection.

- When you filter IBP data using an IN or NOT IN operator, the filtering occurs on the IBP side. Filtered results are then provided to SAP Cloud Integration for data services, which increases performance efficiency. Prior to patch 41, data was read from IBP and the filtering was done in memory on the Agent.
- For recommendations to help you set up data extraction via data flows using calculation scenarios, refer to Best Practices for Extracting Data from SAP IBP. You can **ignore** the item in the section "Attribute-based Filter" that suggests not using IN and NOT IN operators, as this is supported.
- If a job is reading or loading data and a connection attempt fails, the system will reattempt to connect after the number of milliseconds set in the parameter *Interval between Retries (ms)* until it reaches the value defined in the parameter *Number of Connection Retries*. If the reattempt fails, timestamped entries will appear in the trace log. For more information about these parameters, see SAP Integrated Business Planning via WebSocket RFC.

Related Information

Log Files

7 Configuring the SAP Data Services Agent

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

Prerequisite: Create the agent as described in Create an Agent before configuring it.

1. Register the agent in the SAP Cloud Integration for data services 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 Integration for data services server.
- Add or remove directories that may be accessed by the agent.
- Change an adapter configuration.
- Uninstall the agent from the host system.
- For a BW target, you may want to set the parameter `EmbeddedRFCShutdownTimeout` to a short time such as 60000 milliseconds (one minute) or even 5000 milliseconds (five seconds) in situations where multiple jobs might start at the same time and they use the same RFC destination/PROGRAM ID (Registered Server Program). If the protocol sends both requests to the same engine, this shorter parameter setting avoids other engines from waiting the default of 10 minutes before timing out. For more information, see SAP Note 3063345.

Related Information

7.1 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 Integration for data services interface.

1. Log in to SAP Cloud Integration for data services 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.

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 23]
Downloading the Agent Configuration File [page 24]
Configuring the Secure Agent Connection [page 24]

7.1.1 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 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 Integration for data services web UI.

> **i 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

7.2 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 Integration for data services.

1. Log into SAP Cloud Integration for data services 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 23]
Configuring the Secure Agent Connection [page 24]

7.3 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 Integration for data services.

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

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 Integration for data services administrator user name and password and the location of the configuration file you downloaded. If you have set up client authentication using the default IDP from accounts.sap.com, use an email address linked to your SAP S-user or universal ID as the user name and enter the password for that SAP S-user or universal ID account.

   Authentication against SAP accounts.sap.com may need to be reset during an upgrade.
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 Integration for data services 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.
   a. Select *Use proxy server*.
   b. Specify the address and port information for your proxy server.
   c. 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 Integration for data services, uploads security certificates, and verifies that the configuration was successful. If there are no errors, the status of the agent in the SAP Cloud Integration for data services interface changes to indicate that the agent is registered correctly.
7. 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.

Related Information

Reconfiguring the Agent Connection [page 25]
Registering an Agent in the Web Interface [page 23]
Downloading the Agent Configuration File [page 24]

7.3.1 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.

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

7.4 Configuring Client Authentication for SOAP Web Services

If your SOAP Web Services endpoints require client authentication, additional setup is necessary to enable this authentication.

> **!** Restriction
>
> This topic applies only if you are using Data Services Agent version 1.0.11 patch 34 or later.

Configure client authentication as described below, on both the server side and on the agent side.

Import the SOAP Web Services Server Certificates on the Agent

1. On the agent machine, go to `%LINK_DIR%`, and run `ConfigureAgent.bat` as Administrator.
2. Select the *Import Certificates* menu.
3. Select *Download certificates from http server*, and enter the URL of SOAP Web Services server.
4. Select *Import*.

For more information, see Importing Certificates [page 38].

Provide Keystore Path and Password on the Server

Prerequisite: Before you perform the following steps, you must generate the keystore file (`*.jks`) and place it on your agent machine to verify the client.

1. In SAP Cloud Integration for data services, under the Datastore tab, create a new SOAP Web Services datastore or select a SOAP Web Services datastore to edit.
2. For the *Keystore Path*, enter the full path file name of the keystore at the agent. For example, `C:\FolderName\KeystoreFileName`, or in Linux, `/FolderName/KeystoreFileName`. Refer to the agent location that you set previously.
3. For the *Keystore Password*, enter the password for the keystore.
4. Click *OK* or *Save* to save the new or updated datastore.

For details about these and other SOAP Web Services datastore options, see SOAP Web Service in the HELP CENTER.

Set up the Web Services Call With Client Authentication on the Agent

1. On the agent machine, go to `%LINK_DIR%\ext\webservice-c` and open `axis2.xml` in a text editor.

   > **i** Note
   >
   > If you want a separate setting for each WS datastore, you can duplicate `webservice-c` folder and have the datastore configuration point to that directory.

