Informatica® LLC Informatica Cloud Version Spring 2017 Release Notes

April 2017

© Copyright Informatica LLC 2006, 2017

Contents

Spring 2017 Release Notes

This section contains the Release Notes for Spring 2017.

Before You Upgrade

Prepare the Secure Agent for Upgrade

The Secure Agent upgrades the first time that you access the Informatica Cloud Spring 2017 release. To ensure that the Secure Agent upgrades properly, you must prepare each machine where the Secure Agent runs before the Informatica Cloud Spring 2017 upgrade.

Perform the following steps to ensure that the Secure Agent is ready for the upgrade:

1. Ensure that each Secure Agent machine has sufficient disk space available for upgrade. To calculate the free space required for upgrade, use the following formula:

   ```
   Minimum required free space = 2 * (size of current <Secure Agent installation directory>) + 1 GB
   ```

2. If you are using a version of the Secure Agent earlier than version 30.0, back up third-party libraries, security certificates, private patches, and configuration files that you have added to the following directory:

   `<Secure Agent installation directory>/main/bin/rdtm`

   For example, you might want to back up the Microsoft Dynamics CRM `krb5.conf` and `login.conf` files.

   Copy these files to the following directory:

   `<Secure Agent installation directory>/main/bin/rdtm-extra`

   Files in this location will be preserved after the upgrade and copied to the following directories:

   - `<Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm`
   - `<Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm-extra`

   If you are using the Secure Agent version 30.0 or higher, files that you added to the following directory are preserved after the upgrade:

   `<Secure Agent installation directory>/apps/Data_Integration_Server/ext/deploy_to_main/bin/rdtm-extra`

   Note: If you use certain connectors, you might need to copy some driver files, third-party library files, or security certificates to different directories after the upgrade. For details, see the *After You Upgrade* chapter.

3. Ensure that no tasks run during the maintenance window. If you use Informatica Cloud to schedule tasks, you can configure a blackout period for the organization. Click **Configure** > **Schedules** > **Blackout Period**.
4. Close all applications and open files to avoid file lock issues, for example:
   - Windows Explorer
   - Notepad
   - Windows Command Processor (`cmd.exe`)

Early Upgrade to Secure Agent Version 30 and Later

If you are a Cloud Application Integration customer, you can perform an early install of Secure Agent version 30.0 and higher.

Informatica recommends that you perform an early install of Secure Agent version 30.0 and later if your organization falls under any of the following categories:

- You use Linux and run the Secure Agent as a root user.
  If you are a Linux root user, the automatic upgrade to Secure Agent version 33 fails because you cannot start the underlying PostgreSQL database. If you perform an early install, you can log in as a non-root user and install the Secure Agent.
- You use Linux and run multiple Secure Agents on the same server.
  The automatic upgrade fails if you use Linux and run multiple Secure Agents on the same server because you encounter port conflicts. If you opt for an early install, you can perform manual steps to ensure a smooth install.

To perform an early Secure Agent install, see the *Early Migration Guide: Secure Agent Version 30 and Later* at https://network.informatica.com/docs/DOC-17175.

If you perform an early install, you receive Secure Agent version 32.2. Informatica will automatically upgrade you to Secure Agent version 33 with the Spring 2017 release of Informatica Cloud Services.

After You Upgrade

Amazon Redshift Connector Post-Upgrade Tasks

You need to perform upgrade tasks if you want to use Amazon Redshift connections from versions earlier than 30.0 in version 33.0. If you upgraded an ODBC connection from a previous version that used

the 32-bit Redshift ODBC driver, you need to set the appropriate DSN name in the 64-bit Redshift ODBC driver after the upgrade.

Amazon Redshift Connector

To make client-side encryption configured for versions earlier than 30.0 to work in version 33.0, perform the following steps after the Secure Agent upgrades:

1. Move the `US_export_policy.jar` and `local_policy.jar` files, and cacerts files from `<Secure Agent installation directory>\jre2\lib\security` to `<Secure Agent installation directory>\jre\lib\security`.
2. Restart the Secure Agent.

ODBC Driver for Redshift

When you use an ODBC connection that contains the 32-bit ODBC Redshift driver to connect to Redshift from the previous version, the connection fails after the upgrade.

To ensure that the ODBC connection does not fail, perform the following tasks:

1. Install the 64-bit Redshift ODBC driver on the Secure Agent machine.
2. Create or rename the DSN with the same name as the DSN of the 32-bit Redshift ODBC driver from the previous version.

Amazon S3 Connector Post-Upgrade Tasks

You need to perform upgrade tasks if you want to use Amazon S3 connections from versions earlier than 30.0 in version 33.0.

