Informatica® Secure@Source
4.5

Release Guide

Informatica Secure@Source Release Guide
4.5
June 2018

Publication Date: 2018-08-06

Table of Contents

Preface

The *Secure@Source Release Guide* lists new features and enhancements, behavior changes between versions, and tasks you might need to perform after you upgrade from a previous version. The *Secure@Source Release Guide* is written for all types of users who are interested in the new features and changed behavior. This guide assumes that you have knowledge of the features for which you are responsible.

Informatica Resources

Informatica Network

Informatica Network hosts Informatica Global Customer Support, the Informatica Knowledge Base, and other product resources. To access Informatica Network, visit https://network.informatica.com.

As a member, you can:

- Access all of your Informatica resources in one place.
- Search the Knowledge Base for product resources, including documentation, FAQs, and best practices.
- View product availability information.
- Review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to search Informatica Network for product resources such as documentation, how-to articles, best practices, and PAMs.

To access the Knowledge Base, visit https://kb.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

To get the latest documentation for your product, browse the Informatica Knowledge Base at https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx.

If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at infa_documentation@informatica.com.

Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. If you are an Informatica Network member, you can access PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services. Developed from the real-world experience of hundreds of data management projects, Informatica Velocity represents the collective knowledge of our consultants who have worked with organizations from around the world to plan, develop, deploy, and maintain successful data management solutions.

If you are an Informatica Network member, you can access Informatica Velocity resources at http://velocity.informatica.com.

If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that augment, extend, or enhance your Informatica implementations. By leveraging any of the hundreds of solutions from Informatica developers and partners, you can improve your productivity and speed up time to implementation on your projects. You can access Informatica Marketplace at https://marketplace.informatica.com.

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.

Part I: Version 4.5

This part contains the following chapters:

CHAPTER 1

New Features (4.5)

This section describes new features in version 4.5.

Connectivity

This section describes new connectivity features in version 4.5.

Effective in version 4.5, Secure@Source can connect to the following data sources:

Microsoft Azure Blob Storage

You can configure a data store to connect to Microsoft Azure Blob Storage. When you run a scan on the data store, the Secure@Source Service creates a Cloud scan job. The scan job identifies sensitive data in Microsoft Azure Blob Storage.

Microsoft OneDrive

You can configure a data store to connect to files on Microsoft OneDrive. When you run a scan on the data store, the Secure@Source Service creates a File Management scan job. The scan job identifies sensitive data in the file or a folder of files.

You can see the results of the scan at the file and folder levels.

Microsoft SharePoint

You can configure a data store to connect to files on Microsoft SharePoint. You can scan files in the document libraries as well as attachments in lists, events, contacts, calendar, and wiki pages. When you run a scan on the data store, the Secure@Source Service creates a File Management scan job. The scan job identifies sensitive data in the file or a folder of files.

You can see the results of the scan at the file and folder levels.

Data Stores

This section describes changes related to data stores in version 4.5.

Custom Risk Score Factors

Effective in version 4.5, you can customize the risk score calculation by adding your own evaluation criteria.

You can create risk factors where you specify a list or range of values and specify a weight for the factor. You can create up to five risk factors. Within a risk factor, you can specify up to five values or ranges and a weight for each value or range.

For instance, you might want to use tags to indicate production and patch level. You can specify a weight of 100 for the production tag and a weight of 70 for the patch level tag.

To add a custom risk factor, go to the **Settings** workspace, **Risk Score** section and click **Add Custom Risk Score Factors**.

Secure@Source will use the custom risk factors and any out-of-the-box risk factors that you select in the risk score calculation. Secure@Source also displays the custom risk factor as a data store property for existing and future data stores.

When you export the data store details, the custom risk score factors are included in the CSV file. When you import data store details, you can choose to import the custom risk score factor with the value or range for each data store.

Extensions Workspace

Effective in version 4.5, you can use the new **Extensions** workspace to configure and save connection properties for custom, email, protection, service management, and system log extensions. You can then include the extensions in corresponding action and task types.

Custom extensions specify the file path to a directory that contains an executable file, such as a script file, that performs a custom action when it runs.

Email extensions configure the server connection and security settings to use in an action that sends an email to specified recipients when the action runs.

Protection extensions protect sensitive data in data stores. In versions 4.0 and 4.1, protection extensions were called *protection techniques*. Also, versions 4.0 and 4.1 included only one protection technique for Persistent Data Masking. Version 4.5 supports protection extensions for the following applications:

- Cloudera Sentry
- Hortonworks Ranger: Access Control
- Hortonworks Ranger: Dynamic Data Masking
- Persistent Data Masking - Big Data
- Persistent Data Masking - Remote Domain

Service Management extensions create third-party service management tickets for issues that security policy violations identify or issues that require manual action to create tickets immediately. Version 4.5 supports service management extensions for the ServiceNow application.

System Log extensions create a log message that Secure@Source can send to a remote system log server on-demand or in the event of a security policy violation.

For more information, see the "Extensions" chapter in the *Informatica Secure@Source User Guide*.

Manual Actions

In previous versions, you could create and save actions only on the **Actions** workspace. You then attached actions to security policies, and the actions would run only in the event of a security policy violation. In version 4.5, you can now also create new actions or use existing actions and then save or run the tasks from several locations in Secure@Source.

