Solix EDMS Data Masking Standard Edition (SE) 2.2

Quick Reference

SOLIX®

Empowering Data Management

Copyrights

Trademarks

Table of Content

1 Solix EDMS Data Masking Standard Edition (SE)

Solix EDMS Data Masking Standard Edition (SE) ensures data security and compliance by masking sensitive data in test databases using several masking algorithms. At the same time, the referential integrity of the data is maintained to keep the application testing process seamless.

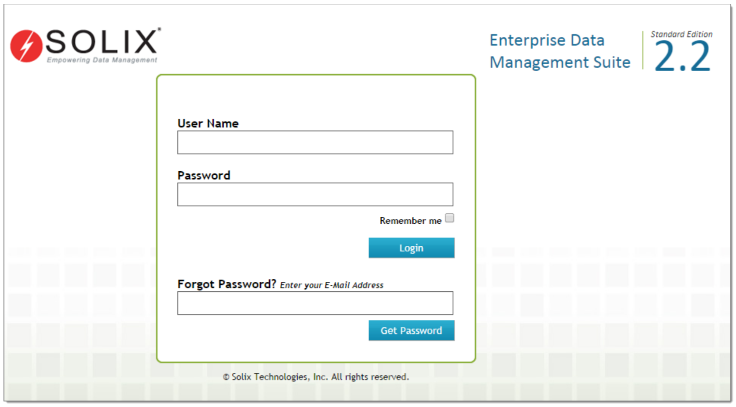
1.1 Benefits of Solix EDMS Data Masking Standard Edition (SE)

- Supports compliance with privacy legislation & policies.
- Increases protection against data theft.
- Access to data can be regulated based on user types (for example, internal users and external users).
- Provides realistic data for testing, development, training, outsourcing, data mining/research, etc.
- Enables off-site and cross-border software development and data sharing.
- Provides ability to secure the confidential and sensitive data in organizations based on standard compliance.
- Enables to preview the sample of masked data before masking the original data in the database during execution.
- Provides feasibility to view the data in the table before and after the data masking process is accomplished.

- Current version of Solix EDMS Data Masking Standard Edition (SE) supports Oracle Database (9i, 10g, and 11g), SQL Server (2005 and 2008) and Sybase ASE (15.5).
- Solix EDMS Data Masking Standard Edition (SE) does not support special data types such as "'BLOB','CLOB','LONG','LONG RAW', 'RAW', 'BFILE', 'XML', 'IMAGE', 'BINARY', 'VARBINARY', 'BIT', 'BINARY_FLOAT', 'BINARY_DOUBLE', 'NCLOB', 'TEXT', 'NTEXT', 'UNITEXT' etc.

1.2 Startup Solix EDMS Standard Edition (SE) Application

Once the Solix EDMS Standard Edition (SE) software is installed successfully, access the application to perform data masking process. To access Solix EDMS Standard Edition (SE), enter the respective URL = http://<ip address>:9090/edms/ in the address bar. The ***Login*** screen for initiating the authentication process will be displayed as shown in the figure below.


SOLIX
Empowering Data Management
Enterprise Data
Management Suite
Standard Edition
2.2
User Name
Password
Remember me □
Login
Forgot Password? Enter your E-Mail Address
Get Password
© Solix Technologies, Inc. All rights reserved.

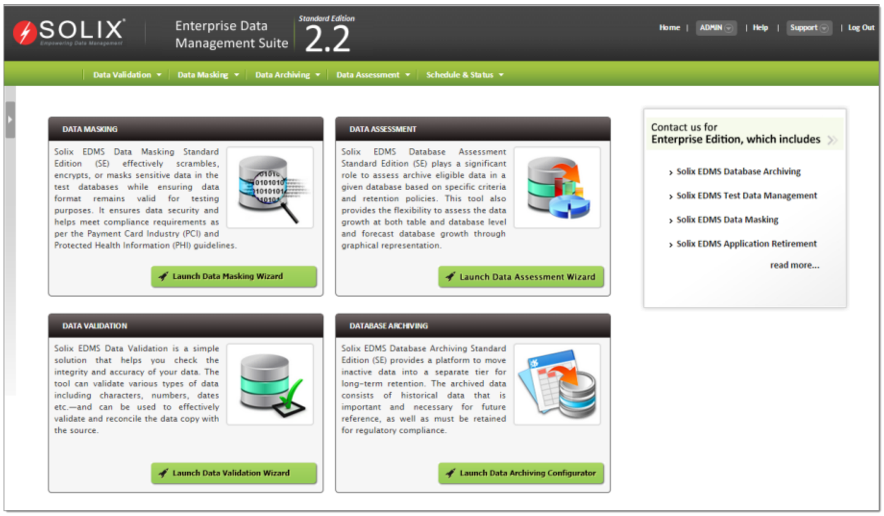
To login to the application, enter the authenticated user name and password provided by the Solix Delivery team.

For example,

User Name**:** ***ADMIN***

Password**:** ***ADMIN***

1. Click ***Login*** to access ***Solix EDMS Standard Edition (SE).***
2. On successful login, the ***Solix EDMS Standard Edition (SE)*** home screen appears as shown in the figure below.


SOLIX
Empowering Data Management
Enterprise Data
Management Suite
Standard Edition
2.2
Home | ADMIN | Help | Support | Log Out
Data Validation
Data Masking
Data Archiving
Data Assessment
Schedule & Status
DATA MASKING
Launch Data Masking Wizard
DATA ASSESSMENT
Launch Data Assessment Wizard
DATA VALIDATION
Launch Data Validation Wizard
DATABASE ARCHIVING
Launch Data Archiving Configurator
Contact us for
Enterprise Edition, which includes
› Solix EDMS Database Archiving
› Solix EDMS Test Data Management
› Solix EDMS Data Masking
› Solix EDMS Application Retirement
read more...

Solix EDMS Data Masking Standard Edition (SE) effectively scrambles, encrypts, or masks sensitive data in the test databases while ensuring data format remains valid for testing purposes. It ensures data security and helps meet compliance requirements as per the Payment Card Industry (PCI) and Protected Health Information (PHI) guidelines.

Solix EDMS Database Assessment Standard Edition (SE) plays a significant role to assess archive eligible data in a given database based on specific criteria and retention policies. This tool also provides the flexibility to assess the data growth at both table and database level and forecast database growth through graphical representation.

Solix EDMS Data Validation is a simple solution that helps you check the integrity and accuracy of your data. The tool can validate various types of data including characters, numbers, dates etc.—and can be used to effectively validate and reconcile the data copy with the source.

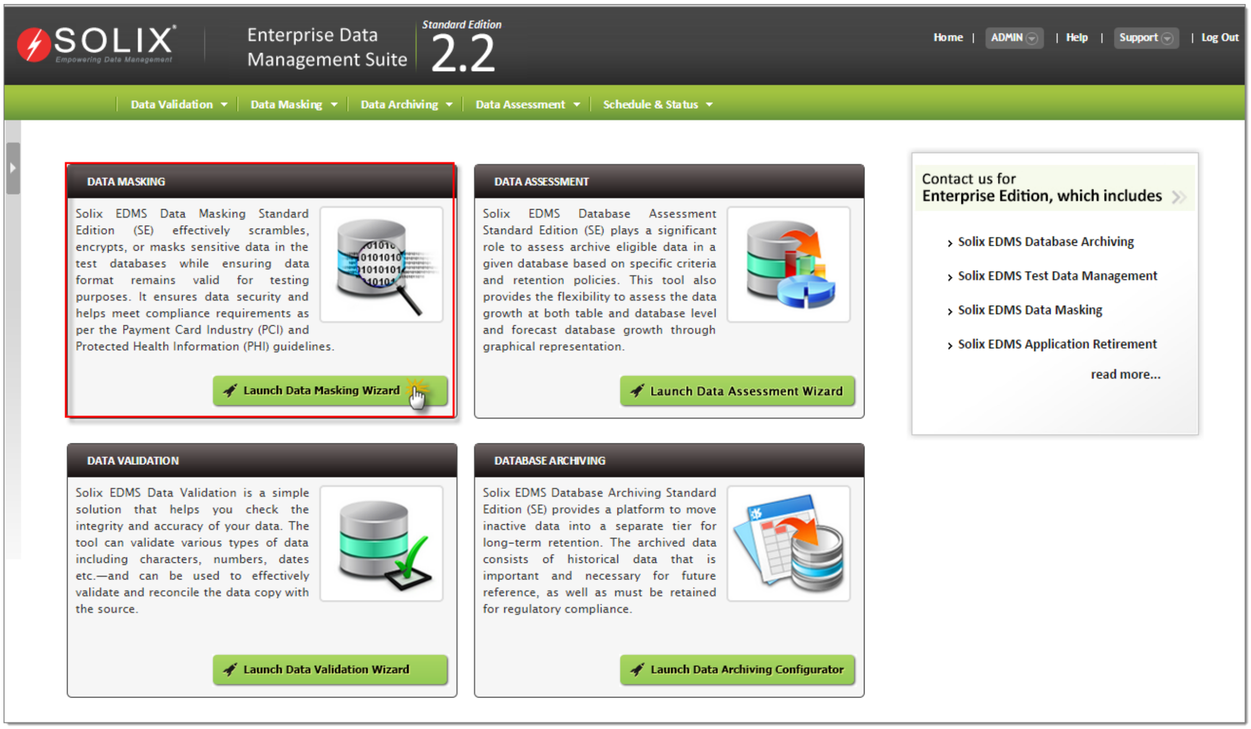
Solix EDMS Database Archiving Standard Edition (SE) provides a platform to move inactive data into a separate tier for long-term retention. The archived data consists of historical data that is important and necessary for future reference, as well as must be retained for regulatory compliance.

- Username and password are case sensitive.
- Based on the privileges authenticated to the login user, the authorized features will populate in the home screen respectively.

2 Data Masking process using Wizard

Solix EDMS Data Masking Standard Edition (SE) Wizard has been designed to provide an intuitive user friendly environment. The user is led through a step-by-step process to perform all the activities required to accomplish the data masking process efficiently.

This section outlines the procedure to setup a connection, setup tables to extract the required data for masking, setup security rule assignments to apply on the selected tables, setup run-time parameter and run the data masking process to mask the data effectively.


SOLIX
Empowering Data Management
Enterprise Data Management Suite
Standard Edition
2.2
Home | ADMIN | Help | Support | Log Out
Data Validation
Data Masking
Data Archiving
Data Assessment
Schedule & Status
Launch Data Masking Wizard
Launch Data Assessment Wizard
Launch Data Validation Wizard
Launch Data Archiving Configurator
read more...

DATA MASKING

Solix EDMS Data Masking Standard Edition (SE) effectively scrambles, encrypts, or masks sensitive data in the test databases while ensuring data format remains valid for testing purposes. It ensures data security and helps meet compliance requirements as per the Payment Card Industry (PCI) and Protected Health Information (PHI) guidelines.

DATA ASSESSMENT

Solix EDMS Database Assessment Standard Edition (SE) plays a significant role to assess archive eligible data in a given database based on specific criteria and retention policies. This tool also provides the flexibility to assess the data growth at both table and database level and forecast database growth through graphical representation.

Contact us for
Enterprise Edition, which includes

- Solix EDMS Database Archiving
- Solix EDMS Test Data Management
- Solix EDMS Data Masking
- Solix EDMS Application Retirement

DATA VALIDATION

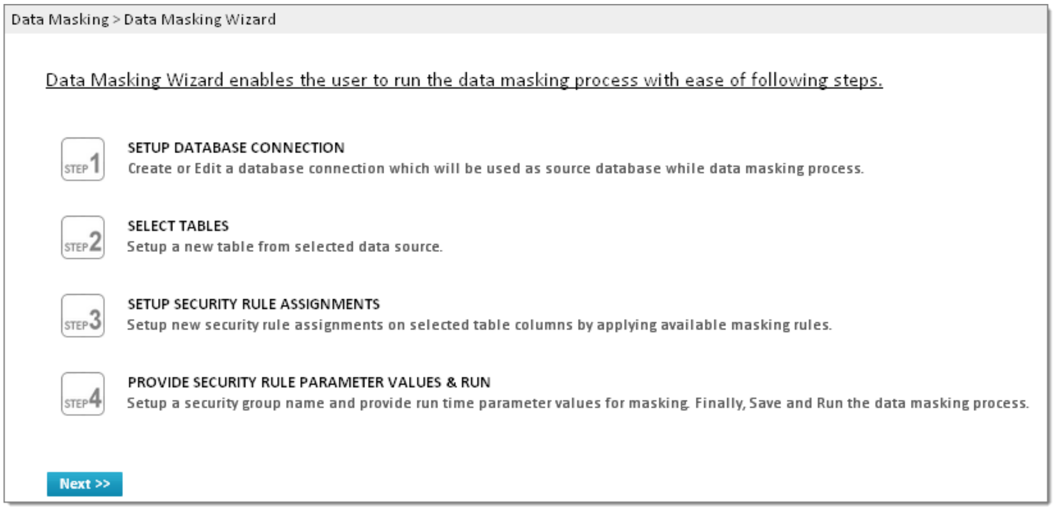
Solix EDMS Data Validation is a simple solution that helps you check the integrity and accuracy of your data. The tool can validate various types of data including characters, numbers, dates etc.—and can be used to effectively validate and reconcile the data copy with the source.