After the Secure Agent with versions earlier than 30.0 upgrades to version 33.0, perform the following steps for Amazon S3 Connector:

1. Copy the `local_policy.jar` and the `US_export_policy.jar` files from the following directory:
   `<Secure Agent installation directory>\jre2\lib\security`
2. Paste the jar files to the following directory:
   `<Secure Agent installation directory>\jre\lib\security`
3. Restart the Secure Agent.

Chatter Connector Post-Upgrade Tasks

If you use proxy support, perform the following steps:

1. Copy the `ProxySettings.ini` file from `<Secure Agent installation directory>\main2\tomcat\plugins\<plugin ID>\` to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\Chatter\`

   Note: If the `deploy_to_main\bin\rdtm-extra\Chatter\` directory does not already exist, create the directory.

   Note: The folder name is case sensitive on Linux.
2. Restart the Secure Agent.

Copy Configuration Files

If you customized configuration files for any of the following connectors, you must copy the configuration files to the `rdtm` and `plugins` folders:

- Avature
  For example, you can copy `customFields.ini` file.
- Big Machines
  For example, you can copy WSDL and jar files.
- Birst
  For example, you can copy `birstconfiguration.ini` file.
- Box API
  For example, you can copy `config.properties` file.
- Coupa
  For example, you can copy `coupa.ini` and `read.xsd` files.
- Dropbox
  For example, you can copy `config.ini` file.
- Eloqua Bulk API
  For example, you can copy `ActivityConfig.json` file.
- Google API
  For example, you can copy `config.properties` file.
- Hadoop
  For example, you can copy `setHadoopConnectorClassPath.sh` file.
- JDBC
  For example, you can copy `jdbc.ini` file.
- Jira
  For example, you can copy `jirafields.ini` files.
- JSON Target
  For example, you can copy `config.ini` file.
- Marketo
  For example, you can copy `activityattributes.csv` file.
- Open Air
  For example, you can copy `OpenAirCodes.properties` file.
- Quickbooks V2
  For example, you can copy `connectionparameters.ini` file.
- TFS
- Workday
  For example, you can copy `fields.ini` file.
- Xactly
  For example, you can copy `xactly-client.jar` file.

- XML Source
  For example, you can copy `config.ini` file.

1. Copy the configuration file from `<Secure Agent installation directory>\main2\bin\rdtm\javalib\<plugin ID>\` to `<Secure Agent installation directory>\downloads\<latest connector zip package>\package\rdtm\javalib\<Plugin ID>`
2. Copy the configuration file from `<Secure Agent installation directory>\main2\tomcat\plugins\<plugin ID>\` to `<Secure Agent installation>\downloads\<latest connector zip package>\package\plugins\<Plugin ID>`
3. Restart the Secure Agent.

Cvent Connector Post-Upgrade Tasks

If you use `ProxySettings.ini`, `relationship.ini`, or `schema.ini` file, perform the following steps:

1. Copy the `ProxySettings.ini`, `relationship.ini`, or `schema.ini` file from `<Secure Agent installation directory>\main2\tomcat\plugins\<plugin ID>\` to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\Cvent\`

   Note: If the `deploy_to_main\bin\rdtm-extra\Cvent\` directory does not already exist, create the directory.

   Note: The folder name is case sensitive on Linux.
2. Restart the Secure Agent.

File Processor Connector Post-Upgrade Tasks

If you use proxy support, perform the following steps:

1. Copy the `ProxySettings.ini` file from `<Secure Agent installation directory>\main2\tomcat\plugins\<plugin ID>\` to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\FileProcessor\`

   Note: If the `deploy_to_main\bin\rdtm-extra\FileProcessor\` directory does not already exist, create the directory.

   Note: The folder name is case sensitive on Linux.
2. Restart the Secure Agent.

JD Edwards EnterpriseOne Connector Post-Upgrade Tasks

After the Secure Agent upgrades from versions earlier than 30.0 to version 33.0, you must perform the following tasks:

1. Navigate to the following directory:
   `<Secure_Agent_installation_directory>\apps\Data_Integration_Server\ext`

2. Create the following directory structures:
   - `deploy_to_main\bin\rdtm\javalib\447200\common`
   - `deploy_to_main\tomcat\plugins\447200\common`
3. Move the third-party jars from the following locations:
   - `<Secure Agent installation directory>\main2\bin\rdtm\javalib\447200\common` to `<SecureAgent_InstallDirectory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm\javalib\447200\common`
   - `<SecureAgent_Install Directory>\main2\ tomcat\plugins\447200\common` to `<SecureAgent_InstallDirectory>\apps\Data_Integration_Server\ext\deploy_to_main\tomcat\plugins\447200\common`
4. Restart the Secure Agent.

