Informatica® Cloud
Version Spring 2017

What's New

Informatica Cloud What's New

Version Spring 2017
September 2017

Publication Date: 2017-09-05

Table of Contents

Preface

What's New describes Informatica Cloud's new features and enhancements, behavior changes between versions, and any tasks you might need to perform before or after an upgrade.

Note: In prior releases, this document was called the *Release Guide*.

CHAPTER 1

Before You Upgrade

This chapter includes the following topics:

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.

CHAPTER 2

After You Upgrade

This chapter includes the following topics:

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.

CHAPTER 3

New Features and Enhancements

This chapter includes the following topics:

Connectors - Enhanced

This section describes enhanced connectors for the Spring 2017 release.

Amazon Aurora

The Spring 2017 release includes the following enhancements for Amazon Aurora Connector:

- On Windows 64-bit and Linux 64-bit operating systems, Amazon Aurora drivers are upgraded to the latest versions.

Amazon S3

The Spring 2017 release includes the following enhancements for Amazon S3 Connector:

- On Windows 64-bit and Linux 64-bit operating systems, Aurora, MySQL, Microsoft SQL Server, and Oracle drivers are upgraded to the latest versions.
- For client-side and server-side encryption, you can configure the customer master key ID generated by AWS Key Management Service (AWS KMS) in the connection.
- You can override and parameterize the Amazon S3 bucket name in the advanced target properties.
- In addition to the existing regions, you can also read data from or write data to the Amazon S3 buckets in the following regions:
  - Asia Pacific (Mumbai)
  - Canada (Central)
  - China (Bejing)

- US East (Ohio)

- When you write data to the Amazon S3 buckets, you can compress the data in GZIP format.
- When you run a task in Secure Agent runtime environment, you can specify a directory path that is available on the corresponding Secure Agent machine in the runtime environment.
- You can write multiple files to Amazon S3 target from a single source. You can configure the **Distribution Column** options in the advanced target properties.
- You can configure the multipart upload option to upload a single object as a set of independent parts. TransferManager API uploads the multiple parts of a single object to Amazon S3. After uploading, Amazon S3 assembles the parts and creates the whole object. TransferManager API uses the multipart uploads option to achieve performance and increase throughput when the content size of the data is large and the bandwidth is high.
- You can read multiple files from Amazon S3 and write data to a target.
- When you create a mapping task to write data to Amazon S3 targets, you can configure partitions to improve performance. You can configure the **Merge Partition Files** option in the advanced target properties.

Amazon Redshift

The Spring 2017 release includes the following enhancements for Amazon Redshift Connector:

- For server-side encryption, you can configure the customer master key ID generated by AWS Key Management Service (AWS KMS) in the connection.
- In addition to the existing regions, you can also read data from or write data to the following regions:
  - Asia Pacific (Mumbai)
  - Canada (Central)
  - China (Bejing)
  - US East (Ohio)
- You can configure the multipart upload option to upload a single object as a set of independent parts. TransferManager API uploads the multiple parts of a single object to Amazon S3. After uploading, Amazon S3 assembles the parts and creates the whole object. TransferManager API uses the multipart uploads option to achieve performance and increase throughput when the content size of the data is large and the bandwidth is high.
- In addition to the existing recovery options in the vacuum table, you can select the **reindex** option to analyze the distribution of the values in an interleaved sort key column.

Coupa

The Spring 2017 release includes the following enhancements for Coupa Connector:

- You can specify the Error Payload Directory to get the details of the failed payload in Coupa.
- You can perform insert or update operation on the following objects in Coupa: AccountValidationRules, Addresses, BudgetLines, CatalogItems, ContentGroups, Contracts, Currencies, ExpenseLines, ExpenseReports, InventoryTransactions, OrderPads

  PurchaseOrders, Requisitions

File Processor

The Spring 2017 release includes the following enhancements for File Processor Connector:

- You can use the CompressAllFiles filter field to zip files to a single zip or .7z file.

- You can perform delete operation on a File Processor target.
  For more information, see the *Informatica Cloud File Processor Connector User Guide*.