   Configuration name: `“Axis2/c configuration file path”`
2. Make sure **https** is not commented out.

```
<transportSender name="https" class="axis2_http_sender">
      <parameter name="PROTOCOL" locked="false">HTTP/1.1</parameter>
      <parameter name="xml-declaration" insert="false"/>
      </transportSender>
```

3. Uncomment the SERVER_CERT, KEY_FILE, and SSL_PASSPHRASE.

```
 <!--

     <parameter name="SERVER_CERT">/path/to/ca/certificate</parameter>
     <parameter name="KEY_FILE">/path/to/client/certificate/chain/file</
parameter>
     <parameter name="SSL_PASSPHRASE">passphrase</parameter>
     -->
```

4. Update these values to refer to the server certificate, key file (pem file), and SSL passphrase.
   For more information, see http://people.apache.org/~dumindu/docs/HowToConfigureSSL.html .
5. Restart the agent.

7.5 Managing Allowlisted Directories

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

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 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.

     > **i Note**
     >
     > Each directory must be explicitly declared. For example if you have a `C:\Data` directory with `C:\Data\2017` and `C:\Data\2018` subdirectories that contain your data, you must add two separate entries: one for C:\Data\2017 and another for C:\Data\2018

     > **! Restriction**
     >
     > The software does not support mapped drives. To add a network location, you must specify the path using UNC notation. For example, `\\<servername>\<sharename>`.

   - 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.

   > **i Note**
   >
   > 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.

7.6 Configuring ODBC data sources in Linux

To configure ODBC data sources in Linux, use the SAP Data Services Connection Manager.

SAP Cloud Integration for data services supports several ODBC data sources natively with DSN connections. Ensure that SAP Cloud Integration for data services supports your ODBC data source. For more information, see the Product Availability Matrix.

Ensure that you have the correct privileges to change the configuration files mentioned in these steps.

Install the GTK+2 library to make a graphical user interface for Connection Manager. The GTK+2 is a free multi-platform toolkit that creates user interfaces. The installation is at https://www.gtk.org/ .

1. To open the DSConnectionManager, enter the following command:

   ```
   $ cd $LINK_DIR/bin/
   $ ./DSConnectionManager.sh
   ```

   The DSConnectionManager GUI opens.
2. Click the *Data Sources* tab, and click *Add* to display the list of database types.
3. Select the database type in the *Select Database Type* dialog box, and click *OK*.
   The *Configuration for...* dialog box opens. The Connection Manager automatically completes the following information:
   - The absolute location of the `odbc.ini` file in which the DSN is defined
   - Driver, if relevant for database type

- Driver Version, if relevant for database type

4. Provide values for additional connection properties, such as Server Name, Instance, or Port, for the specific database type.
5. Provide the following properties:
   - User name
   - Password

   > **Note**
   >
   > The Connection Manager does not save this information for further use.

6. To test the connection, click *Test Connection*.
7. When the connection test is successful, click *Restart Services*.

7.7 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.

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

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:

Option	Description
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.

> **i 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 38]
Importing Certificates [page 38]

7.8 Configuring SSL Support for SOAP Web Services

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

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 38] or Connecting to Secure Web Services by Manually Adding Certificates [page 29]:

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 38]
Connecting to Secure Web Services by Manually Adding Certificates [page 29]

7.9 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.

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.

Option	Description
Adapter Retry Count	The number of times the agent should attempt to start the adapter.
Adapter Retry Interval	The amount of time the agent should wait between attempts to start the adapter, in milliseconds.
Trace Mode	Enables or disables trace logging for the adapter.

Additional Java Launcher Options	Additional options to use when starting the adapter instance. The default information for this parameter is `-Xms64m –Xmx256m`.
	• The proxy can be disabled by removing the default proxy line from this field.
	• To add a proxy server, append the proxy server parameters `-Dhttp.proxyHost=<Your proxy server name>` and `-Dhttp.proxyPort=<Your proxy port number>`.
	For example:
	`-Xms64m –Xmx256m -Dhttp.proxyHost=myproxy -Dhttp.proxyPort=8080`
	If you need to pass a username and password to your proxy as well, then also append:
	`-Dhttp.proxyUser=<Your proxy user name> -Dhttp.proxyPassword=<Your proxy password>`
	Click *Apply*.

Option	Description
	• 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, `Djavax.net.ssl.keyStore="C:\Program Files\SAP\DataServicesAgent\ssl\client_certs\<keystoreName>.jks" -Djavax.net.ssl.keyStorePassword=<*****>`

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.

7.10 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.

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 OData adapter as required for your instance.

Option	Description
Adapter Retry Count	The number of times the agent should attempt to start the adapter.
Adapter Retry Interval	The amount of time the agent should wait between attempts to start the adapter, in milliseconds.
Trace Mode	Enables or disables trace logging for the adapter.

Option	Description
Additional Java Launcher Options	Additional options to use when starting the adapter instance. The default information for this parameter is `-Xms64m –Xmx256m`. • The proxy can be disabled by removing the default proxy line from this field. • To add a proxy server, follow the instructions in Adding a Proxy Server [page 33]. Be sure to click *Apply* after adding your proxy server parameters. • 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 key-store and password. For example, `-Djavax.net.ssl.keyStore="C:\Program Files\SAP\DataServicesAgent\ssl\client_certs\<keystoreName>.jks" -Djavax.net.ssl.keyStorePassword=<*****>`

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.

Related Information

Adding a Proxy Server [page 33]

Authenticating Client Certificates [page 34]

7.10.1 Adding a Proxy Server

Append parameters for your proxy server when configuring an OData adapter.

When configuring the OData adapter as required for your instance, you can set Java Launcher options to use a proxy server when the adapter instance starts.