You can select the **Take Action** option from the **Actions** menu to create a service management ticket, protect data, run a custom script, send an email, or write a system log message from the following pages in Secure@Source:

- **Anomaly Detection** workspace
- **Proliferation** page
- **Security Policy Violations** workspace
- **Sensitive Fields** page
- **Top Data Domains** list page
- **Top Data Stores** grid page

In versions 4.0 and 4.1, the **Actions** menu on these pages included the option **Create Protection Task** to manually create a protection task from these views. This option is replaced in 4.5 with the new **Actions** menu option **Take Action** > **Protect Data**.

For service management, custom, email, and system log actions, you can save and run the task immediately, or save the task to run later manually from the **Tasks** workspace. For protection actions, you save the action as a task. You then configure protection and schedule the protection job to run from the **Tasks** workspace.

For more information, see the "Manual Actions" and "Tasks" chapters in the *Informatica Secure@Source User Guide*.

Online Help

This section describes new online help features in version 4.5.

Hosted Help

In previous versions, online help was limited to help content embedded in the product. Effective in 4.5, help content is also hosted on an Informatica server. This allows us to update help content when necessary.

You access hosted help through the same Help icon on the UI. If the server you are on is connected to the internet, Secure@Source will automatically display hosted help.

Dynamic Help

A more granular level of context-sensitive help is available on certain UI pages such as the **New Action**, **New Data Store**, and **New Extension** pages. A **Help** icon appears at the property level after you specify selections to a key property.

Orchestration Job Type

Effective in version 4.5, the new Orchestration job type performs jobs that accomplish the tasks specified in the new task types listed on the **Tasks** workspace.

When a custom, email, service management, or system log task runs in the event of a security policy violation or manual action, the OrchestrationJobStep performs the specified actions to complete each task. On the **Jobs** workspace, you can click **Orchestration** in the **By Type** dashboard to filter the jobs list and view only Orchestration jobs.

For more information, see the "Jobs" chapter of the *Informatica Secure@Source User Guide*.

Protection Simulation

You can model the effects of data protection to, for example, support a budget request for a masking solution, or help prioritize a data protection initiative.

To model protection, you create a risk simulation plan that includes the data stores you want to monitor. For example, you want to see how the risk factors change if you protect all the data stores in the Human Resources department. For each data store in the plan, you select the data domains and the protection mechanism for the simulation.

You can create the plan by clicking **Manage** > **Risk Simulation Plans** and then **New**. Alternatively, you can select the data stores from the **Top Data Stores** grid page and click **Actions** > **Simulate Risk**.

You apply the simulation for one data store at a time. For structured data, Secure@Source treats the columns that match the data domains as protected. For unstructured data, Secure@Source treats the file as protected if the file contains a match for the data domains. Secure@Source displays the actual and simulated protection status, risk score, and residual risk cost for each data store as well as for the group of data stores in the plan. You can export the results. You can opt to save the plan for future simulations.

Service Management Action

Effective in version 4.5, you can create a reusable service management action on the **Actions** workspace.

The service management action creates ServiceNow service management tickets for issues that security policy violations identify or issues that require manual action to create tickets immediately. In the action, you specify details such as the service management extension and a description, impact, urgency, and category for the action. Optionally upload attachments to the ServiceNow ticket or use placeholders in the long description.

For more information, see the "Actions" chapter in the *Informatica Secure@Source User Guide*.

Synchronize with Enterprise Data Catalog

Effective in version 4.5, you can synchronize data store details and scan results between the Secure@Source repository and the Enterprise Data Catalog.

To import information from Enterprise Data Catalog, go to the **Data Stores** workspace and click **Actions** > **Import** > **Catalog Resources**. Specify a classification policy to limit the list to only the data stores that match a data domain included in the classification policy. You can further filter this list to only the data stores that are missing from Secure@Source.

If Catalog Administrator is connected to ServiceNow, then the import job also shows the data stores from ServiceNow.

An icon next to the data store name indicates that the data store has more recent details or scan results in Enterprise Data Catalog. You can open the data store and click **Actions** > **Import Results from Enterprise Data Catalog** to get the most recent details or scan results.

CHAPTER 2

Changes (4.5)

This section describes changes in version 4.5.

Classification Policies

This section describes changes related to classification policies in version 4.5.

Hierarchical Conditions

Effective in version 4.5, when you create a classification policy and select the **Custom** data match condition, you have the ability to construct multiple levels of rules. For each level, you specify data domain match rules and the risk cost for data stores that match the rule.

For example, you can assign a cost of $50 if the data store matches the `Credit Card` data domain. You can specify a higher cost if the data store matches both the `Credit Card` and the `Zip Code` data domain.

Previously, you could not nest conditions and could only specify one cost value for the classification policy.

Dashboard

This section describes changes related to the dashboard in version 4.5.

Risk Score Calculation

The formula for risk score is updated to more adequately reflect the aggregated risk of the classification policies that the data store matches. When you upgrade to Secure@Source 4.5, the upgrade script automatically recalculates existing risk scores with the new formula. The new risk scores might be lower than the risk scores in the previous release.

Jobs

Effective in the 4.5 release, you can enable the scan job to continue even if the Profiling or Collect Row Count job steps fail. Previously, the scan job failed and you had to manually resume the job.