Google BigQuery

The Spring 2017 release includes the following enhancements for Google BigQuery Connector:

- You can create Google BigQuery target tables based on the columns present in the Google BigQuery source.
- When you write data to a Google BigQuery target, you can configure the create disposition property to define whether the Secure Agent must create the target table if it does not exist.
- You can update data in a Google BigQuery target.
- You can delete data from a Google BigQuery target.
- You can specify the following data formats for the Google BigQuery target staging file:
  - JSON (Newline Delimited)
  - CSV
- You can configure the following advanced writer properties:
  - Number of threads for uploading staging file
  - Local storage file directory
  - Allow quoted newlines
  - Field delimiter
  - Allow jagged rows
- You can use a Google BigQuery object as a source in Data Synchronization tasks, Mapping Configuration tasks, and mappings.
- You can use staging mode to read data. In staging mode, the Secure Agent first downloads BigQuery target data in Google Cloud Storage and then reads the data from Google Cloud Storage.
- You can configure the following properties when you use staging mode to read data from a Google BigQuery source:
  - Number of threads for downloading staging files
  - Local stage file directory
  - Staging file name
  - Enable staging file compression

Google Cloud Storage

The Spring 2017 release includes the following enhancements for Google Cloud Storage Connector:

- You can use Google Cloud Storage Connector to read data from Google Cloud Storage. You can use Google Cloud Storage objects as sources in Data Synchronization tasks, Mapping Configuration tasks, and mappings. You can use Google Cloud Storage Connector to read files that contain string and binary data.
- You can specify the number of threads that the Secure Agent must create to write data to the Google Cloud Storage target. You can configure multi-threading to write data to the Google Cloud Storage target in parallel and improve the performance.
- You can specify whether the Secure Agent must retain the order of text data when it writes to the Google Cloud Storage target. You can retain the order of text data if you configure more than one thread to write text data to a Google Cloud Storage target.

JDBC

When you create a new JDBC connection, you can specify the JDBC driver class name.

LDAP

You can use an LDAP object as a lookup in tasks.

Microsoft Azure Blob Storage Connector

The Spring 2017 release includes the following enhancements for Microsoft Azure Blob Storage Connector:

- When you read data from or write data to Microsoft Azure Blob Storage, you can use the Blob Name Override property to override the default Blob name.
- When you read data from or write data to Microsoft Azure Blob Storage, you can use the Blob Container Override property to override the default container name.
- When you read data from Microsoft Azure Blob Storage and use the header in the first row of blob property, the Secure Agent reads the first row of the blob as a header. When you write data to Microsoft Azure Blob Storage and use the header in the first row of blob property, the Secure Agent writes the first row of blob as a header.
- When you write data to Microsoft Azure Blob Storage, you can use the Compress newly created Blob property to compress the newly created blob when set to True.

Microsoft Azure DocumentDB Connector

You can use the Informatica Cloud Hosted Agent (Hosted Agent) as a runtime environment for a Microsoft Azure DocumentDB connection.

Microsoft Azure SQL Data Warehouse Connector

You can use the Quote Character advanced target property to skip the specified character when you read data from or write data to Microsoft Azure SQL Data Warehouse.

Microsoft Dynamics AX V3

The Spring 2017 release includes the following enhancements for Microsoft Dynamics AX V3 Connector:

- You can set the batch size when you perform a create, update, or delete operation. Default batch size is 50.
- You can use Microsoft Dynamics AX V3 Connector to perform full update operation.
- You can use readAll operation to read all the records from Microsoft Dynamics AX.
- You can use Microsoft Dynamics AX V3 Connector to configure midstream transformation.
- When you read data from or write data to Microsoft Dynamics AX, you can use the following advanced properties:
  - Batch Size. You can write data to the target in batches.
  - Company Name. You can specify the company name.
  - Language. You can localize the data you read from or write to Microsoft Dynamics AX.

Microsoft Dynamics CRM

You can use Microsoft Dynamics CRM Connector to connect to Dynamics 365 Sales.

Microsoft SQL Server

On Windows 64-bit and Linux 64-bit operating systems, Microsoft SQL Server drivers are upgraded to the latest versions.

MySQL

The Spring 2017 release includes the following enhancements for MySQL Connector:

- When you create a Mapping Configuration task to read data from MySQL, you can configure key range partitioning to improve performance.
- On Windows 64-bit and Linux 64-bit operating systems, MySQL drivers are upgraded to the latest versions.

NetSuite

You can use NetSuite Connector to read and write custom segment data from standard objects and custom objects. You can use NetSuite Connector to read custom segment data from saved searches.