> **i** Note
>
> Be sure you know ahead of time whether your server's URL begins with **http** or **https**, as this is important for configuring your OData adapter correctly.

1. In *Additional Java Launcher Options*, append the following parameters: `-Dhttp.proxyHost=<Your proxy server name>` and `-Dhttp.proxyPort=<Your proxy port number>`.

   Example: `-Xms64m -Xmx256m -Dhttp.proxyHost=myproxy -Dhttp.proxyPort=8080`
2. If you need to pass a username and password to your proxy as well, then also append these parameters: `-Dhttp.proxyUser=<Your proxy user name>` and `-Dhttp.proxyPassword=<Your proxy password>`.

Example: `-Xms64m -Xmx256m -Dhttp.proxyHost=myproxy -Dhttp.proxyPort=8080 -Dhttp.proxyUser=cjulian -Dhttp.proxyPassword=abcd1234`

7.11 Authenticating Client Certificates

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

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.

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.

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*.
7. Upload the *Intermediate 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 32]

7.12 Tenant Post-Migration Setup

If the tenant domain URL has changed or migrated to another domain, the agent needs to be redirected to the correct tenant domain URL. To do this, perform these steps after the tenant is ready.

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* in the menu on the left-hand side.
3. Enter your SAP Cloud Integration for data services administrator user name and password.
4. Download the latest *Agent Configuration File* from the new domain using the SAP Cloud Integration for data services web UI. See Downloading the Agent Configuration File [page 24] for more information.
5. Navigate back to the SAP Data Services Agent configuration program and browse to the latest *Agent Configuration File* you downloaded.

   > **Note**
   >
   > If you are migrating to a new tenant, you will need to re-download the latest Agent Configuration File and replace the *Agent Configuration File* in the configuration program.
6. Click *Upload* to save your changes to the agent configuration.
7. 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.

7.13 Updating the Agent Version

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

> **Note**
>
> If you are updating the version of the agent on Windows or Linux platforms, ensure that you have done the following prior to upgrading:

- Back up the `DSConfig.txt` file.
- Back up all `%DSOD_APPDATA%` (Windows) or `$DSOD_APPDATA` (Linux) directories.
- If you are using web services, back up the settings in `%LINK_DIR%\ext\webservice-c\axis2.xml`.
- If you have any client certificates downloaded in any of the following directories within `%LINK_DIR% ->`, back up the client certificate files:
  - `bin`
  - `lib`
  - `ext`
  - `sqla`
  - `admin`

If you are using Linux, you can also automatically back up necessary files by stopping all processes using `/dsod_stop.sh` and copying files to the backup using `cp -rf`.

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 13]

7.14 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.

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`.

     > **Note**
     >
     > 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`.

> **Note**
>
> 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.

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

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 80]
Manually Uninstalling the Agent [page 80]

8 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.

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

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`.

   > **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 using one of the following methods:

Method	General use case	Example
Select a certificate file	SAP Cloud Integration for data services server **Note** This is unusual. When needed, updated certificates are included in support package or patch releases. Proxy server	Browse to the location of the updated or new certificate.
Download certificates from an http server As needed, also specify the proxy server host and port as well as proxy user and password.	Web service Proxy server	`http://<serverabcd>:<8080>`

4. Click *Import*.

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

If you will create a SOAP Web Service datastore that connects to a SOAP-based web service that uses SSL, after importing the certificate you must place the keystore (`*.jks`) on your agent machine to verify the client.

Related Information

Troubleshooting [page 72]

9 Configuring SAP Business Suite Connectivity

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

Related Information

9.1 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 41]

9.1.1 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_ROWCOUNT
- GET_VERSION
- IDOC_SEARCH
- JOB_LOG
- JOB_RUN
- JOB_STATUS
- MODEL_NAVIGATE

- READ_TEXT
- RFC_READ_EXTRACTOR
- RFC_READ_TABLE
- RFC_READ_TABLE_FILE
- RFC_READ_TABLE2
- RFC_STREAM_READ_TABLE
- TABLE_SEARCH
- TEXTS
- TREE_NAVIGATE
- TREE_NAVIGATE40
- TREE_PROF
- TREE_SEARCH
- TREE_SEARCH40

9.2 Descriptions for SAP User Authorizations

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 1:

In order to....	Authorization
Process batch jobs	S_BTCH_JOB: Batch Processing [page 46]
Perform the following actions: • perform a column search • run generated programs on the SAP server • import a table • search for a table	S_DEVELOP: ABAP Workbench [page 47]

