Informatica® Corporation
Informatica® Secure@Source 4.5
Release Notes
June 2018

Contents

This document contains important information about fixed limitations and known limitations for Secure@Source.

Secure@Source Version 4.5

Fixed Limitations (4.5)

The following table describes fixed limitations:

Bug	Description
SATS-7682	When you click the **Scan Status** link on the **Scans** page, the **Jobs** page appears with no jobs listed. Workaround: Click the **Future Jobs** tab and then the **Jobs** tab. Alternatively, use the browser refresh option to reload the page.
SATS-7678	If you import data store details without the required values, the **Data Stores** page fails to load and shows the following message: Call to getAllConnections failed.null Workaround: Examine the data store values in the import file and verify that the required fields have a valid value. Enter **U** in the Actions field in the import file for the updated rows. Then enable the **Replace Duplicates with Items Imported** option on the **Import Data Stores** page and import the file. Alternatively, if you cannot provide values for the required fields, enter **D** in the Actions field of the import file for the data stores that have missing required values. Then import the file again.
SATS-7492	You cannot import details for the GDPR_HIGH_RISK classification policy.
SATS-7115	The Pre-installation System Check utility does not allow the installation to proceed if it detects OpenSSL version 1.0.2 or later. Workaround: 1. Open the `PreValidation.sh` file located in the `$INFA_HOME/services/InfaHadoopService/Binaries` directory. 2. Find the line that begins with `opensslVersion=`. 3. Comment out all the lines in the `opensslVersion=` block.
SATS-7029	The installer does not copy the `LkpFiles` and `SrcFiles` files to the `$INFA_HOME/server/infa_shared` folder. Consequently, the Protection job fails when the associated protection technique uses the Test Data Management substitution rules. Workaround: Copy the `LkpFiles` and `SrcFiles` files from `$INFA_HOME/infa_shared` to `$INFA_HOME/server/infa_shared`.
SATS-7020	Proliferation data for SAP does not appear even when the Compute Lineage job is successful.
SATS-6644	The Sensitive Fields drill-down page shows that all protected fields are protected by the most recently used protection technique even if some fields are protected with other techniques.

Known Limitations (4.5)

The following table describes known limitations:

Bug	Description
SATS-10331	When the locale is set to German or French UTF-8, the installer fails because of an encoding error. Workaround: 1. Run the following command: `export LC_ALL=de_DE.UTF-8` 2. Restart the Informatica domain.
SATS-10308	If an inferred only column in Enterprise Data Catalog is blacklisted and the Validate Range flag is set, Secure@Source does not export the column to the CSV file.
SATS-10300	If you change the setting of a whitelisted column from sensitive to non-sensitive, the column reverts to the sensitive setting after a scan.
SATS-10279	The scan job fails at the profiling job step when a file name in the scan job contains quotation marks. Workaround: Skip the job step and resume the scan job. Or remove the quotation marks from the file name and scan the file again.
SATS-10274	The scan job fails at the data profiling job step when the folder name that contains the files in the scan job contains a special character. Workaround: Skip the job step and resume the scan job. Or remove the special character from the folder name and scan the folder again.
SATS-10273	The Microsoft OneDrive source directory value `/Documents` is always hardcoded even when it is not found.
SATS-10267	For Microsoft SQL Server repositories, if you install Secure@Source 4.5 over an existing domain, the installation fails because of a test connection failure.
SATS-10261	After upgrading to Enterprise Data Catalog, the Instance property for Microsoft SQL Server data stores appears with Instance as the value.
SATS-10260	For Teradata data stores, the **Include Views in the Scan** check box overrides the **Fetch Views Data Types** check box.
SATS-10254	For SAP data stores, the data scan job fails for the SBAC package for the D345T table.
SATS-10247	Secure@Source does not import sensitive data from Enterprise Data Catalog if the column name contains a special character.
SATS-10119	When you export sensitive files from File System data stores, Secure@Source exports the details of all the files to the CSV file even if you specified filter conditions.
SATS-10031	When you perform a metadata profiling scan for Sybase ASE 16 data stores, the scan results do not appear on the UI.
SATS-10016	If Secure@Source is installed using an IBM DB2 repository, file system scans fail if you change the protection status.
SATS-9943	When you perform a metadata profiling scan for MySQL data stores, the results do not appear on the UI.

