IBM Security Verify Governance Identity Manager

StealthBits GDAP Adapter Installation and Configuration Guide

BA21-8475-00

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and an IBM Security Identity server. The StealthBits GDPR adapter enables communication between StealthBits and the IBM Security Identity and Governance Intelligence server.

Features of the adapter

The StealthBits GDPR adapter supports the following operations.

The StealthBits stores Active Directory users and access information for the Active Directory that it monitors. You can perform the following operations on data that is stored by StealthBits.

- Reconciling users.
- Reconciling support data such as group, folder, sensitive data files, and taxonomy.
- Test connection from Verify Governance Identity Manager server to StealthBits resource.

Architecture of the adapter

The StealthBits resource uses Microsoft SQL server to store collected data.

The StealthBits GDPR Adapter queries an SQL server that is configured with StealthBits to fetch all GDPR data such as users, groups, folder, files, and taxonomy. The Security Directory Integrator database connector (JDBC) is used for SQL database access.

The following diagram shows the various components that work together to complete user management tasks in a Security Directory Integrator environment.

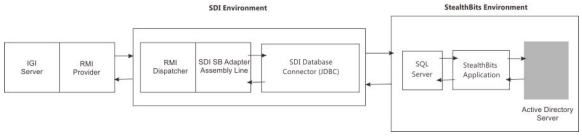


Figure 1. The architecture of the StealthBits GDPR Adapter

Chapter 2. Planning

Plan and prepare to install and configure the adapter by understanding and completing the following tasks.

Prerequisites

Verify that your environment meets the software and hardware requirements for the adapter.

Ensure that you install the adapter on the same workstation as the Security Directory Integrator server.

Table 1. Prerequisites to install the adapter

Prerequisite	Description
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM® Security Directory Integrator Version 7.2 + FP3 or later **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	IBM Security Identity Governance and Intelligence server Version 5.2.3
StealthBits specific requirements	StealthAudit Version 8.0. StealthBits jobs must be scheduled to reflect updated information in SQL database. StealthBits GDPR adapter requires an SQL `Login Account` with administrative privileges on SQL database that is configured with StealthBits. StealthBits User Guide can be downloaded from the following website. https://www.stealthbits.com.
Updated information in MS SQL database that is configured with StealthBits	StealthBits uses Microsoft SQL Server to store collected data. StealthBits Adapter will query SQL server configured against StealthBits to fetch information. StealthBits jobs must be scheduled to have updated information in SQL Database. For more information, see Chapter 6, “GDPR reports overview,” on page 21.

Table 1. Prerequisites to install the adapter (continued)	
Prerequisite	**Description**
Network Connectivity	Install the adapter on a workstation that can communicate with the service through the TCP/IP network.
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for IBM Security Verify Adapters. For more information, see the *Dispatcher Installation and Configuration Guide*.
Install the MS SQL JDBC driver	The Stealthbits Adapter's SDI Assembly Line must connect to the MS SQL Server that is configured with Stealthbits. 1. Download the JDBC driver from the Microsoft page: https://www.microsoft.com/en-us/download. 2. Extract the downloaded package. 3. Depending on the version of the SDI, (jre7 or jre8) navigate to `\sqljdbc_6.0.8112.200_enu \sqljdbc_6.0\enu\jre#` to retrieve the corresponding `sqljdbc*` jar file. 4. Copy the `sqljdbc*` jar file to `SDI_HOME/jars/3rdparty/others`.

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Table 2. Required information to install the adapter

Required information	Description	Value

Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains adapter JAR files. For example, the `jars/connectors` subdirectory contains the JAR file for the UNIX adapter.	If Security Directory Integrator is automatically installed with your Identity server product, the default directory path for Security Directory Integrator is as follows:
		Windows:
		• For Directory Integrator version 7.1.1:
		drive`\Program Files\IBM\TDI\V7.1.1`
		• For Directory Integrator version 7.2:
		drive`\Program Files\IBM\TDI\V7.2`
		UNIX:
		• For Directory Integrator version 7.1.1:
		`/opt/IBM/TDI/V7.1.1`
		• For Directory Integrator version 7.2:
		`/opt/IBM/TDI/V7.2`

Table 2. Required information to install the adapter (continued)		
Required information	**Description**	**Value**
Adapters solution directory	When you install the dispatcher, the installer prompts you to specify a file path for the solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory is at: Windows: • For Directory Integrator version 7.1.1: *drive*\Program Files \IBM\TDI \V7.1.1*isimsoln* • For Directory Integrator version 7.2: *drive*\Program Files \IBM\TDI\V7.2*isimsoln* UNIX: • For Directory Integrator version 7.1.1: /opt/IBM/TDI/V7.1.1/ *isimsoln* • For Directory Integrator version 7.2: /opt/IBM/TDI/V7.2/ *isimsoln*

Chapter 3. Installing

All IBM Security Directory Integrator-based adapters require the Dispatcher for the adapters to function correctly. Download the Dispatcher installer from the IBM Passport Advantage website. For more information about the installation, see the Dispatcher Installation and Configuration Guide.