ODBC

The Spring 2017 release includes the following enhancements for ODBC Connector:

- You can use the ODBC connection to connect to the Teradata database. Specify Other subtype in an ODBC connection to connect to Teradata sources and targets.
- You can enable full or source pushdown optimization for Teradata sources and targets. Specify Other subtype in the ODBC connection properties to enable pushdown optimization when you read data from or write data to Teradata databases. The Secure Agent pushes the supported functions to Teradata sources and targets based on the pushdown optimization session property name you select.
- When you use the ODBC connection to connect to MongoDB, you must use the Simba ODBC driver version 2.4.1.1001 on Windows or Linux to connect to MongoDB. You cannot upgrade Simba ODBC drivers from previous versions.
- You can use the ODBC connection to read and write data from IBM DashDB.
- When you create a new ODBC connection on Linux platform, you can select a driver manager for the Linux Secure Agent. Select one of the following driver managers:

  - Data Direct

  - unixODBC2.3.0

  - unixODBC2.3.4

- You can configure Microsoft Active Directory as the authentication server to connect to Microsoft Azure SQL Data Warehouse through an ODBC connection.
  For more information, see the Informatica Cloud ODBC Connector User Guide.

Oracle

The Spring 2017 release includes the following enhancements for Oracle Connector:

- You can use Oracle bulk API to insert data in bulk mode. When you create a Mapping Configuration task, you can use the Oracle bulk API to perform insert operation.
- On Windows 64-bit and Linux 64-bit operating systems, Oracle drivers are upgraded to the latest versions.

REST V2

The Spring 2017 release includes the following enhancements for REST V2 Connector:

- You can configure the extended JSON mime type, JSON subtype, and JSON custom type for the API response.
- You can create Swagger for an REST API from Informatica Cloud.
- Fault processing is supported for midstream. The fault group contains the RequestXML, ErrorCode, and ErrorMessage. To map the fault group for the business services created in the previous version of connector, recreate the Web Services transformation and map all the required fields..

- You can upload a file to a REST endpoint URL.

Salesforce

The Spring 2017 release includes the following enhancements for Salesforce Connector:

- You can create a Salesforce connection with OAuth authentication.
- You can use an SOQL custom query as a source type in the Mapping Designer when Salesforce Bulk API is enabled.
- Salesforce Connector supports version 39 of Salesforce API.

Satmetrix

Satmetrix connections support Unicode (UTF-8) data. You can read or write Unicode data using a Satmetrix connection.

ServiceNow

The Spring 2017 release includes the following enhancements for ServiceNow Connector:

- You can use the Informatica Cloud Hosted Agent (Hosted Agent) as a runtime environment for a ServiceNow connection.
- ServiceNow Connector uses REST API in SynQ READ operation to fetch data from ServiceNow.

Snowflake

The database override, schema override, and table override properties appear in the Advanced Target Properties section of a Data Synchronization task.

Note: Do not specify values for database override, schema override, or table override in a Data Synchronization task. You can specify the values at PowerCenter session.

You can download the mapping XML for a Data Synchronization task and import the file to the PowerCenter repository. You can specify the values for the database override, schema override, and table override properties at PowerCenter session runtime.

Workday V2

The Spring 2017 release includes the following enhancements for Workday V2 Connector:

Workday Connector supports input streaming which allows you to read large web service responses from Workday even when you do not specify a cache size.

Zuora AQUA

The Spring 2017 release includes the following enhancements for Zuora AQUA Connector:

- You can run a task to download data from the multiple Zuora source objects at once.
- You can define multiple ZOQL queries in the advanced data filters section to download the data from multiple or related source objects.

Connectors - New

This section describes new connectors for the Spring 2017 release.

Microsoft Azure SQL Data Warehouse V2

Microsoft Azure SQL Data Warehouse V2 Connector enables you to read data from or write data to Microsoft Azure SQL Data Warehouse. You can insert or upsert data to or delete data from a Microsoft Azure SQL Data Warehouse target.

Teradata

You can use Teradata Connector to connect to Teradata sources and targets from Informatica Cloud. You can configure a Teradata connection in mappings and Mapping Configuration tasks to connect to Teradata. Teradata Connector uses the Parallel Transporter API, a load and unload utility, to extract, transform, and load data from multiple sources in parallel. You can specify the load, update, or stream system operator to write data to Teradata.

Shared Secure Agent Groups

If you are the administrator of a parent organization, you can share a Secure Agent group with all sub-organizations.