JDBC Connector Post-Upgrade Tasks

After the 32-bit or 64-bit Secure Agent earlier than version 30.0 upgrades to 33.0, perform the following tasks if you use a JDBC connection:

Update the JDBC Jar Directory Path

If the Secure Agent earlier than version 30.0 contains the JDBC driver jars in the Secure Agent installation directory, the existing JDBC connection fails after the upgrade. Manually update the JDBC connection with the valid JDBC Jar Directory path.

Import the SSL Server Certificate

When the Secure Agent earlier than version 30.0 upgrades, perform the following tasks to ensure that the secure connection is successful after the upgrade:

- If the SSL certificates are available in the Secure Agent installation directory in the previous version, the secure connection fails.
  After the upgrade, update the JDBC property in the JDBC URL to point to the valid truststore location.
- If the SSL certificate was imported to the following default truststore location in the previous version: `<Secure Agent installation directory>/jre/lib/security/cacerts`, the secure connection fails.
  To manually import the SSL certificate after the upgrade, run the following command: `keytool -import -trustcacerts -keystore <agent_home>/jre/lib/security/cacerts -storepass <keystore_password> -noprompt -alias <alias_name> -file <certificate>`

LDAP Connector Post-Upgrade Tasks

After the Secure Agent upgrades, you must configure the Java heap size and add the secure certificates for LDAP Connector.

Configure the Java Heap Size for LDAP Connector

If you increased the Java heap size in the `pmrdtm.cfg` file located at `<Secure Agent installation directory>\main\bin\rdtm` in the previous version to read or write binary data or large amounts of data, you must perform the following steps after the Secure Agent upgrades to version 33:

1. In the Informatica Cloud home page, click **Configure** > **Runtime Environments**.
2. Select the Secure Agent for which you want to increase the Java heap size, and click **Edit**.
3. In **System Configuration Details**, select type **DTM**.
4. Set the values for the JVM options, JVMOption1 and JVMOption2, according to the requirement. For example, set JVMOption1 to -Xms1024m and JVMOption2 to -Xmx2048m.
5. Restart the Secure Agent.

Copy the Secure Certificates for LDAP Connections Enabled with Secure Connection

Copy the secure certificates for LDAP Connector on the Secure Agent machine based on the version of the Secure Agent upgrade.

Upgrade from Secure Agent versions earlier than 30.0 to 33.0

After the Secure Agent upgrades from versions earlier than 30.0 to 33.0, the Secure Agent does not retain the certificates available in the following directories from the previous version for LDAP Connector:

- `<Secure Agent installation directory>\main\tomcat`
- `<Secure Agent installation directory>\main\bin\rdtm`

The Secure Agent also does not retain the certificates placed in the cacerts file in the following directory from the previous version:

`<Secure Agent installation directory>\jre\lib\security\cacerts file`

The issue causes the Data Synchronization tasks and mapping tasks to fail after the upgrade.

To ensure that tasks do not fail, perform the following steps:

1. Navigate to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext`.
2. Create the following directory structures:
   - `deploy_to_main\bin\rdtm`
   - `deploy_to_main\tomcat`
3. Copy the certificates from `<Secure Agent installation directory>\main2\tomcat` to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\tomcat`.
4. Copy the certificates from `<Secure Agent installation directory>\main2\bin\rdtm` to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm`.
5. Copy the cacerts file from `<Secure Agent installation directory>\jre2\lib\security` to `<Secure Agent installation directory>\jre\lib\security`.
6. You must restart the Secure Agent after you copy the certificates and files.

Upgrade from Secure Agent version 32.0 to 33.0

After Secure Agent 30.0 or later versions upgrades to 33.0, existing Data Synchronization and Mapping Configuration tasks fail and results in the following error: `javax.net.ssl.SSLHandshakeException`

To ensure that the tasks from the previous version do not fail, perform the following tasks:

1. Navigate to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext`.
2. Create the following directory structures:
   - `deploy_to_main\bin\rdtm`
   - `deploy_to_main\tomcat`
3. Copy the certificates from `<Secure Agent installation directory>\main2\tomcat` to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\tomcat`.
4. Copy the certificates from `<Secure Agent installation directory>\main2\bin\rdtm` to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm`.
5. You must restart the Secure Agent after you copy the certificates.