To enable the scan job to continue running, go to the Administrator Tool. Navigate to the **Secure@Source Processes** tab. Edit the **Advanced Process Configuration** section, and add the following property to the **Additional JVM Options** field: `-DAUTO_SKIP_PROFILING_ERRORS=true`. Then, recycle the Secure@Source Service.

In future scan jobs, if the profiling job step encounters an object that cannot be profiled because the permissions are not valid, for example, Secure@Source automatically skips the object, continues profiling, and lists the objects that were not profiled in the scan.

Protection Task Actions

Beginning in version 4.0, you could create and edit protection task actions on the **Actions** workspace. Effective in version 4.5, when you take manual action to protect data, or a security policy that contains an action to protect data is violated, Secure@Source creates a protection task for each data store.

The protection tasks appear on the **Tasks** workspace with a status of New. You can no longer create a protection task action on the **Actions** workspace.

Fore more information, see the "Actions," "Manual Actions," and "Tasks" chapters of the *Informatica Secure@Source User Guide*.

Protection Techniques

Effective in version 4.5, the **Protection Techniques** workspace that was introduced in version 4.0 is deprecated. Instead, connection properties for protection applications such as Cloudera Sentry, Hortonworks Ranger, and Persistent Data Masking are configured on the **Extensions** workspace.

Protection techniques are replaced by protection extensions based on the protection application names.

For more information, see the "Extensions" chapter of the *Informatica Secure@Source User Guide*.

Tasks

The **Tasks** workspace was introduced in version 4.0 and included only protection tasks. Effective in version 4.5, all actions create tasks that appear on the **Tasks** workspace.

Secure@Source creates a protection task when you take manual action to protect sensitive data, or a security policy violation occurs for a data store or user activity policy that includes a protection action. Protection tasks appear on the **Tasks** workspace with a status of New. You then configure protection for the sensitive fields in the data store and schedule a protection job to run the task.

Secure@Source creates custom, email, service management, and system log tasks when you take manual action to perform the corresponding tasks, or a security policy violation occurs for a policy that includes these actions. The resulting tasks that you either save or run also appear on the **Tasks** workspace. Because you can create manual actions that generate custom, email, service management, and system log tasks and choose to save them on the **Tasks** workspace to run later, the **Actions** menu now includes a new option for these task types: **Run Task**.

Also, in versions 4.0 and 4.1, the **Actions** menu on the **Tasks** workspace included the menu option **Add Proof of Protection** to provide the ability to upload attachments to protection tasks. Effective in version 4.5, since the **Tasks** workspace lists all task types and you can add attachments to any task, this menu option is now called **Upload Attachment**.

For more information, see the "Tasks" chapter of the *Informatica Secure@Source User Guide*.

Part II: Version 4.1

This part contains the following chapters:

CHAPTER 3

New Features (4.1)

This section describes new features in version 4.1.

Localization

Effective in version 4.1, the Secure@Source UI will display in French and German when the browser is set to one of these languages.

Scans

This section describes new scan features in 4.1.

Security Group

When you create a scan for data stores in the Data Integration category, you can choose to either retrieve the security group or specify a security group for the child data stores.

If you select the retrieve option, Secure@Source assigns the child data stores to the same group as the parent data store in the scan. If you select the specify option, you must select a security group for the child data stores.

Report of Tables Changed Since the Previous Scan

You can now access a report that lists the tables or files that were changed since the last time the data store was scanned. The report is in CSV format and you can download the file from the Jobs page or Scan Details page.

Syslog Action

Effective in version 4.1, you can create a reusable syslog action on the **Actions** workspace.

The syslog action creates a log file that Secure@Source sends to a syslog server in the event of a security policy violation. In the action, you specify the server connection details. Then enter the syslog file details in a text format, such as Common Event Format (CEF) or Log Event Extended Format (LEEF).

For more information, see the "Actions" chapter in the *Informatica Secure@Source User Guide*.

User Profile Page

Effective in version 4.1, each user name in Secure@Source has an associated **User Profile** page that displays detailed information about the user.

The information includes the user's title, department, manager, email address, location, and the number of data stores, sensitive fields, and impressions the user has accessed. The **User Profile** page also displays the top data domains and data stores the user accessed, and security policy violations and anomalies associated with the user.

To view a **User Profile** page, click the user name from any of the following views:

- **Anomaly Detection** list
- **Anomaly Detection** details page
- **Anomaly Detection** workspace, **View By** > **User**
- **Top Users** widget on the **Overview** workspace
- **Security Policy Violations** list
- **Security Policy Violation** details page
- **Suppression Rules** list
- **Users** page
- **User Access** page
- **User Activity** page

For more information, see the "Overview Workspace" chapter in the *Informatica Secure@Source User Guide*.

CHAPTER 4

Changes (4.1)

This section describes changes in version 4.1.

Classification Policies

This section describes changes related to classification policies in version 4.1.

GDPR

Effective in version 4.1, the out-of-the-box GDPR classification policy includes 49 data domains with the data domain match condition configured.

Dashboard

This section describes changes related to the dashboard in version 4.1.

Classification Policy Filter

Effective in version 4.1, you can filter the information on the dashboard by classification policy.

Residual Risk Cost

Effective in version 4.1, the Risk Cost field is renamed as Residual Risk Cost. The monetary value displayed on the dashboard is the cost of exposing unprotected sensitive data. Previously, the risk cost was the cost of exposing protected and unprotected data.