Share a Secure Agent group to optimize the use of Secure Agent resources across sub-organizations. For example, you can add multiple Secure Agents to a Secure Agent group and share the Secure Agent group with the sub-organizations. All sub-organizations can then run tasks on the Secure Agents within the group.

REST API

The Spring 2017 release includes the following enhancements to the REST API:

Mapping Image Request Using mapping Resource

Effective in the Spring 2017 release (September update), you can request an image of a deployed or undeployed mapping using the mapping resource.

isShared Attribute for runtimeEnvironment Resource

The runtimeEnvironment resource now includes the isShared attribute which indicates whether the Secure Agent group is shared.

Secure Agent Audit Filters

You can filter the Secure Agent audit information on the **Agent Audit** page.

To filter the audit information, use the following filters:

- Component name. Select the services for which you want to view the audit information. You can also view the system audit information.
- Type. Filter the information by message type such as Fatal, Error, or Debug.
- To and From dates. Display messages for a specific date range.

Data Masking Task

You can use a passive mapplet that requires an extra connection to a relational database or a flat file.

Before you add the mapplet, you must add the connection. When you configure the mapplet, you must select the dictionary and lookup connections.

If the dictionary information for the mapplet is in a flat file, the flat file must be present in the following location:

```
<Secure Agent installation directory>\apps\Data_Integration_Server\data
```

If the lookup connection for the mapplet is a flat file connection, the connection name must be the name of the flat file.

Structure Parser Transformation

Effective in the Spring 2017 release, Intelligent Structure Discovery has an additional Table tab in which you can edit the model table elements. You can rename fields, remove columns, or exclude columns. Excel tables are shown in name-value pairs.

Effective in the Spring 2017, the Structure Parser designates a separate output group for each data group that has been identified in the Intelligent Structure Discovery model. You map each output group to a different Target transformation for further processing.

Effective in the Spring 2017 (August update), the Structure Parser provides an additional output group for data that was not identified and included in the Intelligent Structure Discovery model. The unidentified data group can be mapped to a Target transformation and processed for further analysis.

For more information, see *Transformations*.

Application Integration

This section describes some of the new features and enhancements added for the December, January, February, March, and April Cloud Application Integration (the Informatica Cloud Real Time service) releases.

For additional details, see the *Release Notes* published with the monthly releases of Cloud Application Integration.

Secure Agent Version 33

Cloud Application Integration customers benefit from the capabilities offered by Secure Agent version 33.

The Process Server service is a new engine of the Secure Agent platform that executes independently to help overall resilience. Process Server executes Cloud Application Integration processes deployed to the Secure Agent.

Cloud Application Integration customers gain the following additional benefits from the latest Secure Agent version:

- **PostgreSQL Replaces H2**: The new underlying database, PostgreSQL, can handle a larger amount of data than H2, the earlier underlying database. You will also see performance improvements.

- **HTTPS Listener Support**: You can run processes published to a Secure Agent from within the enterprise through HTTPS/REST or HTTPS/SOAP calls in addition to JMS and AMQP queues and topics.
- **Agent Group Awareness**: Use the Agent Group feature to logically group agent-based Process Servers and distribute the load across each member of the group. You can use this feature to scale.
- **Agent Clustering**: You can cluster two or more Agent Group members into a single logical Process Server instance. You gain many advantages with the Agent Clustering feature. For example, if a node failure occurs, a process instance failover kicks in to recover the instance.

New API Management Capabilities

You can use the API management features delivered with Informatica Cloud Real Time Advanced and Informatica Cloud Premium editions.

Use the Informatica Cloud Real Time service to create REST/XML, JSON, or SOAP/WSDL composite or OData data service APIs. You can expose the managed APIs you created to partners, customers, and internal consumers through the Informatica Cloud API Gateway. Together with the API Manager, you can use the API gateway to control and secure access to the APIs you expose.

New Connectors

Workday and OData connectors are available to customers that license these capabilities.

Service Connector Timings

You can see the **HTTP Execution Time**, the **HTTP Response Parsing Time**, and the **Redirect Count** of a service connector on the Test Results tab of the service connector UI.

Process Tracing Level 'Terse' maps to Logging Level 'Fault'

The Terse tracing level maps to the Fault logging level. At the Fault logging level, Process Server logs only fault information, which decreases the size of the log file and improves processing speed. To improve processing speed, perform no logging or minimum logging. Informatica recommends that you use the None or Terse logging levels.

Bulk Retry on the Process Console

You can retry multiple faulting suspended processes on the **Active Processes** page. Earlier, you could only retry a single process at a time.