DATABASE ARCHIVING

Solix EDMS Database Archiving Standard Edition (SE) provides a platform to move inactive data into a separate tier for long-term retention. The archived data consists of historical data that is important and necessary for future reference, as well as must be retained for regulatory compliance.

To initiate the data masking process,

- In Solix EDMS Standard Edition (SE) home page, click ***Launch Data Masking Wizard*** button adjacent to the Data Masking**.** By default, the ***Data Masking Wizard*** initial screen will be displayed which depicts the summary of each step designed to accomplish the data masking process successfully.



Data Masking > Data Masking Wizard

Data Masking Wizard enables the user to run the data masking process with ease of following steps.

STEP 1 SETUP DATABASE CONNECTION
Create or Edit a database connection which will be used as source database while data masking process.

STEP 2 SELECT TABLES
Setup a new table from selected data source.

STEP 3 SETUP SECURITY RULE ASSIGNMENTS
Setup new security rule assignments on selected table columns by applying available masking rules.

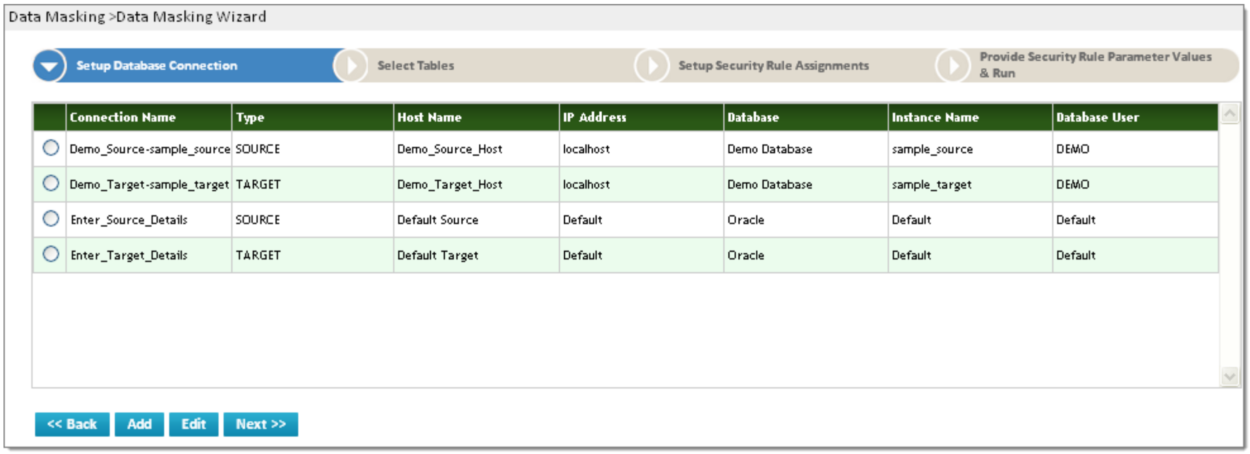
STEP 4 PROVIDE SECURITY RULE PARAMETER VALUES & RUN
Setup a security group name and provide run time parameter values for masking. Finally, Save and Run the data masking process.

Solix EDMS Data Masking Standard Edition (SE) Wizard provides feasibility to run the data masking process and mask the data in the database with ease of four steps given below.

1. Setup Database Connection
1. Select Tables
2. Setup Security Rule Assignments
3. Provide Security Rule Parameter Values & Run

2.1 Setup Database Connection

In step 1, the user needs to configure the database connection to provide accessibility to the database. This section illustrates the process to configure the connection details in order to connect to the database and accomplish the data masking process effectively.



Data Masking >Data Masking Wizard

Setup Database Connection
Select Tables
Setup Security Rule Assignments
Provide Security Rule Parameter Values & Run

	Connection Name	Type	Host Name	IP Address	Database	Instance Name	Database User
○	Demo_Source-sample_source	SOURCE	Demo_Source_Host	localhost	Demo Database	sample_source	DEMO
○	Demo_Target-sample_target	TARGET	Demo_Target_Host	localhost	Demo Database	sample_target	DEMO
○	Enter_Source_Details	SOURCE	Default Source	Default	Oracle	Default	Default
○	Enter_Target_Details	TARGET	Default Target	Default	Oracle	Default	Default

To setup the database connection for data masking, do the following:

1. In ***Data Masking Wizard*** initial screen, click ***Next*** button to initiate the data masking process and navigates to the first step in the wizard. The ***Setup Database Connection*** screen with the list of existing database connections will be displayed and provides the ability to create/edit connections.

- If the required database connection already exists, then the user can navigate to the second step by clicking ***Next*** button.

2. To create a new database connection, do the following:

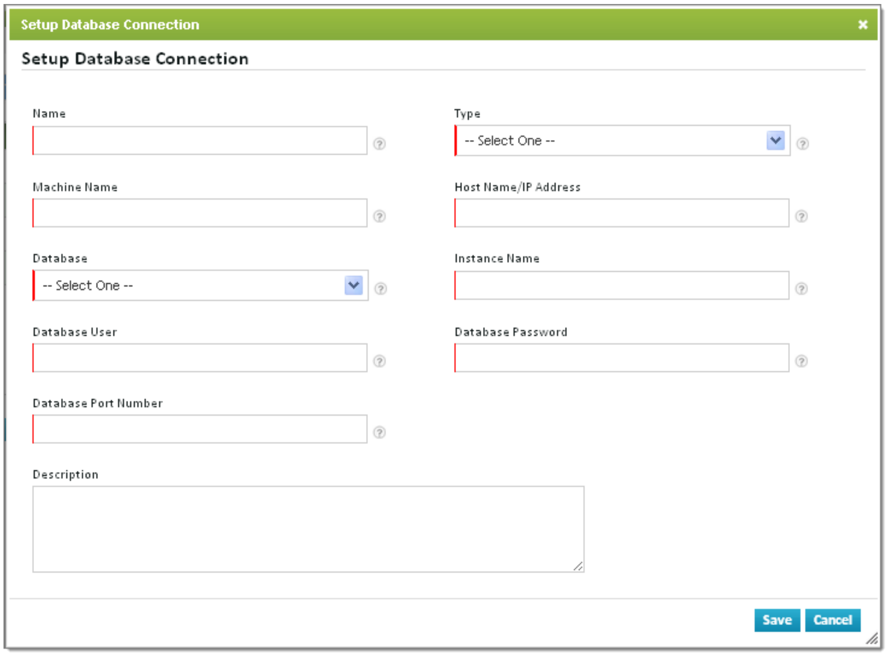
   a. Click ***Add*** button (or) Hover on any existing database connection, the three links (Create Like, New and Edit) will appear to create/edit the database connection.

      - ***Create Like*** – enables the user to create a replica of the selected database connection. The same connections details are maintained It is recommended to define a new name for the replica.

      - ***Create*** - enables the user to create a new database connection.

      - ***Edit -*** enables the user to edit the details of an existing database connection.

   b. The ***Setup Database Connection*** popup window is displayed. A new database connection can be created here as shown in the figure below.



i. Enter the name of the database connection in the ***Name*** text field.

ii. Select an appropriate datasource type from the ***Type*** drop down list and designate the database as a source or target.

iii. Enter the database server name associated to the datasource in the ***Machine Name*** text field.

iv. Enter the host name/ IP address associated to the database server in the ***Host Name/ IP Address*** text field.

v. Select the database which is compatible to the datasource from the ***Database*** (such as Oracle, Demo database) drop down list.

vi. Enter the instance name/service name of the database in the ***Instance Name*** text field.

vii. Enter the login user name of the database in ***Database User*** text field.

viii. Enter the password corresponding to the username of the database in ***Database Password*** text field.

ix. Enter the port number of the database in the ***Database Port Number*** field.

x. Enter the comments in the ***Description*** text box**.**

xi. Click ***Save*** button. Once the database connection details are saved successfully, a confirmation message is prompted in the ***Setup Database Connection*** screen.

3. Once database connection setup is completed successfully, click ***Next*** button. The ***Select Tables*** screen to select the table(s) for data masking will be displayed.

- The fields marked as * are mandatory fields.
- User has provided flexibility to hover on the existing database connection in order to create a replica of existing database connection (i.e., using ***Create like***) and recommended to define a new name for the replica of database connection.
- Ensure that the specified databases are accessible and running.
- To navigate to ***Setup Database Connection*** screen from the ***Setup Database Connection*** popup window, click ***Cancel*** button.

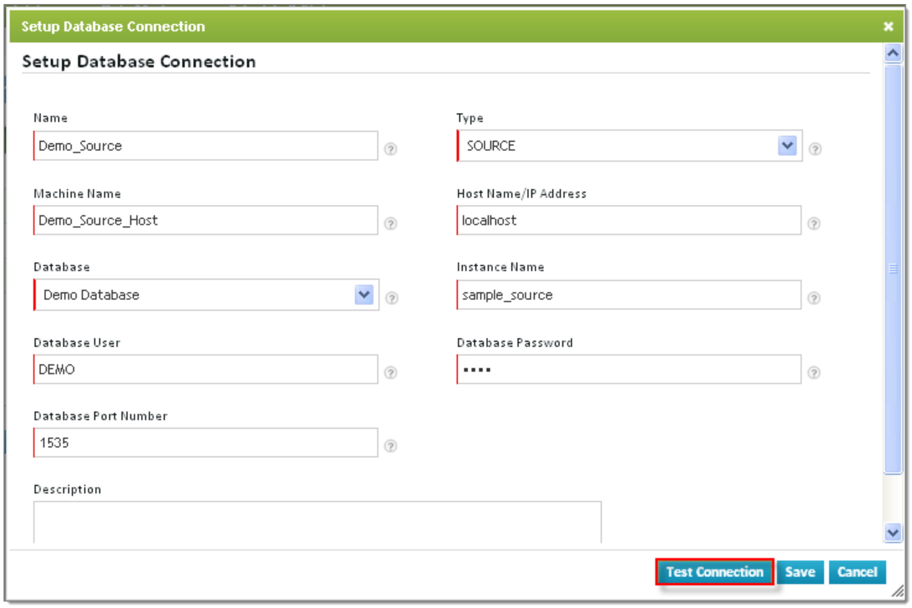
2.1.1 Create Like, Editing or Testing the database connections

Test Connection feature is designed to provide feasibility to verify whether the connection details specified during database connection creation are valid.

To test the database connection, do the following:

1. In ***Setup Database Connection*** screen, hover on the database connection the needs to be verified. The three links (Create Like, New and Edit) will appears beneath the database connection.

2. Click ***Create Like or Edit*** button, to verify the connection details of the database connection. The ***Setup Database Connection*** popup window is prompted to edit /create a replica of the database connection as shown in the figure below.



Setup Database Connection

Name: Demo_Source

Type: SOURCE

Machine Name: Demo_Source_Host

Host Name/IP Address: localhost

Database: Demo Database

Instance Name: sample_source

Database User: DEMO

Database Password: ••••

Database Port Number: 1535

Description:

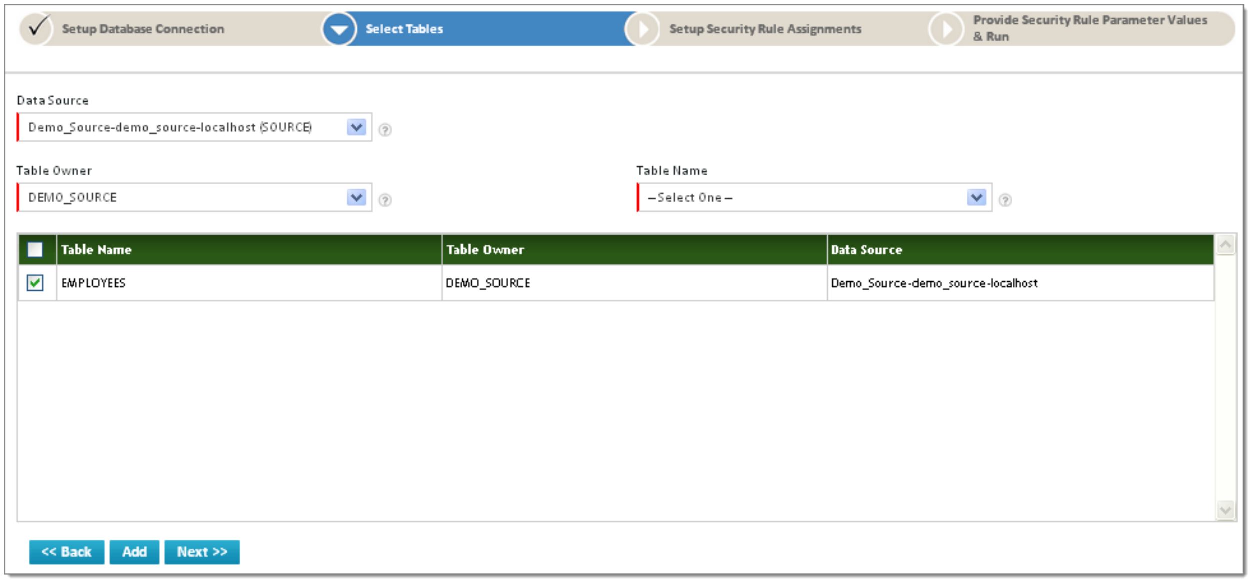
3. Once the database connection details are saved successfully, in order to test the connection to the database based on the given details, click ***Test Connection*** button.