Microsoft Access Connector Post-Upgrade Tasks

After the 32-bit Secure Agent upgrades to 64-bit Secure Agent version 33.0 on Windows, you need to restore the DSN name in the upgraded version. You must avoid changing the DSN name in the Microsoft Access connection. You also need to manually copy any third-party libraries available from the previous version.

Perform the following step to restore the DSN entries:

1. Uninstall the 32-bit Microsoft Access ODBC driver.
2. Remove the DSN entry for the 32-bit Microsoft Access ODBC driver from the Secure Agent machine.
3. Install the 64-bit Microsoft Access ODBC driver on the Secure Agent machine.
4. Create the required DSN with the same name as provided in the 32-bit driver from the previous version.
5. Restart the Secure Agent.

Microsoft Dynamics CRM Connector Post-Upgrade Tasks

After the Secure Agent versions earlier than 30.0 upgrades to version 33.0, perform the following steps for Microsoft Dynamics CRM Connector:

1. Move the `US_export_policy.jar` and `local_policy.jar` files, and cacerts files from `<SecureAgent_InstallDirectory>\jre2\lib\security` to `<SecureAgent_InstallDirectory>\jre\lib\security`.
2. Restart the Secure Agent.

Microsoft Dynamics Navision Connector Post-Upgrade Tasks

After you upgrade Microsoft Dynamics Navision Connector from a previous version, the Secure Agent does not retain the `Nav.ini` file, which was available in the following directories:

- `<Secure Agent installation directory>\main\tomcat\plugins\503800\`
- `<Secure Agent installation directory>\main\bin\rdtm\javalib\503800\`

The Data Synchronization tasks and mapping tasks fail after the upgrade. To ensure that the tasks do not fail, perform the following steps:

1. Create the following directory structures:
   - `<Secure Agent installation directory\apps\Data_Integration_Server\ext \deploy_to_main\tomcat\plugins\503800\`
   - `<Secure Agent installation directory>\apps\Data_Integration_Server\ext \deploy_to_main\bin\rdtm\javalib\503800\`
2. Copy the `Nav.ini` file from `<Secure Agent installation directory>\main2\bin\rdtm\javalib \503800\` to `<Secure Agent installation directory>\ apps\Data_Integration_Server\ext \deploy_to_main\bin\rdtm\javalib\503800\`
3. Copy the `Nav.ini` file from `<Secure Agent installation directory>\main2\tomcat\plugins \503800\` to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext \deploy_to_main\tomcat\plugins\503800\`
4. Restart the Secure Agent.

Microsoft SQL Server Connector Post-Upgrade Tasks

If the SSL certificates are available in the Secure Agent installation directory in versions earlier than 30.0, the secure connection fails after the upgrade. You must update the **Trust Store** property in the Microsoft SQL Server connection after the upgrade.

MySQL Connector Post-Upgrade Tasks

When the 32-bit Secure Agent upgrades to 64-bit in version 33.0, the timestamp value of the MySQL source in existing tasks modifies.

For example, if the MySQL source has a timestamp value of `"01/01/1970 05:30:01"`, you can view the following timestamp values before and after the upgrade:

- Before the upgrade, the timestamp value of the MySQL source reads as `"01/01/1970 00:00:01"` in tasks with the 32-bit Secure Agent.
- After the upgrade, the timestamp value of the MySQL source reads as `"01/01/1970 05:30:01"` in tasks with the 64-bit Secure Agent.

To retain the timestamp value in existing tasks after the upgrade, perform the following tasks:

1. In the Informatica Cloud home page, click **Configuration** > **Runtime Environments**.
2. Select the Secure Agent for which you want to add a custom flag to set the timestamp value, and click **Edit**.

3. In the **Custom Configuration Details** section, add a custom property with the following configurations:
   - **Service**: Data Integration Server
   - **Type**: DTM
   - **Name**: OdbcMySQLConnectionOptions
   - **Value**: 3;initstmt = set time_zone = '+00:00'
4. Click **OK**.

ODBC Connector Post-Upgrade Tasks

When the earlier versions of the Secure Agent upgrades to version 33.0 on Windows or Linux, you need to perform some manual steps. If you use third-party drivers with the generic ODBC connection, you need to perform upgrade tasks based on the Secure Agent version from which you upgrade both on Windows and Linux.

Upgrading from 32-Bit Secure Agent to 64-Bit Secure Agent Version 33.0 on Windows

When the 32-bit Secure Agent upgrades to 64-bit Secure Agent version 33.0 on Windows, you need to restore the DSN name in the upgraded version. You must avoid changing the DSN name in the ODBC connection. You also need to manually copy any third-party libraries available from the previous version.