In order to....	Authorization
Execute remote functions on an SAP server	S_RFC: Authorization Check for RFC Access [page 50]
Access table data in an SAP system	S_TABU_DIS: Table Maintenance [page 56]
• Access specific transactions • Execute functions in the Data Warehousing Workbench	S_TCODE: Authorization Check for Transaction Start [page 56]
Access ERP hierarchies	G_800S_GSE: Special Purpose Ledger Sets [page 46]
Check background processing privileges	S_BTCH_ADM: Background Processing [page 46]
Perform CTS operations	S_CTS_ADMI: Administration Functions in Change and Transport System [page 47]
Work with IDocs	S_IDOCDEFT: Access to IDoc Development [page 50]
Stream using RFC	S_RFC_ADM: Administration for RFC Destination [page 51]
Check DataSource access privileges	S_RO_OSOA: SAP DataSource Authorizations [page 51]
Load to BW	S_RS_ADMWB: Administrator Workbench - Objects [page 52]
Access an InfoCube	S_RS_ICUBE: Data Warehousing Workbench - InfoCube [page 52]
Access a DataStore Object	S_RS_ODSO: Data Warehousing Workbench - DataStore Object [page 52]
Read SAP texts	S_SCRP_TXT: SAPscript [page 53]
Access the SAP Data Services Agent functions	S_SDSAUTH: SBOP Data Services - General Authorization [page 54] S_DSAUTH: SBOP Data Services - General Authorization [page 48] ZDSAUTH: SBOP Data Services - General Authorization [page 58]
SAP Data Services Agent-specific equivalent of the SAP S_DEVELOP authorization object	S_SDSDEV: SBOP Data Services Authorization Object for Development [page 54] S_DSDEV: SBOP Data Services Authorization Object for Development [page 49] ZDSDEV: SBOP Data Services Authorization Object for Development [page 58]

In order to....	Authorization
Execute programs	S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 55] S_DSPGMCHK: SBOP Data Services Authorization Object for Program Names [page 49] ZPGMCHK: SBOP Data Services Authorization Object for Program Names [page 59]
Define whether the SAP system should be treated as a development or production system	S_SDSS: Data Services Authorization Object for Functions [page 55] S_SDS: Data Services Authorization Object for Functions [page 53] ZDSDEV: SBOP Data Services Authorization Object for Development [page 58]
Access the Transport Organizer	S_TRANSPRT: Transport Organizer [page 57]
Establish a connection to the SAP server	S_USER_GRP: User Master Maintenance [page 57]
Import an authorization profile	S_USER_PRO: User Master Maintenance [page 58]
Use the Open Hub interface	Open Hub: Administration for RFC Destination [page 45]
Browse metadata in an SAP BW source datastore	Browse Metadata for an SAP BW Source Datastore [page 60]

Related Information

Open Hub: Administration for RFC Destination [page 45]
G_800S_GSE: Special Purpose Ledger Sets [page 46]
S_BTCH_ADM: Background Processing [page 46]
S_BTCH_JOB: Batch Processing [page 46]
S_CTS_ADMI: Administration Functions in Change and Transport System [page 47]
S_DEVELOP: ABAP Workbench [page 47]
S_DSAUTH: SBOP Data Services - General Authorization [page 48]
S_DSDEV: SBOP Data Services Authorization Object for Development [page 49]
S_DSPGMCHK: SBOP Data Services Authorization Object for Program Names [page 49]
S_IDOCDEFT: Access to IDoc Development [page 50]
S_RFC: Authorization Check for RFC Access [page 50]
S_RFC_ADM: Administration for RFC Destination [page 51]
S_RO_OSOA: SAP DataSource Authorizations [page 51]
S_RS_ADMWB: Administrator Workbench - Objects [page 52]
S_RS_ICUBE: Data Warehousing Workbench - InfoCube [page 52]

9.2.1 Open Hub: Administration for RFC Destination

To use the Open Hub interface, use the profile S_BI_WHM_RFC profile and the S_RFC_ADM authorization.

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

Field	Values
Activity	03
RFCTYPE	T
RFCDEST	List of RFC destinations the user is allowed to access
ICF_VALUE	Authorizations for destination in transaction SM59

Related Information

S_RFC_ADM: Administration for RFC Destination [page 51]

9.2.2 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

Field	Values
Authorization group	Not used
Activity	03

9.2.3 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

Field	Values
Background administrator ID	Y

9.2.4 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

Field	Values
Job operation	RELE
Summary of jobs for a group	Not used

9.2.5 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

Field	Values
Administration Tasks for Change and Transport System	PROJ

9.2.6 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

Field	Values
Package	List of packages for tables that a user is allowed Package to access
Object type	TABL
Object name	List of tables that a user is allowed to access
Authorization group ABAP/4 program	Not used
Activity	03

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

Field	Values
Package	$TMP
Object type	PROG

Field	Values
Object name	List of temporary program names that are allowed to be generated
Authorization group ABAP/4 program	Not used
Activity	01 and 02

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

Field	Values
Package	List of packages for tables that a user is allowed to access
Object type	VIEW, TABL and TTYP
Object name	List of tables and views that a user is allowed to access
Authorization group ABAP/4 program	Not used
Activity	03

9.2.7 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

Field	Values
ACTVT: Activity	16 (Execute)

> **i 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

ZDSAUTH: SBOP Data Services - General Authorization [page 58]
S_SDSAUTH: SBOP Data Services - General Authorization [page 54]

9.2.8 S_DSDEV: SBOP Data Services Authorization Object for Development

S_DSDEV 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

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

> **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 54]
ZDSDEV: SBOP Data Services Authorization Object for Development [page 58]

9.2.9 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

Field	Values
ACTVT: Activity	16 (Execute)

Field	Values
PROGRAM: ABAP program name	Program names that are allowed to be executed in a production environment

> **i** 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 55]
ZPGMCHK: SBOP Data Services Authorization Object for Program Names [page 59]