If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded.

Install the Dispatcher

You must install the RMI Dispatcher, if this is the first Security Directory Integrator-based adapter installation

Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter. Download the installer from IBM Passport Advantage. For more information about the installation, see the Dispatcher Installation and Configuration Guide.

If the RMI Dispatcher is already installed for another adapter, you do not need to reinstall it.

Importing the adapter profile

You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Before you begin

- The Identity server is installed and running.
- You have administrator authority on the Identity server.
- The file to be imported must be a Java™ archive (JAR) file. The `<Adapter>Profile.jar` file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.

About this task

Target definition files are also called adapter profile files. The profile definition files are provided with the various IBM Security Verify Adapter. The adapter profile must be imported because it defines the types of resources that the Verify Governance Identity Manager server can manage.

The adapter profile definition file is used to create a target profile on the Verify Governance Identity Manager server and to establish communication with the adapter. If the adapter profile is not imported, you cannot create a connector for that adapter type.

An upload error might occur when no file is selected, or when the file is empty, or due to any upload operation error, such as a timeout or connection error. If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a connector with the adapter profile or open and account on the service. You must import the adapter profile again.

This task can be completed from the Enterprise Connectors module in the Administration Console. To import an adapter target profile, complete these steps:

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.

4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Profile**.
   b) Click **Browse** to locate the JAR file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported a profile.
7. Click **Close**.
   The new profile is displayed in the list of profiles.

Results

The upload is synchronous but has a timeout. The progress bar on the **Import** page accurately indicates the upload status. However, when a timeout is reached, the following message occurs: "The import is still in progress and will complete shortly. Close this window to proceed." If you see that message, allow a few minutes for the upload to complete and for the profile to be available.

What to do next

After the target profile is imported successfully, complete these tasks.

- Import the attribute mapping file. See "Importing attribute mapping file" on page 8.
- Create a connector that uses the target profile. See "Adding a connector" on page 10.

Importing attribute mapping file

After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

About this task

This task involves importing an account attribute mapping definition file, which is included in the adapter package. The imported file must be a DEF file.

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Attribute Mapping**.
   b) Click **Browse** to locate the attribute mapping file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported the file.
7. Click **Close**.

Bulk loading

The business activities must be defined in IBM Security Verify Governance Identity Manager before permissions can be mapped to a business activity. Verify Governance Identity Manager provides an option to bulk load business activities.

Importing activities with bulk upload

User a bulk upload file to load business activities.

Procedure

1. Log in to the IBM Security Verify Governance Identity Manager Administration Console.
2. On the **Access Risk Controls** tab, select **Tools** > **Bulk Data Load**.
3. Click **Insert Activities Hierarchy** and upload the **IGI Bulk Load Activities File**, `Insert+Activities+Hierarchy_GDPR.xlsx`.
4. Refresh the operation until it is complete.

Contents of Activities Bulk Load file

The file format is the pre-determined format of the bulk load files in Identity server.

Table 3.

Information	Description	Validation
CODE	Activity code	Mandatory
ACTIVITY	Activity name	Mandatory
ENVIRONMENT	Environment identifier name	Optional
DESCRIPTION	Activity description	Optional
PARENT_CODE	Activity parent code	Optional

The **ENVIRONMENT** field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used (Working Environment).

The **CODE** and **ACTIVITY** fields contain the activity code and name, respectively. The existence of an activity with the given code is verified. If the given name does not match the activity name, the row is skipped. If there is no such activity, it is inserted.

The **PARENT_CODE** field is used for positioning the activity in the hierarchy. If this field is left blank, the activity is inserted as a child of the root activity. If there is no such activity associated to the given parent code, the activity is inserted as a child of a technical activity called "Undefined", which is created as needed.