Scheduled Deletion of Server Log Data

You can specify a **Server Log Retention** period. Process Server deletes Server Log data that is older than the time you specify. For more information, see the *Scheduled Maintenance* topic in the *Administer* section of the Cloud Application Integration online help. Previously, you could not schedule Server Log data deletion. You had to manually delete Server Log data when needed.

Limit on Attachments Size

Informatica enforces a maximum attachment size for API requests made on the Cloud Server. Previously, Informatica enforced a maximum message payload size of 5 MB. Now, if you have attachments to a message, the maximum total size of attachments is also 5 MB. This only affects processes that you deploy to the Cloud Server. If you deploy processes to the Secure Agent, the default size remains 5 MB for both payload and attachments. There is no upper size limit.

Swagger 2.0 Specification for Processes

You can get the Swagger 2.0 JSON specification of the API exposed by a process that you create in Informatica Process Designer. Service consumers can now use Swagger 2.0, JSON Schema, and WSDL interface documents to introspect endpoints for processes developed in Process Designer.

Max Wait Value for Service Call Step

When you use the Service Call step to run Informatica Cloud applications, you must enter a cannot enter a Max Wait value greater than seven days.

Improved XQuery Expression Syntax Support

The following enhancements support XQuery expression syntax:

- Improved handling of spaces, tabs, and new lines.
- Removal of limits on the complexity of supported XQuery expressions.
- Comments and strings can now include temporary fields.
- Improved field references processing.
- Improved local and process variable support.
- Improved expression predicate handling.
- Corrected array handling.

CHAPTER 4

Changed Behavior

This chapter includes the following topics:

Connectors

This section describes the changed behavior for connectors in the Spring 2017 release.

Google BigQuery Connector

Effective in the Spring 2017 release, you cannot override the Google BigQuery source table name in a Data Synchronization task and mapping. The **Source Table Name** property has been removed from the Data Synchronization task and mapping advanced properties.

Previously, in a Data Synchronization task and mapping, you were able to override the Google BigQuery source table name that you specified in the **Source** transformation.

REST V2 Connector

Effective in the Spring 2017 release, the following changes affect mappings that use REST V2 Connector:

Single "body" string for requests containing JSON values

If JSON data value is passed to a REST request as a single string value, the double quotes inside the JSON value are now escaped. For example, using the value "{"emp":"abc","empid":"em01"}":

- Prior to the Spring 2017 release, the request is constructed as {"emp":"abc","empid":"em01"}
- Beginning with the Spring 2017 release, the request is constructed as {\"emp\":\"abc\",\"empid\":\"em01\"}

It is recommended that you expand the request body definition using Swagger and map individual fields. Informatica Global Support can help you generate the Swagger specification.

Single element array values

Single values passed for properties defined as arrays are included in the request as arrays.

Prior to the Spring 2017 release, these values were included as individual values.

Numeric values

Numeric values for text properties are included as text values.

Prior to the Spring 2017 release, numeric values for text properties were automatically included in the request as numeric.

Fields with empty values

Fields with empty values are included in the request only if the following Secure Agent configuration property is set:

`-DRestRequestMode=Strict`

Earlier, fields with empty values were included in the request even when the fields were not mapped.

If you do not set the `-DRestRequestMode=Strict` property, unmapped fields are not included in the request by default.

To set the `-DRestRequestMode=Strict` property, perform the following steps:

1. Click **Configure** > **Runtime Environments**.
2. Select the Secure Agent that you use for REST V2 connections.
3. Click **Edit** on the **View Secure Agents** page.
4. Select the Data Integration Server service.
5. Select the DTM type.
6. Add the following property to an empty JVM Option: `-DRestRequestMode=Strict`
7. Click **OK** to save your changes.

String literal values as "null"

If a property has a value of "null", it is treated as a null/empty value.

Prior to the Spring 2017 release, if a property had a value of "null", "null" was passed as a text value.

If your configuration is not affected by these behavior changes, no change is required in your mappings. However, if your mappings are affected by any of these changes, you can set the `-DPromoteToArray=FALSE` flag, or you can modify your mappings to work with the new behavior. From a long-term perspective, it is recommended that you change your mappings as soon as possible. The default value for `-DPromoteToArray` is `true`. The `-DRestRequestMode=Strict` property works only if you set `-DPromoteToArray=TRUE`.