    - If the database is connected successfully, a message stating the successful connection to the database will be prompted.
    - If the database connection fails, an alert message to verify the given connection details will be prompted.

- The fields marked as ▌are mandatory fields.
- To create a replica of database, click ***Create Like*** link. In ***Setup Database Connection*** enter the name of the replica in the ***Name*** text field.

2.2 Select Tables

Once the database connection setup is completed successfully the user needs to select table(s) from the database to perform data masking process effectively.


Setup Database Connection
Select Tables
Setup Security Rule Assignments
Provide Security Rule Parameter Values & Run
<< Back
Add
Next >>

Data Source
Demo_Source-demo_source-localhost (SOURCE)

Table Owner
DEMO_SOURCE

Table Name
--Select One--

□	Table Name	Table Owner	Data Source
☑	EMPLOYEES	DEMO_SOURCE	Demo_Source-demo_source-localhost

To select the intended table, do the following:

1. In ***Select Tables*** screen, select the database from the ***Source Database*** drop down list. Based on the database selected, the corresponding schemas/table owners will be listed in the ***Table Owner*** drop down list.

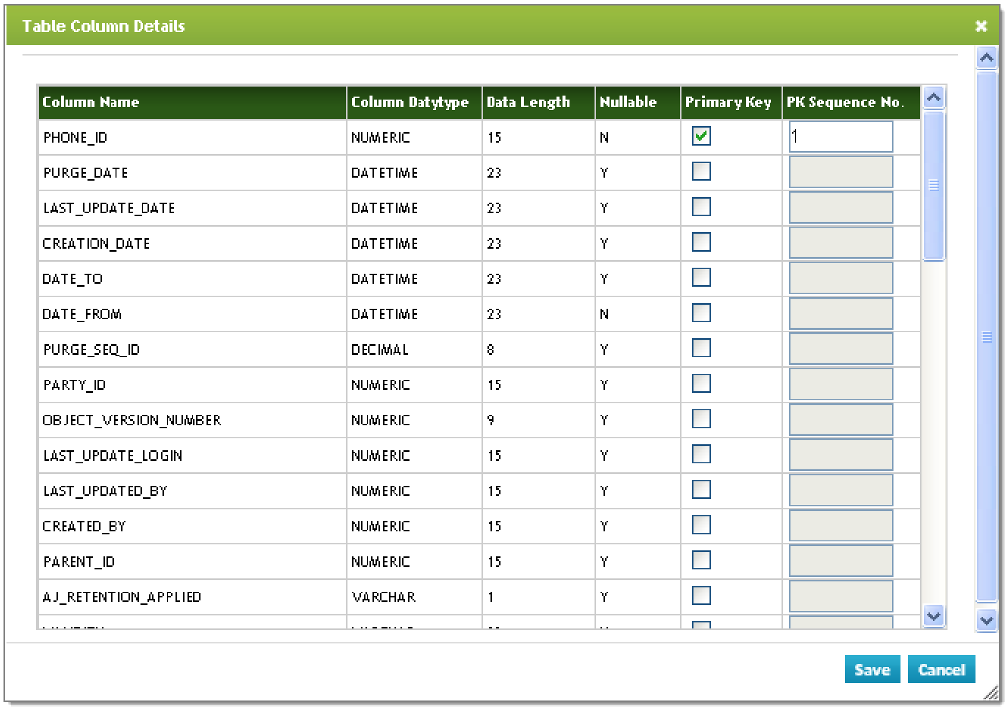
2. Select a schema/table owner from the ***Table Owner*** drop down list. Based on the schema/table owner selected, the corresponding tables will be listed in the Table Name drop down list.

3. Select the intended table from the ***Table Name*** drop down list.

4. Click ***Add*** button, to save and append the selected table information to the list. Once the information is saved successfully, a message stating "***New Table Saved Successfully"*** is prompted on the screen and the respective table information will be appended to the list.

   - To view the columns that exist in the table, do the following:

a. Hover on the table name in the list and click ***Column*** link. The ***Table Column Details*** popup window depicts the columns and comprehensive information of the column such as data type, data length as shown in the figure below.

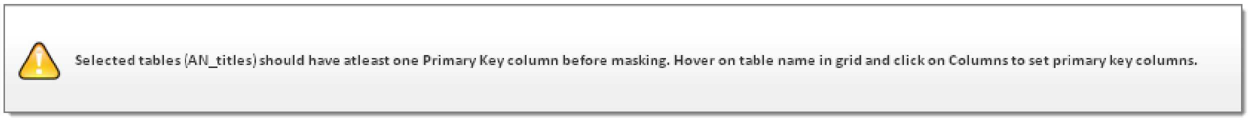


Column Name	Column Datytype	Data Length	Nullable	Primary Key	PK Sequence No.
PHONE_ID	NUMERIC	15	N	☑	1
PURGE_DATE	DATETIME	23	Y	☐	
LAST_UPDATE_DATE	DATETIME	23	Y	☐	
CREATION_DATE	DATETIME	23	Y	☐	
DATE_TO	DATETIME	23	Y	☐	
DATE_FROM	DATETIME	23	N	☐	
PURGE_SEQ_ID	DECIMAL	8	Y	☐	
PARTY_ID	NUMERIC	15	Y	☐	
OBJECT_VERSION_NUMBER	NUMERIC	9	Y	☐	
LAST_UPDATE_LOGIN	NUMERIC	15	Y	☐	
LAST_UPDATED_BY	NUMERIC	15	Y	☐	
CREATED_BY	NUMERIC	15	Y	☐	
PARENT_ID	NUMERIC	15	Y	☐	
AJ_RETENTION_APPLIED	VARCHAR	1	Y	☐	

b. Click ***Cancel*** button, to exit the popup window.

5. Click ***Next*** button, to navigate to the next step. The ***Setup Security Rule Assignments*** screen appears to configure an appropriate security rule on the column of the selected table to perform data masking process accordingly.

- The fields marked as * are mandatory fields.
- While performing data masking in other Oracle database (such as SQL Server, Sybase ASE and Demo database), it is mandatory that the table(s) selected must have alteast one Primary key column in a table. In case, if the table(s) selected does not have primary key column then the user will be restricted to proceed further and a warning message will be prompted as shown in the figure below.



Selected tables (AN_titles) should have atleast one Primary Key column before masking. Hover on table name in grid and click on Columns to set primary key columns.

2.3 Setup Security Rule Assignments

This step enables the user to assign an appropriate security rule on the required column of the selected table and mask the data that exist in the column based on the security rule applied.

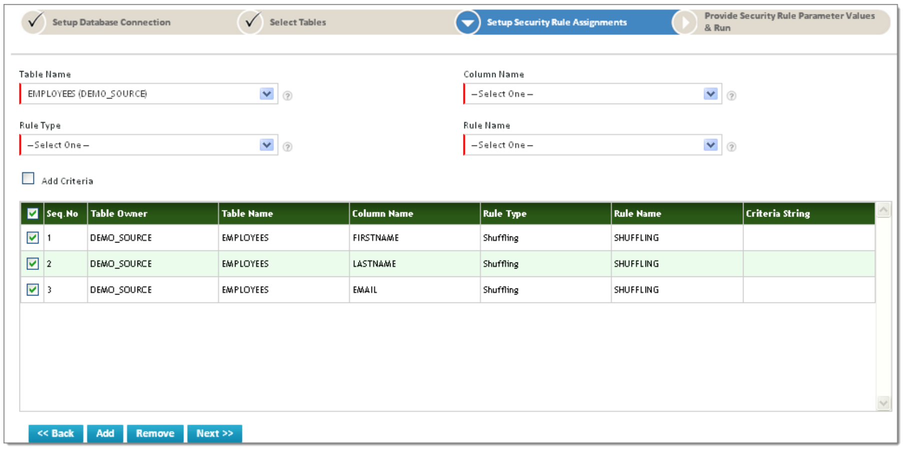

Setup Database Connection
Select Tables
Setup Security Rule Assignments
Provide Security Rule Parameter Values & Run
<< Back
Add
Remove
Next >>

Table Name: EMPLOYEES (DEMO_SOURCE)

Column Name: --Select One--

Rule Type: --Select One--

Rule Name: --Select One--

☐ Add Criteria

☑	Seq.No	Table Owner	Table Name	Column Name	Rule Type	Rule Name	Criteria String
☑	1	DEMO_SOURCE	EMPLOYEES	FIRSTNAME	Shuffling	SHUFFLING	
☑	2	DEMO_SOURCE	EMPLOYEES	LASTNAME	Shuffling	SHUFFLING	
☑	3	DEMO_SOURCE	EMPLOYEES	EMAIL	Shuffling	SHUFFLING	

To setup security rule assignment, do the following:

1. Select a table from the ***Table Name*** drop down list, to extract the columns of the selected table.

2. Select a column from the ***Column Name*** drop down list, to apply the security rule on the selected column while masking**.**

3. Select an appropriate masking method from the ***Rule Type*** drop down list.

4. Based on the column data type and rule type selected, the corresponding security rules will be displayed in the ***Rule Name*** drop down list. Select an appropriate security rule from the list, to perform masking based on the algorithm defined in the security rule**.**

   For example,

   - If table column of ***Numeric*** type and rule type as ***Masking Data*** is selected, then the security rule associated to Masking and numeric data type will be displayed. (For example, Random Number (Numeric)).

5. To customize a criterion for the respective security rule assignment, select check box adjacent to the ***Add Criteria*** check box. Automatically, the ***Criteria*** text box will appear on the screen.

   - Enter the custom SQL statement in the ***Criteria*** text box to assign security rule on the data extracted based on the criteria exclusively.

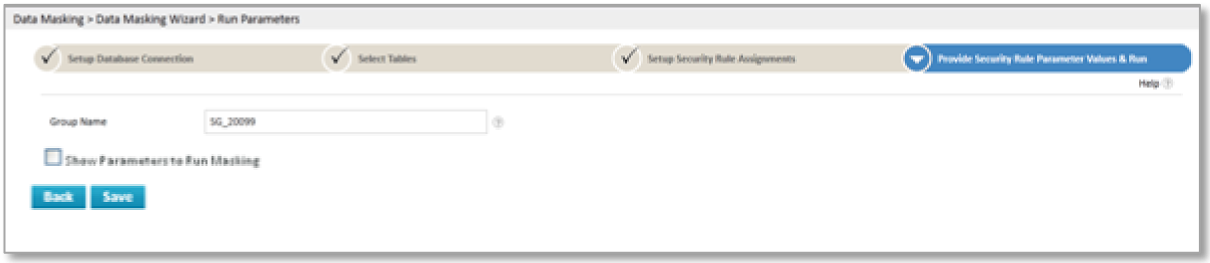
6. Click ***Add*** button to save and append the configured security rule assignment in the list. Once the security rule is assigned successfully, a message stating "***Security Rule Assignment Saved Successfully"*** is prompted on the screen.

7. Click ***Next*** button, to navigate to the next step to accomplish the data masking process. The security group name will be automatically generated for the respective security rule assignment in the ***Provide Security Rule Parameter Values & Run*** screen.

- The fields marked as | are mandatory fields.
- For each application/database, the total number of masking columns is restricted to only '**10**' in Solix EDMS Data Masking Standard Edition (SE).
- Exclusively, for table columns of ***Character*** type, the security rules of all the data types(i.e., character, Numeric and Date) and corresponding rule type will be displayed irrespectively.
- While masking a huge data, it is recommended to assign/setup the security rule assignment in the Security Rule Assignment screen (***Settings*** > ***Data Masking*** > ***Security Rule Assignment***). And, define the commit frequency and parallel thread to perform data masking process on the huge data efficiently. In such cases, the tables been registered in the Solix EDMS Data Masking Standard Edition (SE) Wizard will be populated automatically in the Security Rule Assignment screen to carry out the data masking process.