1. Uninstall the 32-bit ODBC driver.
2. Remove the DSN entry for the 32-bit ODBC driver from the Secure Agent machine.
3. Install the 64-bit ODBC driver on the Secure Agent machine.
4. Create the required DSN with the same name as provided in the 32-bit driver from the previous version.
5. If you had copied any third-party driver files in the `<Secure Agent installation directory>/main` directory in the previous version, the Secure Agent backs up the content after the upgrade. Perform the following tasks for third-party files:
   a. Copy the backed-up third-party files from the following directory: `<Secure Agent installation directory>/main2 directory`.
   b. Paste the third-party files in the following directory: `<Secure Agent installation directory>/*`

Upgrading from 64-Bit Secure Agent Version Earlier than 30.0 to 64-Bit Secure Agent Version 33.0 on Windows

When the 64-bit Secure Agent with versions earlier than 30.0 upgrades to 64-bit Secure Agent version 33.0 on Windows, you must manually copy any third-party libraries available from the previous version and re-create the registry entries for the ODBC driver.

1. If there are third-party driver files in the `<Secure Agent installtion directory>/main/drivers` directory in the previous version, the Secure Agent backs up the content after the upgrade. Perform the following tasks for third-party files:
   a. Copy the backed-up third-party files from the following directory: `<Secure Agent installation directory>/main2/drivers` directory.
   b. Replace the files in the following directory: `<Secure Agent installation directory>/drivers/*`.
2. Re-create the registry entries for the ODBC driver and ensure that you set the correct path for the driver.

Upgrading from 64-Bit Secure Agent Version Later than 30.0 to 64-Bit Secure Agent Version 33.0 on Windows

When the 64-bit Secure Agent versions later than 30.0 upgrades to 64-bit Secure Agent version 33.0 on Windows, you must manually copy any third-party libraries available from the previous version.

1. Copy the third-party libraries from the following directory: `<Secure Agent installation directory>/drivers/odbc/datadirect/win64/*`
2. Replace the files in the following directory: `<Secure Agent installation directory>/drivers/odbc/datadirect/r27/win64/*`

Upgrading from 32-Bit Secure Agent to 64-Bit Secure Agent Version 33.0 on Linux

When the 32-bit Secure Agent upgrades to 64-bit Secure Agent version 33.0, you need to restore the DSN name in the upgraded version. You must avoid changing the DSN name in the ODBC connection. You also need to manually copy any third-party libraries available from the previous version.

1. Uninstall the 32-bit ODBC driver.
2. Remove the DSN entry for the 32-bit ODBC driver on the Secure Agent machine.
3. Install the 64-bit ODBC driver on the Secure Agent machine.
4. Create the required DSN with the same name as provided in the 32-bit driver from the previous version.
5. Ensure that you set the ODBCINI environment variable on the Linux machine to the location of the `odbc.ini` file that contains the DSN entry.
6. If you had copied any third-party driver files in the `<Secure Agent installation directory>/main` directory in the previous version, the Secure Agent backs up the content after the upgrade. Perform the following tasks:
   a. Copy the backed-up third-party files from the following directory: `<Secure Agent installation directory>/main2` directory.

b. Paste the third-party files in the following directory: `<Secure Agent installation directory>/*`

7. If you had configured custom properties in the `[ODBC]` section in the `<Secure Agent installation directory>/odbcinst.ini` file in the previous version, the Secure Agent backs up the content in the `[ODBC - R26]` section after the upgrade. As the Secure Agent reads only the `[ODBC]` section, perform the following tasks in the `odbcinst.ini` file:
   a. Copy the custom properties from the `[ODBC-R26]` section.
   b. Paste the content into the `[ODBC]` section.

Upgrading from 64-Bit Secure Agent Version Earlier than 30.0 to 64-Bit Secure Agent Version 33.0 on Linux

When the 64-bit Secure Agent with versions earlier than 30.0 upgrades to 64-bit Secure Agent version 33.0 on Linux, you must manually copy any third-party libraries available from the previous version and re-create the DSN entries for the ODBC driver.