9.2.10 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

Field	Values
Activity	03
Extension	Not used
Basic type	Not used
Transaction code	WE30

9.2.11 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

Field	Values
Activity	16

Field	Values
Name of RFC to be protected	BAPI, CADR, RFC1, SCAT, SDIF, SLST, SUNI, SUTL, SDTX, SYST, /SAPDS, RSAB, SDIFRUNTIME, and any other required function group
Type of RFC object to be protected	FUGR

9.2.12 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

Field	Values
Activity	03
Type of Entry in RFCDES	Not used
Logical Destination (Specified in Function Call)	RFC destination
Internet Communication Framework Values	Not used

9.2.13 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

Field	Values
Activity	03
DataSource (OSOA/OSOD)	DataSource for data extraction
Application Component of a DataSource (OSOA/OSOD)	Not used
Subobject for DataSource	DATA

9.2.14 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

Field	Values
Administrator Workbench object	WORKBENCH, SOURCESYS, APPLCOMP, INFOAREA, INFOOBJECT, INFOPACKAG, ODSOBJECT
Activity	03

9.2.15 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

Field	Values
InfoArea	List of InfoAreas that a user is allowed to access
InfoCube	List of InfoCubes that a user is allowed to access
InfoCube Subobject	DEFINITION
Activity	03

9.2.16 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

Field	Values
InfoArea	List of InfoAreas that a user is allowed to access

Field	Values
DataStore Object	List of DataStore Objects that a user is allowed to access
Subobject for ODS Object	DEFINITION
Activity	03

9.2.17 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

Field	Values
Language Key	List of language keys that a user is allowed to access
Text ID	List of text IDs that a user is allowed to access
Name	List of text names that a user is allowed to access
Activity	SHOW

9.2.18 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
ACTVT	Not used
ZSYSTYPE	D: Development system Any other value: Production system

> **i** 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

ZSDS: Data Services Authorization Object for Functions [page 60]
S_SDSS: Data Services Authorization Object for Functions [page 55]

9.2.19 S_SDSAUTH: SBOP Data Services - General Authorization

The S_SDSAUTH 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

Field	Values
ACTVT: Activity	16 (Execute)

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

9.2.20 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

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

> **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 49]
ZDSDEV: SBOP Data Services Authorization Object for Development [page 58]

9.2.21 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

Field	Values
ACTVT: Activity	16 (Execute)
PROGRAM: ABAP program name	Program names that are allowed to be executed in a production environment

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

9.2.22 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

Field	Values
ACTVT	Not used
ZSYSTYPE	D: Development system Any other value: Production system

> **i** Note
>
> In some SAP NetWeaver versions, this authorization object is named ZSDS or S_SDS. The objects are identical except for the name.

Related Information

ZSDS: Data Services Authorization Object for Functions [page 60]
S_SDS: Data Services Authorization Object for Functions [page 53]

9.2.23 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

Field	Values
Activity	03
Authorization group	Table groups that a user is allowed to access

9.2.24 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

Field	Values
Transaction code	SE37, SE38, SU53

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

Field	Values
Transaction code	RSA1

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

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

9.2.25 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

Field	Values
Request Type (Change and Transport System)	DTRA
Activity	01

9.2.26 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

Field	Values
User group in user master maintenance	User group for the SAP Data Services Agent user

9.2.27 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

Field	Values
Auth. profile in user master maintenance	Authorization Profile to be imported
Activity	03

9.2.28 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

Field	Values
ACTVT: Activity	16 (Execute)

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

Related Information

S_DSAUTH: SBOP Data Services - General Authorization [page 48]
S_SDSAUTH: SBOP Data Services - General Authorization [page 54]

9.2.29 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

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

> **i** 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_DSDEV: SBOP Data Services Authorization Object for Development [page 49]
S_SDSDEV: SBOP Data Services Authorization Object for Development [page 54]

9.2.30 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

Field	Values
ACTVT: Activity	16 (Execute)
PROGRAM: ABAP program name	Program names that are allowed to be executed in a production environment

> **i** 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_DSPGMCHK: SBOP Data Services Authorization Object for Program Names [page 49]
S_SDSPGMCK: SBOP Data Services Authorization Object for Program Names [page 55]

9.2.31 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

Field	Values
ACTVT	Not used
ZSYSTYPE	D: Development system Any other value: Production system

> **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 55]
S_SDS: Data Services Authorization Object for Functions [page 53]

9.2.32 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.

9.3 Authenticating with Secure Network Communications (SNC)

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

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

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*.

Related Information

SAP NetWeaver Security Guide

9.4 Considerations for Running ABAP Programs

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

In all cases where you use an ABAP transform in SAP Cloud Integration for data services, 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 Integration for data services data flow, it can be used in two ways:

- *Generate and Execute*

  > → Tip
  >
  > 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*

  > → Tip
  >
  > 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".

Custom ABAP transform

When you use a Custom ABAP transform in an SAP Cloud Integration for data services data flow, the generated ABAP program will contain the custom ABAP FORM. In the datstore, 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 62]
Manually Uploading ABAP Programs to the SAP System [page 63]

9.4.1 Configuring the RFC Destination

Before you can extract from SAP Business Suite application sources in an SAP Cloud Integration for data services 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:

Field Name	Value
RFC Destination	SAPDS
Connection Type	T (TCP/IP connection)
Description (Optional)	User-defined description of the RFC destination

Technical Settings tab

Field Name	Value
Activation Type	Registered Server Program
Program ID	<must always be empty>

> **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 Integration for data services task is currently running.