2.4 Provide Security Rule Parameter Values & Run

Once the security rule assignment is configured successfully, the security group name will be automatically generated for the respective security rule assignment in the ***Provide Security Rule Parameter Values & Run*** screen. This enables the user to provide the parameter value and preview the sample of masked data before executing the data masking process effectively.



Data Masking > Data Masking Wizard > Run Parameters

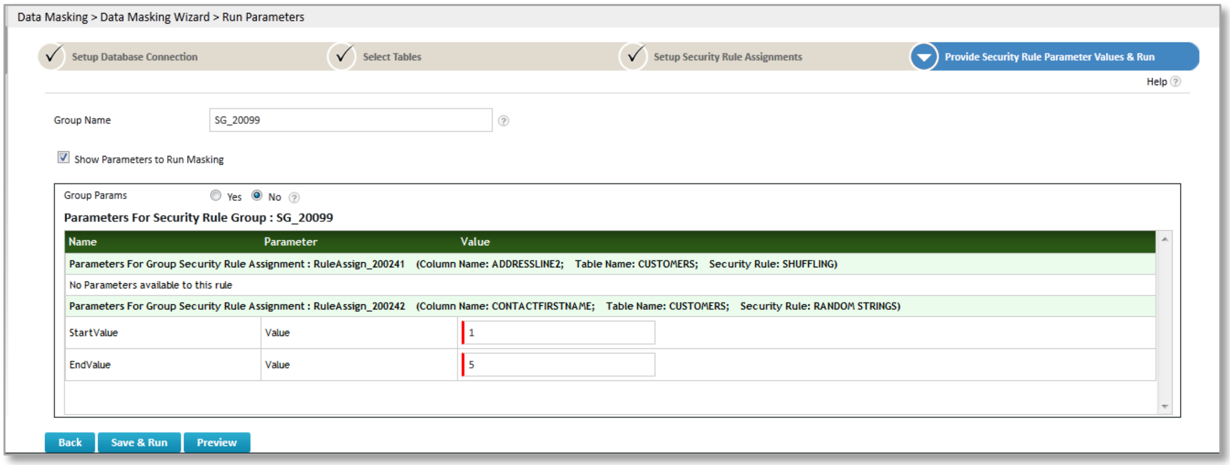
✓ Setup Database Connection
✓ Select Tables
✓ Setup Security Rule Assignments
Provide Security Rule Parameter Values & Run
Help

Group Name: SG_20099

□ Show Parameters to Run Masking

To save and execute the data masking process, do the following:

1. Select check box adjacent to the ***Show Parameters to Run Masking*** to enter the value of the parameter. Based on the security rule assignment, the run-time parameters will be prompted on the screen as shown in the figure below.



Data Masking > Data Masking Wizard > Run Parameters

✓ Setup Database Connection
✓ Select Tables
✓ Setup Security Rule Assignments
Provide Security Rule Parameter Values & Run
Help

Group Name: SG_20099

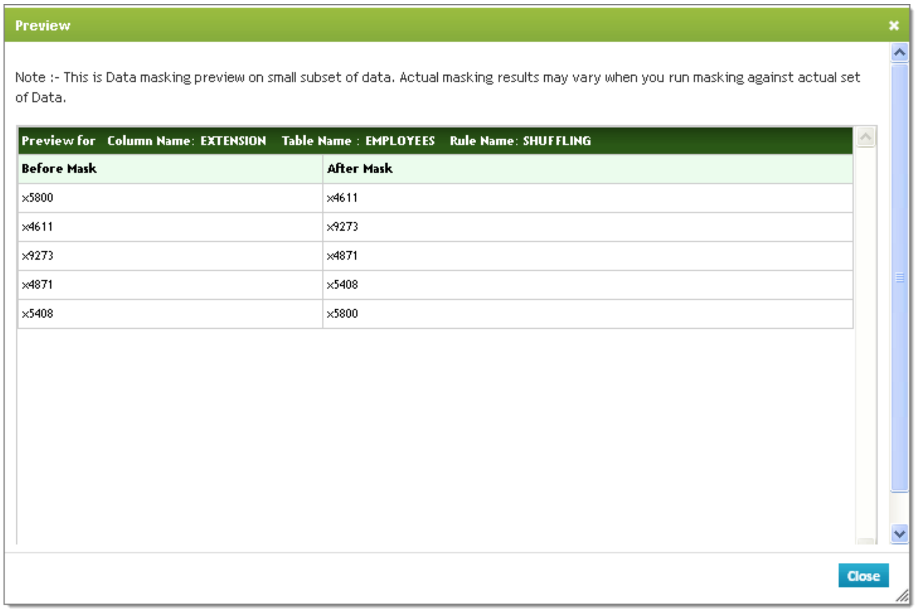
☑ Show Parameters to Run Masking

Group Params ○ Yes ● No

Parameters For Security Rule Group : SG_20099

Name	Parameter	Value
Parameters For Group Security Rule Assignment : RuleAssign_200241 (Column Name: ADDRESSLINE2; Table Name: CUSTOMERS; Security Rule: SHUFFLING)		
No Parameters available to this rule		
Parameters For Group Security Rule Assignment : RuleAssign_200242 (Column Name: CONTACTFIRSTNAME; Table Name: CUSTOMERS; Security Rule: RANDOM STRINGS)		
StartValue	Value	1
EndValue	Value	5

2. To enter the single value for a group of parameters at a time, select ***Yes*** option adjacent to the ***Group Params***. (Or) select ***No*** option, to enter the value of the parameters individually.
3. Enter the value of the parameters in the corresponding fields.
    - To view the sample of masked data before masking the original data, do the following:
        a. Click ***Preview*** button. The ***Preview*** popup window will be prompted which depicts the data of all the tables before and after masking as shown in the figure below.



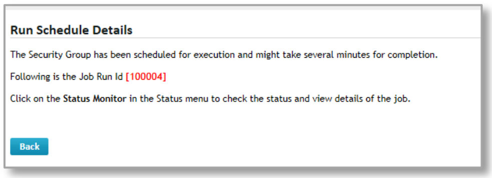
Note :- This is Data masking preview on small subset of data. Actual masking results may vary when you run masking against actual set of Data.

Preview for Column Name: EXTENSION Table Name : EMPLOYEES Rule Name: SHUFFLING

Before Mask	After Mask
x5800	x4611
x4611	x9273
x9273	x4871
x4871	x5408
x5408	x5800

        b. Click ***Close*** button, to navigate to the ***Run Parameters*** screen.

4. Click ***Save & Run*** button to save and execute the security group accordingly. Once the security group is executed successfully, automatically a Run ID is generated for the respective job in ***Run Schedule Details*** screen.



Run Schedule Details

The Security Group has been scheduled for execution and might take several minutes for completion.

Following is the Job Run Id [100004]

Click on the **Status Monitor** in the Status menu to check the status and view details of the job.

5. To monitor the status and view the details of the job, click Run ID or navigate to the ***Status Monitor*** screen (***Schedule & Status>Status Monitor***).

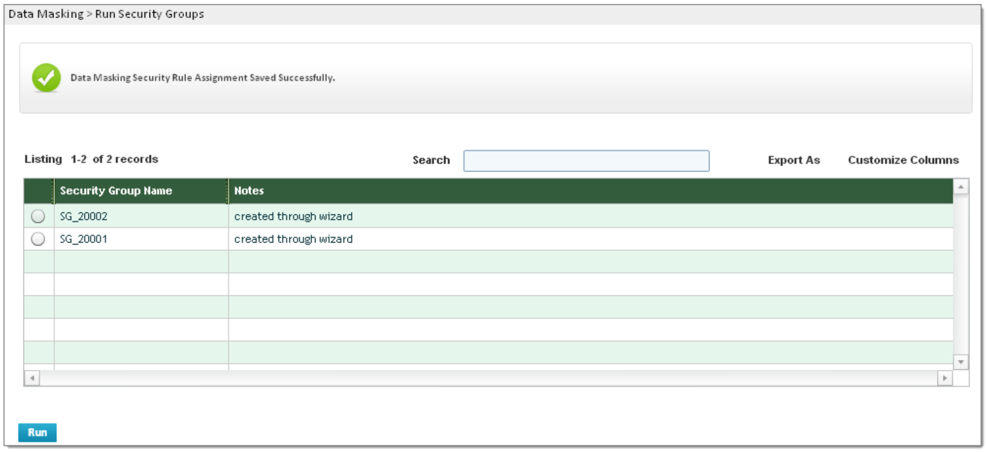
- The fields marked as * are mandatory fields.
- Based on the rule type and rule of the security rule assignment, the parameter will be initialized in the security group.

- To limit the rows in the preview results, set the value of mask preview rows count in ***MASK_PREVIEW_ROWS*** parameter in the ***Parameter*** screen. For example, to limit the rows to 10 then set the default value of mask preview rows count in ***MASK_PREVIEW_ROWS*** parameter to "10". Henceforth, the Preview results screen will display 10 mask preview records exclusively.

2.4.1 To Save Security group and execute it later

To save the security group and execute it later, do the following

1. In ***Provide Security Rule Parameter Values & Run*** screen, click ***Save*** button, to save the security group and append it in the ***Security Groups*** screen. The tool automatically navigates to the ***Run Security Groups (Data Masking > Run Security Groups)*** screen and a message stating "***Data Masking Security Rule Assignment Saved Successfully***" is prompted on the screen as shown in the figure below.

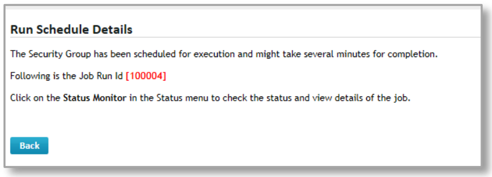


✓ Data Masking Security Rule Assignment Saved Successfully.

Listing 1-2 of 2 records

	Security Group Name	Notes
○	SG_20002	created through wizard
○	SG_20001	created through wizard

2. Select the intended security group and click ***Run*** button, to execute the security group for data masking process. Once the security group is executed successfully, automatically a Run ID is generated for the respective job in ***Run Schedule Details*** screen.



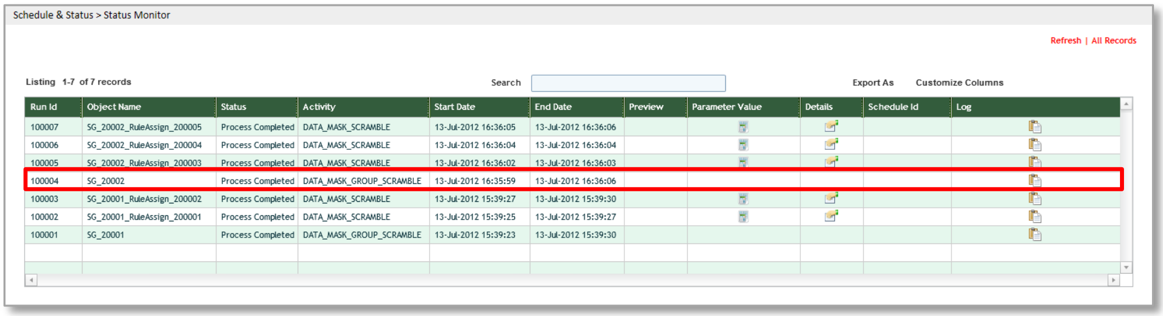
Run Schedule Details

The Security Group has been scheduled for execution and might take several minutes for completion.

Following is the Job Run Id [100004]

Click on the **Status Monitor** in the Status menu to check the status and view details of the job.

3. To monitor the status and view the details of the job, click Run ID or navigate to the ***Status Monitor*** screen (***Schedule & Status>Status Monitor***).