Bug	Description
SATS-9861	When you perform a scan job from Informatica Intelligent Cloud Services data stores that include SAP connections, Secure@Source does not import the SAP connection details.
SATS-9843	For Salesforce data stores, the profiling job step fails for the StaticResource standard object. Workaround: Add the StaticResource standard object to the skip list.
SATS-9842	For Salesforce data stores, the profiling job step fails for the Site standard object. Workaround: Add the Site standard object to the skip list.
SATS-9829	For Salesforce data stores, the metadata with data profiling option fails for standard objects on the exclude list because the standard objects are included in the profiling.
SATS-9815	The Collect Row Count job step fails when scanning Salesforce data stores.
SATS-9730	If you delete the child connections, the Informatica Big Data Management scan job fails at the Copy Augmentation step.
SATS-9592	For anomaly security policies and manual actions taken from the **Anomaly Detection** and **Security Policy Violations** workspaces, Secure@Source can only perform actions or create tasks if the anomaly or anomaly violation is associated with at least one data store.
SATS-8505	PowerCenter Repository Service data stores do not get imported into Secure@Source from the Import from Enterprise Data Catalog page.

Secure@Source Version 4.1

Fixed Limitations (4.1)

The following table describes fixed limitations:

Bug	Description
SATS-7071	On the Overview workspace, if you use the Refresh option from the Actions menu and then click the Risk Score value, you get an error.
SATS-7012	SAP scans fail at the Identify Proliferation and Data Protection job steps.
SATS-7008	When Secure@Source contains the metadata of more than 50,000 user accounts, the dashboard takes more than 10 seconds to load.

Known Limitations (4.1)

The following table describes known limitations:

Bug	Description
SATS-7682	When you click the **Scan Status** link on the **Scans** page, the **Jobs** page appears with no jobs listed. Workaround: Click the **Future Jobs** tab and then the **Jobs** tab. Alternatively, use the browser refresh option to reload the page.
SATS-7678	If you import data store details without the required values, the **Data Stores** page fails to load and shows the following message: Call to getAllConnections failed.null Workaround: Examine the data store values in the import file and verify that the required fields have a valid value. Enter **U** in the Actions field in the import file for the updated rows. Then enable the **Replace Duplicates with Items Imported** option on the **Import Data Stores** page and import the file. Alternatively, if you cannot provide values for the required fields, enter **D** in the Actions field of the import file for the data stores that have missing required values. Then import the file again.
SATS-7674	The Object and FieldName/FileType fields in the Scan report do not appear in alphabetical order.
SATS-7581	Secure@Source can only detect anomalies if the username, data domain name, schema name, table name, column name, and data store name are in English.
SATS-7492	You cannot import details for the GDPR_HIGH_RISK classification policy.
SATS-7406	When the browser is set to German or French, the filtering is not case insensitive.
SATS-7208	When you filter the dashboard by classification policy or by data domains, the number of sensitive fields or files displayed in the **Top Data Stores** indicator is different from the number of fields displayed on the **Sensitive Fields** or **Sensitive Files** page.

Secure@Source Version 4.0

Fixed Limitations (4.0)

The following table describes fixed limitations:

Bug	Description
SATS-3307	The installer displays an incorrect warning when the installer validates the Java version in the Hadoop Gateway host.
SATS-3204	Test connection fails for a data store that connects to Informatica Big Data Management 10.1.1 because the scan job failed to create the EDR Service. Workaround: Contact Informatica Global Customer Support for the fix.
SATS-2562	When you delete a parent repository data store, such as an Informatica PowerCenter or an SQL Server Integration Services data store, the child data stores are also deleted.
SATS-2346	SQL Server Integration Services scan job does not extract connections if the mapping contains connections that do not connect to Microsoft SQL Server.