The table shows a sample of the bulk load file:

	A	B	C	D	E
1	**CODE**	**ACTIVITY**	**ENVIRONMENT**	**DESCRIPTION**	**PARENT_CODE**
2	**GDPR**	**GDPR**			**Root**
3	**42**	**Credit Cards**			**GDPR**
4	**74**	**Passwords**			**GDPR**

Adding a connector

After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

About this task

The connectors consolidate, extract, and reconcile user identities, organization units, permissions, and user entitlements with the most common enterprise applications. Configure a connector to keep the Access Governance Core repository synchronized with the target system.

This task can be completed from the Enterprise Connectors module in the Administration Console.

Procedure

To add a connector, complete these steps.

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions** > **Add**.
   The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:
   a) Assign a name and description for the connector.
   b) Select the target profile type as `Identity Brokerage` and its corresponding target profile.
   c) Select the entity, such as **Account** or **User**.
      Depending on the connector type, this field might be preselected.
   d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.
      The available trace levels are DEBUG, INFO, and ERROR.
   e) Optional: Select **History ON** to save and track the connector usage.
   f) Click **Save**.
      The fields for enabling the channels for sending and receiving data are now visible.
   g) Select and set the connector properties in the **Global Config** accordion pane.
      For information about the global configuration properties, see Global Config accordion pane.
   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

The connector is saved and added to the list of connectors in the **Connectors** pane.

If you cannot create a connector with the target profile or open an account on an existing connector, the target profile was not installed correctly during the import. You must import the target profile again.

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager. For more information, see “Enabling connectors” on page 11.

Enabling connectors

After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Before you begin

Table 4. Prerequisites for enabling a connector	
Prerequisite	**Find more information**
A connector must exist in Verify Governance Identity Manager.	"Adding a connector" on page 10.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 12.

Procedure

To enable a connector, complete these steps:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

   Enable write-to channel
   Propagates every change in the Access Governance Core repository into the target system.

   For connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

   Enable read-from channel
   Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

   For HR feed connectors, only the check box for enabling the read-from channel is available.

   Enable reconciliation
   Synchronizes the modified data between the Access Governance Core repository and the target system.

Results

The connector is enabled.

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager.

Reviewing and setting channel modes for each new connector

Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

About this task

Note: Legacy Verify Governance Identity Manager Enterprise connectors use `Reconciliation` channel, whereas Identity Brokerage Enterprise connectors use `Read From Channel` and `Change Log Sync`.

For more information about any of tasks in the following steps, see the IBM® Security Identity Governance and Intelligence product documentation.

Procedure

To enable the read-from and write-to channels, and to set the change log synchronization schedule for each new connector, complete these steps in Verify Governance Identity Manager V5.2.3:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

      Enable write-to channel
      Propagates every change in the Access Governance Core repository into the target system.

      Enable read-from channel
      Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

      Enable reconciliation
      Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor** > **Change Log Sync Status**.

   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
   b) Select a connector, and click **Actions** > **Sync Now**.

      The synchronization process begins.
   c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.

      Information about the synchronization is displayed in the **Sync History** tab.
10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:
    a) Select **Manage** > **Connectors**.

b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.

c) Click **Save**.

For more information, see "Enabling connectors" on page 11.

For Identity Brokerage connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

For Identity Brokerage HR feed connectors, only the check box for enabling the read-from channel is available.

12. Start the connector by selecting **Monitor** > **Connector Status**. Select the connector that you want to start, and then select **Actions** > **Start**.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

About this task

This task involves an account attribute mapping definition file, which is included in the adapter package.

The file consists of Verify Governance Identity Manager account attributes and their equivalent attributes in the managed target. The file is structured as *<IGI_attribute> = <target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<target_attribute>* of `eraccount`.

Some *<IGI_attribute>* do not have a defined *<target_attribute>* and you can assign the mapping. For example:

```
USER_TYPE=USER_TYPE
ATTR1=ATTR1
```

Note:

- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.
- It might take up to 10 minutes for the attribute mapping changes to take effect once the file is imported.

Procedure

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.
3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Verify Governance Identity Manager attribute values.
   a) `[conversion].<target_attribute>.<IGI_attribute> = [<target_attribute_value1>=<IGI_attribute_value1>;...;`
   b) *<target_attribute_valuen>=<IGI_attribute_valuen>*
4. For attributes that contains date and time, use the following syntax to convert its values.
   For example,
   a) `[conversion.date].erbirthDate.BIRTHDAY=[yyyyMMdd=dd/MM/yyyy HH:mm:ss]`
   b) `[conversion.date].ACCOUNT_EXPIRY_DATE.ACCOUNT_EXPIRY_DATE=`
   c) `[dd/MM/yyyy HH:mm:ss=dd/MM/yyyy HH:mm:ss]`
5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.