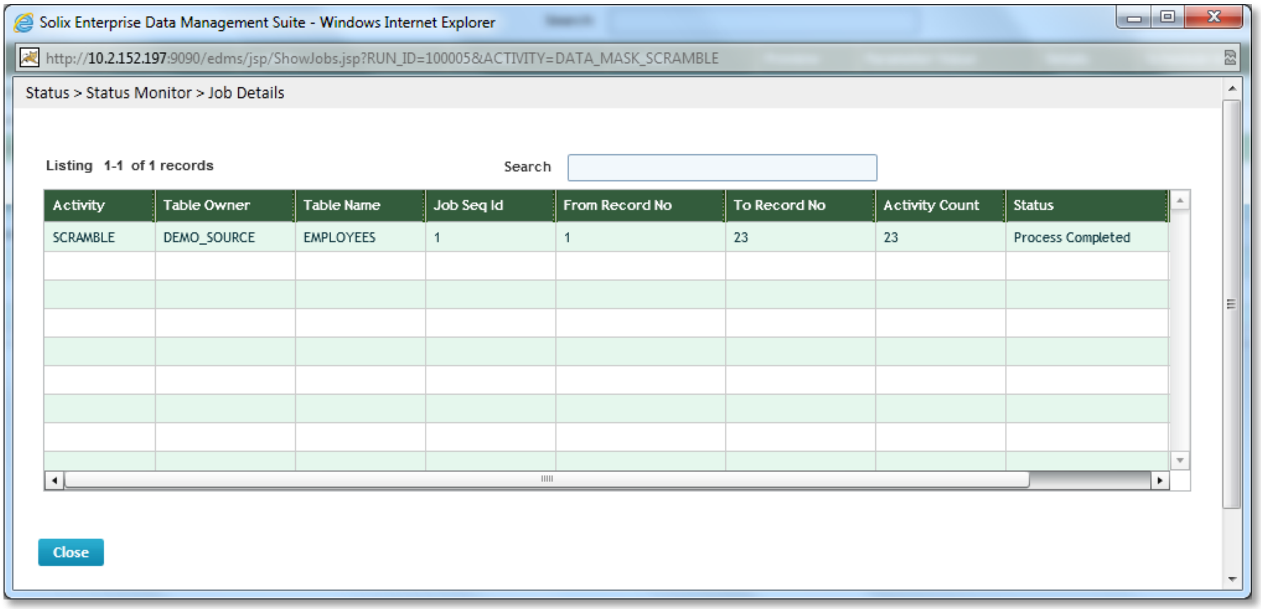


Schedule & Status > Status Monitor

Listing 1-7 of 7 records

Run Id	Object Name	Status	Activity	Start Date	End Date	Preview	Parameter Value	Details	Schedule Id	Log
100007	SG_20002_RuleAssign_200005	Process Completed	DATA_MASK_SCRAMBLE	13-Jul-2012 16:36:05	13-Jul-2012 16:36:06					
100006	SG_20002_RuleAssign_200004	Process Completed	DATA_MASK_SCRAMBLE	13-Jul-2012 16:36:04	13-Jul-2012 16:36:04					
100005	SG_20002_RuleAssign_200003	Process Completed	DATA_MASK_SCRAMBLE	13-Jul-2012 16:36:02	13-Jul-2012 16:36:03					
100004	SG_20002	Process Completed	DATA_MASK_GROUP_SCRAMBLE	13-Jul-2012 16:35:59	13-Jul-2012 16:36:06					
100003	SG_20001_RuleAssign_200002	Process Completed	DATA_MASK_SCRAMBLE	13-Jul-2012 15:39:27	13-Jul-2012 15:39:30					
100002	SG_20001_RuleAssign_200001	Process Completed	DATA_MASK_SCRAMBLE	13-Jul-2012 15:39:25	13-Jul-2012 15:39:27					
100001	SG_20001	Process Completed	DATA_MASK_GROUP_SCRAMBLE	13-Jul-2012 15:39:23	13-Jul-2012 15:39:30					

4. To view the job details, click Details icon adjacent to the Run ID. The Job Details screen will be displayed as shown in the figure below.



Solix Enterprise Data Management Suite - Windows Internet Explorer

http://10.2.152.197:9090/edms/jsp/ShowJobs.jsp?RUN_ID=100005&ACTIVITY=DATA_MASK_SCRAMBLE

Status > Status Monitor > Job Details

Listing 1-1 of 1 records

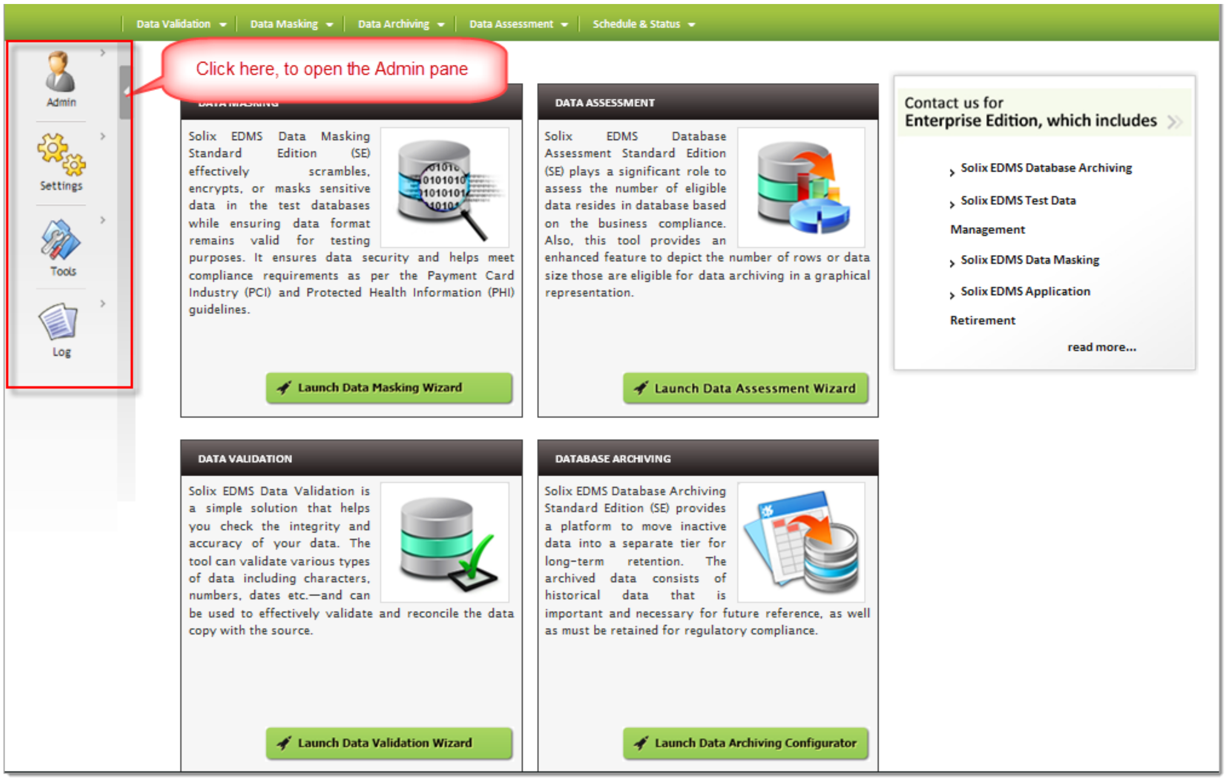
Activity	Table Owner	Table Name	Job Seq Id	From Record No	To Record No	Activity Count	Status
SCRAMBLE	DEMO_SOURCE	EMPLOYEES	1	1	23	23	Process Completed

- The fields marked as * are mandatory fields.

2.4.2 View Data

View Data feature provides an option to view the data existing in the table or extracted using custom SQL. Also, it provides flexibility to view the data before and after the data masking process to verify whether the data has been masked appropriately or not.

To access view data, click bar appears on the left hand side of the screen. Once the bar is clicked, the administrative menus will be opened as shown in the picture below.


Data Validation
Data Masking
Data Archiving
Data Assessment
Schedule & Status
Admin
Settings
Tools
Log
Click here, to open the Admin pane
Launch Data Masking Wizard
Launch Data Assessment Wizard
Launch Data Validation Wizard
Launch Data Archiving Configurator
read more...

DATA MASKING

Solix EDMS Data Masking Standard Edition (SE) effectively scrambles, encrypts, or masks sensitive data in the test databases while ensuring data format remains valid for testing purposes. It ensures data security and helps meet compliance requirements as per the Payment Card Industry (PCI) and Protected Health Information (PHI) guidelines.

DATA ASSESSMENT

Solix EDMS Database Assessment Standard Edition (SE) plays a significant role to assess the number of eligible data resides in database based on the business compliance. Also, this tool provides an enhanced feature to depict the number of rows or data size those are eligible for data archiving in a graphical representation.

Contact us for
Enterprise Edition, which includes

- Solix EDMS Database Archiving
- Solix EDMS Test Data Management
- Solix EDMS Data Masking
- Solix EDMS Application Retirement

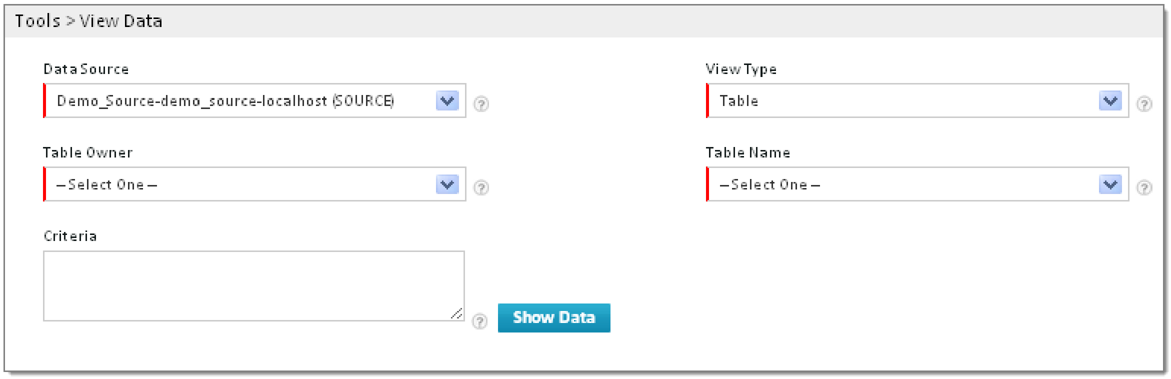
DATA VALIDATION

Solix EDMS Data Validation is a simple solution that helps you check the integrity and accuracy of your data. The tool can validate various types of data including characters, numbers, dates etc.—and can be used to effectively validate and reconcile the data copy with the source.

DATABASE ARCHIVING

Solix EDMS Database Archiving Standard Edition (SE) provides a platform to move inactive data into a separate tier for long-term retention. The archived data consists of historical data that is important and necessary for future reference, as well as must be retained for regulatory compliance.

1. Navigate to the following path: ***Tool*** > ***View Data***. The ***View Data*** screen will be displayed and it enables the user to view the data in the table.



Tools > View Data

Data Source: Demo_Source-demo_source-localhost (SOURCE)

View Type: Table

Table Owner: – Select One –

Table Name: – Select One –

Criteria:

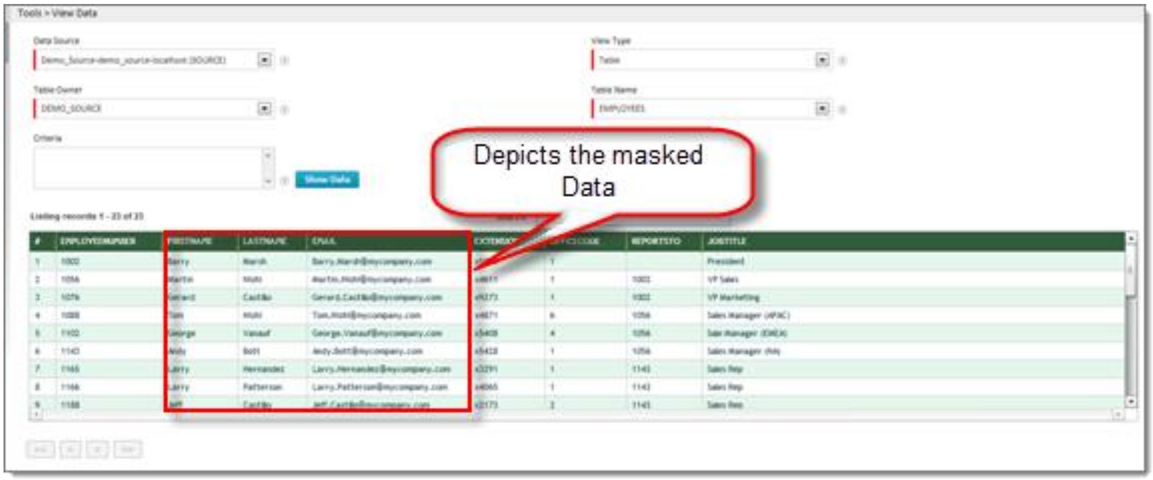
2. Select database from the ***Source Database*** drop down list.

3. Select an appropriate option (i.e., Table or Custom SQL) from the ***View Type*** drop down list.

   - ***Table*** – enables the user to show all the data exist in the table.

- ***Custom SQL*** – enables the user to customize SQL statement to extract the data from the table and show the data extracted based on the specified SQL statement.

4. If ***Table*** option is selected, select appropriate information associated to the intended table in the corresponding fields (such as table owner and table name) and click ***Show Data*** button. The data (including masked data) in the table will be displayed beneath the fields as shown in the figure below.