1. If there are any third-party driver files in the `<Secure Agent installation directory>/main/drivers` directory in the previous version, the Secure Agent backs up the content after the upgrade. Perform the following tasks:
   a. Copy the backed-up third-party files from the following directory: `<Secure Agent installation directory>/main2/drivers`.
   b. Paste the third-party files in the following directory: `<Secure Agent installation directory>/drivers/*`
2. Re-create the DSN entries for the ODBC driver in the `odbc.ini` file.
3. Ensure that you set the correct path for the ODBC drivers.
4. Ensure that you set the ODBCINI environment variable on the Linux machine to the location of the `odbc.ini` file that contains the DSN entry.
5. If you had configured custom properties in the `[ODBC]` section in the `<Secure Agent installation directory>/odbcinst.ini` file in the previous version, the Secure Agent backs up the content in the `[ODBC - R26]` section after the upgrade. As the Secure Agent reads only the `[ODBC]` section, perform the following tasks in the `odbcinst.ini` file:
   a. Copy the custom properties from the `[ODBC-R26]` section.
   b. Paste the content into the `[ODBC]` section.

Upgrading from 64-Bit Secure Agent Version Later than 30.0 to 64-Bit Secure Agent Version 33.0 on Linux

When the 64-bit Secure Agent versions later than 30.0 upgrades to 64-bit Secure Agent version 33.0 on Linux, you must manually copy any third-party libraries available from the previous version.

1. Copy the third-party libraries from the following directory: `<Secure Agent installation directory>/drivers/odbc/datadirect/linux/*`
2. Replace the files in the following directory: `<Secure Agent installation directory>/drivers/odbc/datadirect/r27/linux/*`

3. If you had configured custom properties in the `[ODBC]` section in the `<Secure Agent installation directory>/odbcinst.ini` file in the previous version, the Secure Agent backs up the content in the `[ODBC - R26]` section after the upgrade. As the Secure Agent reads only the `[ODBC]` section, perform the following tasks in the `odbcinst.ini` file:
   a. Copy the custom properties from the `[ODBC-R26]` section.
   b. Paste the content into the `[ODBC]` section.

Oracle EBS Connector Post-Upgrade Tasks

If you want to modify the `EBSWSDLConfig.ini` file, perform the following steps:

1. Go to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\reserved\userfiles\EBSMidStream\`

   Note: If the `\reserved\userfiles\EBSMidStream\` directory does not already exist, create the directory.

   Note: The folder name is case sensitive on Linux.
2. Modify the `EBSWSDLConfig.ini` file.
3. Restart the Secure Agent.

Post-Upgrade Tasks for Lookups Configured in Amazon Redshift and Microsoft Azure SQL Data Warehouse Connectors

Earlier versions of Amazon Redshift Connector and Microsoft Azure SQL Data Warehouse Connector do not support advanced options for lookup in Data Synchronization tasks. You could, however, perform a lookup through the JDBC query.

After the upgrade, you can configure a lookup for Amazon Redshift and Microsoft Azure SQL Data Warehouse objects in the Data Synchronization task. You must specify the mandatory properties in the **Field Lookup** dialog box to save and run tasks successfully.

To use existing tasks from previous versions that were configured for lookup through the JDBC query, perform the following tasks after the upgrade:

- If you edit existing tasks, you must specify the mandatory properties required for lookup to save and run the task successfully.
- If you do not edit existing tasks, you can continue to run the tasks successfully.

ReST API Connector Post-Upgrade Tasks

If you use proxy support, perform the following steps:

1. Copy the `ProxySettings.ini` file from `<Secure Agent installation directory>\main2\tomcat\plugins\<plugin ID>\` to `<Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\Rest\`

   Note: If the `deploy_to_main\bin\rdtm-extra\Rest\` directory does not already exist, create the directory.

   Note: The folder name is case sensitive on Linux.
2. Restart the Secure Agent.

SAP Connector Post-Upgrade Tasks

Upgrading the Secure Agent from a 32-bit operating system to a 64-bit operating system

If you upgrade the Secure Agent from a 32-bit operating system to a 64-bit operating system, you must complete the following post-upgrade tasks for SAP Connector:

1. Download the appropriate 64-bit libraries based on the functionality you use:

Functionality	Libraries to be downloaded
SAP Table Reader, SAP Table Writer, SAP BW Reader, SAP RFCs/BAPI	SAP JCo libraries
SAP Table Writer, SAP RFCs/BAPI, SAP IDocs	SAP NetWeaver RFC SDK 7.20 libraries

   Note: To import IDoc metadata by using the SAP Metadata utility, you must download the 32-bit SAP JCo libraries. For more information, see the *Informatica Cloud SAP Connector Guide*.
2. Copy the 64-bit libraries to the appropriate directories:

Libraries	Directory where the libraries must be copied
SAP JCo libraries	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap`
SAP NetWeaver RFC SDK 7.20 libraries	`<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm` **Note:** You must also copy the `sapnwrfc.ini` file to this directory.