Known Limitations (4.0)

The following table describes known limitations:

Bug	Description
SATS-7115	The Pre-installation System Check utility does not allow the installation to proceed if it detects OpenSSL version 1.0.2 or later. Workaround: 1. Open the `PreValidation.sh` file located in the `$INFA_HOME/services/InfaHadoopService/Binaries` directory. 2. Find the line that begins with `opensslVersion=`. 3. Comment out all the lines in the `opensslVersion=` block.
SATS-7071	On the Overview workspace, if you use the Refresh option from the Actions menu and then click the Risk Score value, you get an error. Workaround: Use the browser refresh option to reload the page.
SATS-7029	The installer does not copy the `LkpFiles` and `SrcFiles` files to the `$INFA_HOME/server/infa_shared` folder. Consequently, the Protection job fails when the associated protection technique uses the Test Data Management substitution rules. Workaround: Copy the `LkpFiles` and `SrcFiles` files from `$INFA_HOME/infa_shared` to `$INFA_HOME/server/infa_shared`.
SATS-7020	Proliferation data for SAP does not appear even when the Compute Lineage job is successful.
SATS-7012	SAP scans fail at the Identify Proliferation and Data Protection job steps.
SATS-7008	When Secure@Source contains the metadata of more than 50,000 user accounts, the dashboard takes more than 10 seconds to load.
SATS-7005	When you scan a data store, the scan fails at the Load job step if the data store name ends with an hyphen. Example: `Connection-`. Workaround: Remove the trailing hyphen in the data store name and scan the data store.
SATS-6853	You cannot apply advanced email masking for Hive sources.
SATS-6841	When you apply random and key data masking to Hive data, the rows in the table are distorted if the value contains a delimiter character. Workaround: Define a masking rule with the Use all Except option and specify the delimiter character.
SATS-6827	The SAP scan job fails with the following error: Error occurred during character conversion. Workaround: Use the Skip and Resume option to continue the scan.
SATS-6764	The Protection job fails if you specified Shuffle or Substitution Rules when the storage is either Oracle or IBM DB2 for the following sources: - Microsoft SQL Server - Sybase - Microsoft Azure SQL Database - Microsoft Azure SQL Data Warehouse Workaround: You can perform one of the following actions: - Change the substitution dictionary connection to Oracle. - Delete the value in the SET QUOTED_IDENTIFIER ON property in the ODBC connection.

Bug	Description
SATS-6728	The Protection job fails at the ExportProjectXML job step if the connection to Test Data Management was not created during installation. Workaround: When you install Secure@Source, log in to Test Data Management before you configure protection.
SATS-6719	Child data stores that are created during a PowerCenter Repository scan cannot be updated by importing an `odbc.ini` file. Workaround: Update the data store properties from the Edit Data Store page.
SATS-6715	VARCHAR, CHAR, and BOOLEAN data type columns in Hive become null when masked.
SATS-6699	Unsupported PDM rules such as rules with flat file and Hive connections are listed on the UI.
SATS-6644	The Sensitive Fields drill-down page shows that all protected fields are protected by the most recently used protection technique even if some fields are protected with other techniques.
SATS-6628	Metadata profiling cannot identify a match for the data domain if the column headings contain multi-byte or special characters and the metadata match condition has the following pattern: `(E_NAME)|(.NAME.)` Workaround: Reorder the expression in the metadata match condition to: `(.NAME.)|(E_NAME)`
SATS-6553	During a scan, JDBC data stores that are created for MySQL data sources fail the profiling step if the schema name is blank or different from the database name. Workaround: When you create the JDBC data store for a MySQL source, enter the database name in the Schema field. The database name must match the database name you provided in the URL field.
SATS-5885	You cannot apply a protection technique to an imported sensitive column because the data types are not imported.
SATS-5762	When you configure a protection task that uses a Ranger protection technique, if the Hortonworks Ranger policy excludes any table columns, the Ranger policy does not display in Secure@Source for included columns.
SATS-5686	When you export SAP data store details, the csv file does not contain the full set of SAP connection properties. Consequently, when you use the same csv file as a template to import SAP data stores, some required SAP connection properties do not have values and the Test Connection fails.
SATS-5629	The Protection job fails when the associated protection technique contains multiple substitution and shuffle rules that require different dictionaries. Workaround: Do not use shuffle and substitution rules in the same protection job.