9.4.2 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.

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.

To upload the ABAP program to the SAP system:

> **i** 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 Integration for data services user interface.

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.

Related Information

Generate and Load an ABAP Program

9.5 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 Integration for data services to SAP BW.

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.

   > i Note
   >
   > *Connection Test* is not available in this case.

10 Log Management

The `DSOnPremiseAgentXXX.log` file contains all agent log files. This section details various parameters and methods to optimize your log storage to avoid loss of files or memory overload.

> **i** Note
>
> If the agent restarts, a new log, `DSOnPremiseAgent_yyyymmdd_hhmmssms_threadid_num.log`, will be created.

The parameters listed below are hidden but configurable within the `DSConfig.txt` file.

Important: When you modify a parameter's value, you must restart the agent for your change to take effect.

Parameter	Description
`AgentlogFileCount = 25`	By default, there is a limit of 25 files for the log, after which the files wrap around.
`AgentlogsizePerFile = 10485760`	By default, there is a limit of 10MB per log file.
`EnableTrace = false`	By default, this parameter is set to false, which provides minimal information. If you want more debugging information, change the value to `True`.

Related Information

Log Retention [page 65]

10.1 Log Retention

The agent is scheduled to continuously check and clean out log files that are not needed in order to optimize space.

The `AgentLogRetentionInHours = 720` flag stores all agent log files for a default of 720 hours.

11 PGP Management

SAP Cloud Integration for data services 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 Integration for data services 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:

Key	Use
Organization public key	Used by external third-party to encrypt data
Organization private key	Used to decrypt the data from the external third-party
External third-party public key	Imported and then used to verify the digital signature

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

Key	Use
External third-party public key	Used by SAP Cloud Integration for data services to encrypt data
Organization private key	Used when generating the optional digital signature.
Organization public key	Exported from SAP Cloud Integration for data services. Sent to third party to use to verify the digital signature

Related Information

Generating a PGP Key Pair [page 67]
Moving your Organization Key Pair [page 67]
Importing an External Public Key [page 68]
Exporting your Public Key [page 69]
Reading from PGP-protected Source Files [page 69]
Loading into PGP-protected Target Files [page 71]

11.1 Generating a PGP Key Pair

Within an SAP Cloud Integration for data services organization, generate a single PGP key pair.

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 Integration for data services can decrypt the data using the organization private key.

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 *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*.

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

11.2 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.

A PGP key pair has been generated for the organization.

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.

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.

11.3 Importing an External Public Key

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

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

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

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

11.4 Exporting your Public Key

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

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 *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*.

11.5 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.

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

	Prerequisite	More information
☐	A PGP key pair exists for your organization.	Generating a PGP Key Pair [page 67]

	Prerequisite	More information
☐	The organization key pair is imported to the system hosting your agent.	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 67]
☐	The owner of the source file has your public key.	Export your public key and send it to the owner of the source file. Exporting your Public Key [page 69]
☐	The owner of the source file has encrypted the file using your public key.	

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

	Prerequisite	More information
☐	You have received the external (third-party) public key from the owner of the source file.	
☐	You have imported the external (third-party) public key to the system which hosts your agent.	Importing an External Public Key [page 68]

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

1. In the SAP Cloud Integration for data services 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*.

Validate and run the task as usual.

11.6 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.

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

	Prerequisite	More information
☐	You have received the public key of the external third-party that will receive the target.	Make sure to get the user ID of the key. The user ID can be an email address, name, or other identifying information.
☐	You have imported the external third-party public key.	Importing an External Public Key [page 68]

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

Table 5: Prerequisites to generate a digital signature

	Prerequisite	More information
☐	A PGP key pair exists for your organization.	Generating a PGP Key Pair [page 67]
☐	The organization key pair is imported to the server hosting your agent.	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 67]
☐	You have exported your organization's public key.	Exporting your Public Key [page 69]
☐	You have sent your public key to the external third-party that owns the target.	

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

1. In the SAP Cloud Integration for data services 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:

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.

Log file	Filename
Installation log	`Install_<timestamp>.log`
Configuration log	`Config_<timestamp>.log`

- 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 Integration for data services and the SAP Data Services Agent, see *SAP Note 1800845* on the SAP Service Marketplace.

Related Information

Collect Agent Diagnostic Information [page 73]
Stopping the Internal Database [page 80]
Manually Uninstalling the Agent [page 80]
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 file to attach is noted at the end of the results.

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

You can run the Agent diagnostic tool via a user interface to obtain the following types of information for analysis:

- 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 Integration for data services server
- TCP/IP port information
- Security certificate information

You can also run the Agent diagnostic tool using the command line to obtain an export of an entire repository as well as a specific task or process. The export can be in ATL format or in XML formatted for Data Services Designer.

Related Information

Using the Agent Diagnostic Tool User Interface [page 73]
Running the Agent Configuration Tool via the Command Line [page 74]
Configuring the SAP Data Services Agent [page 22]

A.1.1 Using the Agent Diagnostic Tool User Interface

You can run the tool via its interface rather than by the command line.