Data Domains

This section describes changes related to data domains in version 4.1.

Conformance Row Count

Effective in version 4.1, when you create or edit data domain, you cannot enter a value that is less than one in the Conformance Row Count field. This change prevents non-sensitive fields from being mistakenly identified as sensitive in a scan where the Data Domain Match Criteria is Rows.

Data Stores

This section describes changes related to data stores in version 4.1.

Hive Data Stores

Effective in version 4.1, you can specify one of the following Hadoop distribution services when you create a Hive data store:

- Amazon EMR
- Azure HDInsight
- Cloudera
- Hortonworks
- IBM BigInsights
- MapR

Export Enhancements

Effective in version 4.1, when you export data stores, the exported file includes additional data store details such as storage type, source directory, and source connection name.

Jobs

This section describes changes related to jobs in version 4.1.

Category

Effective in version 4.1, the Job Type for a scan job is renamed to match the category name of the data store. For example, the job type for a Salesforce scan job now matches the Salesforce category name, Cloud.

You can filter jobs by job type to view data stores in a specific category.

Security Policy Violations

This section describes changes related to security policy violations in version 4.1.

Sort order for Top Security Policies list on the Security Policy Violations page

By default, the list of security policies is sorted by the number of violations in descending order, then by severity level, and then by the security policy name in ascending order.

Previously, the list was sorted by the number of violations in descending order and then by security policy name in ascending order.

User Access

This section describes changes related to user access in version 4.1.

Instant Page Load

The User Access page loads immediately and there is no delay when you scroll through the list of users, data stores, and user groups.

Previously, if there was a large number of the users, data stores, or user groups, the page was slow to load as you scrolled.

Part III: Version 4.0

This part contains the following chapters:

CHAPTER 5

New Features (4.0)

This section describes new features in version 4.0.

Actions

This section describes new actions features in version 4.0.

Protection Task Action

Effective in 4.0, you can create a reusable protection task action on the Actions workspace. In the action, you specify the protection technique. You can then add the action to a security policy for data stores or user activity. In the event of a security policy violation, Secure@Source uses the details specified in the protection task action to create a protection task for each data store associated with the violation. Secure@Source also assigns the protection tasks to the respective data owners.

Note: You cannot add a protection task action to an anomaly security policy because the violation for this type of policy might be associated with diverse data stores that cannot be protected by the same protection technique.

Anomaly Detection

This section describes new anomaly detection features in 4.0.

Anomaly Score

Effective in version 4.0, Secure@Source assigns a score to each anomaly. Secure@Source calculates the anomaly score based on the anomalous factors that triggered the anomaly.

Secure@Source displays the anomaly score on the Anomaly Detection page. Use the score to prioritize the anomalies for investigation.

You can rank and filter anomalies by anomaly score. You can also create an anomaly security policy based on the anomaly score.

The Customize Advanced Analytics Configuration privilege allows you to customize the calculation of the anomaly score. To customize, go to the Settings page and reset the weights of the anomalous factors in the anomaly score calculation. Secure@Source will calculate the anomaly score for future anomalies based on the new weights.

For more information, see the *Informatica Secure@Source User Guide*.

Anomaly Suppression

You can suppress certain types of anomalies from appearing on the UI. To suppress anomalies, you must create a suppression rule. In the rule you specify the anomalous factors for which you do not want to view anomalies. After anomaly detection, Secure@Source will not display anomalies that are solely based on the suppressed factors.

You create suppression rules from the Anomaly Detection workspace. After you create the suppression rule, you can view, filter, sort, edit, export, and delete the suppression rule from the Suppression Rules workspace.

For more information, see the *Informatica Secure@Source User Guide*.

Create a Protection Task

You can create a protection task from the Anomaly Detection workspace to protect the data stores that are associated with the anomaly. In the protection task, you must select a protection technique and remove any data stores that cannot be protected by the technique.

For a list of the protection techniques and the data store types each technique supports, see "Protection" on page 29 or the "Protection Techniques" chapter in the *Informatica Secure@Source User Guide*.

Classification Policies

This section describes new classification policy features in version 4.0.

Default GDPR

Effective in version 4.0, Secure@Source contains a ready-to-use GDPR classification policy based on the data domains that are included in Secure@Source. The data match condition in the classification policy is designed to identify GDPR risks in enterprise data. You can modify the policy to meet your unique business needs.

Connectivity

This section describes new connectivity features in version 4.0.

Effective in version 4.0, Secure@Source can connect to the following data sources:

SAP ECC 6.0 EHPx (1 to 7)

You can configure a data store to connect to SAP. When you run a scan on the data store, the Secure@Source Service creates a Database scan job. The scan job can identifies sensitive data in SAP custom, cluster, and pooled tables.

Amazon Redshift

You can configure a data store to connect to Amazon Redshift. When you run a scan on the data store, the Secure@Source Service creates a Cloud scan job. The scan job identifies sensitive data in Amazon Redshift.

Microsoft Azure SQL Database

You can configure a data store to connect to Microsoft Azure SQL Database. When you run a scan on the data store, the Secure@Source Service creates a Cloud scan job. The scan job identifies sensitive data in Microsoft Azure SQL Database.