Tools > View Data

Data Source: Demo_Source-demo_source-localhost (SOURCE)

View Type: Table

Table Owner: DEMO_SOURCE

Table Name: EMPLOYEES

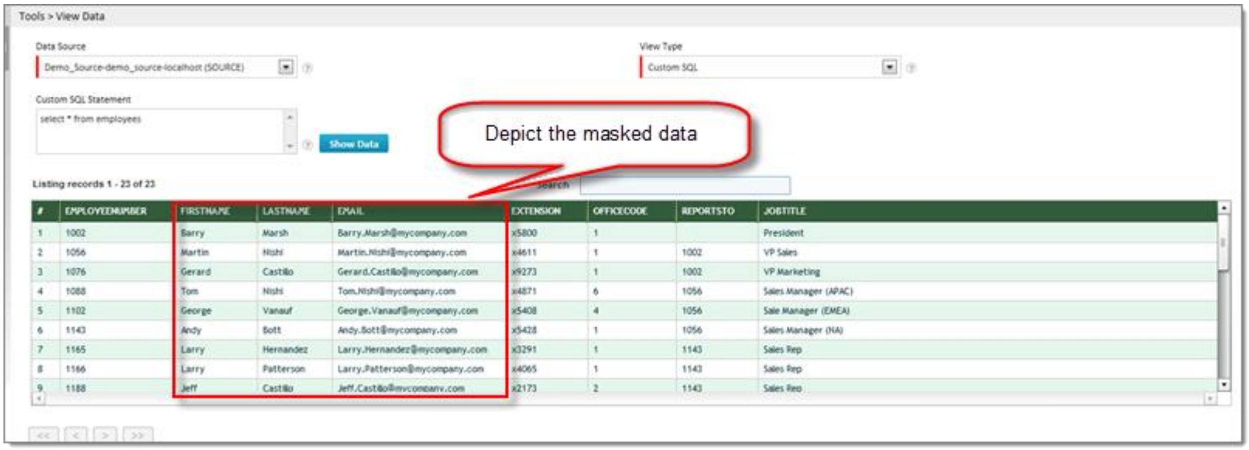
Criteria:

Depicts the masked Data

Listing records 1 - 23 of 23

#	EMPLOYEENUMBER	FIRSTNAME	LASTNAME	EMAIL	EXTENSION	OFFICECODE	REPORTSTO	JOBTITLE
1	1002	Barry	Marsh	Barry.Marsh@mycompany.com	[illegible]	1		President
2	1056	Martin	Mishi	Martin.Mishi@mycompany.com	x4611	1	1002	VP Sales
3	1076	Gerard	Castillo	Gerard.Castillo@mycompany.com	x9273	1	1002	VP Marketing
4	1088	Tom	Mishi	Tom.Mishi@mycompany.com	x4871	6	1056	Sales Manager (APAC)
5	1102	George	Vanauf	George.Vanauf@mycompany.com	x5408	4	1056	Sale Manager (EMEA)
6	1143	Andy	Bott	Andy.Bott@mycompany.com	x5428	1	1056	Sales Manager (NA)
7	1165	Larry	Hernandez	Larry.Hernandez@mycompany.com	x3291	1	1143	Sales Rep
8	1166	Larry	Patterson	Larry.Patterson@mycompany.com	x4065	1	1143	Sales Rep
9	1188	Jeff	Castillo	Jeff.Castillo@mycompany.com	x2173	2	1143	Sales Rep

5. If ***Custom SQL*** option is selected, the ***Custom SQL Statement*** text box appear on the screen. Enter the SQL Statement in the ***Custom SQL Statement*** text box and click ***Show Data*** button to show the data extracted based on the specified criteria as shown in the figure below.



Tools > View Data

Data Source: Demo_Source-demo_source-localhost (SOURCE)

View Type: Custom SQL

Custom SQL Statement:

```
select * from employees
```

Depict the masked data

Listing records 1 - 23 of 23

#	EMPLOYEENUMBER	FIRSTNAME	LASTNAME	EMAIL	EXTENSION	OFFICECODE	REPORTSTO	JOBTITLE
1	1002	Barry	Marsh	Barry.Marsh@mycompany.com	x5800	1		President
2	1056	Martin	Nishi	Martin.Nishi@mycompany.com	x4611	1	1002	VP Sales
3	1076	Gerard	Castillo	Gerard.Castillo@mycompany.com	x9273	1	1002	VP Marketing
4	1088	Tom	Nishi	Tom.Nishi@mycompany.com	x4871	6	1056	Sales Manager (APAC)
5	1102	George	Vanauf	George.Vanauf@mycompany.com	x5408	4	1056	Sale Manager (EMEA)
6	1143	Andy	Bott	Andy.Bott@mycompany.com	x5428	1	1056	Sales Manager (NA)
7	1165	Larry	Hernandez	Larry.Hernandez@mycompany.com	x3291	1	1143	Sales Rep
8	1166	Larry	Patterson	Larry.Patterson@mycompany.com	x4065	1	1143	Sales Rep
9	1188	Jeff	Castillo	Jeff.Castillo@mycompany.com	x2173	2	1143	Sales Rep

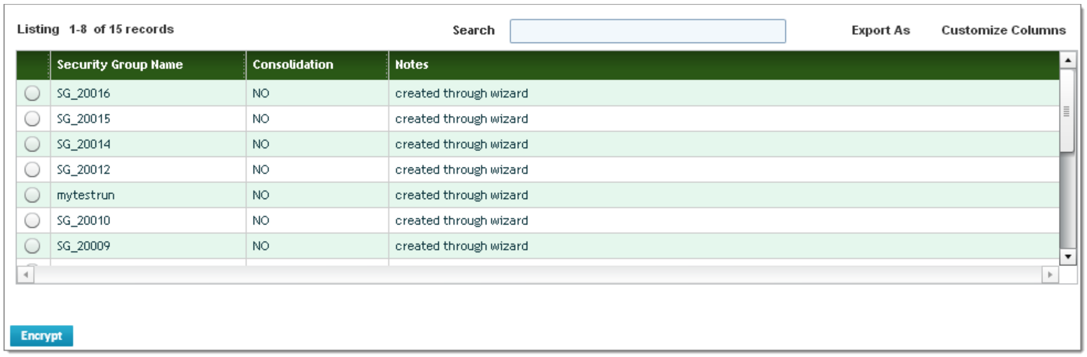
- The fields marked as | are mandatory fields.
- When the status of data masking turns to 'Process Completed' the user would be able to view the masked data/encrypted data in the table.

3 Rerun the Data Masking

Once the data masking is created and executed successfully, it will be automatically appended to the list of Security Groups on the ***Run Security Groups*** screen (***Data Masking*** > ***Run Security Groups***). This feature allows the user to rerun the executed security group recursively.

To rerun the data masking process, do the following:

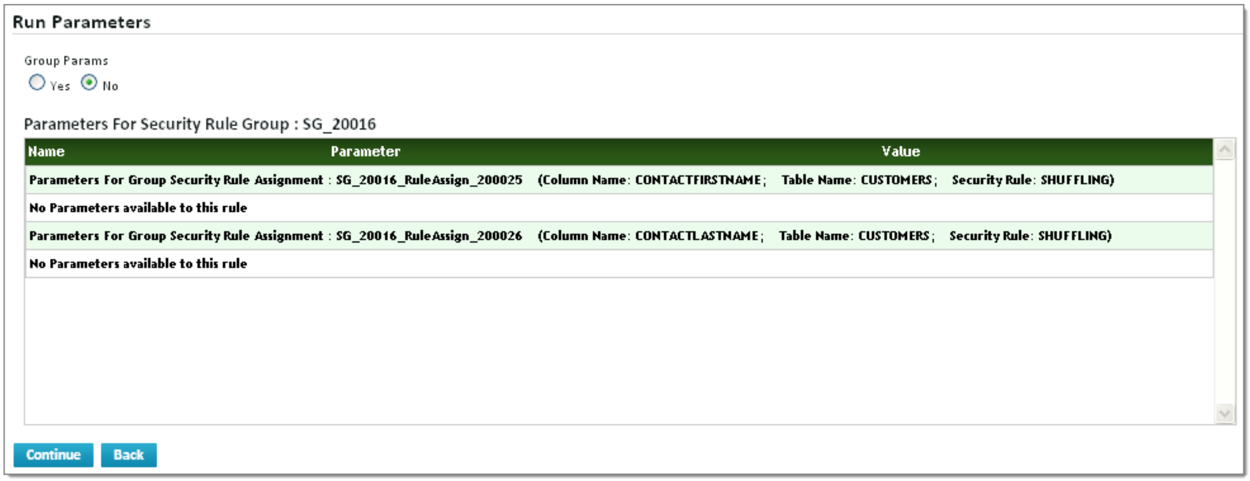
1. Navigate to the following path: ***Data Masking*** > ***Run Security Groups.*** The ***Security Groups*** screen with the list of security groups created will be displayed as shown in the figure below.



Listing 1-8 of 15 records

	Security Group Name	Consolidation	Notes
○	SG_20016	NO	created through wizard
○	SG_20015	NO	created through wizard
○	SG_20014	NO	created through wizard
○	SG_20012	NO	created through wizard
○	mytestrun	NO	created through wizard
○	SG_20010	NO	created through wizard
○	SG_20009	NO	created through wizard

2. Select the intended security group and click ***Run*** button. The ***Run Parameters*** screen to enter the run-time parameters will be displayed as shown in the figure below.



Run Parameters

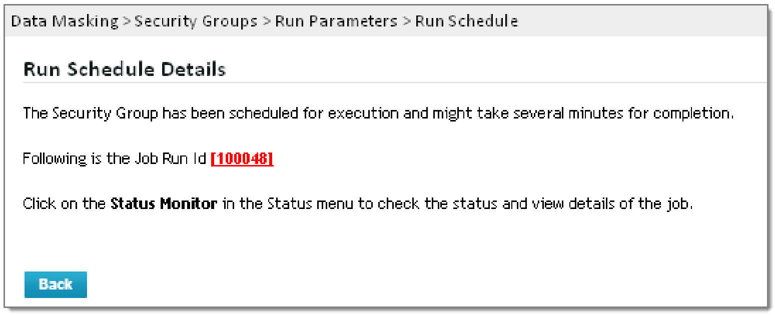
Group Params

○ Yes ● No

Parameters For Security Rule Group : SG_20016

Name	Parameter	Value
Parameters For Group Security Rule Assignment : SG_20016_RuleAssign_200025 (Column Name: CONTACTFIRSTNAME; Table Name: CUSTOMERS; Security Rule: SHUFFLING)		
No Parameters available to this rule		
Parameters For Group Security Rule Assignment : SG_20016_RuleAssign_200026 (Column Name: CONTACTLASTNAME; Table Name: CUSTOMERS; Security Rule: SHUFFLING)		
No Parameters available to this rule		

3. Click ***Continue*** button, to execute the security group for data masking process. Once the security group is executed successfully, automatically a Run ID is generated for the respective job in ***Run Schedule Details*** screen.



Data Masking > Security Groups > Run Parameters > Run Schedule

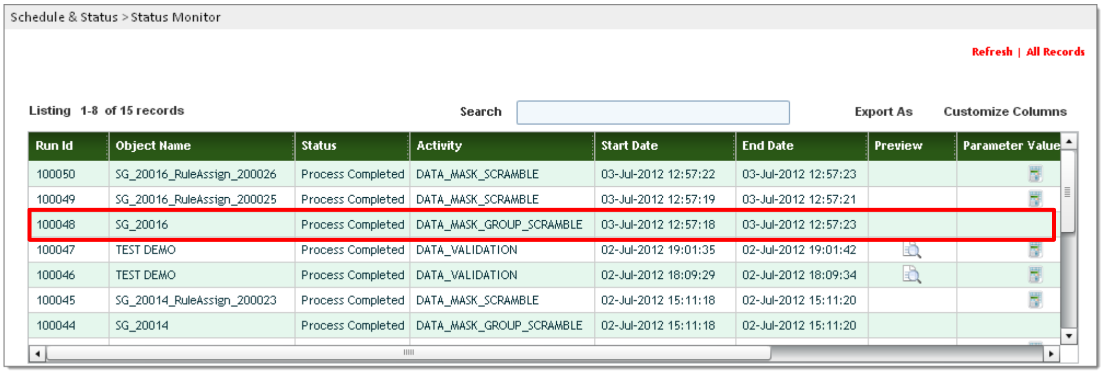
Run Schedule Details

The Security Group has been scheduled for execution and might take several minutes for completion.

Following is the Job Run Id [100048]

Click on the **Status Monitor** in the Status menu to check the status and view details of the job.

4. To monitor the status and view the details of the job, click Run ID or navigate to the ***Status Monitor*** screen (***Schedule & Status>Status Monitor***).