To set the `-DPromoteToArray=FALSE` property so that Informatica Cloud treats the above situations the way it did in prior releases, perform the following steps:

1. Click **Configure** > **Runtime Environments**.
2. Select the Secure Agent that you use for REST V2 connections.
3. Click **Edit** on the **View Secure Agents** page.
4. Select the Data Integration Server service.
5. Select the DTM type.
6. Add the `-DPromoteToArray=FALSE` property to an empty JVM Option.
7. Click **OK** to save your changes.

For more information, contact Informatica Global Customer Support.

SAP Connector

Effective in the Spring 2017 release, SAP Connector contains the following changes:

- You must copy 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`

  Previously, if you were using a Secure Agent version earlier than 30, you copied the SAP JCo libraries to the following directory:

  `<Informatica Secure Agent installation directory>\main\bin\rdtm-extra\tpl\sap`
- You must copy the SAP NetWeaver RFC SDK 7.20 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`

  Previously, if you were using a Secure Agent version earlier than 30, you copied the SAP NetWeaver RFC SDK 7.20 libraries and the `sapnwrfc.ini` file to the following directory:

  `<Informatica Secure Agent installation directory>\main\bin\rdtm`

Data Masking Task

Effective in the Spring 2017 release, when you perform an upsert operation, you can select a unique field or an idlookup field for objects on which you cannot create an external ID.

Previously, you could use only external IDs to perform an upsert operation.

Mappings

Effective in the Spring 2017 release, when you select the Data Driven option for a relational target in a mapping, the update strategy expression is optional.

If you select the Data Driven option but do not configure an update strategy expression, the target uses one of the following update strategies:

- If the source captures change information, the target uses the update strategy that is defined in the source.
- If the source does not capture change information, the target treats all rows as inserts.

Previously, when you selected the Data Driven option, the update strategy expression was required.

Secure Agent

This section describes changes to the Secure Agent for the Spring 2017 release.

Independent Services for the Secure Agent

Effective in the Spring 2017 release, the Secure Agent can run multiple services independently. You can configure each service independently from other services.

For example, the Data Integration Server runs as an independent service to run all data integration jobs. The Process Server runs as an independent service to run application integration and process orchestration.

Each service has a unique set of configuration properties, such as Tomcat and Tomcat JRE settings.

The ability to run services independently provides the following benefits:

- The Secure Agent does not restart when you add a connector or package.
- The Secure Agent does not restart during Informatica Cloud upgrades.
- No service is impacted when another service restarts. For example, a long standing process continues to run even if the Data Integration Server service is restarted.

Reduced Downtime During Upgrades

Effective in the Spring 2017 release, the upgrade process is optimized to significantly reduce Secure Agent downtime. This functionality addresses the problem of Secure Agent availability during upgrades for customers who cannot afford downtime for data integration jobs or who prefer that the upgrade process be transparent.

The upgrade process installs a new version of the Secure Agent, updates to connector packages, and configuration changes for the Data Integration Server. To minimize downtime, the old agent remains available and continues to run data integration jobs during the upgrade. The new version of the Secure Agent runs jobs that start after the upgrade process completes.

Previously, the Secure Agent was not available to run jobs during the entire upgrade process.

Secure Agent Configuration Properties

Effective in the Spring 2017 release, the Secure Agent can run multiple services. You set the configuration properties separately for each service. Because of this change, some properties associated with previous versions of the Secure Agent are replaced or removed, and other properties are added for the Data Integration Server service.

Replaced Configuration Properties

The following configuration properties are obsolete but are replaced with alternate configuration properties:

Tomcat configuration properties

The following Tomcat configuration properties are replaced with alternate Tomcat properties for the Data Integration Server:

Obsolete Property	Replacement Property	Description
TunnelTimeoutPeriod	NetworkTimeoutPeriod	Controls the length of time, in seconds, that the Secure Agent tries to reestablish communication with Informatica Cloud after a network interruption. Default is 300 seconds.
TunnelRetryInterval	NetworkRetryInterval	Determines the frequency with which the Secure Agent tries to contact Informatica Cloud within the specified timeout period. Default is five seconds.

If you changed the value of a Tomcat configuration property that has been replaced, the changes are preserved after the upgrade. For example, if you changed TunnelTimeoutPeriod from 300 to 600 seconds, the NetworkTimeoutPeriod is set to 600 seconds. You do not need to update the replacement properties after the upgrade.