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 *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.

A.1.2 Running the Agent Configuration Tool via the Command Line

Running the Data Services Agent Configuration Tool via a command line allows you to export a specific task or process or an entire repository in ATL and XML format for troubleshooting purposes. An ATL file is a proprietary SAP text file type that contains repository information.

You can add the various generated files from this command line tool to customer support cases, which provides useful information to SAP.

You can run the Agent Configuration Tool for both sandbox and production (prod) repositories.

Accessing the Data Services Agent Configuration Tool

For Windows:

1. Open the command prompt and run as administrator.
2. Cd to %LINK_DIR%.
3. Enter **`ConfigureAgent.bat`**. Add arguments as explained in the topics listed in the Related Information below for specific output.

For Linux:

1. Open the terminal window.
2. Cd to InstallDir.
3. Enter **`./configureAgent.sh`**. Add arguments as explained in the topics listed in the Related Information below for specific output.

Important Usage Notes about the Data Services Agent Configuration Tool

- SAP Cloud Integration for data services does not allow the task or process name to have a space, so the -name option is always the entire name. There is no need to use quotes.
- In SAP Cloud Integration for data services, a task or process name is case insensitive; therefore, you can use mixed case in the tool.
- `-export` or `-agentdiagnostic` must be the first parameter.
- -export has to be followed by `atl` or `xml`.
- -repo has to be followed by `sandbox` or `prod`.
- Microsoft Windows is case-insensitive; Linux is case-sensitive.

Viewing On-screen Instructions in the Data Services Agent Configuration Tool

Enter one of the following:

- For Microsoft Windows, enter **`ConfigureAgent -h`**.
- For Linux, enter **`./configureAgent -h`**.

Related Information

Export a Task or Process in ATL Format [page 75]
Export a Task or Process in XML Format [page 75]
Export an Entire Agent Repository in ATL Format [page 76]
Export an Entire Agent Repository in XML Format [page 76]
Agent Diagnostics Available via the Command Line [page 77]

A.1.2.1 Export a Task or Process in ATL Format

You can export the details of a task or process in ATL format, which you can attach to an SAP Support ticket for analysis and troubleshooting.

The Agent Configuration Tool provides timestamp information in the output file name.

Within the SAP Data Services Agent Configuration Tool, enter one of the following:

Option	Description
For Microsoft Windows	`ConfigureAgent.bat -exportatl -repo<sandbox_or_prod> -name<task_or_process_name>`
For Linux	`./configureAgent.sh -exportatl -repo<sandbox_or_prod> -name<task_or_process_name>` Linux is case-sensitive.

The output path for the exported ATL file is indicated in the tool and will be similar to this example:

`C:\ProgramData\SAP\DataServicesAgent\log\RepoOutput\BWInfoPackage_<20210727_201132413>_sandbox.atl`.

A.1.2.2 Export a Task or Process in XML Format

You can export the details of a task or process in Data Services XML format, which you can attach to an SAP Support ticket for analysis and troubleshooting.

The Agent Configuration Tool provides timestamp information in the output file name.

Within the SAP Data Services Agent Configuration Tool, enter one of the following:

Option	Description
For Microsoft Windows	`ConfigureAgent.bat -exportxml -repo<sandbox_or_prod> -name<task_or_process_name>`

Option	Description
For Linux	`./configureAgent.sh -exportxml -repo<sandbox_or_prod> -name<task_or_process_name>` Linux is case-sensitive.

The output path for the exported XML file is indicated in the tool and will be similar to this example: `C:\ProgramData\SAP\DataServicesAgent\log\RepoOutput\BWInfopackage_<20210730_452484>_sandbox.xml`.

A.1.2.3 Export an Entire Agent Repository in ATL Format

You can export the details of an agent repository in ATL format, which you can attach to an SAP Support ticket for analysis and troubleshooting

The Agent Configuration Tool provides timestamp information in the file name.

Within the SAP Data Services Agent Configuration Tool, enter one of the following:

Option	Description
For Microsoft Windows	`ConfigureAgent.bat -exportatl -repo<sandbox_or_prod>`
For Linux	`./configureAgent.sh -exportatl -repo<sandbox_or_prod>` Linux is case-sensitive.

The output path for the exported ATL file is indicated in the tool and will be similar to this example:

`%DS_COMMON_DIR%\RepoOutput\all_<20210730_452484>_sandbox.atl`.

A.1.2.4 Export an Entire Agent Repository in XML Format

You can export the details of an agent repository in Data Services XML format, which you can attach to an SAP Support ticket for analysis and troubleshooting.

The Agent Configuration Tool provides timestamp information in the file name.

Within the SAP Data Services Agent Configuration Tool, enter one of the following:

Option	Description
For Microsoft Windows	`ConfigureAgent.bat -exportxml -repo<sandbox_or_prod>`
For Linux	`./configureAgent.sh -exportxml -repo<sandbox_or_prod>` Linux is case-sensitive.

The output path for the exported XML file is indicated in the tool and will be similar to this example:

`%DS_COMMON_DIR%\RepoOutput\all_<20210730_452484>_sandbox.xml`.