3. Restart the Secure Agent.

For more information, see the *Informatica Cloud SAP Connector Guide*.

Upgrading the Secure Agent from Version 30.0 or Earlier

If you upgrade the Secure Agent from version 30.0 or earlier, you do not need to perform any post-upgrade task.

If you had configured the SAP JCo libraries earlier, the Secure Agent copies the SAP JCo libraries to the following directory:

<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\tpl\sap

If you had configured the SAP NetWeaver RFC SDK 7.20 libraries and the sapnwrfc.ini file earlier, the Secure Agent copies the libraries and the sapnwrfc.ini file to the following directory:

<Informatica Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm\

For more information, see the *Informatica Cloud SAP Connector Guide*.

WebServices V2 Connector Post-Upgrade Tasks

If you use proxy support, perform the following steps:

1. Copy the ProxySettings.ini file from <Secure Agent installation directory>\main2\tomcat\plugins\<plugin ID>\ to <Secure Agent installation directory>\apps\Data_Integration_Server\ext\deploy_to_main\bin\rdtm-extra\Webservices V2\

   Note: If the deploy_to_main\bin\rdtm-extra\Webservices V2\ directory does not already exist, create the directory.

   Note: The folder name is case sensitive on Linux.
2. Restart the Secure Agent.

Workday V2 Connector Post-Upgrade Tasks

If you had set the WorkdayBatchSize property in the pmrdtm.cfg file located at the <Secure Agent installation directory>\main\bin\rdtm directory in versions earlier than 30.0, you must set the batch size in the advanced source properties of Workday V2 Connector after the upgrade.

Fixed Limitations in Prior Releases

You can find information on fixed limitations in prior releases of Informatica Cloud on the Informatica Network.

Refer to these topics for details:

- Fall 2016
- Summer 2016
- Winter 2016

Known Limitations in Spring 2017

The following table describes general Informatica Cloud known limitations in this release:

CR	Description
ICS-9410	When you specify query parameters in the Query Params field to generate a Swagger file, the tool tip and the validation error message show an incorrect format of the query parameter. Workaround: Specify the query parameter in the following format: `{"name1":"value1"}`
ICS-9385	The Web Services transformation does not support SOAP 1.2. Workaround: Use SOAP 1.1 for Web Services transformations.
ICS-8850 ICS-8859 ICS-8860 ICS-8881 ICS-8887	SQL Server metadata with column names that include spaces is not supported.
ICS-7988	When you partition a mapping that uses an ODBC connection to connect to an IBM DB2 database, you cannot use columns of Date data type for key range values.
ICS-7742	When you partition a mapping, you cannot include subseconds in date/time key range values.
ICS-7332	When you create a task with a flat file, Salesforce, or SAP source and use a parameter file, the task fails to run if you assign a Unicode value to the parameter. This occurs for previously created tasks and if you copy or migrate an existing task. It no longer occurs when you create a new task. Workaround: Re-create the task.
ICS-5172 (formerly INFA 279686)	Data Synchronization tasks configured to run in real time upon arrival of outbound messages run even when Run permission is revoked.
ICS-5170 (formerly INFA 293502)	In Data Synchronization tasks with database targets, the Update Target property is cleared if you click the Refresh Fields option on the Field Mappings page of the Data Synchronization wizard.
ICS-5169 (formerly INFA 361543)	You can delete a connection that is used in a mapping. You must not be able to delete connections that are used in Data Synchronization, Data Replication, Mapping Configuration or any other tasks.
ICS-5166 (formerly INFA 391533)	Mapping Configuration tasks that pass binary data through a Normalizer transformation fail with data type conversion errors. The Normalizer transformation does not support binary data types.
ICS-5159 (formerly INFA 281843)	Contact Validation tasks that validate postal addresses sometimes fail due to memory allocation, internal server, or transformation errors. Workarounds: If the task fails with the following error, use the Buffer Block Size advanced option to adjust the buffer block size: `FATAL ERROR : Failed to allocate memory. Out of virtual memory.` For other errors, try running the task again. If the problem persists, contact Informatica Global Customer Support.
ICS-5158 (formerly INFA 282057)	The Street With Number advanced option is ignored in Contact Validation tasks. The building number is always included with the street name at this time.