Microsoft Azure SQL Data Warehouse

You can configure a data store to connect to Microsoft Azure SQL Data Warehouse. When you run a scan on the data store, the Secure@Source Service creates a Cloud scan job. The scan job identifies sensitive data in Microsoft Azure SQL Data Warehouse.

File System

You can configure a data store to connect to an unstructured file. When you run a scan on the data store, the Secure@Source Service creates a File System scan job. The scan job identifies sensitive data in the file or a folder of files.

You can see the results of the scan at the file and folder levels.

Secure@Source can scan the following file types:

File Type	File Extension
Compressed Files	7z, Z, ZIP, xz, Bz2, Gz, Tar.bz2, Tar.bz2, Tar.gz, and Tar.xz
Delimited and Text	csv and txt
Email	EML, MHT, OFT, and MSG
Extended Unstructured Formats	Apple documents supported by Apache Tika
JSON	json
Microsoft Excel	xlsx, xls, xlam, xlsm, xltm, and xltx
Microsoft Power Point	ppt, pptx, pps, ppsx, ppsm, pptm, pot, potm, and potx
Microsoft Word	docx, doc, dot, dotx, dotm, and docm
Adobe Portable Document Format	pdf
Web page	html and htm
XML	xml

Dashboard

This section describes new dashboard features in version 4.0.

Effective in version 4.0, you can perform the following actions on the Overview workspace:

Refresh

You can refresh the data on an Overview workspace page by clicking **Actions** > **Refresh**.

Create Protection Task

You can create a protection task from the following Overview workspace pages:

- Proliferation page
- Sensitive Fields page

- Top Data Domains page
- Top Data Stores grid page

Upstream Proliferation

On the Proliferation page, you can see the data stores from where sensitive data originated. You can click on the link between the target and upstream data stores to see the data domains that proliferated. You can click an upstream data store to see details such as risk score and protection status.

Data Domains

This section describes new data domain features in version 4.0.

Synchronize Data Domains

Effective in version 4.0, you can sync data domain details between the Secure@Source repository and the Enterprise Information Catalog.

Delink Associations

Effective in version 4.0, you can remove the links between a data domain and the data store associated with it. You must have the Add or Modify Data Domain privilege to disassociate data domains from data stores. The data domains cannot be associated with a scan that is in progress, a protection task, or user access data.

Conformance Row Count

Effective in version 4.0, when you create a data domain, you can specify the minimum number of rows in a field that must match the data domain for Secure@Source to identify the field as sensitive data.

When you scan a data store, you can select either the minimum number of rows or the minimum percentage of rows that must match the data domain to be considered sensitive for the data domain.

Specify a Protection Technique

Effective in version 4.0, when you create a data domain, you can specify one or more protection techniques and protection rules for each technique. When you run a protection job for a data store, based on the data store type, Secure@Source applies the protection technique and corresponding protection rule to protect the data that matches the data domain.

Note: You can keep the default protection rule or select a different protection rule when you configure the protection task.

Data Stores

This section describes new data store features in version 4.0.

Synchronize Data Stores

Effective in version 4.0, you can sync data store details between the Secure@Source repository and the Enterprise Information Catalog.

Synchronize Users

Effective in version 4.0, you can sync user details between the Secure@Source repository and the Enterprise Information Catalog.

Import Connection Assignment

Effective in version 4.0, you can import information about the data stores that are connected to a parent repository, such as Informatica PowerCenter.

Protection

Effective in version 4.0, Secure@Source provides protection methods for sensitive data in data stores. The sensitive data protection methods that Cloudera Sentry, Hortonworks Ranger, and Persistent Data Masking provide are integrated with Secure@Source as protection techniques.

Secure@Source 4.0 introduces the following protection technique types:

- Cloudera Sentry
- Hortonworks Ranger: Access Control
- Hortonworks Ranger: Dynamic Data Masking
- Persistent Data Masking

Protection techniques are associated with compatible data stores and the techniques determine the configuration of protection tasks. The following table lists the supported data store types for each protection technique:

Protection Technique	Supported Data Store Types
Cloudera Sentry	Hive
Hortonworks Ranger: Access Control	Hive
Hortonworks Ranger: Dynamic Data Masking	Hive
Persistent Data Masking	- Azure SqlDB - Azure SqlDW - DB2 - DB2i5 - DB2zOS - Hive - JDBC - Microsoft SQL Server - Netezza - Oracle - Sybase - Teradata

After you create protection techniques, you can create, configure, edit, run, and close protection tasks. You can also create protection task actions to include in security policies, and you can schedule protection jobs to run protection tasks. Each protection task is associated with one data store, and each task is dependent on one protection technique. A protection task applies the default rules or access conditions of the associated protection technique to sensitive fields in data stores.

For more information, see "Part IV: Protection" in the *Informatica Secure@Source User Guide*.

Security

Effective in version 4.0, a new privilege group, named Data Protection, and a new custom role, named Secure@Source Operator, is available.

The Data Protection privilege group contains privileges that allow users to create and manage protection tasks and techniques.

The Secure@Source Operator role allows the user to monitor and run routine operations. A user with the Operator role can view dashboards, jobs, protection tasks, and scans. In addition, the user can run protection tasks and scans.

For more information, see the *Informatica Secure@Source Administrator Guide*.

Security Policy

This section describes new security policy features in version 4.0.