Service or target form details

You must create a user account for the adapter on the managed resource. Provide the account information when you create a managed target for the adapter on IBM Security Identity Governance and Intelligence.

StealthBits GDPR adapter requires an SQL `Login Account` with administrative privileges on SQL database that is configured with StealthBits.

The **StealthBits Service** tab describes the service details and the attributes to specify to establish a remote connection to StealthBits database from the Security Directory Integrator.

Table 5. Attributes for an adapter target

Attribute	Description	Required attribute?
Name	Specify a name that defines the adapter connector on Identity Governance and Intelligence server.	Yes
Description	Specify a description that identifies the connector for your environment.	No
Security Directory Integrator location	Specify the URL for the Security Directory Integrator instance. The valid syntax for the URL is `rmi://ip-address:port/ITDIDispatcher` where `ip-address` is the Security Directory Integrator host and `port` is the port number for the RMI Dispatcher. The default URL is `rmi://localhost:1099/ITDIDispatcher`.	Yes
StealthBits SQL HostName	SQL Server Host Name that is configured against StealthBits Application.	Yes
StealthBits SQL Port	Port number on which SQL Server is listening.	Yes
StealthBits SQL Database	StealthBits SQL Database that is configured with StealthBits. For more information, see Chapter 6, “GDPR reports overview,” on page 21.	Yes

Table 5. Attributes for an adapter target (continued)		
Attribute	**Description**	**Required attribute?**

Taxonomy Mapping File Path	A property file path that contains mapping between `CriteriaName` and `CriteriaID`. For example, `C://TDI7.2//taxonomy.properties`. A property file sample data:
	`##############################`
	`Birth Records=10`
	`Credit Cards=20`
	`Passwords=30`
	`US SSN=40`
	`##############################`
	If file path is not specified, then the adapter use `CriteriaID` values from StealthBits.
		No

Administrator Name	Sign on to the database by using this user name.	Yes
Password	A user password that is used to sign on.	Yes

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Procedure

1. Test the connection for the service that you created on the Identity server.
2. Run a full reconciliation from the Identity server.
3. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
4. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Chapter 4. Troubleshooting

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Error messages and problem solving

You might encounter some problems at run time. Use this information to resolve some of these common runtime problems.

Table 6. Runtime problems

Warning or error message	**Corrective action**
An error occurred while establishing communication with the Security Directory Integrator server.	Identity and Governance Intelligence server cannot establish a connection with Security Directory Integrator. To fix this problem, ensure that: • Security Directory Integrator is running. • The URL specified on the service form for Security Directory Integrator is correct.
CTGDIJ109E Unable to connect to the database. Login failed for user.	Verify that correct login credentials are specified.
CTGDIJ109E Initialize Error. Unable to connect to the database.	Verify the connection properties. Make sure that an instance of SQL Server is running on the host and accepting TCP/IP connections at the port. Make sure that TCP connections to the port are not blocked by a firewall.
Cannot open database that is requested by the login.	Verify that the database name is correctly specified.

Chapter 5. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables.

Adapter attributes and object classes

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network. After you install the adapter profile, the StealthBits GDPR Adapter supports a standard set of attributes.

Attributes in `erSBIGIAccount` object class

Table 7. Supported attributes in `erSBIGIAccount` object class

Attribute	Adapter attribute	Description	Single or Multi-value	Data type	Required attribute?
SamAccountName	eruid	Login name that is used to log in to the system.	Single	String	Yes
PrincipalId	erSBAccPrincipalID	Principal identifier for a user.	Single	Number	No
CN	Cn	Common name	Single	String	No
Mail	mail	Email address of a user.	Single	String	No
DomainName	erSBAccDomain	A short domain name of the current domain.	Single	String	No
Groups	erSBAccGroups	A user is a member of these groups.	Multi-value	String	No
Folders	erSBAccFolders	A user has direct access to these folders.	Multi-value	String	No
Files	erSBAccFiles	Users have permissions for these files that contain sensitive data.	Multi-value	String	No

Attributes in `erSBIGIGroup` object class

Table 8. Supported attributes in `erSBIGIGroup` object class

Attribute	Adapter attribute	Description	Single or Multi-value	Data type	Required attribute?
SamAccountName	erSBGrpSamAccName	Login name that is used to log in to the system.	Single	String	Yes
PrincipalID	erSBGrpPrincipalID	Principal identifier for a group.	Single	String	Yes
Cn	erSBGrpCommonName	Common name	Single	String	No
Description	erSBGrpDesc	A group description.	Single	String	No
DomainName	erSBGrpDomainName	A short domain name of the current domain.	Single	String	No
GroupType	erSBGrpType	A type of a group object.	Single	String	No
GroupScope	erSBGrpScope	Global, Universal, or Local.	Single	String	No
Folders	erSBGrpFolders	Groups to which, a group has permissions.	Multi-value	String	No
Files	erSBGrpFiles	Files to which, a group has permissions.	Multi-value	String	No