Tomcat Log4J properties

If you ran a Secure Agent earlier than version 30.0, some Tomcat Log4J configuration properties are replaced.

The following Tomcat Log4J configuration properties are replaced with alternate Tomcat Log4J properties for the Data Integration Server:

Obsolete Property	Replacement Property
log4j.rootLogger	log4j_rootLogger
log4j.logger.org.apache	log4j_logger_org_apache
log4j.logger.org.springframework	log4j_logger_org_springframework
log4j.appender.tomcatLog	log4j_appender_tomcatLog
log4j.logger.com.informatica.saas.tunnel. TunnelClientHttpCommonsImpl	log4j_logger_com_informatica_saas_tunnel_ TunnelClientHttpCommonsImpl
log4j.appender.tomcatLog.layout. ConversionPattern	log4j_appender_tomcatLog_layout_ ConversionPattern
log4j.logger.httpclient.wire	log4j_logger_httpclient_wire
log4j.appender.tomcatLog.File	log4j_appender_tomcatLog_File
log4j.logger.org.apache.commons. httpclient.auth.AuthChallengeProcessor	log4j_logger_org_apache_commons_ httpclient_auth_AuthChallengeProcessor
log4j.logger.org.apache.commons. httpclient	log4j_logger_org_apache_commons _httpclient
log4j.logger.org.hibernate	log4j_logger_org_hibernate

Obsolete Property	Replacement Property
org.apache.axis.utils.JavaUtils	org_apache_axis_utils_JavaUtils
log4j.logger.net.sf	log4j_logger_net_sf
log4j.logger.com.informatica.saas	log4j_logger_com_informatica_saas
log4j.appender.tomcatLog.layout	log4j_appender_tomcatLog_layout
log4j.logger.com.informatica.saas.tunnel.TunnelClientImpl	log4j_logger_com_informatica_saas_tunnel_TunnelClientImpl
log4j.appender.tomcatLog.MaxFileSize	log4j_appender_tomcatLog_MaxFileSize
log4j.appender.tomcatLog.MaxBackupIndex	log4j_appender_tomcatLog_MaxBackupIndex

If you changed the value of a Tomcat Log4J configuration property that has been replaced, the changes are preserved after the upgrade. For example, if you changed log4j.appender.tomcatLog.MaxFileSize from '10MB' to '20MB,' the log4j_appender_tomcatLog_MaxFileSize is set to '20MB.' You do not need to update the replacement properties after the upgrade.

Removed Configuration Properties

If you ran a Secure Agent earlier than version 30.0, some configuration properties are removed.

The following configuration properties are obsolete and are removed from the Edit Secure Agent Page:

- All Agent Core properties
- All Agent Manager properties
- DTM $PMRootDir, JVMLibPath, and MappingImportLogDir properties
- All Agent Core JRE properties
- All Agent Core Log4J properties
- Tomcat Log4J log4j.logger.com.informatica.ics.adapters.relational.writeback.WriteBack property
- All Agent Manager Log4J properties

These properties are no longer needed. You do not need to configure alternate properties for any configuration property that was removed.

New Configuration Properties

New configuration properties are added for the Data Integration Server. Do not change the property values unless Informatica Global Customer Supports instructs you to do so.

Secure Agent Proxy File

Effective in the Spring 2017 release, the proxy.ini file is moved to a different directory.

The proxy.ini file is preserved after the upgrade and is copied to the following directory:

```
<Secure Agent installation directory>/apps/agentcore/conf
```

For Secure Agents earlier than version 30.0, the proxy.ini file was in the following directory:

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

User-Defined Parameter Files

Effective in the Spring 2017 release, the directory where you store user-defined parameter files for integration templates and Mapping Configuration tasks is changed.

User-defined parameter files are preserved after the upgrade and are copied to the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/data/userparameters
```

For Secure Agents earlier than version 30.0, user-defined parameter files were stored in the following directory:

```
<Secure Agent installation directory>/main/rdtmDir/userparameters
```

PowerCenter Source and Target Files

Effective in the Spring 2017 release, the directory where you store PowerCenter source and target files when the workflow uses the $PMSourceFileDir or $PMTargetFileDir variable is changed.

PowerCenter source and target files are preserved after the upgrade and are copied to the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/data
```

For Secure Agents earlier than version 30.0, PowerCenter source and target files were stored in the following directory:

```
<Secure Agent installation directory>/main/rdtmDir
```

Secure Agent Directory Changes

Effective in the Spring 2017 release, some Secure Agent directories are changed.