Specify a Protection Task Action

Effective in 4.0, when you create a data-store or user-activity security policy, you can include a protection task as an action in the event of a security policy violation. If the security policy is violated, Secure@Source uses the specifications in the protection task action to create a protection task for each data store associated with the violation. Secure@Source then assigns the protection tasks to the respective data owners for task configuration.

Security Policy Violations

This section describes new security policy violation features in 4.0.

Create a Protection Task

You can create a protection task from the Security Policy Violations workspace to protect the data stores that are associated with the violation. In the protection task, you must select a protection technique and remove any data stores that cannot be protected by the technique.

For a list of the protection techniques and the data store types each technique supports, see "Protection" on page 29 or the "Protection Techniques" chapter in the *Informatica Secure@Source User Guide*.

Settings

This section describes new settings features in 4.0.

Anomaly Score

Effective in version 4.0, you can customize the calculation of the anomaly score on the Settings workspace. To customize, reset the weights of the anomalous factors in the anomaly score calculation. Secure@Source will calculate the anomaly score for future anomalies based on the new weights.

You must have the Customize Advanced Analytics Configuration privilege to customize the calculation of the anomaly score.

For more information, see the *Informatica Secure@Source User Guide*.

Anomaly Severity Level

Effective in version 4.0, you can specify the anomaly score range for each anomaly severity level on the Settings workspace. For example, you can specify that anomalies with a score from 90 through 100 must be categorized in the High severity level. After you save, Secure@Source will use the updated setting to assign future anomalies that have a score of 90 or higher to the High severity level.

For more information, see the *Informatica Secure@Source User Guide*.

CHAPTER 6

Changes (4.0)

This section describes changes in version 4.0.

Anomaly Detection

This section describes changes related to anomaly detection in version 4.0.

Anomalous Factor Sensitive Fields

Effective in version 4.0, the Sensitive Fields anomalous factor is deprecated. Secure@Source will not use the Sensitive Fields factor to identify unusual behavior and to detect an anomaly.

Classification Policies

This section describes changes related to classification policies in version 4.0.

Custom Data Domain Match Condition

Effective in version 4.0, when you create a classification policy, you can define a data domain match condition that specifies the minimum number of data domains the data store must match for Secure@Source to designate the data store a match to the classification policy. The number of data domains you specify must be equal to or less than the number of data domains in the classification policy.

Data Stores

This section describes changes related to data stores in version 4.0.

Category

Effective in version 4.0, on the New Data Store page, the connection property Repository Type is now named Category. When you create a data store, you must select a category for the data store type. Data store types are organized in the following categories:

Category	Data Store
Application	SAP
Big Data	- Cloudera Navigator - Hadoop Distributed File System - Hive
Cloud	- Amazon Redshift - Amazon S3 - Microsoft Azure SQL Database - Microsoft Azure SQL Data Warehouse - Salesforce
Data Integration	- Informatica Big Data Management - Informatica Cloud - Informatica PowerCenter on IBM DB2 database - Informatica PowerCenter on Microsoft SQL Server database - Informatica PowerCenter on Oracle database - Microsoft SQL Server Integration Services
Database Management	- IBM DB2 - IBM DB2 for i5 - IBM DB2 for z/OS - JDBC - Microsoft SQL Server - Netezza - Oracle - Sybase - Teradata
File Management	File systems such as text, email, csv, PDF, and Microsoft Office applications such as Word, Excel, and PowerPoint.

Installation

This section describes changes related to the installation in version 4.0.

Vibe Data Stream Not Required

Effective in version 4.0, the Secure@Source installer does not install the Vibe Data Stream component.

Scans

This section describes changes related to scans in version 4.0.

Data Profile Based on Metadata Profile Results

Effective in version 4.0, you can save time by running a data profile based on the metadata profile results. Secure@Source will run a data profile on only the sensitive fields discovered in the metadata profile.

Data Domain Match Criteria

Effective in version 4.0, you can specify whether you want the number or the percentage of rows in the sample to match the data domain. Previously, you could only specify the percentage.

Security

This section describes changes related to security in version 4.0.

Privilege Groups

The privileges in the following privilege groups have changed:

- Classification
- Security Policy
- UI/Analysis

Custom Roles

Privileges and privilege groups in the following custom roles have changed:

- Secure@Source Data Owner
- Secure@Source External API
- Secure@Source Policy Author
- Secure@Source Security Analyst
- Secure@Source Security Manager
- Secure@Source Technical Administrator

The Secure@Source User Administrator role is deprecated.

For more information, see the *Informatica Secure@Source Administrator Guide*.

Terminology

This section describes changes related to terminology in version 4.0.

The following table lists the terminology changes in version 4.0:

Old Term	New Term
Live Data Map	Enterprise Information Catalog
Live Data Map platform	Enterprise Unified Metadata platform
Live Data Map Administrator	Catalog Administrator
Sensitive Records	Domain Impressions
Policy Match Count	Related Classification Policies
Impression Count	Domain Impressions
Rows Matched	Profile Matches
Repository Type	Category

Part IV: Version 3.0

This part contains the following chapters:

CHAPTER 7

New Features (3.0)

This section describes new features in version 3.0.