Secure@Source Version 3.0

Fixed Limitations (3.0)

Note: Informatica is migrating bugs to a different bug tracking system. The bug numbers in the bug ID column are replaced with the bug number in the new tracking system. You can find the bug IDs from the previous tracking system after the bug description. For example, (440143).

The following table describes fixed limitations:

Bug	Description
SATS-2636	When you create a Microsoft SQL Server data store, the Support Mixed-Case Identifiers property is not defaulted to true.
SATS-2627	When you run a scan on a Microsoft SQL Server data store, the scan job fails during the Profiling job step if the table column names contain keywords.
SATS-2545	When you run a scan on an IBM DB2 data store for the first time, the scan job fails during the Evaluate Policies job step.
SATS-1834	Rule names in the Secure@Source repository are not in sync with rule names in the Model repository.
SATS-1728	When you change the name for a data store that was imported from a parent repository scan and you run the parent repository scan again, the scan job imports the data store again.
SATS-1601	The profiling job step does not return schema and table names when the user does not have permissions on the table and the profiling sampling technique is Auto Random. (410451)
SATS-1479 SATS-10	When you resume a scan job that failed after the job profiled all tables, the job resumes profiling from the beginning instead of resuming from the failure point. (455931)
SATS-1439	On the Users drill-down page, if you expand every user record and specify a different time period, an SQL error appears intermittently. (445113)
SATS-173	The Secure@Source installer includes localized files, but the installer does not support localization. The localized files are removed from the installer.
461221	When you pause and resume a scan job, the job runs indefinitely under the following conditions: - You paused the scan job during the Profiling job step. - The profile fetcher sub-step is in queued status and is paused.

Known Limitations (3.0)

Note: Informatica is migrating bugs to a different bug tracking system. The bug numbers in the bug ID column are replaced with the bug number in the new tracking system. You can find the bug IDs from the previous tracking system after the bug description. For example, (440143).

The following table describes known limitations:

Bug	Description
SATS-3307	The installer displays an incorrect warning when the installer validates the Java version in the Hadoop Gateway host. Workaround: You can ignore the warning.
SATS-3300	On a multi node internal cluster, the node manager on Ambari agent nodes do not start. Workaround: Copy the file `spark-1.6.2-yarn-shuffle.jar` located at `/usr/hdp/2.3.4.0-3485/hadoop-yarn/lib/` to the gateway agent nodes. Then, restart the node manager.
SATS-3269	When you create or edit a security policy, you cannot delete conditions when there are two condition groups.

Bug	Description
SATS-3241	When you expand the Sensitive Data Locations page, Australia and New Zealand are not visible.
SATS-3211	Secure@Source does not check user privileges for the following actions: - Import Proliferation - Import Sensitive Data Locations A user cannot perform the following actions in Secure@Source even when the associated privilege is assigned: - Access Embedded URL - Import Audit Logs - Import Enterprise User and Accessibility Information: From Database Catalog - Validate Classification Exceptions - View User Activity Requests
SATS-3204	Test connection fails for a data store that connects to Informatica Big Data Management 10.1.1 because the scan job failed to create the EDR Service. Workaround: Contact Informatica Global Customer Support for the fix.
SATS-2812	In an anomaly security policy, if you specify a condition with the attribute Anomaly Factor Observed Value and the operator Contains, Secure@Source generates incorrect anomaly violations.
SATS-2562	When you delete a parent repository data store, such as an Informatica PowerCenter or an SQL Server Integration Services data store, the child data stores are also deleted.
SATS-2346	SQL Server Integration Services scan job does not extract connections if the mapping contains connections that do not connect to Microsoft SQL Server.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through Online Support on Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
http://www.informatica.com/us/services-and-training/support-services/global-support-centers.

If you are an Informatica Network member, you can use Online Support at
http://network.informatica.com.