Schedule & Status > Status Monitor

Listing 1-8 of 15 records

Run Id	Object Name	Status	Activity	Start Date	End Date	Preview	Parameter Value
100050	SG_20016_RuleAssign_200026	Process Completed	DATA_MASK_SCRAMBLE	03-Jul-2012 12:57:22	03-Jul-2012 12:57:23		▦
100049	SG_20016_RuleAssign_200025	Process Completed	DATA_MASK_SCRAMBLE	03-Jul-2012 12:57:19	03-Jul-2012 12:57:21		▦
100048	SG_20016	Process Completed	DATA_MASK_GROUP_SCRAMBLE	03-Jul-2012 12:57:18	03-Jul-2012 12:57:23		
100047	TEST DEMO	Process Completed	DATA_VALIDATION	02-Jul-2012 19:01:35	02-Jul-2012 19:01:42	🔍	▦
100046	TEST DEMO	Process Completed	DATA_VALIDATION	02-Jul-2012 18:09:29	02-Jul-2012 18:09:34	🔍	▦
100045	SG_20014_RuleAssign_200023	Process Completed	DATA_MASK_SCRAMBLE	02-Jul-2012 15:11:18	02-Jul-2012 15:11:20		▦
100044	SG_20014	Process Completed	DATA_MASK_GROUP_SCRAMBLE	02-Jul-2012 15:11:18	02-Jul-2012 15:11:20		

5. Once the status of execution is '***Process Completed'*** the masked data can be viewed as follows:

   - Navigate to the following path: ***Tool*** > ***View Data***. The ***View Data*** screen displays the data in the table after data masking process.

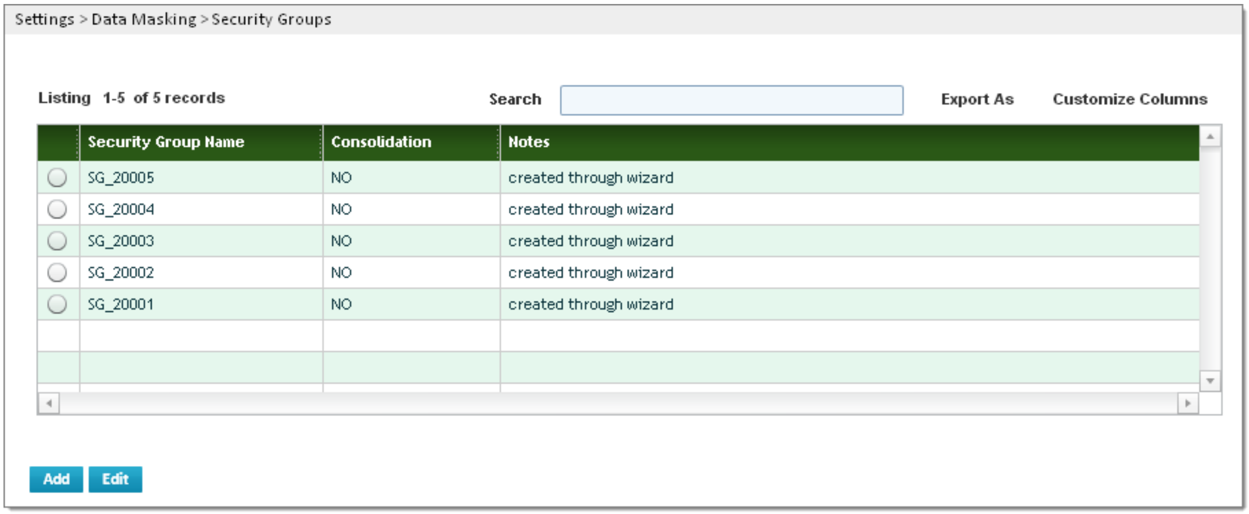
- The fields marked as * are mandatory fields.
- ***View Data*** screen provides feasibility to view the data in the table before data masking process and after data masking process to verify whether the data has been masked appropriately or not.

4 Edit the existing Data Masking

Once the security group is created and executed for data masking process successfully it will be automatically appended in the ***Security Groups*** screen (***Setting*** > ***Data Masking*** > ***Security Groups***). Henceforth, Solix EDMS Data Masking Standard Edition (SE) provides feasibility to edit the security group details and alter the security rule assignment details (such as rule type or rule name) in the existing security group. This section illustrates the process to modify the details/criteria in the existing security group.

To edit the existing data security group, do the following:

- Navigate to the following path: ***Setting*** > ***Data Masking*** > ***Security Groups.*** The ***Security Groups*** screen will be displayed as shown in the figure below.

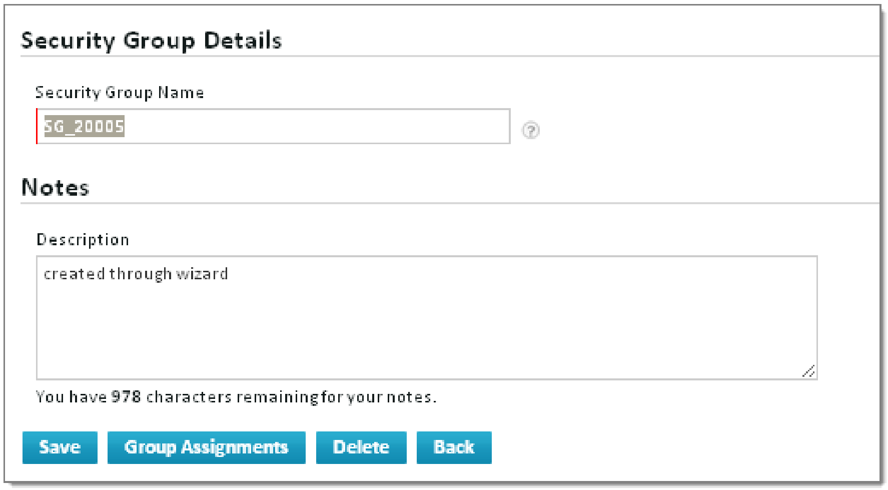


	Security Group Name	Consolidation	Notes
○	SG_20005	NO	created through wizard
○	SG_20004	NO	created through wizard
○	SG_20003	NO	created through wizard
○	SG_20002	NO	created through wizard
○	SG_20001	NO	created through wizard

4.1 Edit Security Group details

To edit the security group details, do the following:

1. In ***Security Groups*** screen, select the intended security groups and click ***Edit*** button to edit the security group details. ***The Security Group Details*** screen will be displayed as shown in the figure below.

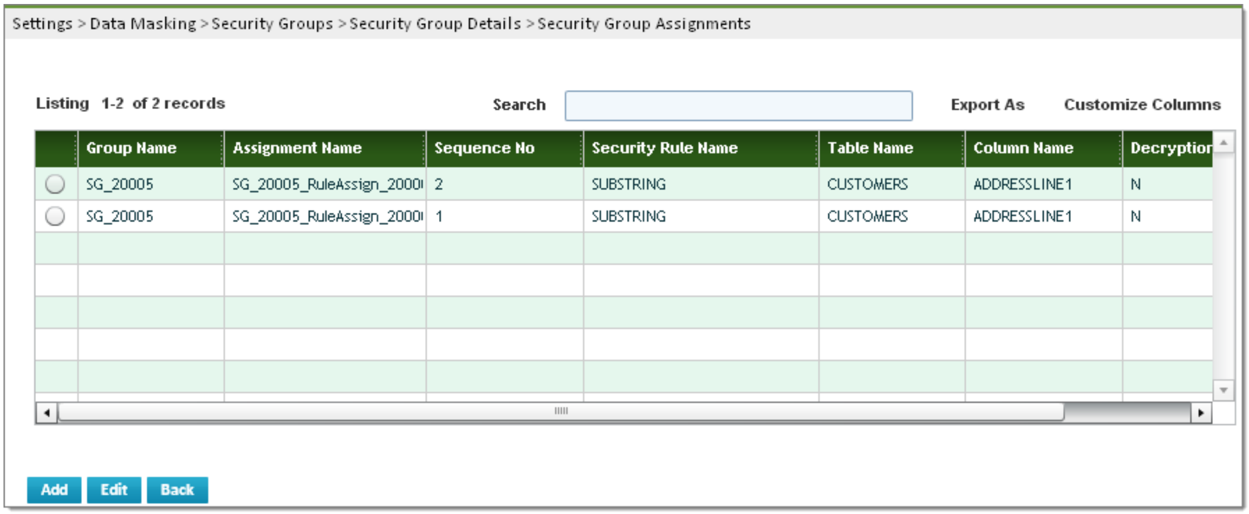


Security Group Name: SG_20005

Description: created through wizard

You have 978 characters remaining for your notes.

2. Click ***Group Assignments*** button. The ***Security Group Assignments*** screen with the list of security rule assignments grouped in the selected security group will be displayed as shown in the figure below.



Settings > Data Masking > Security Groups > Security Group Details > Security Group Assignments

Listing 1-2 of 2 records

	Group Name	Assignment Name	Sequence No	Security Rule Name	Table Name	Column Name	Decryptior
○	SG_20005	SG_20005_RuleAssign_2000	2	SUBSTRING	CUSTOMERS	ADDRESSLINE1	N
○	SG_20005	SG_20005_RuleAssign_2000	1	SUBSTRING	CUSTOMERS	ADDRESSLINE1	N

3. The ***Security Group Assignments*** screen provides feasibility to add or delete the security rule assignments in the respective security group.

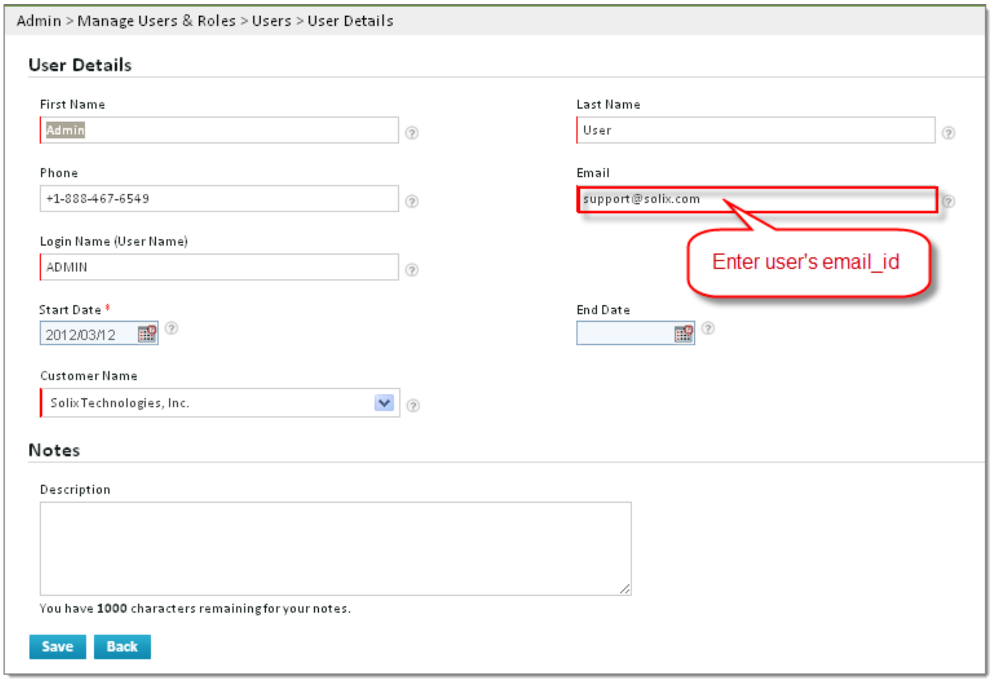
- The fields marked as * are mandatory fields.

5 Change Password

The default User ID and pass word provided by Solix Technologies logs the user in as an Admin user.

To change the password, do the following:

1. Login to the Solix EDMS Standard Edition (SE) using the authenticated user name and password.
2. When user wants to change the password for the first time, it is requisite to change the default email-id provided by Solix in order to send new password to the email-id specified by the user). To change user email-id,
    a. Navigate to the following path: ***Admin*** > ***Manage Users & Roles*** > ***Users***. The ***User*** screen will be displayed.
    b. Select radio button adjacent to Admin and click ***Edit*** button. The ***User Details*** screen with the information associated to admin user will be displayed as shown in the figure below.



Admin > Manage Users & Roles > Users > User Details

User Details

First Name: Admin

Last Name: User

Phone: +1-888-467-6549

Email: support@solix.com

Login Name (User Name): ADMIN

Start Date *: 2012/03/12

End Date:

Customer Name: Solix Technologies, Inc.

Notes

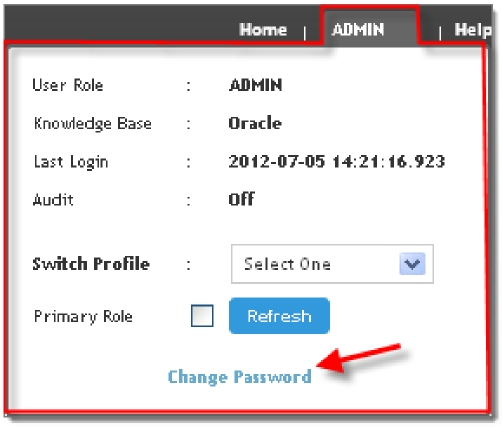
Description

You have 1000 characters remaining for your notes.

Enter user's email_id

    c. Enter email address of the user in the ***Email_id*** text box.
    d. Click ***Save*** button, to update the user information.