CR	Description
ICS-5145	The Japanese Secure Agent fails to uninstall on an English operating system. Workaround: Navigate to the `<Secure Agent installation directory>/Uninstall_Informatica Cloud Secure Agent` directory and rename the following files: - Rename Informatica Cloud Secure Agent をアンインストール.exe to Informatica Cloud Secure Agent.exe. - Rename Informatica Cloud Secure Agent をアンインストール.lax to Informatica Cloud Secure Agent.lax. After you rename the files, redo the steps to uninstall the Secure Agent.
ICS-4819	When you run a Data Synchronization task and perform a cached lookup on an SAP HANA source that contains a quoted identifier, the task fails with an error. Workaround: Use a command task with uncached lookup.
ICS-4791	When you use the Japanese version of Informatica Cloud, errors generated from scheduled tasks appear in English.
ICS-4790	When you switch between English and Japanese in your browser, the activity log error messages are not translated. The messages show in the language originally output when the task was completed.
ICS-4655	An error occurs when you export PowerCenter workflows with Command tasks from PowerCenter version 9.1 HotFix 5 and above into Informatica Cloud. Workaround: Remove the EXECORDER attributes manually from the XML file or export the workflow from PowerCenter version 9.1 HotFix 4 or below.
ICS-4429	When you use the Japanese version of Informatica Cloud, error messages related to expressions in unconnected lookup functions appear in English instead of Japanese.
ICS-4081	When you use the Japanese version of Informatica Cloud, Java exception error messages appear in English.
ICS-3975	When you run Data Synchronization tasks, the task hangs indefinitely and does not display an error message in the Activity Monitor. Workaround: Commit the session in the database and the task will complete.
ICS-3306	To reconfigure a business service operation for a Web Services transformation, you need to delete it from the business service and select it again. Workaround: When you define a business service for a Web Services transformation, configure all choice elements or derived types before you close the **Configure Operation** window.
ICS-2869	You can use PowerCenter workflows with flat file, database, web service, NetSuite, Salesforce, Oracle On Demand, and Microsoft Dynamics connections in PowerCenter tasks. All other connection types are not supported.
ICS-1491	If a mapping uses more than one Web Services transformation, you cannot pass the new endpoint URL returned from the first Web Service transformation to any downstream Web Service transformations. Workaround: Create another WSConsumer connection using the URL returned from the first Web Service transformation and define a business service that uses the connection. Use the new business service for the downstream Web Services transformation.
ICS-1478	In a Web Services transformation, you cannot map a source field to more than one request field.

CR	Description
ICS-1320	In a Web Services transformation, if you change the data type of an incoming field after you have mapped fields, you have to clear the mapping for the field and map it again. Workaround: Change the data type of an incoming field before you map the field.
ICS-385	In the Mapping Designer, you can edit advanced relationships in View mode.
DMT-76	In environments with a non-English locale, the names of masking techniques appear in English on the **Masking Rules** tab of the Data Masking transformation Properties panel.
DMT-66	A mapping that includes the SIN masking technique fails when you disable the property Start Digit. Workaround: Enable the property Start Digit and enter a start digit value when you use the SIN masking technique.
DMT-54	When you search for and add fields from the **Add Fields** window of the Data Masking transformation properties, the transformation clears fields that you selected. Workaround: Scroll down if needed and select required fields instead of searching for fields.
CTDM-401	An inplace masking task fails when you apply a custom substitution masking rule with a lookup condition. Workaround: Assign a nullification masking rule to the field that you configured as the lookup input port in the custom substitution masking rule.
CTDM-319	You cannot configure expressions for additional master-detail type relationship fields in the target connection. Workaround: Hide or delete the master-detail type relationship fields in the Salesforce target.
CTDM-255	The Data Masking task fails if the task contains objects with self-reference relationships and if the task uses the lookup based reconciliation strategy. Workaround: Use the external ID reconciliation strategy, or remove self-reference relationships from the task.
CTDM-209	When you run an inplace masking that contains self-reference relationships, the Data Masking task fails. Workaround: Remove the self-reference relationships from the source and run the task again.
CTDM-208	The Data Masking task fails when the task contains a single object with self-reference relationships. Workaround: Add more objects in the source, or remove the self-reference relationships from the source. Run the task again.

Third-Party Limitations in Spring 2017

The following table describes third-party known limitations:

Third Party CR	Description
CTDM-279	Due to a Salesforce limitation, the upsert operation in a Data Masking task fails when there are objects with fields that you cannot update. Workaround: Ignore the error rows and warnings that you view in the task activity logs.
CTDM-402	Due to a Salesforce limitation, the Data Masking task fails when the SOQL exceeds 20,000 characters. Workaround: Contact Salesforce to increase the SOQL character limit for the account.
CTDM-2	Due to a Salesforce limitation, the Data Masking task with the upsert operation fails when the external ID or custom field for lookup does not exist or cannot be created in the targets.