Actions

Effective in 3.0, you can use templates in the Actions workspace to create a reusable email or custom action. After you create the reusable action, you can include them in security policies.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

Anomaly Detection

Effective in version 3.0, Secure@Source can identify irregular or unusual patterns of user activity on sensitive data. Irregular or unusual user activity can indicate malicious behavior, such as a data breach or stolen credentials. Secure@Source analyzes user activity events to determine baseline behavior for a user and for the user's peer group. When user activity behavior deviates from the baseline, Secure@Source detects an anomaly. For example, Secure@Source detects an anomaly when a user downloads a high amount of sensitive data outside of the user's normal working day and time.

Use the anomaly detection workspace to view the anomalies that Secure@Source detected. You can mark an anomaly as read or flag an anomaly to review at a later time. You can also delete anomalies. To generate security policy violations, email notifications, or custom actions when Secure@Source detects an anomaly, you must configure a security policy.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

Connectivity

This section describes new connectivity features in version 3.0.

Amazon S3

Effective in version 3.0, Secure@Source includes the following support for Amazon S3 sources:

- You can configure a data store to connect to Amazon S3. When you run a scan on the Amazon S3 data store, the Secure@Source Service creates a File System scan job. The scan job identifies sensitive data in CSV, XML, and JSON files.
- The Informatica Cloud scan job can import Amazon S3 connections from Informatica Cloud. The scan job can identify sensitive data proliferation between the imported Amazon S3 data stores and identify the protection status of the sensitive data.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

Hadoop

Effective in version 3.0, the Hadoop scan job includes the following new features:

Blaze Engine

The Hadoop scan job uses the Blaze engine to run mappings. Before you run a scan, you must run the Big Data Edition Configuration utility to create a Hadoop connection in the Informatica domain. When you create a Hadoop data store in Secure@Source, you specify the Hadoop connection name. When you scan the Hadoop data store, the scan job uses the Hadoop connection in the Informatica domain to start the Blaze Grid Manager in the Hadoop cluster.

To run mappings in the native environment, configure the `-DdisableBlazeMode` property in the Advanced JVM options in the Secure@Source Service process properties.

For more information, see the Source Connectivity and Data Store Properties chapters in the *Informatica Secure@Source Administrator and User Guide*.

Hive Datatypes

The Hadoop scan job includes support for the following Hive datatypes:

- Char
- Varchar
- Decimal

Kerberos Authentication

The Hadoop scan job can connect to Hive sources that use Kerberos authentication.

Before you run a scan, you must set up connectivity to the source. For more information, see the Source Connectivity and Data Store Properties chapters in the *Informatica Secure@Source Administrator and User Guide*.

Hadoop Distributed File System (HDFS)

Effective in version 3.0, you can configure a data store to connect to a Hadoop Distributed File System (HDFS). You can connect to HDFS on a normal cluster or a cluster that is highly available or Kerberos-enabled. When you run a scan on a HDFS data store, the Secure@Source Service creates a File System scan job. The scan job identifies sensitive data in CSV, XML, and JSON files.

Before you run a scan, you must set up connectivity to the source. For more information, see the Source Connectivity and Data Store Properties chapters in the *Informatica Secure@Source Administrator and User Guide*.

Microsoft SQL Server Integration Services

Effective in version 3.0, you can configure a data store to connect to Microsoft SQL Server Integration Services. When you run a scan on a SQL Server Integration Services data store, the Secure@Source Service creates a SQL Server Integration Services scan job. The scan job identifies the proliferation of sensitive data between connections in the Microsoft SQL Server repository.

Before you run a scan, you must set up connectivity to the source. For more information, see the Source Connectivity and Data Store Properties chapters in the *Informatica Secure@Source Administrator and User Guide*.

Dashboard

This section describes new dashboard features in version 3.0.

Customization

Effective in version 3.0, you can customize the following items in the Overview workspace:

Indicator Sequence

You can customize the order in which indicators appear in the Overview workspace. To change the order, you drag an indicator to another location. The changes apply to the logged in user and persist for future sessions.

Indicator State

When you expand or collapse an indicator, the indicator state persists for future sessions. The changes apply to the logged in user.

Filters

Effective in version 3.0, the filter pane for the Overview workspace includes an option to filter data stores based on data store tags. You can specify one or more data store tags. When you apply the filter condition, the Overview workspace and the drill-down pages display information specific to the data stores that match the data store tags you selected.

Sensitive Data for Locations

Effective in version 3.0, the default view of the Sensitive Data for Locations indicator shows the region that contains the most number of sensitive data stores.

Top Data Domains

Effective in version 3.0, the Overview workspace includes a Top Data Domains indicator. The indicator shows the top 10 data domains based on the highest number of fields that matched the data domain conditions. You can click the indicator label to access the drill-down page. The drill-down page includes a list of all the data domains that include at least one matched field. You can export the data domain list.

Data Stores

This section describes new data store features in version 3.0.

Bulk Update of User Credentials

Effective in version 3.0, you can update the user name and password for multiple data stores at the same time. You select one or more data stores to update. Then, enter a new user name and password. The changes apply to the selected data stores. To select data stores, you can sort or filter the list by user name.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

Scanning Views

Effective in version 3.0, a scan job can analyze data in views for database or Hadoop data stores. When you configure a data store, you specify if a scan job reads data from views. When enabled, a scan job can identify sensitive data in views and identify the proliferation of sensitive data in views.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

Jobs

This section describes new job features in version 3.0.