The following directories are changed:

Connection log files directory

Each time a user selects a connection for use in a task, Informatica Cloud creates a connection log named `<PluginShortName>_<connection_timestamp>.log`. The connection logs are in the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/<version>/ICS/main/tomcat/log
```

For Secure Agents earlier than version 30.0, Informatica Cloud created connection logs in the following directory:

```
<Secure Agent installation directory>/main/tomcat/log
```

Connection properties storage directory

The default directory for the connection properties that you store with a local Secure Agent is the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/data
```

For Secure Agents earlier than version 30.0, the default connection properties storage directory was the following directory:

```
<Secure Agent installation directory>/main/data
```

Console agent manager file directory

The console agent manager files consoleAgentManager.bat and consoleAgentManager.sh are in the following directory:

```
<Secure Agent installation directory>/apps/agentcore
```

For Secure Agents earlier than version 30.0, the console agent manager files were in the following directory:

```
<Secure Agent installation directory>/main/agentcore
```

Default data masking rules directory

You can view the default_rules.xml, fields.properties, and salesforce_default_values.properties files in the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/$version/ICS/main/dmask
```

For Secure Agents earlier than version 30.0, the default data masking rules were packaged in the following directory:

```
<Secure Agent installation directory>/Informatica Cloud Secure Agent/main/dmask
```

Default flat file target directory for PowerCenter tasks

If you create a PowerCenter task with an FTP/SFTP target connection and the IS_STAGED option is enabled for the underlying PowerCenter session, Informatica Cloud writes the flat file to the remote machine and the following local directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/data
```

For Secure Agents earlier than version 30.0, Informatica Cloud wrote the flat file to the remote machine and the following local directory:

```
<Secure Agent installation directory>/main/rdtmDir
```

Dictionary file directory for the Data Masking task

When you install or upgrade the Secure Agent in a runtime environment, the Data Masking task downloads and saves the dictionary files to the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/data
```

For Secure Agents earlier than version 30.0, the dictionary file directory was the following directory:

```
<Secure Agent installation directory>/main/rdtmDir
```

Error rows file directory

Informatica Cloud generates target error rows files in the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/data/error
```

For Secure Agents earlier than version 30.0, Informatica Cloud generated target error rows files in the following directory:

```
<Secure Agent installation directory>/main/rdtmDir/error
```

Secure Agent process directory on Linux

To start or stop the Secure Agent on Linux, run the `infaagent startup` or `infaagent shutdown` commands from the following directory:

```
<Secure Agent installation directory>/apps/agentcore
```

For Secure Agents earlier than version 30.0, you ran these commands from the directory where you installed the Secure Agent.

Session log file directory

Informatica Cloud generates session logs in the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/logs
```

For Secure Agents earlier than version 30.0, Informatica Cloud generated session logs in the following directory:

```
<Secure Agent installation directory>/main/rdtmDir/logs
```

Staging directory for the Data Masking task

You can run the startup script for the staging database manually from the following directory:

```
<Secure Agent installation directory>/apps/Data_Integration_Server/$version/ICS/main/
tomcat/cmask
```

For Secure Agents earlier than version 30.0, the Data Masking task used the following directory:

```
<Secure Agent installation directory>/Informatica Cloud Secure Agent/main/database
```

Transformations

This section describes changes to transformations for the Spring 2017 release.

Hierarchy Builder Transformation

Effective in the Spring 2017 release, you can create a hierarchical schema within the Hierarchy Builder transformation. Create the hierarchical schema from an XML sample file or from a JSON sample file. You can explicitly validate the schema and correct errors before adding it to the transformation.

Previously you created a hierarchical schema first, and then you could add it to the transformation. Now you can select either method.

For more information, see *Transformations*.

Hierarchy Parser Transformation

Effective in the Spring 2017 release, you can create a hierarchical schema within the Hierarchy Parser transformation. Create the hierarchical schema from an XML sample file or from a JSON sample file. You can explicitly validate the schema and correct errors before adding it to the transformation.

Previously you created a hierarchical schema first, and then you could add it to the transformation. Now you can select either method.

For more information, see *Transformations*.

Target Transformation

When you create a flat file target at run time and specify to append a time stamp to the file name, the time stamp is based on the organization's time zone.

Previously, the time stamp information was based on the time zone of the Informatica Cloud server.

INDEX