Attributes in `erSBIGIFolder` object class

Table 9. Supported attributes in `erSBIGIFolder` object class

Attribute	Adapter attribute	Description	Single or Multi-value	Data type	Required attribute?
ID	erSBFolderID	Unique identifier of the share or folder.	Single	String	Yes

Table 9. Supported attributes in `erSBIGIFolder` object class (continued)					
Attribute	**Adapter attribute**	**Description**	**Single or Multi-value**	**Data type**	**Required attribute?**
Name	erSBFolderName	Name of the share or folder.	Single	String	Yes
Path	erSBFolderPath	UNC path to the resource.	Single	String	No
Owner	erSBFolderOwner	Unique identifier of an owner.	Single	String	No
Files	erSBFolderFiles	A folder that contains these files, which have sensitive data.	Multi-value	String	No
Host	erSBFolderHost	Host name of a folder.	Single	String	No

Attributes in `erSBIGIFile` object class

Table 10. Supported attributes in `erSBIGIFile` object class					
Attribute	**Adapter attribute**	**Description**	**Single or Multi-value**	**Data type**	**Required attribute?**
FileName	erSBFileName	Display name of a file that is returned based on specific criteria.	Single	String	Yes
ResourceID	erSBFileID	An identifier for a file.	Single	String	No
NetworkPath	erSBFileNwPath	Full path to the file that is returned based on specific criteria.	Single	String	No
HostName	erSBFIleHostName	Host name of the file system.	Single	String	No
CriteriaName	erSBFileCriteriaName	Name of criteria type (type of sensitive data) that is found.	Multi-value	String	No
CriteriaNumber	erTaxonomyCriteria	An identifier of a criteria.	Multi-value	String	No

Chapter 6. GDPR reports overview

The StealthBits resource uses Microsoft SQL server to store collected data.

The StealthBits GDPR Adapter runs a query on SQL server that is configured with StealthBits to fetch all GDPR data such as users, groups, folder, files, and taxonomy.

StealthBits jobs and scheduling

StealthBits jobs must be scheduled to reflect updated information in the SQL database.

StealthBits jobs

Active Directory Inventory job set

The Active Directory Inventory job set is designed to provide essential user and group membership details to several StealthAUDIT built in solution sets. Key information includes manager, email addresses, and direct membership. The SQL scripting analysis module provides views of the tables that are created in the database. User inventory details are stored in `SA_ADInventory_Users` table, group membership inventory details are stored in `SA_ADInventory_GroupMembers` table, and group inventory details are stored in the `SA_ADInventory_Groups` table. The analysis module automatically references these tables for use with other StealthAUDIT generated tables.

FileSystem job set

The FileSystem Solution Set contains jobs that are configured to interrogate multiple aspects of your infrastructure. Categories within this job set include `Content`, `Activity`, `Permissions`, `Broken Inheritance`, `Probable Owner`, and `Open Access` among others. The Access Information Center Web Console retrieves its data from this set. This solution set is compatible against Microsoft® File Systems, NetApp® Filers, EMC® Celerra, and other windows compatible file sharing systems.

By default all jobs are configured to extract information from the top-most level unless designated within the job descriptions. The extraction scope for each query can be rehomed as necessary to streamline job run time or to audit only the systems or folders of interest.

Scheduling StealthBits Jobs

To schedule an action such as job discovery query or inventory query, complete the following steps:

1. Right-click the corresponding item.
2. From the context menu, select **Schedule**.

Host management

The `Host Management` container helps to discover and manage your hosts. Go to host management to create host lists based on host discovery queries that you define and view the host information.

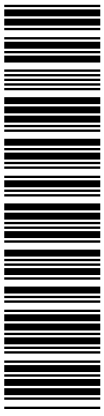
Host discovery

The `Discovery` container helps to create and manage host discovery queries. Host discovery queries provide you a control over how hosts are discovered on your network.

Host inventory

The `All Hosts` container provides a consolidated view of all your hosts. This container displays hosts that are generated by host discovery queries and individual host lists that you created.

Part Number: 99F1234
Product Number: 1234-SS1



BA21-8475-00