Scan Job Warning Status

Effective in version 3.0, scan jobs can have a warning job status. A scan job can have a warning job status if the scan option for email notification is enabled and the Secure@Source Service encounters an error while sending an email.

Managing Jobs from the Job Details Panel

Effective in version 3.0, you can manage a job from the job details panel. For example, you can pause, resume, terminate, or stop a job. The actions that you can perform depend on the status of the job.

Job Filtering

Effective in version 3.0, you can filter jobs from the jobs list panel. You can filter the list of jobs based on each job property. For example, you can filter the list of jobs based on the job name. The jobs list panel includes a filter icon that displays or hides the filters.

Locations

This section describes new locations features in version 3.0.

Location Import

Effective in version 3.0, you can import locations in bulk from a CSV file. You can export a list of locations and use the export file as a template for the import. The export file contains the same format that is required for the import. After you import locations, you can assign the locations to data stores.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

IP Addresses

Effective in version 3.0, you can add an IP address range to a location. The IP address range identifies the geographic area from which user activity originates. The Secure@Source uses the IP address range to detect anomalies in user activity based on location.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

Scans

This section describes new scan features in version 3.0.

Email Notifications

Effective in version 3.0, you can receive an email notification when the status of a scan job changes. For example, when a scan job status changes from running to completed. When you configure a scan, you enable the email notification and specify the recipient email addresses. The email is sent from the mail server defined in the Secure@Source Service. The email includes a link to the job details page. The email notification is valid only for jobs that are associated with the scan.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

Security Policies

Effective in 3.0, you can specify security policies to detect and monitor high risk situations across enterprise data. When the security policy conditions are met, Secure@Source creates a security policy violation.

Use the Security Policy workspace to create security policies for anomalies, data stores, or user activity events. For example, you can set up a data store security policy to notify you when sensitive data moves across countries and when the risk cost exceeds a threshold. You can choose to notify recipients with an email or you can provide a custom script that Secure@Source runs when a security policy violation occurs.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

Security Policy Groups

Effective in 3.0, Secure@Source you can group related security policies. After you assign security policies to a group, you can use security policy groups as a filter option to quickly find security policy violations.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

Security Policy Violations

Effective in 3.0, you can view security policy violations on the Security Policy Violations workspace. A security policy violation occurs when the conditions in a security policy are met.

For example, you set up a user activity security policy to detect column activity over a certain threshold and during a time period. If both conditions are met, the Secure@Source Service creates a security policy violation. Secure@Source lists violations on the Security Policy Violations workspace. The violations you see involve at least one data store that you have access to.

For more information, see the *Informatica Secure@Source Administrator and User Guide*.

CHAPTER 8

Changes (3.0)

This section describes changes in version 3.0.

Dashboard

This section describes changes related to the dashboard in version 3.0.

Sensitive Data by Locations

Effective in version 3.0, by default, the Sensitive Data by Locations indicator displays the region with the most number of sensitive data stores. If there are no sensitive data stores in any region, the indicator displays North America.

Data Stores

This section describes changes related to data stores in version 3.0.

Importing Sensitivity and Protection Statuses from CSV Files

Effective in version 3.0, the required column heading names changed for the CSV import file that you use to import sensitivity and protection status. The following table describes the column heading name changes:

New column heading	Previous column heading
SchemaName/FolderName	SchemaName
Object	TableName
FieldName	ColumnName
Verified	Action

If you try to import a file that includes the old column headings, you receive an error.

Locations

This section describes changes related to locations in version 3.0.

Regular Expressions

Effective in version 3.0, the regular expression property is no longer a required field when you create or edit a location. A location can represent the location of a data center, the location from which user activity originates, or both. The Secure@Source uses the regular expression to identify the location of data stores, not the location of user activity. If the location only represents the origin of user activity, then a regular expression is not needed. Configure the IP address range to identify the location of user activity.

Secure@Source Service

This section describes changes related to the Secure@Source Service in version 3.0.

Advanced Properties for the Secure@Source Service Process

Additional JVM Options

Effective in version 3.0, the -DIncludeViewsForScan Additional JVM Options property is deprecated. The property determined if scan jobs evaluated views for all data stores.

You configure if a scan job evaluates data in views at the data store level for database and Hadoop data stores.

Scans

This section describes changes related to scans in version 3.0.

Concurrent Scans

Effective in version 3.0, you can run a concurrent scan on related data stores. A related data store is a parent, child, or sibling data store. A parent data store is a repository, such as Informatica PowerCenter or Informatica Cloud, from which a scan job imported data stores. A child data store is a data store that a scan job imported from a parent data store. A sibling data store is a data store that a scan job imported from the same parent data store.

Previously, you could only run a scan on data stores if the related data stores had a not analyzed status, or if the data stores were included in a scan job that was in a terminated or completed job state. If the related data stores were in a scan job with any other job state, you had to wait until the scan job completed, or you had to terminate the job.

Terminology

This section describes changes related to terminology in version 3.0.

The following table lists the terminology changes in version 3.0:

Old Term	New Term
alerts	security policy violations
alert rules	security policies
Informatica Big Data Edition (repository type for data stores and scans)	Informatica Big Data Management
Informatica Big Data Edition scan (job type)	Informatica Big Data Management scan
policy	classification policy
PowerCenter repository (repository type for data stores and scans)	Informatica PowerCenter
PowerCenter repository scan (job type)	Informatica PowerCenter scan