3. Once email_id of the user is changed, click ***Role*** (by default-ADMIN) appears at the top right corner of screen as shown in the figure below.



User Role : ADMIN

Knowledge Base : Oracle

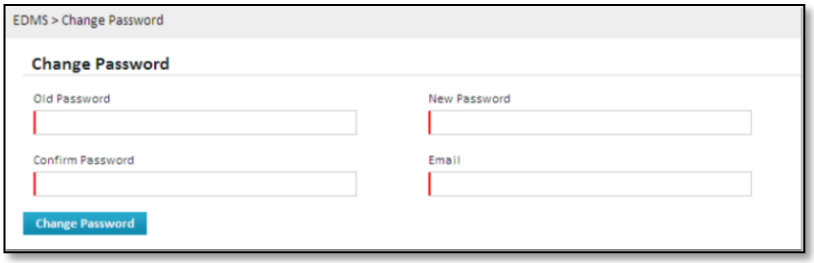
Last Login : 2012-07-05 14:21:16.923

Audit : Off

Switch Profile : Select One

Primary Role □

4. In ***Role Popup*** window, click ***Change Password*** hyperlink to change the password. The ***Change Password*** pop-up window will be displayed as shown in the figure below.



   a. Enter current password in the ***Old Password*** text field.

   b. Enter the new password in the ***New Password*** text field.

   c. Re-enter the new password in the ***Confirm Password*** text field.

   d. Enter the email address of the user in the ***Email*** in the text field, to send the confirmation mail.

   e. Click ***Change Password*** button. A message stating that "***Password is changed successfully***" appears and the confirmation message would be sent to the email address specified by the user.

- The field marked as |are mandatory fields.
- It is mandatory to enter the email address of the user in the ***User Details*** screen only when the password is changed for the first time.

6 Appendix

6.1 Appendix-A: Java based Algorithms

Location: Application

Java algorithms which support data masking in Solix EDMS Data Masking Standard Edition (SE) are listed in the table given below.

SECURITY RULE NAME	Data Type	DESCRIPTION
EMAIL	Character	Mask Email column value with first name, last name and domain name values in FIRST_NAME.LAST_NAME@Domainname format. Both FIRST_NAME and LAST_NAME columns should be available in same table. For example, Carl.Douglas@mycompany.com
FULL NAME	Character	Mask Full Name Value with first name and last name. Both FIRST_NAME and LAST_NAME columns should be available in same table. For example, Carl Douglas
SALARY PERCENT	Numeric	Mask Numeric value with a percentage variation of given range. For example, provide 10 percent at run time means + or -10 percent variation can be seen after masking.
SHUFFLE CHARS NUMERIC	Numeric	Mask Numeric Data by Shuffling the digits of a column value. For example, if original value is 123456789 then mask value could be 579314628.
SHUFFLE CHARS	Character	Mask Character Data by Shuffling the characters of a column value. For example, If original value is ABCDEFGH then mask value could be EGACBHFD.
NUMERIC DATA ENCRYPT	Numeric	Encrypts Numeric Column Data.
CHAR DATA ENCRYPT	Character	Encrypts Character Column Data.
TRUNCATE DATA	Character, Numeric and Date	Truncates Table Data.
MASK_CREDIT_CARD_WITH_FMT	Character	Mask Character Data with Randomly generated Credit Card Numbers (LUHN validated) based on selected Card Type with format character. For example, 4872-2670-0856-2847
MASK_CREDIT_CARD	Character	Mask Character Data with Randomly generated Credit Card Numbers (LUHN validated) based on selected Card Type. For example,

		4338818716421722
MASK_PHONE_NUMBER_WITH_FMT	Character	Mask Character Data with Randomly generated US Phone Numbers with valid area codes along with format character. For example, 443-801-1719
MASK_PHONE_NUMBER	Character	Mask Character Data with randomly generated US Phone Numbers with valid area codes. For example, 4346565661
MASK_UK_SSN	Character	Mask Character Data with randomly generated UK National Identifier. For example, KR671426W
MASK_US_SSN_WITH_FMT	Character	Mask Character Data with randomly generated US Social Security Numbers along with format character. For example, 471-56-6525
MASK_US_SSN	Character	Mask Character Data with randomly generated US Social Security Numbers. For example, 934525467
NULLING OUT	Character	Mask Character column value with null values.
RANDOM DIGITS NUMERIC	Numeric	Masking Numeric data value with randomly generated digits in the given range.
RANDOM DIGITS CHAR COL	Character	Masking character data value having numeric data with randomly generated digits in the given range.
RANDOM DATES	Date	Masking Date values with randomly generated dates in the given date range. For example, 01-JAN-2001.
RANDOM NUMBERS	Numeric	Masking Numeric Data with randomly generated numeric values in the given range. For example, 9999.
RANDOM STRINGS	Character	Masking Character Data with randomly generated character string. For example, ABCDEFGH
NUMERIC ARRAYLIST VALUES	Numeric	Masking Numeric Data with the given list of numeric values separated by comma.
STR ARRAYLIST VALUES	Character	Masking Character Data with the given list of character values separated by comma.
FIXED NUMBER	Numeric	Masking Numeric data with the given fixed numeric value. For example, 9999 (fixed value)
FIXED STRING	Character	Masking character data with the given fixed string

		value. For example, ABCDEFGH (constant value)
FIXED DATE	Date	Masking character data with the given fixed date value. For example, 01-01-2013
SUBSTRING	Character	Masking data with Substring of the each column value. For example, If original value ABCDEFGH then mask value could be ABCD.
SHUFFLING NUMERIC	Numeric	Shuffling Numeric Column Values from one row to another. For example, Row one numeric value shuffles with row “n” value.
SHUFFLING STRING	Character	Shuffling Character Column Values from one row to another. For example, Row one character value shuffles with row “n” value.
SHUFFLING STRING	Date	Shuffling Date Column Values from one row to another. For example, Row one character value shuffles with row “n” value.

6.2 Appendix-B: Database Algorithms

Location: Database (Exclusively, Oracle)

- To make use of DB algorithms to mask the data, it is mandatory to compile the following script in Oracle database where masking process is performing:

  "***edms_database_security_algorithm.sql***" under ***EDMS_Home*** > ***scripts*** folder.

DB algorithms which support data masking in Solix EDMS Data Masking Standard Edition (SE) are listed in the table given below.

Security Rule Name	Data Type	Description
DB-DATE	Date	This security rule generates the value of day and month randomly in date column, whereas the value of Year remains the same (i.e., Original value)
DB-EMAIL	Character	This security rule masks the email column values based on the given First Name Column, Last Name Column and Domain name value.
DB-FULLNAME	Character	This security rule masks the Full Name based on the column values provided in the FIRST_NAME and LAST_NAME parameters. Pre-requisite: Both the parameters (for example, FIRST_NAME and LAST_NAME) provided for the Full Name should be in Source table.
DB-SALARY	Numeric	This security rule increments or decrements the column values based on the given percentage of value. For example if the user provides 10, then the column value will be incremented or decremented randomly within the range of +10 to -10. [Source Value : 1500, Masked Value : 1545]
DB-SHUFFLE	Character	This security rule shuffles the characters within a string. For example, "SOLIX" is a string and after shuffling it is masked as "XOSLI"
DB-CREDIT-CARD-ALL-MASKX	Character	This security rule masks all the Numeric Characters with X. For example, if the value is equal to 123-234, then the value after masking is XXX-XXX
DB-CREDIT-CARD-PARTIAL-MASK	Character	Mask All Numeric Characters with X apart from first 4 Characters, like 1234-5678 masks with 1234-XXXX

DB-SHUFFLE-COLUMN-CHARS	Character	Masking the table on which this security rule is assigned based on the source column value (provided during runtime). This algorithm enables the user to mask the source column value randomly by leaving the first N number of characters.
DB-RANGE-MASK-ALONG-CHILD-TABLE	Numeric	This security rule masks the column of the parent table and replicates the masked value on the child table column data.
DB-FIXED-STRING	Character	This security rule masks the column value with the given fixed string value. [Parameter Value : Blake, Source Value : Miller, Masked Value : Blake]
DB-RANDOM-CCARD-GEN	Character	This security rule generates the Credit Card Valid Number randomly as per LUHN based on Card Type selected. [Parameter Value : Visa, Source Value : 4503 8803 9903 2326, Masked Value : 4322678416974018]
DB-RANDOM-US-SSN-GEN	Character	This security rule generates the US Social Security Number randomly. [Source Value : 554-98-2445, Masked Value : 315531544]
DB-RANDOM-US-SSN-GEN-FMT	Character	This security rule generates the US Social Security Number randomly along with format character (i.e, character used as separator). [Parameter Value : - , Source Value : 554-98-2445, Masked Value : 315-53-1544]
DB-RANDOM-NUMBERS-GEN-CHAR	Character	This security rule generates random numbers within a specified range for Character datatype columns. [Parameter Values : 10000,99999 , Source Value : 34782, Masked Value : 64669]
DB-RANDOM-NUMBERS-GEN-NUM	Numeric	This security rule generates random numbers within a specified range for NUMBER datatype columns. [Parameter Values : 10000,99999 , Source Value : 34782, Masked Value : 64669]
DB-SUBSTRING	Character	This security rule generates SUBSTRING of Original Value based on provided from character value to No of characters. [Parameter Values : 1, 5 , Source Value : Debbie, Masked Value : Debbi]
DB-RANDOM-VALUE-FROM-LIST-CHAR	Character	This security rule generates a random STRING value from provided comma separated strings like abc, def, ghi. [Parameter Value : Debbie,Blake,Smith,Tunner , Source Value : Miller, Masked Value : Smith]
DB-RANDOM-DATES-GEN	Date	This security rule generates random dates within a specified DATE range. [Parameter Values : 2001-06-20,2012-06-20 , Source Value : 05/16/2012, Masked Value : 12/21/2007]

DB-RANDOM-DIGITS-CHAR	Character	This security rule generates a numeric number between given minimum and maximum digits for CHARACTER data type columns. [Parameter Values : 2, 6 , Source Value : 9785, Masked Value : 835840]
DB-US-PHONE-NUM-GEN	Character	This security rule generates random US Phone Numbers with valid area codes. [Source Value : 4085671234, Masked Value : 6498628963]
DB-US-PHONE-NUM-GEN-FMT	Character	This security rule generates random US Phone Numbers with valid area codes along with provided format character. [Parameter Value : - , Source Value : (408)5671234, Masked Value : 302-809-4281]
DB-VALUE-SHUFFLE	Character	This security rule is used to randomly generate the characters of First N Chars or Last N Chars or All Characters. For example if the Parameter values are provided as FIRST-N, 5. Then, Miller John will be masked as Ehyzfr, John
DB-FIXED-NUMBER	Numeric	This security rule masks the column value with the given fixed numeric value. [Parameter Value : 15000, Source Value : 1255, Masked Value : 15000]
DB-RANDOM-CCARD-GEN-FMT	Character	This security rule generates the Credit Card Valid Number randomly as per LUHN along with the format character (i.e., character used as separator) based on Card Type. [Parameter Values : Visa And - , Source Value : 4503 8803 9903 2326, Masked Value : 4322-6784-1697-4018]
DB-RANDOM-UK-SSN-GEN	Character	This security rule generates the UK Social Security Number randomly. [Source Value : JR567078H, Masked Value : LS648045P]
DB-RANDOM-STRINGS-GEN	Character	This security rule generates RANDOM STRING within given minimum and maximum length characters. [Parameter Values : 5,15 , Source Value : Blake, Masked Value : VxGNiUqHP]
DB-RANDOM-VALUE-FROM-LIST-NUM	Numeric	This security rule generates a random NUMERIC value from provided comma separated string like 26781, 99999, 355667, 13234. [Parameter Value : 26781,99999,355667,13234 , Source Value : 8778, Masked Value : 355667]
DB-RANDOM-DIGITS-NUM	Numeric	This security rule generates a Numeric number between given minimum and maximum digits for NUMBER data type columns. [Parameter Values : 2 , 6 , Source Value : 9785, Masked Value : 835840]

7 About Solix Technologies

Solix Technologies, Inc. is a leading provider of Enterprise Data Management solutions for public and private clouds. Solix data growth solutions help businesses improve application performance, reduce storage costs and meet compliance and data privacy requirements by achieving Information Lifecycle Management (ILM) goals. The Solix Cloud provides a pay-as-you-go model for database archiving and application retirement. The Solix Enterprise Data Management Suite (EDMS) software enables organizations to implement Database Archiving, Test Data Management (Data Subsetting), Data Masking and Application Retirement across all enterprise data. Solix Technologies is headquartered in Santa Clara, California and operates worldwide through an established network of value added resellers (VARs) and systems integrators.

Visit Solix Technologies on the web at http://www.solix.com and follow Solix on,

- Twitter (http://www.twitter.com/solixedms)
- Facebook (http://www.facebook.com/solixtechnologies)