A.1.2.5 Agent Diagnostics Available via the Command Line

The Agent Diagnostic Tool supports using the command line to examine the communication between the agent and the server.

Running the Agent Diagnostic Tool via the command line provides additional functionality compared to the *Run agent diagnostics* button that is available within the Configure Agent user interface. Running this by the command line provides a more granular set of diagnostic information. For example, the command line method enables you to specifically generate diagnostic logs whereas running the tool from the user interface generates all diagnostic information, which may take some time depending on the contents of the agent.

The following information is available:

General Information

- Lists the key information in DSConfig.txt
- Operating system information
- Network IP
- Available processors (cores)
- Free memory (bytes)
- Max memory (bytes)
- File system root, total space, free space, and usable space

Privilege Information

Checks the privilege of the user running the tool

System Information

Gathers information about:

- win
- netstat -av
- tcpip maxuserport/tcptimewaitdely if there is one
- List all the process (tasklist or ps -ef)
- List all the files under %LINK_DIR%\ssl\trusted_certs

The following are only for Linux if available for the user to run:

- lsof
- ulimit -a

Network communication between the agent and server for the C++ part

Checks to see if there is a certificate issue.

Simulates Data Services' concatenating the qualified certificates under %LINK_DIR%\ssl\trusted_certs and allows the curl command to the server.

For example, curl -S -v https://hcidstest2.hana.ondemand.com/DSoD.

Network communication between the agent and server for the Java part

Checks to see if there is a certificate issue.

Agent has C++ and Java code that needs to communicate to the server. C++ is using dsod.pem and Java is using a Java keystore. This action is to use the Java keystore information to communicate with the server.

Certification Information

Lists all the certificates in the Java keystore.

Collect logs from %DS_COMMON_DIR%

Collects conf, adapters, abap, logs under %DS_COMMON_DIR%\.

If the agent has set up network communication with the server, then the following table applies:

Actions	All	systemdump	checkcerts	logsonly
General Information	Yes	Yes	Yes	Yes
Privilege Info	Yes	Yes	Yes	Yes
System Information	Yes	Yes	No	No
Network communication between the agent and server for the C++ part	Yes	Yes	No	No
Network communication between the agent and server for the Java part	Yes	Yes	No	No
Certification Information	Yes	No	Yes	No
Collect logs from %DS_COMMON_DIR%	Yes	No	No	Yes

If the agent has **not** set up network communication with the server, then the following table applies:

	All/Full	systemdump	checkcerts	logsonly
General Information	Yes	Yes	Yes	Yes
Privilege Info	Yes	Yes	Yes	Yes
System Information	Yes	Yes	No	No
Network communication between the agent and server for the C++ part	Yes	No	No	No
Network communication between the agent and server for the Java part	Yes	No	No	No

	All/Full	systemdump	checkcerts	logsonly
Certification Information	Yes	No	Yes	No
Collect logs from %DS_COMMON_DIR%	Yes	No	No	Yes

> **Note**
>
> There is general information, privilege information, network information, netstat information, Java keystore information, and all certificates in the Java keystore.

For Windows:

1. Open the command prompt and run as administrator.
2. Cd to %LINK_DIR%.

For Linux:

1. Open the terminal window.
2. Cd to InstallDir.

Enter one of the following commands:

Option	Description
To run a full diagnostic	For Windows, enter **`ConfigureAgent.bat -agentdiagnostic`** or **`ConfigureAgent.bat -agentdiagnosticall`**. For Linux, enter **`./configureAgent.sh -agentdiagnostic`** or **`./configureAgent.sh -agentdiagnosticall`**. The result is a ZIP file with the name `log<timestamp>.zip`.
To run a system dump diagnostic	For Windows, enter **`ConfigureAgent.bat -agentdiagnosticsystemdump`**. For Linux, enter **`./configureAgent.sh -agentdiagnosticsystemdump`**. The result is a LOG file as `%DS_COMMON_DIR%\log\Diagnostic_<timestamp>.log`.
To run a certificate diagnostic	For Windows, enter **`ConfigureAgent.bat -agentdiagnosticcheckcerts`**. For Linux, enter **`./configureAgent.sh -agentdiagnosticcheckcerts`**.

Option	Description
	The result is a LOG file as `%DS_COMMON_DIR%\log\Diagnostic_<timestamp>.log`.
To run a logs-only diagnostic	For Windows, enter **`ConfigureAgent.bat -agentdiagnosticlogsonly`**. For Linux, enter **`./configureAgent.sh -agentdiagnosticlogsonly`**. The result is a ZIP file with the name `log<timestamp>.zip`.

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.

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` (prior to SP11 patch 31)

   `regsvr32 /u "%LINK_DIR%"\sqla\dbodbc17DSAgent.dll` (SP11 patch 31 or later)
6. Delete the installed files and folders under `%LINK_DIR%`, `%DS_COMMON_DIR%`, `%DSOD_APPDATA%` (applicable only to patch 38 or later), and `%DS_USER_DIR%`.
7. Remove the `%LINK_DIR%`, `%DS_COMMON_DIR%`, `%DSOD_APPDATA%` (applicable only to patch 38 or later), and `%DS_USER_DIR%` system environment variables.

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 an 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.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

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.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP