EPI-USE LABS
value through innovation

DSM Data Secure

Flexible, accurate, secure masking of data in SAP clients

User Guide

documentation@labs.epiuse.com

Data Sync Manager™ 5
Document version A
29 March 2019

Contents

1. Introduction

1.1 Welcome

Welcome to Data Sync Manager™ (DSM) Data Secure™, a product developed by EPI-USE Labs for data-masking.

Data Secure is available for all SAP® NetWeaver environments – including ERP, CRM, SRM, SCM and BW.

In this guide, the following icons will be used:

Take Note	Recommended	Warning
Example	Step-by-step	

For more general information, refer to the appendices: Key concepts and definitions (Appendix A) and Icons used in EPI-USE Labs documentation (Appendix B).

1.2 Why use Data Secure?

All companies have a need for non-production systems with representative data for testing, training, problem resolution or other project-related needs. The easiest way to create this representative data is to copy it from the Production system to non-Production systems.

In general, the users of these non-production systems have less stringent authorization checks, to enable them to perform their required functions. This, however, leads to security concerns, since these users could gain access to sensitive information that they might not normally be authorized to access in the Production environment.

For this reason, it is imperative that all sensitive data in the non-Production systems is masked to comply with statutory requirements and industry standards.

Data Secure provides a standard, extendable solution to meet these needs.

1.3 How Data Secure works

Data Sync Manager™ (DSM) is an integrated solution with five complementary products: Client Sync™, Object Sync™, Data Secure™, System Builder™ and System Compare™, each addressing the following aspects:

- **Object Sync** allows you to select and transfer specific data objects, easily and accurately, as you need them.
- **Client Sync** provides a table-oriented approach to copying a subset of a client (known as a Sync).
- **Data Secure** provides in-place data-masking and provides integrated masking for other DSM suite products.
- **System Builder** allows you to make complete repository copies easily, then add the client data as you need it.
- **System Compare** allows you to easily discover misalignments between systems in the SAP repository.

Data Secure is an extendable solution for masking sensitive data in non-production systems to comply with statutory requirements and industry standards. It provides an extendable set of masking rules via user-defined (or EPI-USE Labs-provided) policies that can be applied to an SAP client to mask sensitive data to comply with statutory requirements and industry standards.

Data Secure has a simple user interface that allows functional teams to define a set of rules, which the basis team can re-use easily whenever they create or refresh a client. Data Secure is versatile where it can be run as a standalone or as part of Object Sync and Client Sync or just within Data Secure itself via In-Place Masking.

This user guide provides you with the knowledge you require to use Data Secure effectively. The guide has hyperlinks to allow you to jump directly to relevant sections:

When Data Secure is executed to mask a particular set of data according to the masking rules specified in a data security Policy, this process is defined as a Data Secure Run. Creating a Run is a simple process, though there will generally be several different teams involved:

1. **Functional teams**: A functional expert from each team will need to decide which data in the system is sensitive and should be masked.

2. **Basis team**: This team is responsible for the system as a whole and for ensuring its stability, availability and performance. Since a Data Secure Run could affect a large portion of the system, the Basis team may be the ones to decide when the Run should be executed.

1.4 Overview of Data Secure Concepts

★ For first-time users, it is highly recommended that they familiarize themselves with the concepts relating to Data Secure.

1.4.1 Rules

The first step in masking a system is to decide which data needs to be masked. Within Data Secure, you will select rules to apply to the data. These rules are called Data-masking Rules and they define which tables and fields are to be modified and what the new values will be. Data Secure comes preconfigured with a large number of common Rules that you can use in your system. Rules are client-dependent.

1.4.2 Policy

Although your company’s Basis team will actually execute the Data Secure Run, it is the functional expert who knows which data needs to be masked. Data Secure, therefore, provides the option of creating Policies where functional experts can store their selections of Rules. The Basis team can then select the Policy to perform a Run without needing to know the details of what is being masked. Policies can be used within Data Secure (when doing in-place masking) or are used in the context of Object Sync and Client Sync. Policies are client-dependent and many policies can be created in the same client.

Policies and Rules can be shared online with the DSM community from the Client Central website or by using embedded functionality within Data Secure.

1.4.3 Business Objects and the Business Object Workbench

The Business Object Workbench (BOW) is a major component used by Data Sync Manager. Its purpose is to store, define and refine new and existing Business Object definitions. It provides the flexibility to update and define Business Objects to suit business requirements.

The BOW contains a complete list of all the Business Object Definitions that are supported by Data Sync Manager. By using the BOW, it is possible to extend a Business Object Definition, e.g. enhance a Business Object with additional custom tables, which may also require masking.

EPI-USE Labs provides continuous support and updates to Business Object Definitions. This includes creating and supplying updated versions of Business Object Definitions for each new SAP release and ensuring that it will work after each upgrade.

Data Secure uses Business Object Definitions maintained in the BOW. Before a field is added to an Integrity Map the table that contains it is added to a Business Object Definition in the BOW. This can be an extension of an existing Business Object Definition or be contained in a new Customer Business Object Definition that is defined by the customer.

The Business Object Workbench allows a single user role, Developer, to enhance delivered Business Object Definitions or to create Customer Business Objects.

1.4.4 Integrity Maps

Integrity Maps are defined in a Business Object Context as a set of fields that store the same or similar information in a redundant fashion and therefore need to be updated with the same or similar values when masked in order to retain semantic data integrity. Integrity Maps can be linked in dependency relationships to reflect fields that store related values that are not entirely redundant. The Data Conversion engine will process Integrity Maps for masking according to their definitions and relationships as described later in this document.

> Integrity Maps can be shared online with the DSM user community. This is done via Client Central or through Client Central functionality embedded within Data Secure.

1.4.5 Transformation Functions

Transformation Functions are associated with Integrity Maps to form a Data-masking Rule. They specify how the masking should occur by producing output values according to input parameters. Within the context of a data-masking Rule, these values are assigned to the groups of fields represented by an Integrity Map. Multiple Transformation Functions are delivered as part of Data Secure. Custom Transformation Functions can also be created in Data Secure.

> Custom Transformation Functions can be shared online with the DSM user community. This is done via Client Central or through Client Central functionality embedded within Data Secure.

1.4.6 User groups

User Groups group SAP users for shared access purposes, for example, access to and coverage by Policies are controlled through User Groups.

Data Secure ships with the group EVERYONE which includes all product users. The 'Default' data security policy is assigned to the EVERYONE group, implying that masking applies to all product users.

2. Starting Data Secure

To access Data Secure, type **/n/use/ds** in the SAP GUI transaction code bar. The initial screen that opens will be the Data Secure Launchpad.

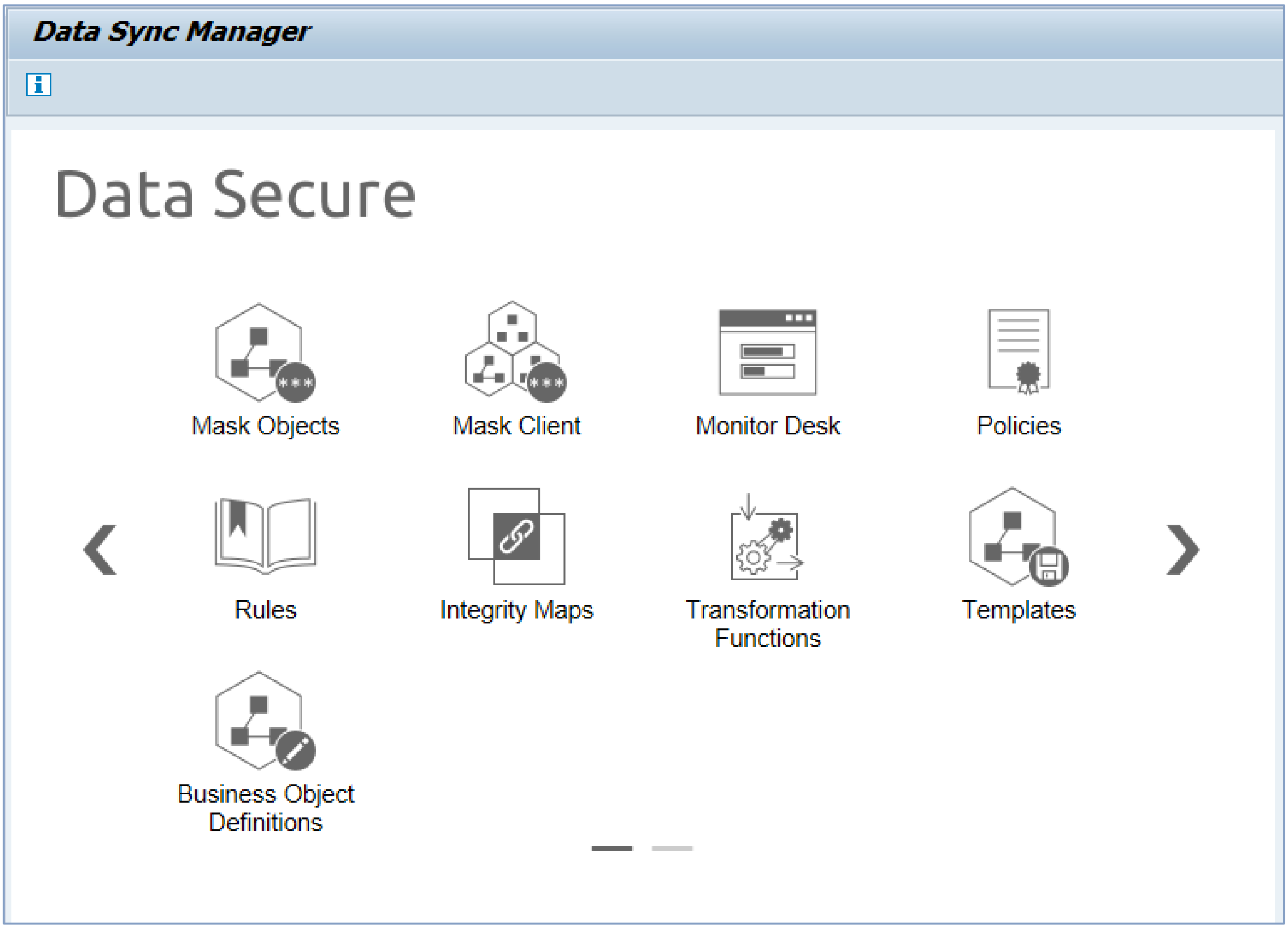
If DSM 4 is installed on the current system, an option to 'Choose your DSM version' (either DSM 4 or DSM 5) will be displayed in a pop-up screen. Select the 5 option to use the functionality described in this document. For more details, refer to the related knowledge base article.

2.1 Launchpad

From here, you can access the various features along with the necessary Administration functions to set up Data Secure.

2.1.1 Data Security Page

This is the first page accessed when entering **/n/use/ds** in the SAP GUI Transaction code window. It contains the functions related to data-masking activities.



The functions that are accessible from the Data Secure Launchpad are described in the following table.

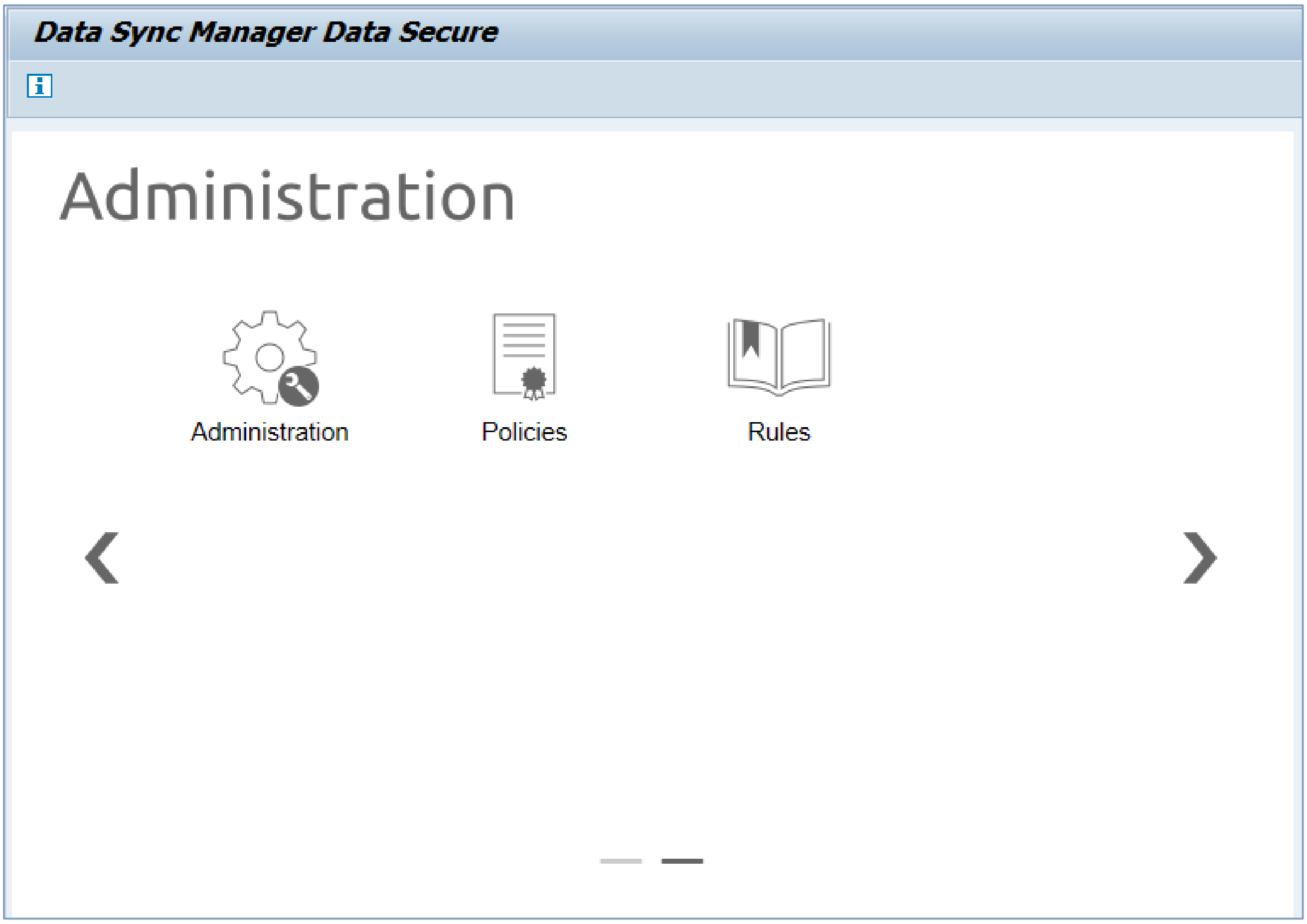
The Data Secure functions are as follows:

Button	Name	Description
Mask Objects	**Mask Objects**	Masks a subset of sensitive data corresponding to a selection of Business Objects on the current client and its associated clients.
Mask Client	**Mask Client**	Masks all the sensitive data present on the current client and its associated clients.
Monitor Desk	**Monitor Desk**	Monitors and audits the execution of data-masking runs.
Policies	**Policies**	Maintains data security Policies.
Rules	**Rules**	Maintains data-masking Rules.
Integrity Maps	**Integrity Maps**	Maintains Integrity Maps.
Transformation Functions	**Transformation Functions**	Maintains Transformation Functions.
Templates	**Templates**	Create data-masking run templates.

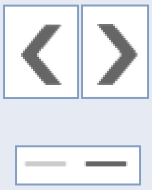
Business Object Definitions	**Business Object Definitions**	Launches the Business Object Workbench. Details for the use of the Workbench can be found in the BOW Extensions User Guide.
❮ ❯ — —	**Navigation**	Navigates between the different areas of the Data Secure Launchpad. The highlighted line indicates the current page.

2.1.2 Administration Page

The Administration Page is accessed by clicking one of the navigation arrows on the main Landing Page or by clicking the second grey dash at the bottom of the Launchpad.



The following administrative functions are available from this page:

Button	Name	Description
	Administration	Accesses the functions of the Administration Desk. Please refer to the Administration and Admin guide for more details.
	Policies	**See the previous table**
	Rules	**See the previous table**
	Users and Groups	To set up User Groups for access control to Templates and Data Security policies.
	**Navigation**	Navigates between the different areas of the Data Secure Launchpad. The highlighted line indicates the current page.

For all these items, users can refer to the Installation, Control Center and Configuration Guide for more details.

3. Data Secure Runs

This section discusses Data Secure Runs, which is the process of masking a selection of data according to a set of masking Rules specified in a data security Policy.

Two types of Data Secure Runs are possible:

- **In-place Run**: A Run that is started manually to mask data present on the current client and clients logically associated with it. In-place Runs are classified either as client-masking runs where all data matching the Policy on the current client(s) is masked or object-masking runs where only a selection of data is masked as matched to the Policy.
- **In-line Run**: A Run that is started automatically as part a Sync done using DSM Client Sync or DSM Object Sync, to transfer the data from the Source to the Target client and mask it. The masking is done on the source client of the export and clients logically associated with it. Some masking may be repeated on the target clients once the data is imported.

3.1 In-place Data Secure Runs

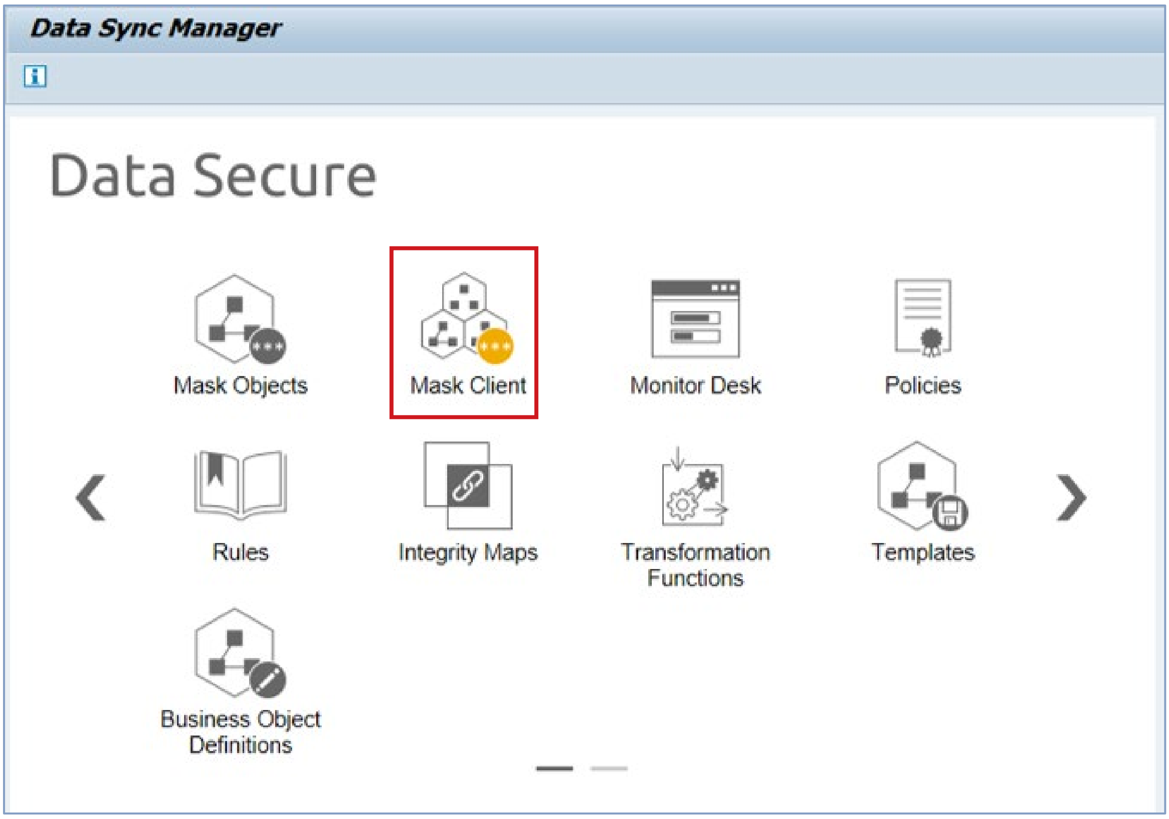
In-place Data Secure Runs are created from the Data Secure launchpad.

> In-place Data Secure Runs always execute in the current client.

3.1.1 Execute a 'Mask Client' in-place Run

Step 1: Start the Data Secure launchpad using transaction **/n/use/ds.** If you are already in Data Secure you can return to the launchpad by selecting the Back button.

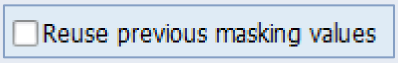
Step 2: Select 'Mask Client' from the Data Secure launchpad.



Step 3: Select the Policy to be used for the run.

Note: The data security Policies listed are based on the Policies assigned to User Groups that the current user belongs to. Make sure that the executing user is assigned to a User Group that has access to the Policy intended for the client masking.

On the Masking options screen, next to the Policy field for which you must make a selection, there is also a checkbox to re-use previous masking values:



☐ Reuse previous masking values

If the checkbox is selected, this will default your settings to the masking values used in the last Masking run that was executed on this system.

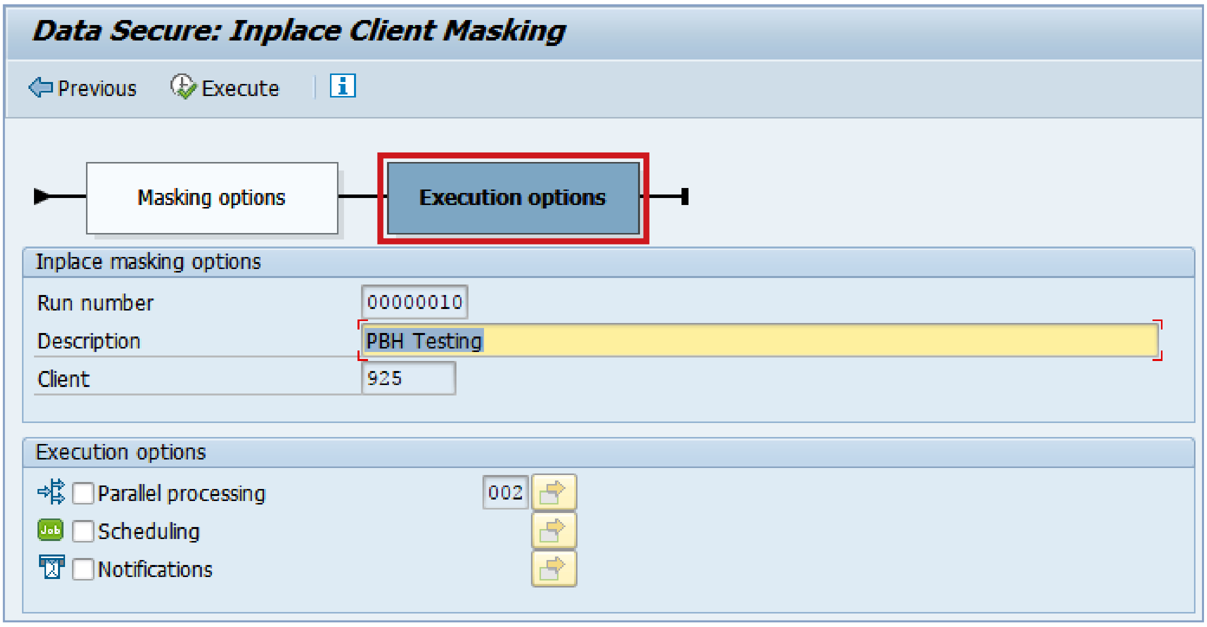
Step 4: Review the data-masking Rules and set the options to be used for each Rule. The available options are as follows:

Icon	Name	Functions
☑	Rule selection	Selecting the radio button indicates whether the rule will be executed in the run or not.

○ ●	Option selection	The selected radio button indicates which Rule option to use for the current masking run.
✎	Default assigned	A default user input has been assigned to the associated Rule option. Select this button to change this value.
✎	Requires input	The masking Rule option requires user input. Input is required if the option is selected or the rule has no other options.

Step 5: Click on the 'Next' ⇨ Next button or select the 'Execution Options' in the roadmap to proceed to the Execution Options screen.

Step 6: Specify the execution options. The available execution options are as follows:



Inplace masking options

Run number	00000010
Description	PBH Testing
Client	925

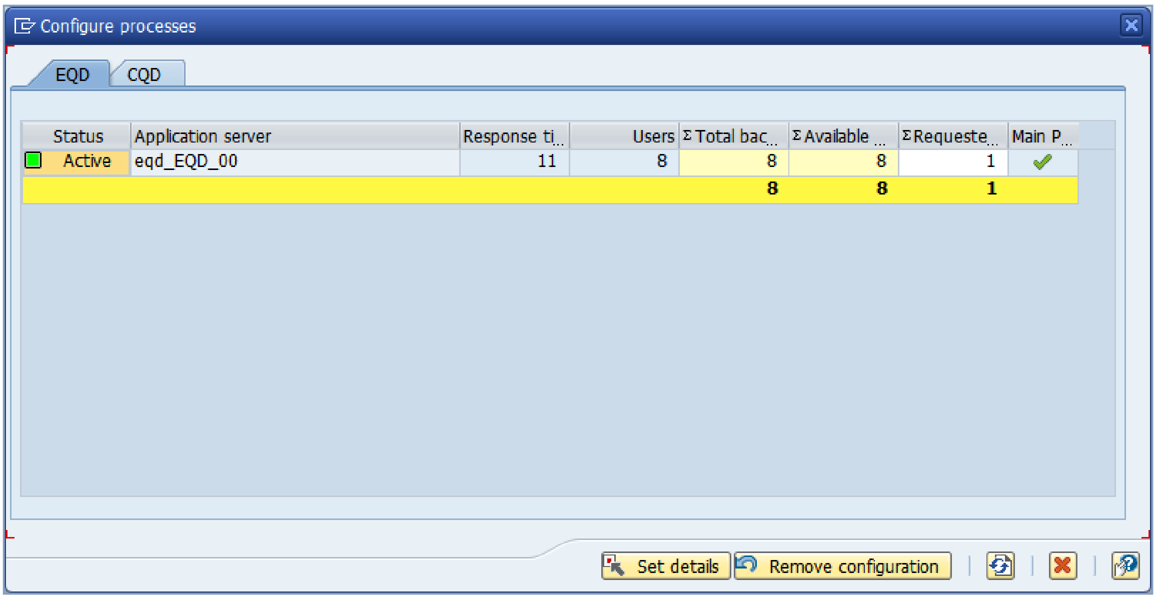
Execution options

□ Parallel processing	002
□ Scheduling	
□ Notifications	

- **Description**
  Create a description for the new Run so that you will be able to identify it in the Monitor Desk later. The default description will be the name of the Data Secure policy that you selected in step 3 above.

- **Parallel processing**
  Select this checkbox if you wish to configure the distribution of work through parallel processes. This allows you to use more than one background work process to do the work, thus achieving faster execution times.

  Once you have selected parallel processing, you can change the number of processes to be used. SAP will distribute the processes to the least busy application servers.



Status	Application server	Response ti...	Users	ΣTotal bac...	ΣAvailable ...	ΣRequeste...	Main P...
🟩 Active	eqd_EQD_00	11	8	8	8	1	✓
				8	**8**	**1**	

If you wish to override this by configuring the distribution yourself, click on the 'Configure' button. This will open a pop-up screen allowing you to view and configure the distribution of parallel processes, where for each system you select the number of processes to use and the application server that they should execute on, manually.

If the Data-masking run involves multiple systems and/or clients, different settings can be maintained to be used for each system/client. To do so, select the tab corresponding to the system and then specify the distribution of processes among the Application servers of that system as detailed above. If the number of processes is specified before the parallel processing is defined, the number of processes will be scheduled for each system unless changed.

> Runs are always executed in the background, as they generally affect a large amount of data and have long run times.

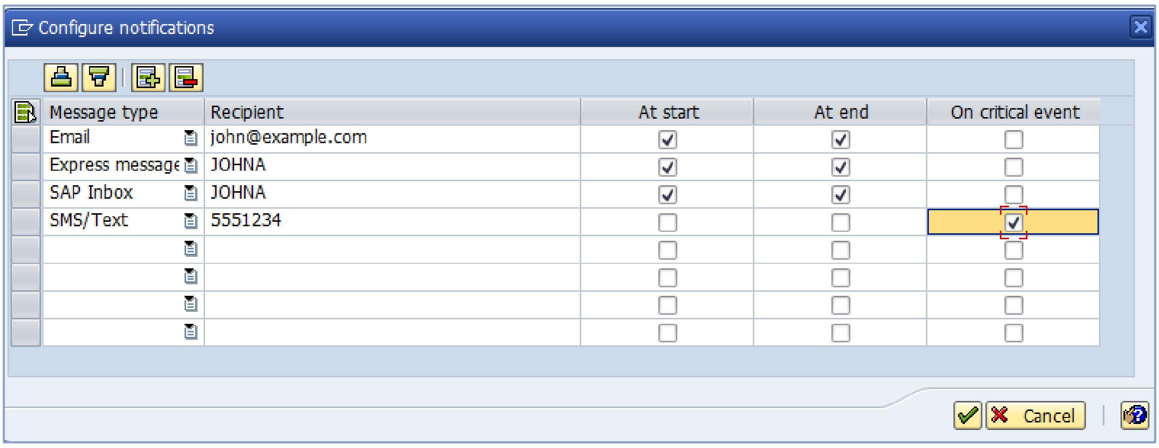
- **Scheduling**

  Select this checkbox to schedule the Run at a future date and/or time. You can click the 'Configure' button to set the execution date and time.

- **Notifications**

  Select this checkbox to notify users of Sync progress and events. Click the 'Configure' button to specify notification methods, the recipients and set the types and frequency of notification messages.

The following pop-up will appear:



Message type	Recipient	At start	At end	On critical event
Email	john@example.com	☑	☑	□
Express message	JOHNA	☑	☑	□
SAP Inbox	JOHNA	☑	☑	□
SMS/Text	5551234	□	□	☑
		□	□	□
		□	□	□
		□	□	□
		□	□	□

Complete the following sections:

- **Message type:** This indicates how the notifications must be sent:
  - Email: will send an email notification to the email address specified in the Recipient column.
  - Express message: will send an SAP Express message to the SAP User account specified in the Recipient column.
  - SAP Inbox: will send a message to the SAP Inbox of the SAP User account specified in the Recipient column.
  - SMS/Text: will send a notification via Short Message Service (SMS) or Text to the mobile phone number specified in the Recipient column.
- **Recipient:** The content to be entered in this field depends on the message type you selected. Enter the required email address, User account ID or mobile phone number.
- **At start:** Selecting this checkbox will send a notification to the specified recipient when the execution of the Sync has started.
- **At end:** Selecting this checkbox will send a notification to the specified recipient when the execution of the Sync has ended.
- **On critical event:** Selecting this checkbox will send a notification to the specified recipient if a critical event, such as an error that prevents further execution of a Sync process, occurs.

Confirm the pop-up. The Sync will then be configured to send out the specified notifications.

Step 7: Click 'Execute' Execute to execute the data-masking Run according to its current configuration.

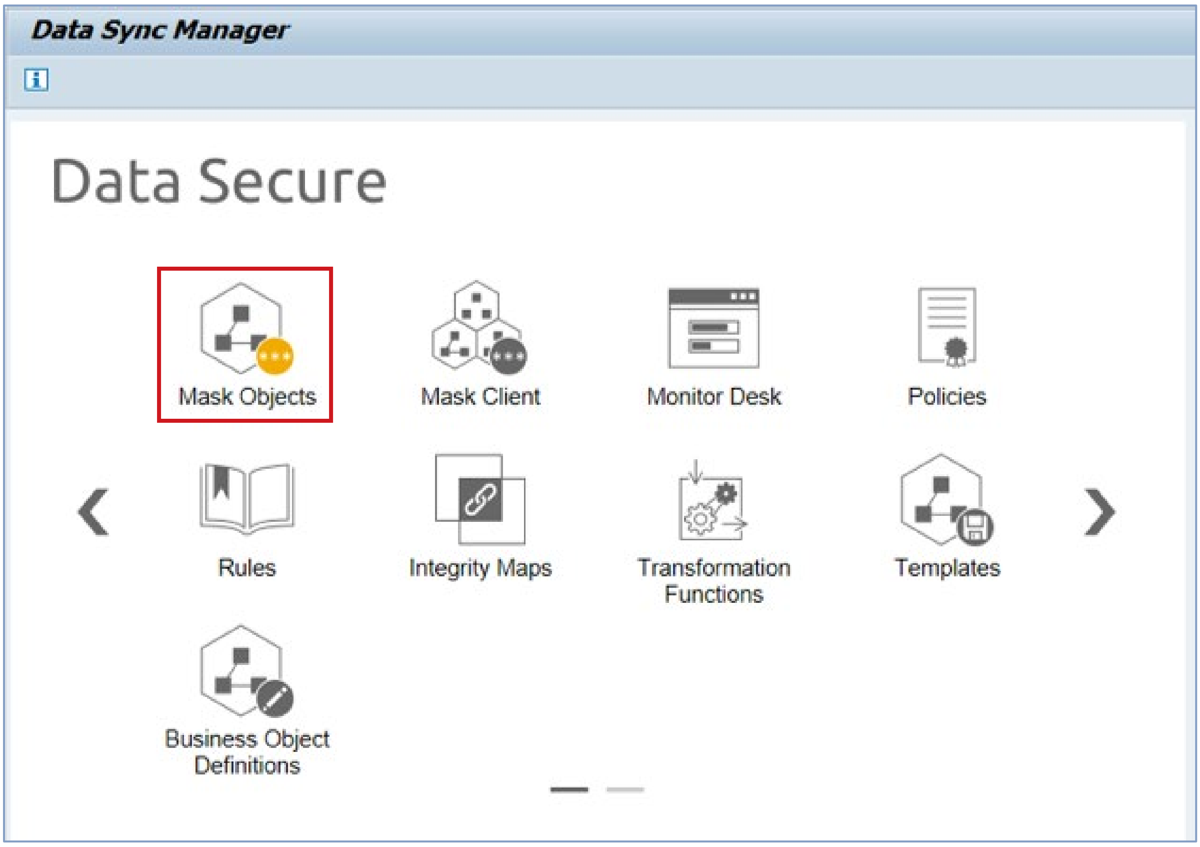
The Data Secure Run will start as soon as a background work process becomes available in the system or, if it is scheduled for later, will start at the time you specified.

DSM Data Secure will take you to the Monitor Desk, where you can monitor the progress of the Run and access details of and information on the Run.

3.1.2 Executing a 'Mask Object' in-place Run

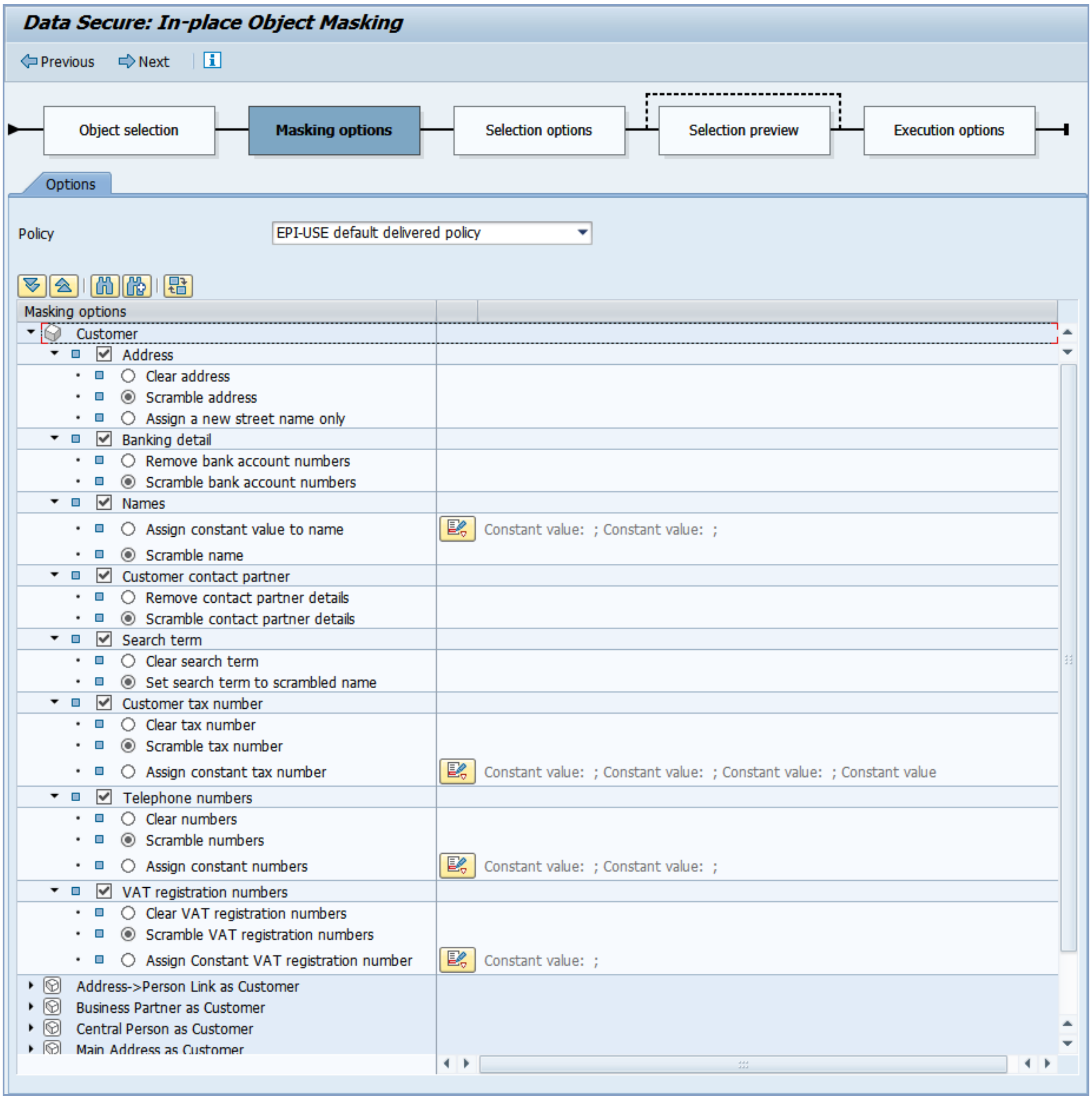
Step 1: Start the Data Secure launchpad using transaction **/n/use/ds.** If you are already in Data Secure, you can return to the launchpad by selecting the Back « button.

Step 2: Select 'Mask Objects' from the Data Secure launchpad.



Step 3: Select the Business Object that the data-masking Run will be based on.

Note: The listed objects are those that data-masking Rules have been defined for in the data security Policies associated with the User Groups that the current user belongs to. Ensure that the user is assigned to a User Group associated with the data security Policy that contains the data-masking Rules desired for the Business Object.



Policy: EPI-USE default delivered policy

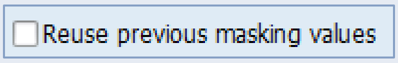
Masking options

- Customer
  - ☑ Address
    - ○ Clear address
    - ● Scramble address
    - ○ Assign a new street name only
  - ☑ Banking detail
    - ○ Remove bank account numbers
    - ● Scramble bank account numbers
  - ☑ Names
    - ○ Assign constant value to name — Constant value: ; Constant value: ;
    - ● Scramble name
  - ☑ Customer contact partner
    - ○ Remove contact partner details
    - ● Scramble contact partner details
  - ☑ Search term
    - ○ Clear search term
    - ● Set search term to scrambled name
  - ☑ Customer tax number
    - ○ Clear tax number
    - ● Scramble tax number
    - ○ Assign constant tax number — Constant value: ; Constant value: ; Constant value: ; Constant value
  - ☑ Telephone numbers
    - ○ Clear numbers
    - ● Scramble numbers
    - ○ Assign constant numbers — Constant value: ; Constant value: ;
  - ☑ VAT registration numbers
    - ○ Clear VAT registration numbers
    - ● Scramble VAT registration numbers
    - ○ Assign Constant VAT registration number — Constant value: ;
- Address->Person Link as Customer
- Business Partner as Customer
- Central Person as Customer
- Main Address as Customer

Step 4: Select the Policy to be used for the Run.

The policies listed are those that are assigned to the User Groups the current user belongs to. The Policies are further filtered to those that contain Rules for the Business Object selected in step 3. Ensure that the Policy that contains the Rules intended for the Business Object is assigned to the User group the executing user belongs to.

On the Masking options screen for masking objects, next to the Policy field for which you must make a selection, you will also find a checkbox to re-use previous masking values:


☐ Reuse previous masking values

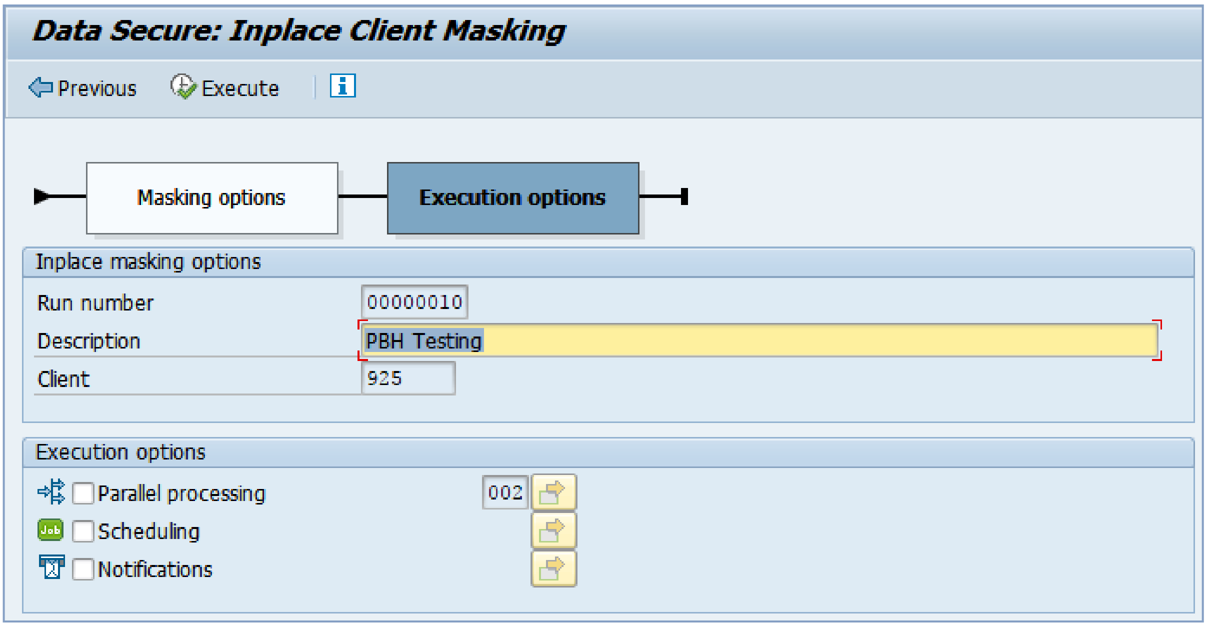
If the checkbox is selected, this will default your settings to the masking values used in the last Masking run that was executed on this system.

Step 5: Review the data-masking Rules and set the options to be used for each Rule. The available options are as follows:

Icon	Name	Functions
⇦ Previous	Previous	Moves you to the previous step on the Roadmap.
⇨ Next	Next	Progresses the Roadmap to the next Screen.
i	Information	Provides additional information about this screen.
☑	Rule Selection	The Checkbox indicates an active rule selection.
○ ●	Option selection	The selected radio button indicates an active behavior so that the user can select which Rule option to use for the current masking run.
✎	Default Assigned	A default user input has been assigned to the associated Rule option. Select the button to change this value.
✎	Requires input	Masking rule options require user input. Input is required if the option is selected or the rule has no other options.

Step 6: Click the ‘Next’ button or select ‘Execution options’ in the roadmap to proceed to the Execution options screen.

Step 7: Specify the execution options. The execution options available are as follows:



Data Secure: Inplace Client Masking

Inplace masking options

Run number 00000010

Description PBH Testing

Client 925

Execution options

□ Parallel processing 002

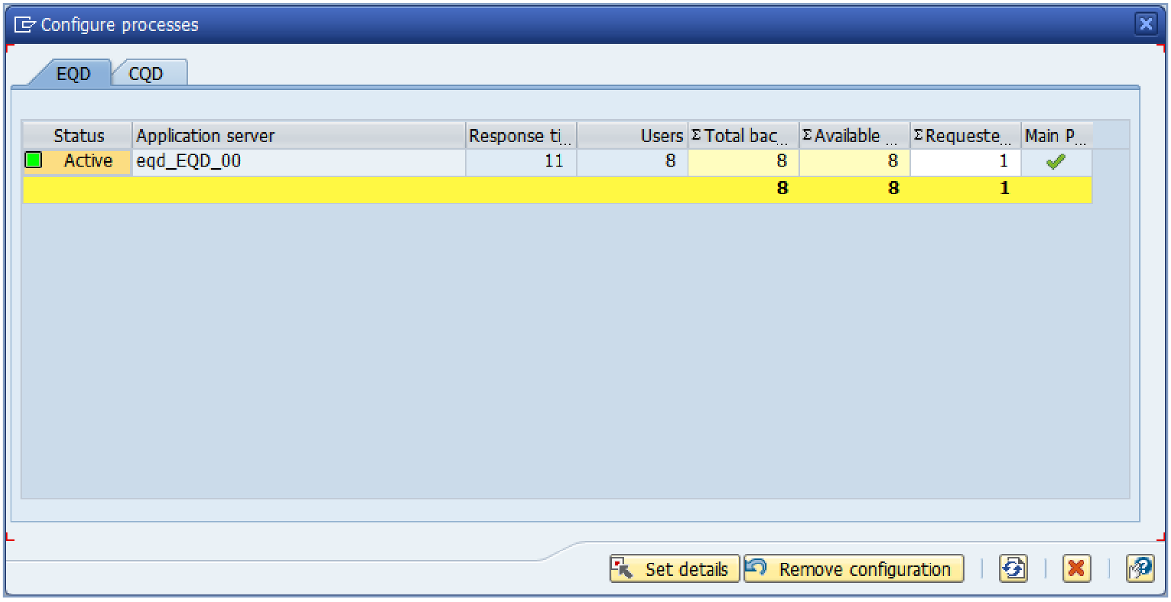
□ Scheduling

□ Notifications

- **Description**
  Create a description for the new Run so that you will be able to identify it in the Monitor Desk later. The default description will be the name of the Data Secure policy that you selected in step 3 above.

- **Parallel processing**
  Select this checkbox if you wish to configure the distribution of work through parallel processes. This allows you to use more than one background work process to do the work, thus achieving faster execution times.

  Once you have selected parallel processing, you can change the number of processes to be used. SAP will distribute the processes to the least busy application servers.



Configure processes

EQD CQD

Status	Application server	Response ti...	Users	ΣTotal bac...	ΣAvailable ...	ΣRequeste...	Main P...
🟩 Active	eqd_EQD_00	11	8	8	8	1	✓
				8	**8**	**1**	

If you wish to override this by configuring distribution yourself, click on the ‘Configure’ button. This will open a pop-up screen allowing you to view and configure the distribution of parallel processes, where for each system you select the number of processes to use and the application server that they should execute on, manually.

If the Data-masking run involves multiple systems and/or clients, different settings can be maintained to be used for each system/client. To do so, select the tab corresponding to the system and then specify the distribution of processes among the Application servers of that system as detailed above. If the number of processes is specified before the parallel processing is defined, the number of processes will be scheduled for each system unless refined.

> Runs are always executed in the background, as they generally affect a large amount of data and so have long run times.

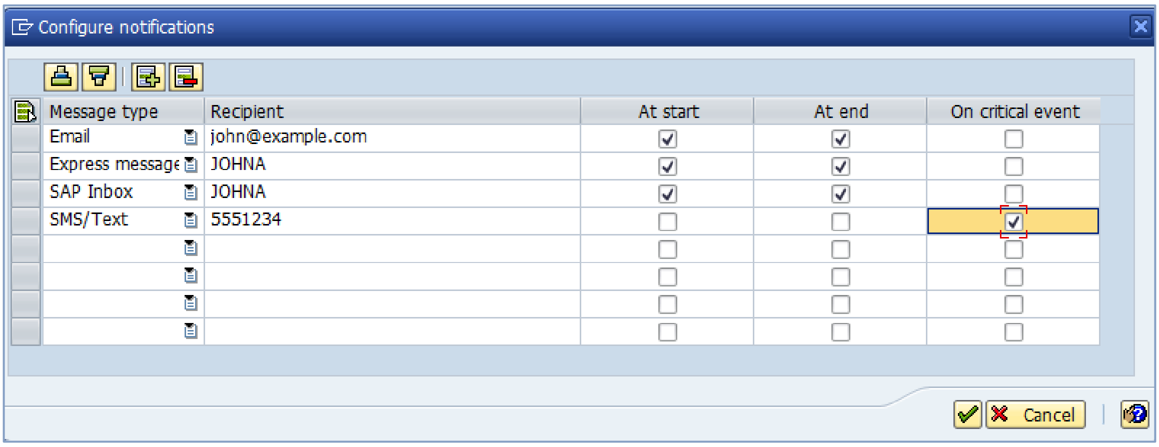
- **Scheduling**

  Select this checkbox to schedule the Run at a future date and/or time. You can click the ‘Configure’ button to set the execution date and time.

- **Notifications**

  Select this checkbox to notify users of Sync progress and events. Click the ‘Configure’ button to specify notification methods, the recipients and set the types and frequency of notification messages.

  The following pop-up will appear:



Message type	Recipient	At start	At end	On critical event
Email	john@example.com	☑	☑	□
Express message	JOHNA	☑	☑	□
SAP Inbox	JOHNA	☑	☑	□
SMS/Text	5551234	□	□	☑
		□	□	□
		□	□	□
		□	□	□
		□	□	□

Complete the following sections:

- **Message type:** This indicates how the notifications must be sent:
  - Email: will send an email notification to the email address specified in the Recipient column.
  - Express message: will send an SAP Express message to the SAP User account specified in the Recipient column.
  - SAP Inbox: will send a message to the SAP Inbox of the SAP User account specified in the Recipient column.
  - SMS/Text: will send a notification via Short Message Service (SMS) or Text to the mobile phone number specified in the Recipient column.
- **Recipient:** The content to be entered in this field depends on the message type you selected. Enter the required email address, User account ID or mobile phone number.
- **At start:** Selecting this checkbox will send a notification to the specified recipient when the execution of the Sync has started.
- **At end:** Selecting this checkbox will send a notification to the specified recipient when the execution of the Sync has ended.
- **On critical event:** Selecting this checkbox will send a notification to the specified recipient if a critical event, such as an error that prevents further execution of a Sync process, occurs.

Confirm the pop-up. The Sync will then be configured to send out the specified notifications.

Step 8: Click 'Execute' Execute to execute the data-masking Run according to its current configuration. The Data Secure Run will start as soon as a background work process becomes available in the system or, if it is scheduled for later, will start at the time you set.

DSM Data Secure will take you to the Monitor Desk, where you can monitor the progress of the Run and access details of and information on the Run.

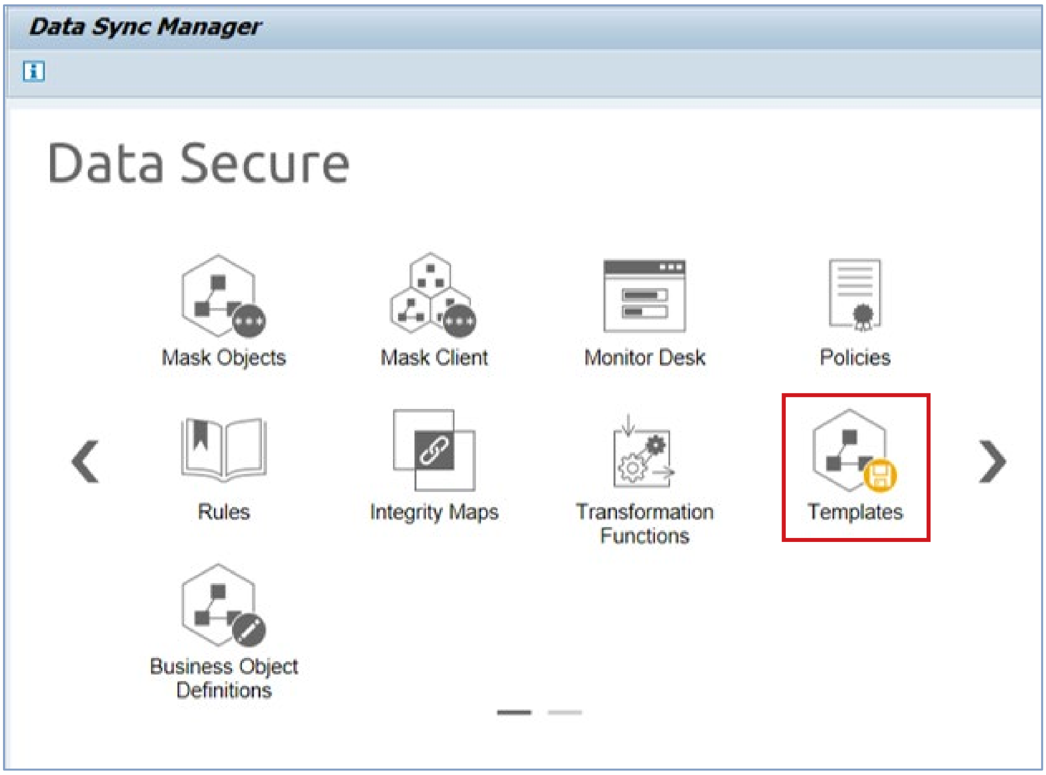
3.2 In-line Data Secure Run

Data Secure can also be used in conjunction with Data Sync Manager Object Sync and Data Sync Manager Client Sync when transferring data between source and target clients. For more information regarding the setup of Data Secure Runs that execute as part of DSM Object Sync or DSM Client Sync, please refer to the respective User Guides for Data Sync Manager Object Sync and Client Sync.

3.3 Create 'In-place' Data Secure run templates

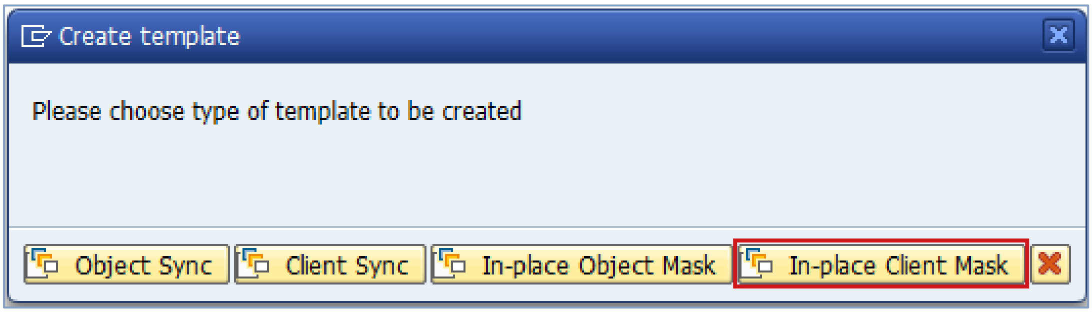
To create custom templates as part of the In-place masking runs process, select the 'Templates' icon on the Data Secure page. Alternatively, click on the Create Template icon on the Template Maintenance toolbar to start. The template creation process has four steps:

1. Select the type of template.
2. In-place Object Masking only: Select the Object to be masked in the template.
3. Select the masking policy and masking options.
4. Define the Execution options for the template.



3.3.1 Create an In-place 'Mask Client' run template

a. Select the type of template.

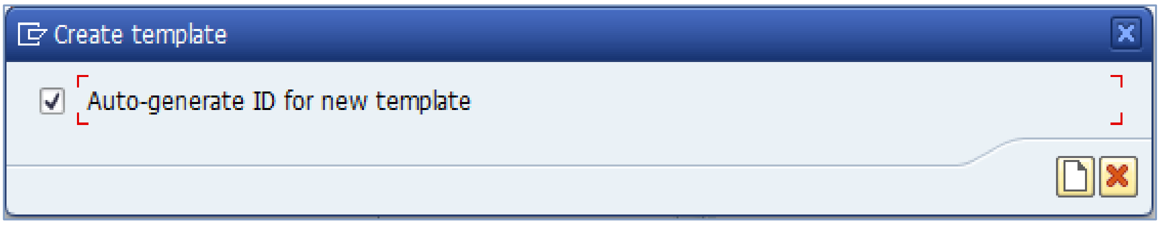


Create template

Please choose type of template to be created

To create a template for In-place Client Mask select the 'In-place Client Mask' button.

For the 'Client Sync' and 'Object Sync' template creation instructions, please refer to the respective product manuals.

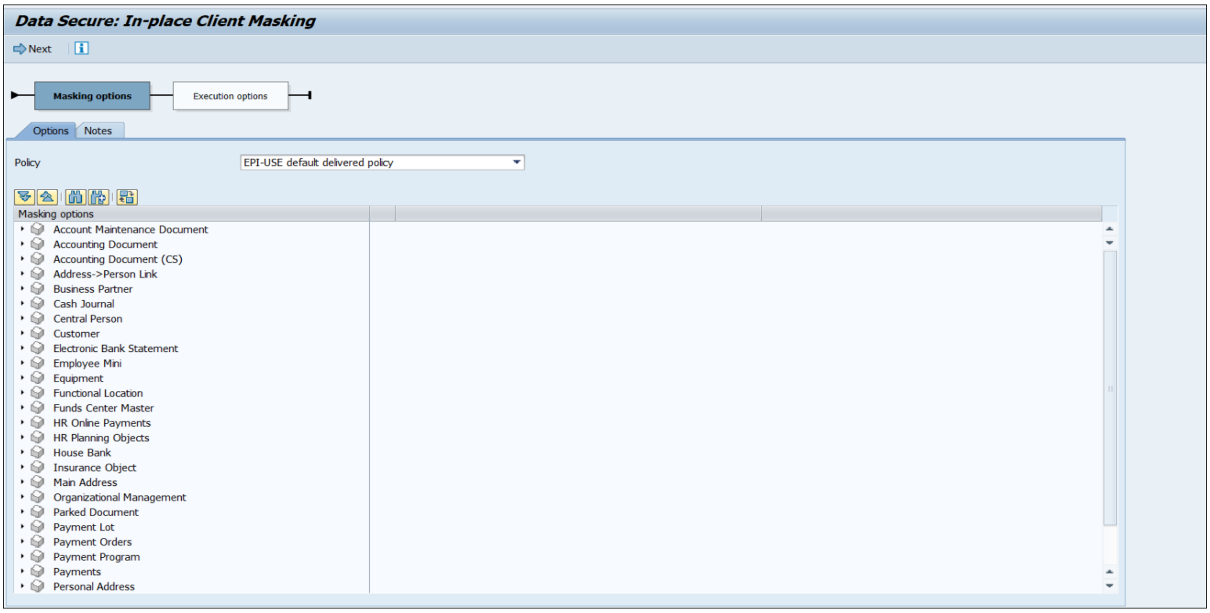


Create template

☑ Auto-generate ID for new template

As a default 'Auto-generate ID for new template' will be selected and this will assign your template an ID number automatically in sequence. To give your template a specific ID name, deselect the 'Auto-generate…' checkbox and enter the ID you want in the text box that appears. Customized IDs should have a technical name starting with a Z or Y to match with SAP customizing naming conventions.

b. Masking Options



Data Secure: In-place Client Masking

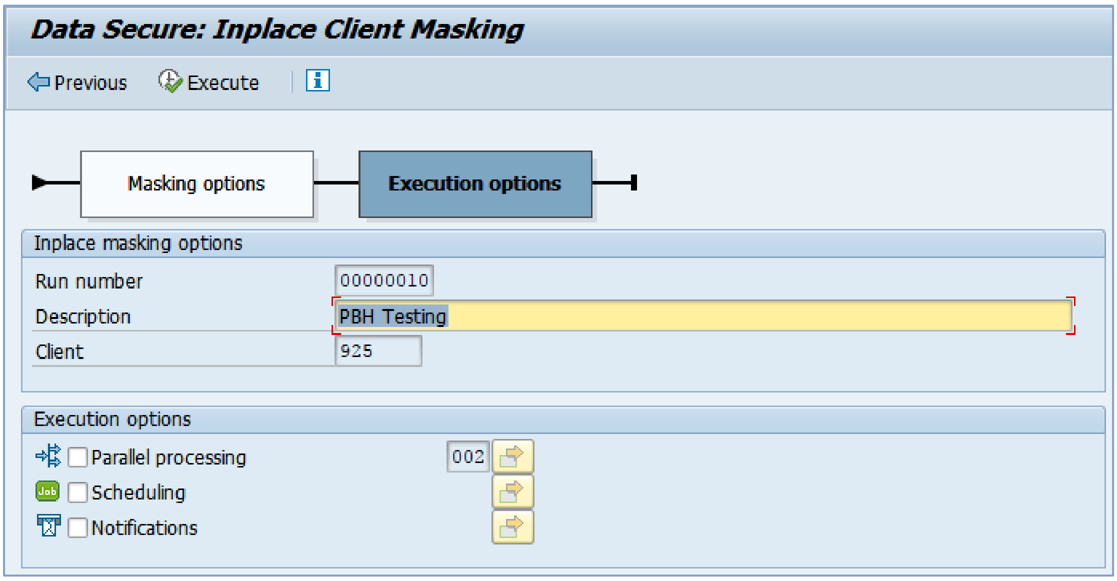
Policy: EPI-USE default delivered policy

Masking options
- Account Maintenance Document
- Accounting Document
- Accounting Document (CS)
- Address->Person Link
- Business Partner
- Cash Journal
- Central Person
- Customer
- Electronic Bank Statement
- Employee Mini
- Equipment
- Functional Location
- Funds Center Master
- HR Online Payments
- HR Planning Objects
- House Bank
- Insurance Object
- Main Address
- Organizational Management
- Parked Document
- Payment Lot
- Payment Orders
- Payment Program
- Payments
- Personal Address

Select the Policy to use for the run (Refer to Section 5 of this guide). Review the data-masking Rules (Refer to Section 6 of this guide) and set the options, input values and required default values (if any), to be used for each Rule. See Section 3.1.1 step 4 for detailed information about this screen.

c. Execute Options

Specify the execution options. See Section 3.1.1 step 6 for detailed information about this screen. The available execution options are as follows:



Data Secure: Inplace Client Masking

Inplace masking options

Run number	00000010
Description	PBH Testing
Client	925

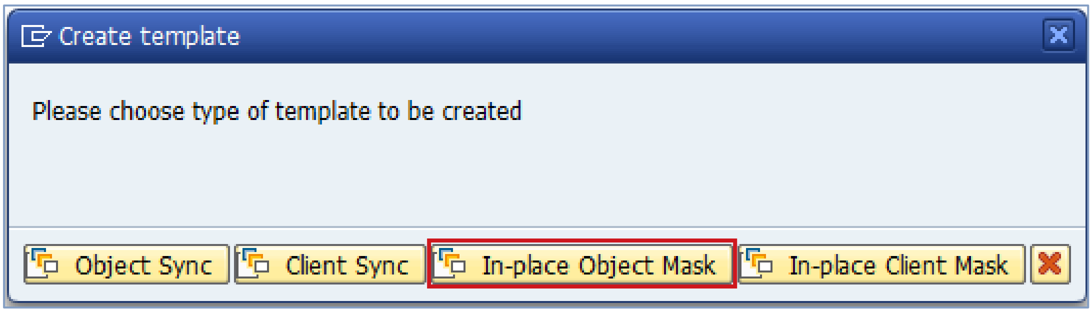
Execution options

- □ Parallel processing 002
- □ Scheduling
- □ Notifications

After you have specified your template selections, click on the ‘Save’ button to save the template.

3.3.2 Create an In-place 'Mask Object' run template

a. Select the type of template.

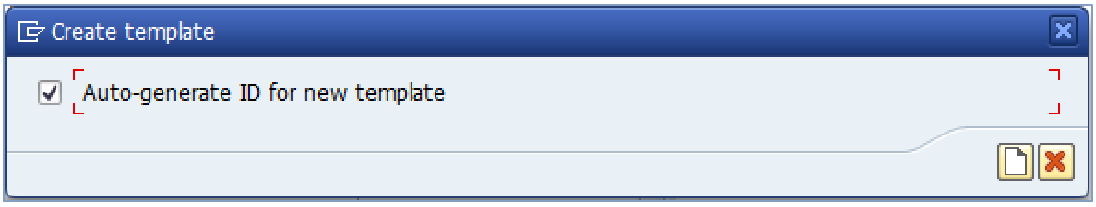


Create template

Please choose type of template to be created

To create a template for In-place Object Mask select the 'In-place Object Mask' button.

For the 'Client Sync' and 'Object Sync' template creation instructions, please refer to the respective product manuals.

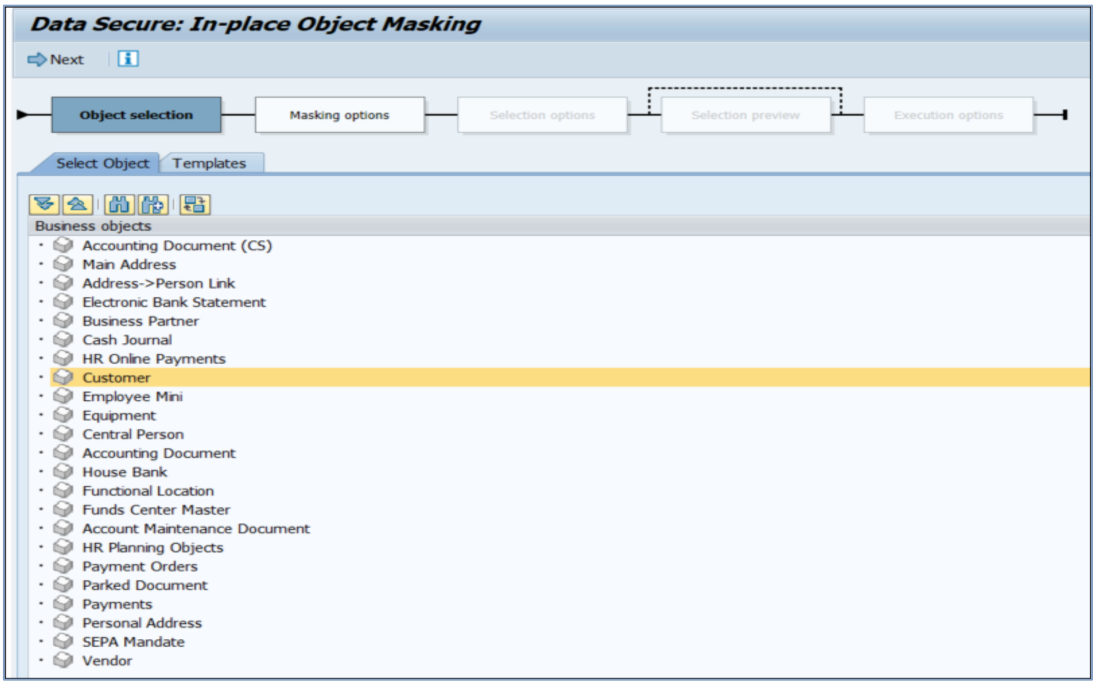


Create template

☑ Auto-generate ID for new template

As a default 'Auto-generate ID for new template' will be selected and this will assign your template an ID number automatically in sequence. To give your template a specific ID name, deselect the 'Auto-generate…' checkbox and enter the ID you want in the text box that appears. Customized IDs should have a technical name starting with a Z or Y to match with SAP customizing naming conventions.

b. Object selection



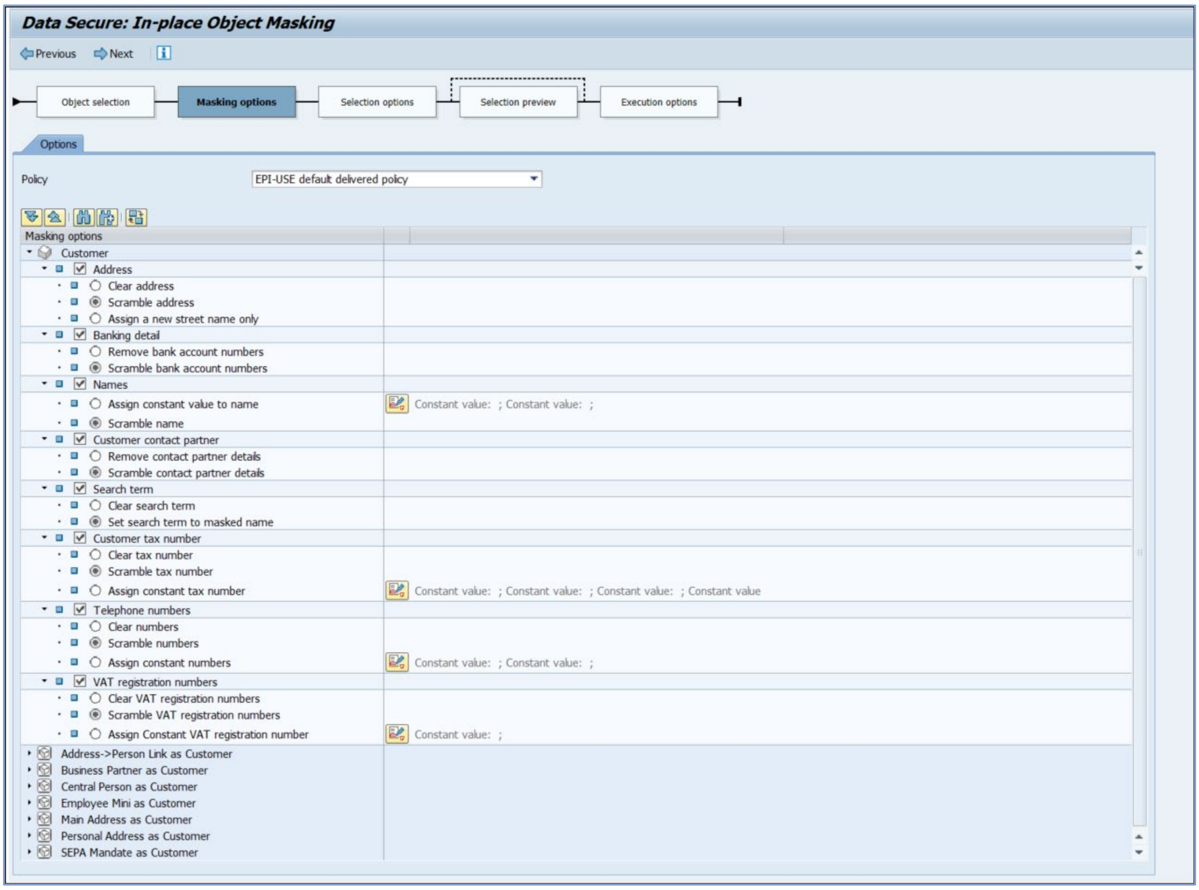
Business objects

- Accounting Document (CS)
- Main Address
- Address->Person Link
- Electronic Bank Statement
- Business Partner
- Cash Journal
- HR Online Payments
- Customer
- Employee Mini
- Equipment
- Central Person
- Accounting Document
- House Bank
- Functional Location
- Funds Center Master
- Account Maintenance Document
- HR Planning Objects
- Payment Orders
- Parked Document
- Payments
- Personal Address
- SEPA Mandate
- Vendor

The ‘Object selection’ screen allows you to select the main object you wish to use in the Run template. Select the Business Object that the data-masking Run Template will be based on.

c. Masking Options

Select the Policy to be used for the Run.



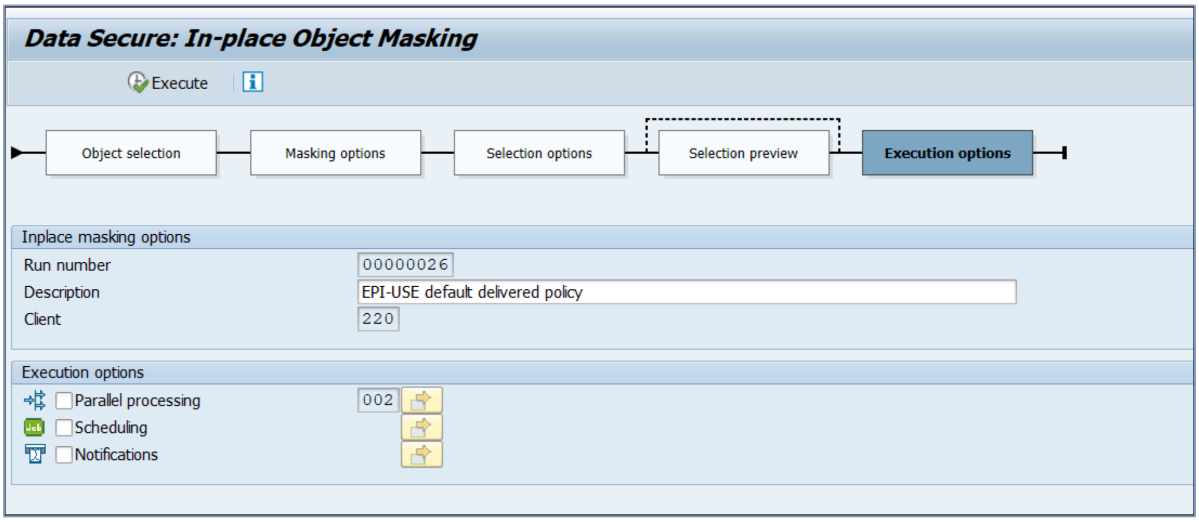
Data Secure: In-place Object Masking

Policy: EPI-USE default delivered policy

Masking options
- Customer
  - ☑ Address
    - ○ Clear address
    - ● Scramble address
    - ○ Assign a new street name only
  - ☑ Banking detail
    - ○ Remove bank account numbers
    - ● Scramble bank account numbers
  - ☑ Names
    - ○ Assign constant value to name — Constant value: ; Constant value: ;
    - ● Scramble name
  - ☑ Customer contact partner
    - ○ Remove contact partner details
    - ● Scramble contact partner details
  - ☑ Search term
    - ○ Clear search term
    - ● Set search term to masked name
  - ☑ Customer tax number
    - ○ Clear tax number
    - ● Scramble tax number
    - ○ Assign constant tax number — Constant value: ; Constant value: ; Constant value: ; Constant value
  - ☑ Telephone numbers
    - ○ Clear numbers
    - ● Scramble numbers
    - ○ Assign constant numbers — Constant value: ; Constant value: ;
  - ☑ VAT registration numbers
    - ○ Clear VAT registration numbers
    - ● Scramble VAT registration numbers
    - ○ Assign Constant VAT registration number — Constant value: ;
- Address->Person Link as Customer
- Business Partner as Customer
- Central Person as Customer
- Employee Mini as Customer
- Main Address as Customer
- Personal Address as Customer
- SEPA Mandate as Customer

The policies listed here are those that are assigned to the User Groups that the current user belongs to. The Policies are further filtered to include only those that contain Rules for the Business Object selected in the previous step. Ensure that the Policy that contains the Rules you want to use to mask the Business Object data are assigned to the User group the executing user belongs to.

d. Execution options



Data Secure: In-place Object Masking

Inplace masking options

Run number: 00000026

Description: EPI-USE default delivered policy

Client: 220

Execution options

☐ Parallel processing 002

☐ Scheduling

☐ Notifications

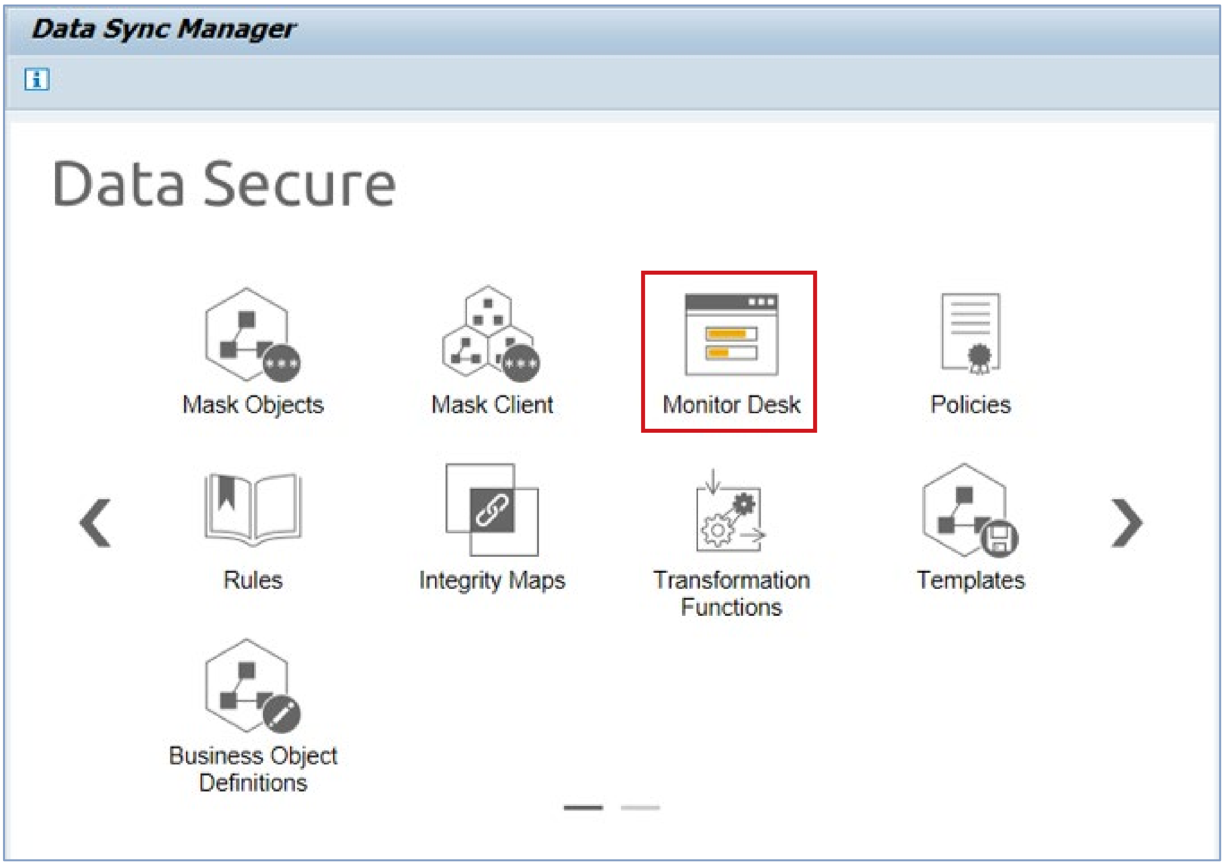
Refer to Section 3.1.2 step 7 for the 'Execution options' for a detailed description of this step. After you have specified your template selections, click on the 'Save' button to save these selections in the template.

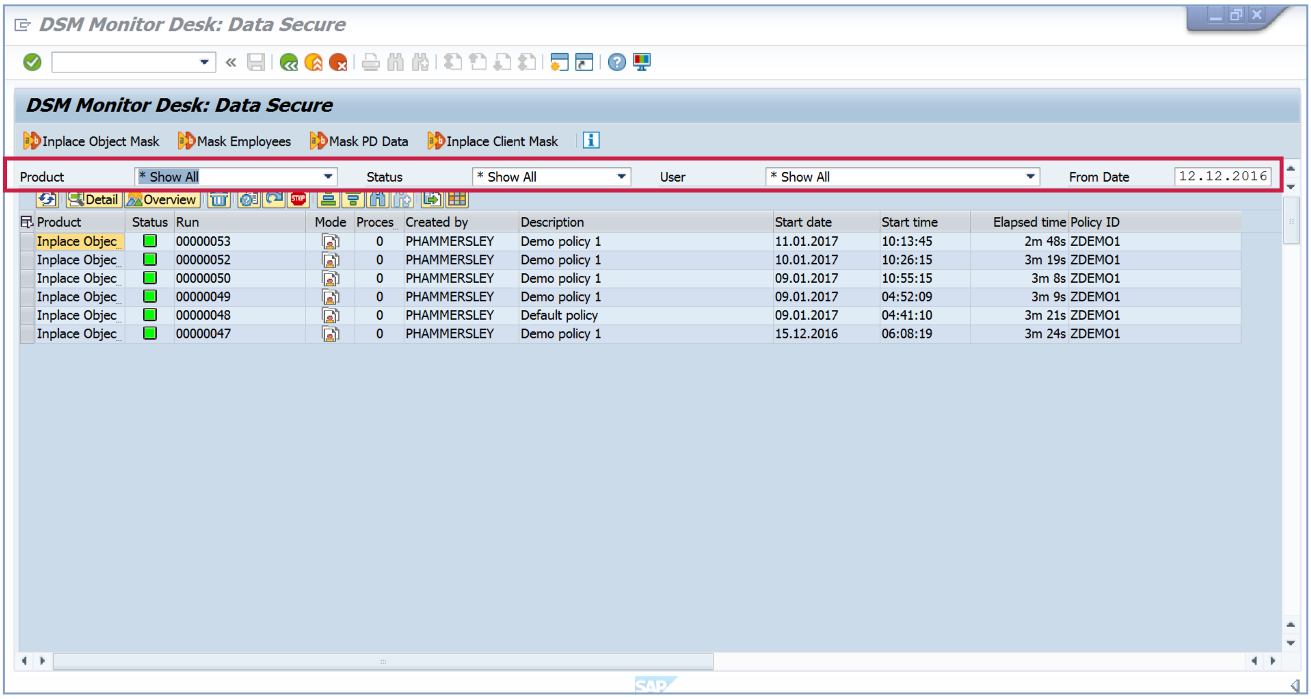
4. Monitor Desk

The Data Secure Monitor Desk is reached as follows:

Step 1: Enter the transaction code **/n/use/ds**. The Data Secure launchpad is displayed.

Step 2: Select the ‘Monitor Desk’ icon to display the Data Secure Run Monitor Desk screen.



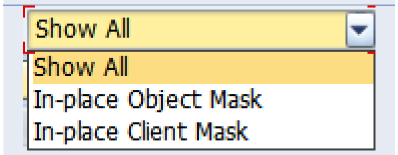
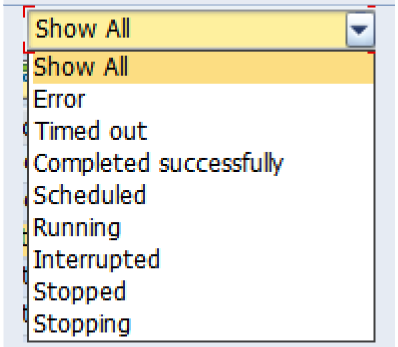


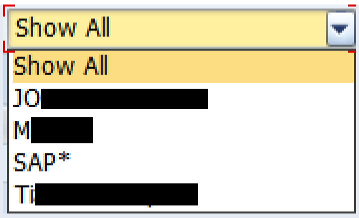
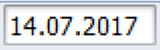
Product: * Show All Status: * Show All User: * Show All From Date: 12.12.2016

Product	Status	Run	Mode	Proces	Created by	Description	Start date	Start time	Elapsed time	Policy ID
Inplace Objec	🟩	00000053		0	PHAMMERSLEY	Demo policy 1	11.01.2017	10:13:45	2m 48s	ZDEMO1
Inplace Objec	🟩	00000052		0	PHAMMERSLEY	Demo policy 1	10.01.2017	10:26:15	3m 19s	ZDEMO1
Inplace Objec	🟩	00000050		0	PHAMMERSLEY	Demo policy 1	09.01.2017	10:55:15	3m 8s	ZDEMO1
Inplace Objec	🟩	00000049		0	PHAMMERSLEY	Demo policy 1	09.01.2017	04:52:09	3m 9s	ZDEMO1
Inplace Objec	🟩	00000048		0	PHAMMERSLEY	Default policy	09.01.2017	04:41:10	3m 21s	ZDEMO1
Inplace Objec	🟩	00000047		0	PHAMMERSLEY	Demo policy 1	15.12.2016	06:08:19	3m 24s	ZDEMO1

4.1 Monitor Desk Overview

The Monitor Desk overview bar lists Data Secure Runs according to the filtering options specified. The available filtering options are:

Name	View	Functions
Product	 Show All Show All In-place Object Mask In-place Client Mask	Filters Runs to display In-place Object Masking only, In-place Client Masking only or to show Runs of both types.
Status	 Show All Show All Error Timed out Completed successfully Scheduled Running Interrupted Stopped Stopping	Filters Runs according to the following statuses: ■ Error: Run was stopped due to a critical error detected. ■ Timed out: Run has exceeded wait time for action in other process/system and has stopped. ■ Completed: Completed successfully without critical errors. ■ Scheduled: Run is scheduled to execute at future date and time. ■ Running: Run is currently executing. ■ Interrupted: Run status is inactive because one or more processes ended unexpectedly. ■ Stopped: Run processes were stopped by user. ■ Stopping: Run instructed to stop and awaiting termination of all processes.

Users	 Show All Show All JO[redacted] M[redacted] SAP* Ti[redacted]	Filters Runs by user executing it.
From Date	 14.07.2017	Filters runs by start date.

The following options are available for the Data Secure Runs listed in the Monitor Desk overview:

Icon	Name	Functions
⟳	Refresh	Refreshes the Run Summary.
Detail	Details	Opens and displays the selected Run's details in the Run Details screen.
Overview	Run Overview	View the selected Run's original settings. You can re-use the Run by clicking on the Reuse 'Reuse' button available in the Run Overview. Data Secure will then create a new Run with a new Run number, but the same setup and options as the original Run. You may change the options if you wish.
🗑	Delete	Deletes the selected Run or series of Runs. The Run settings and any history of the execution details are deleted. Any Audit Logs associated with the Run are also deleted.
?	Download Diagnostic Log	Download the (Diagnostic log) file to send to EPI-USE Labs for analysis for support purposes: ▪ Click on the button to select a file name and destination where the file will be saved. ▪ Submit the file to EPI-USE Labs via the EPI-USE Labs Support Portal, by attaching it to a ticket. This file can only be viewed by the EPI-USE Labs Support and Development teams.
↻	Resume	Will resume a stopped Run.
STOP	Stop	Will stop a Run. The Run can be resumed later.
✂	Trim	Reduces DSM's data footprint by removing old data.
▲	Sort in Ascending Order	Displays the Run List in ascending Run number order.
▼	Sort in Descending Order	Displays the Run List in descending Run number order.

🔍 🔍	Find/Find Next	Allows you to search for a specific Run in the list by entering a search string.
📤	Export	Exports the Run List to different formats such as a local file, HTML format or Excel spreadsheet, etc.
▦	Change layout	Changes the layout and appearance of the display of the Run List, such as which columns are displayed and the sorting order.

To display detailed information regarding a single Data Secure Run, select the Run and click on the Detail Detail button or double-click on the Run entry in the list.

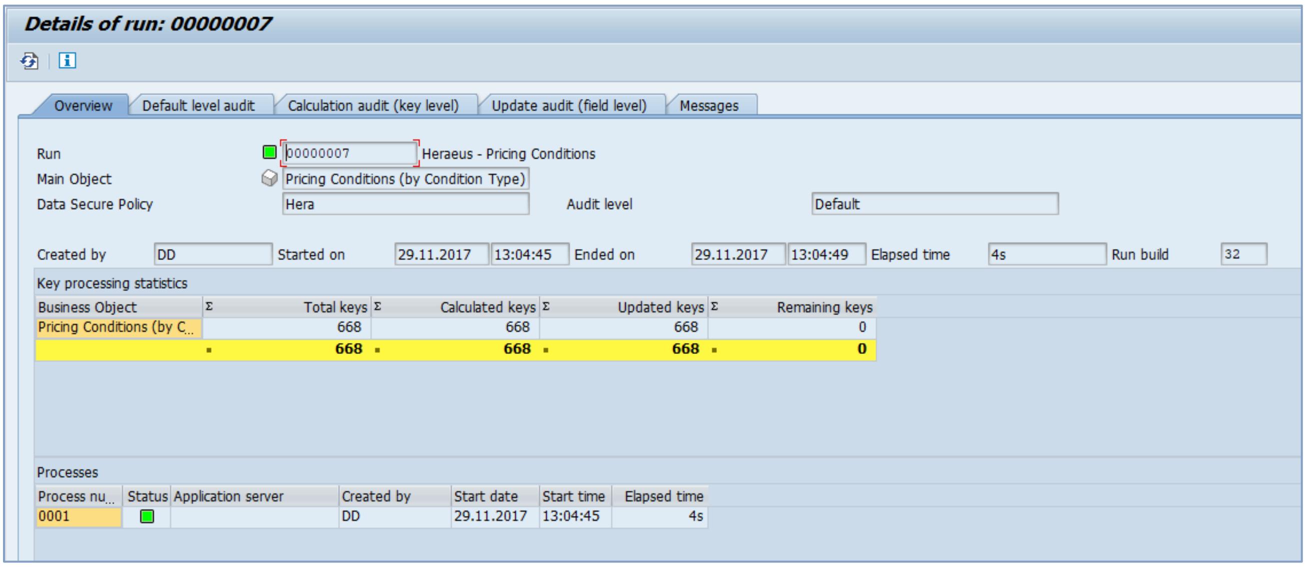
4.2 Status icons

The following icons are used to indicate the status of a Run or its processes and appear in the Status column of the list of Runs on the Monitor Desk and/or on the Run information screens.

Icon	Meaning	Functions
🔴	Error	There was an error during the Run that needs to be investigated.
⚠	Warning	There were warnings during the Run. Read the messages in the Messages tab.
🟩	Completed	The Run completed successfully.
⛔	Interrupted	The Run was terminated due to an unexpected event.

4.3 Run detail

The Run detail screen contains multiple areas, in the form of tabs, that display the details of a Data Secure Run. The areas/tabs are as follows:



Details of run: 00000007

Overview | Default level audit | Calculation audit (key level) | Update audit (field level) | Messages

Run	🟩 00000007	Heraeus - Pricing Conditions							
Main Object	Pricing Conditions (by Condition Type)								
Data Secure Policy	Hera	Audit level	Default						
Created by	DD	Started on	29.11.2017 13:04:45	Ended on	29.11.2017 13:04:49	Elapsed time	4s	Run build	32

Key processing statistics

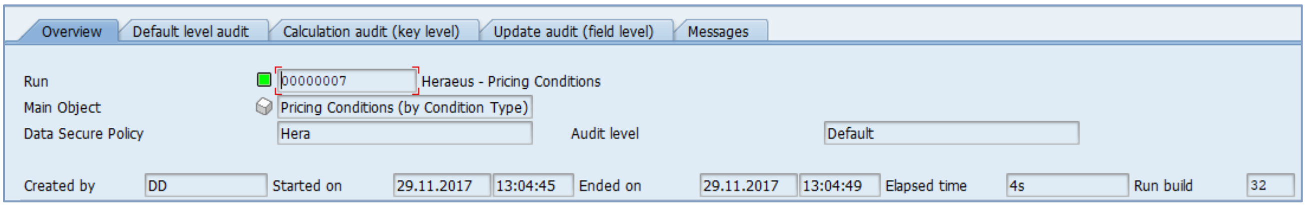
Business Object	Σ Total keys	Σ Calculated keys	Σ Updated keys	Σ Remaining keys
Pricing Conditions (by C...	668	668	668	0
	668	668	668	0

Processes

Process nu...	Status	Application server	Created by	Start date	Start time	Elapsed time
0001	🟩		DD	29.11.2017	13:04:45	4s

4.3.1 Run detail overview

The Run 'Overview' provides high-level information on the execution status of the Run. The details listed are as follows:

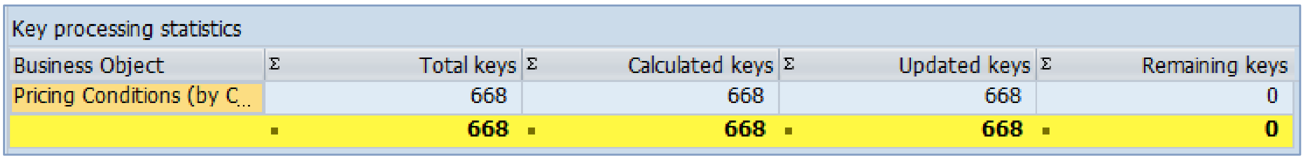


Overview | Default level audit | Calculation audit (key level) | Update audit (field level) | Messages

Run	🟩 00000007	Heraeus - Pricing Conditions							
Main Object	Pricing Conditions (by Condition Type)								
Data Secure Policy	Hera	Audit level	Default						
Created by	DD	Started on	29.11.2017 13:04:45	Ended on	29.11.2017 13:04:49	Elapsed time	4s	Run build	32

Heading	Functions
Run	Shows the status of the Run, the identification number of the Run and the Run description.
Main Object	The Business Object the run is based on (if any).
Data Secure Policy	The technical name of the Policy used in the masking Run.
Audit level	The Audit level detail used for the masking Run. (This is discussed in greater detail in the next section.)
Created By	The user that executed the Run.
Started on	The date the Run was executed.
Ended on	The date the Run completed.
Elapsed time	The total amount of execution time.
Run build	The build number of the Data Secure version that executed the masking Run.

The Run 'Overview' lists the key processing statistics for the Run. The meanings of the columns are as follows:

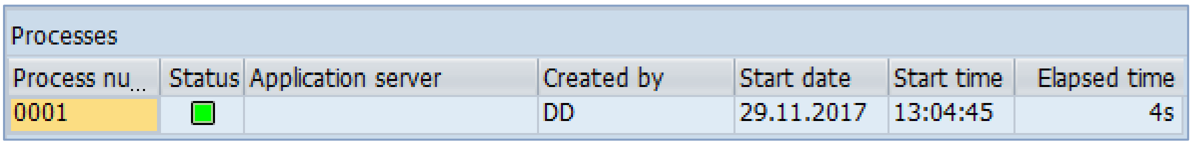


Key processing statistics

Business Object	Σ Total keys	Σ Calculated keys	Σ Updated keys	Σ Remaining keys
Pricing Conditions (by C...	668	668	668	0
	▪ 668	▪ 668	▪ 668	▪ 0

Heading	Functions
Business Object	Lists all the objects used in the Run.
Total keys	The total number of keys processed for the Business Object on this line.
Calculated keys	The total number of Business Object keys for which masking values were calculated.
Updated keys	The total number of Business Object keys for which updates were executed.
Remaining keys	The total number of keys to be processed that have not been calculated and/or updated to completion.

The 'Processes overview' window at the bottom of the screen lists the process statuses for the processes utilized by the Run. The meanings of all the columns are as follows:

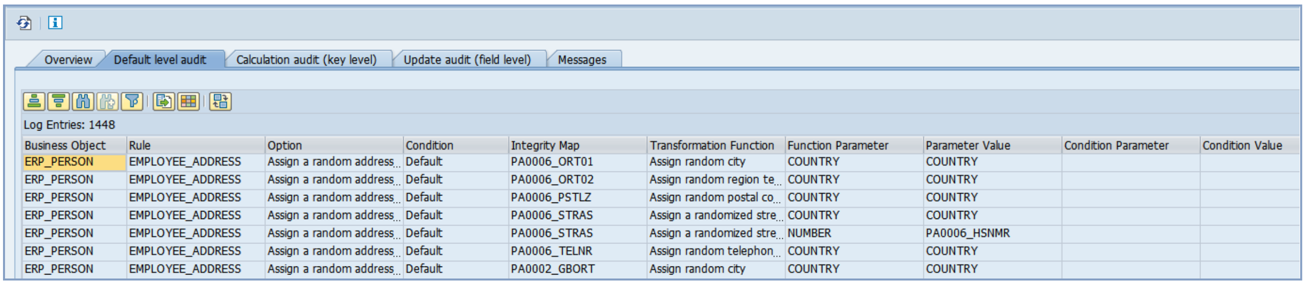


Processes

Process nu...	Status	Application server	Created by	Start date	Start time	Elapsed time
0001	🟩		DD	29.11.2017	13:04:45	4s

Heading	Functions
Process Number	The sequential number of the process used in the execution of the masking Run.
Status	The execution status of the process.
Application server	The sever used to execute the process for the Run.
Created by	The user that executed the process of the Run
Start date	The date the Run process started execution.
Start time	The time the Run process started execution.
Elapsed time	The total execution time for the process.

1.1.2 Default level audit



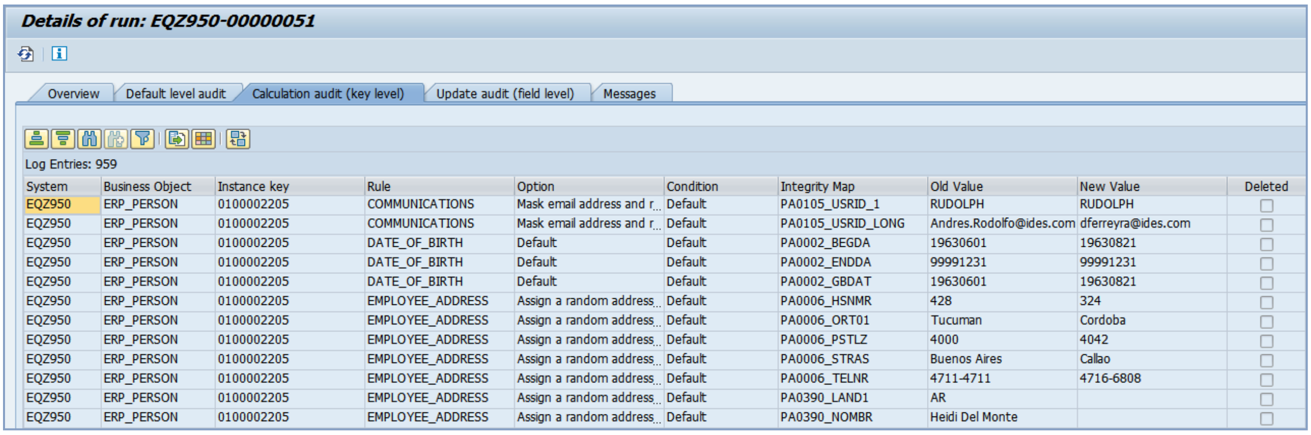
Log Entries: 1448

Business Object	Rule	Option	Condition	Integrity Map	Transformation Function	Function Parameter	Parameter Value	Condition Parameter	Condition Value
ERP_PERSON	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_ORT01	Assign random city	COUNTRY	COUNTRY		
ERP_PERSON	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_ORT02	Assign random region te...	COUNTRY	COUNTRY		
ERP_PERSON	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_PSTLZ	Assign random postal co...	COUNTRY	COUNTRY		
ERP_PERSON	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_STRAS	Assign a randomized stre...	COUNTRY	COUNTRY		
ERP_PERSON	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_STRAS	Assign a randomized stre...	NUMBER	PA0006_HSNMR		
ERP_PERSON	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_TELNR	Assign random telephon...	COUNTRY	COUNTRY		
ERP_PERSON	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0002_GBORT	Assign random city	COUNTRY	COUNTRY		

The ‘Default audit level’ tab provides a break-down of the masking Rules that were active when the data-masking Run was executed. The detail of the information provided starts with the Business Object context on the left and proceeds all the way down to the individual parameter values provided to masking Rules on the right. This allows you to view the exact detail for all active rules in the run:

Heading	Function
Business object	The Business Object context for the masking Rule.
Rule	The name of the Rule.
Option	The name of the (active) Option selected in the Rule.
Condition	The name of a condition placed on the Rule.
Integrity Map	The Integrity Map representing the list of fields affected by the Rule.
Transformation Function	The Transformation Function is used to assign values to the fields grouped by the Integrity Map.
Function Parameter	The name of an input parameter to the Transformation function.
Parameter value	The value assigned to the input parameter of the Transformation function for the Option-Condition combination.
Condition Parameter	The name of an input parameter to a condition on a Rule.
Condition Value	The value assigned to an input parameter of a condition parameter.

4.3.3 Calculation audit (key level)



Details of run: EQZ950-00000051

Log Entries: 959

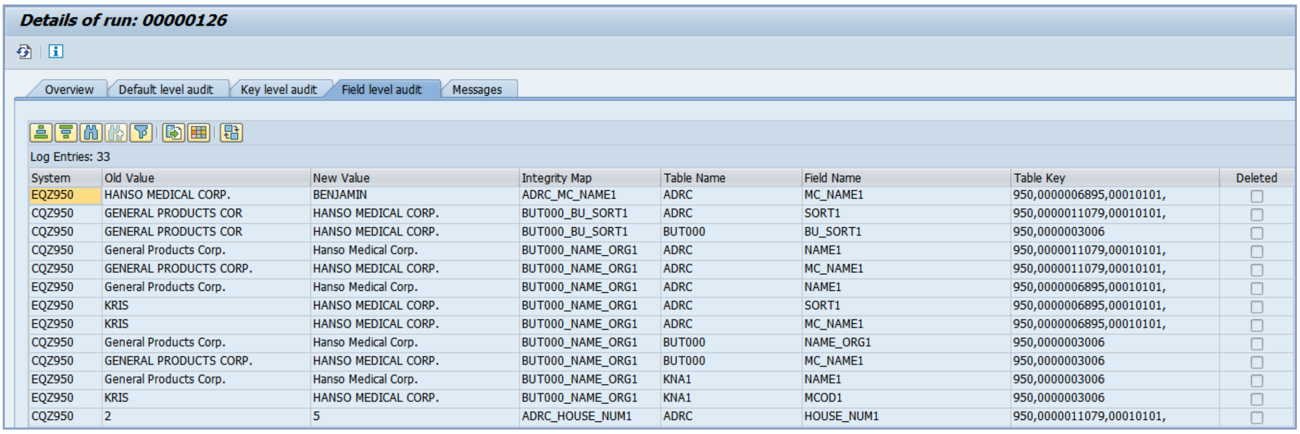
System	Business Object	Instance key	Rule	Option	Condition	Integrity Map	Old Value	New Value	Deleted
EQZ950	ERP_PERSON	0100002205	COMMUNICATIONS	Mask email address and r...	Default	PA0105_USRID_1	RUDOLPH	RUDOLPH	□
EQZ950	ERP_PERSON	0100002205	COMMUNICATIONS	Mask email address and r...	Default	PA0105_USRID_LONG	Andres.Rodolfo@ides.com	dferreyra@ides.com	□
EQZ950	ERP_PERSON	0100002205	DATE_OF_BIRTH	Default	Default	PA0002_BEGDA	19630601	19630821	□
EQZ950	ERP_PERSON	0100002205	DATE_OF_BIRTH	Default	Default	PA0002_ENDDA	99991231	99991231	□
EQZ950	ERP_PERSON	0100002205	DATE_OF_BIRTH	Default	Default	PA0002_GBDAT	19630601	19630821	□
EQZ950	ERP_PERSON	0100002205	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_HSNMR	428	324	□
EQZ950	ERP_PERSON	0100002205	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_ORT01	Tucuman	Cordoba	□
EQZ950	ERP_PERSON	0100002205	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_PSTLZ	4000	4042	□
EQZ950	ERP_PERSON	0100002205	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_STRAS	Buenos Aires	Callao	□
EQZ950	ERP_PERSON	0100002205	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0006_TELNR	4711-4711	4716-6808	□
EQZ950	ERP_PERSON	0100002205	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0390_LAND1	AR		□
EQZ950	ERP_PERSON	0100002205	EMPLOYEE_ADDRESS	Assign a random address...	Default	PA0390_NOMBR	Heidi Del Monte		□

If active, the 'Calculation audit (key level)' details the behavior of the masking Run during the masking value calculation per Business Object Key. The detail of the information provided starts with the System where the masking occurs on the left down to the assigned masking values (per Business Object Key) on the right and are as follows:

Heading	Function
System	The system and client where the value assignment occurred.
Business object	The Business Object context for the masking Rule.
Instance key	A single key value processed for the Business Object, i.e. a single Customer or Vendor.
Rule	The name of the masking Rule.
Option	The name of the (active) Option selected in the Rule.
Condition	The name of the condition placed on the Rule.
Integrity Map	The Integrity Map representing the list of fields affected by the Rule.
Old Value	An original value found for the Instance key.
New Value	The masked value calculated to replace the old (original) value found for the Instance key by the assigned Transformation function.
Deleted	If checked, this indicates that records holding the old (original) value were flagged for removal.

The 'Calculation audit (key level)' and the 'Update audit (field level)' do not show content if they are not enabled on the Policy level. Also, content is not displayed, even if active, if the current user does not have auditing authorizations.

4.3.4 Update audit (field level)



Details of run: 00000126

Log Entries: 33

System	Old Value	New Value	Integrity Map	Table Name	Field Name	Table Key	Deleted
EQZ950	HANSO MEDICAL CORP.	BENJAMIN	ADRC_MC_NAME1	ADRC	MC_NAME1	950,0000006895,00010101,	□
CQZ950	GENERAL PRODUCTS COR	HANSO MEDICAL CORP.	BUT000_BU_SORT1	ADRC	SORT1	950,0000011079,00010101,	□
CQZ950	GENERAL PRODUCTS COR	HANSO MEDICAL CORP.	BUT000_BU_SORT1	BUT000	BU_SORT1	950,0000003006	□
CQZ950	General Products Corp.	Hanso Medical Corp.	BUT000_NAME_ORG1	ADRC	NAME1	950,0000011079,00010101,	□
CQZ950	GENERAL PRODUCTS CORP.	HANSO MEDICAL CORP.	BUT000_NAME_ORG1	ADRC	MC_NAME1	950,0000011079,00010101,	□
EQZ950	General Products Corp.	Hanso Medical Corp.	BUT000_NAME_ORG1	ADRC	NAME1	950,0000006895,00010101,	□
EQZ950	KRIS	HANSO MEDICAL CORP.	BUT000_NAME_ORG1	ADRC	SORT1	950,0000006895,00010101,	□
EQZ950	KRIS	HANSO MEDICAL CORP.	BUT000_NAME_ORG1	ADRC	MC_NAME1	950,0000006895,00010101,	□
CQZ950	General Products Corp.	Hanso Medical Corp.	BUT000_NAME_ORG1	BUT000	NAME_ORG1	950,0000003006	□
CQZ950	GENERAL PRODUCTS CORP.	HANSO MEDICAL CORP.	BUT000_NAME_ORG1	BUT000	MC_NAME1	950,0000003006	□
EQZ950	General Products Corp.	Hanso Medical Corp.	BUT000_NAME_ORG1	KNA1	NAME1	950,0000003006	□
EQZ950	KRIS	HANSO MEDICAL CORP.	BUT000_NAME_ORG1	KNA1	MCOD1	950,0000003006	□
CQZ950	2	5	ADRC_HOUSE_NUM1	ADRC	HOUSE_NUM1	950,0000011079,00010101,	□

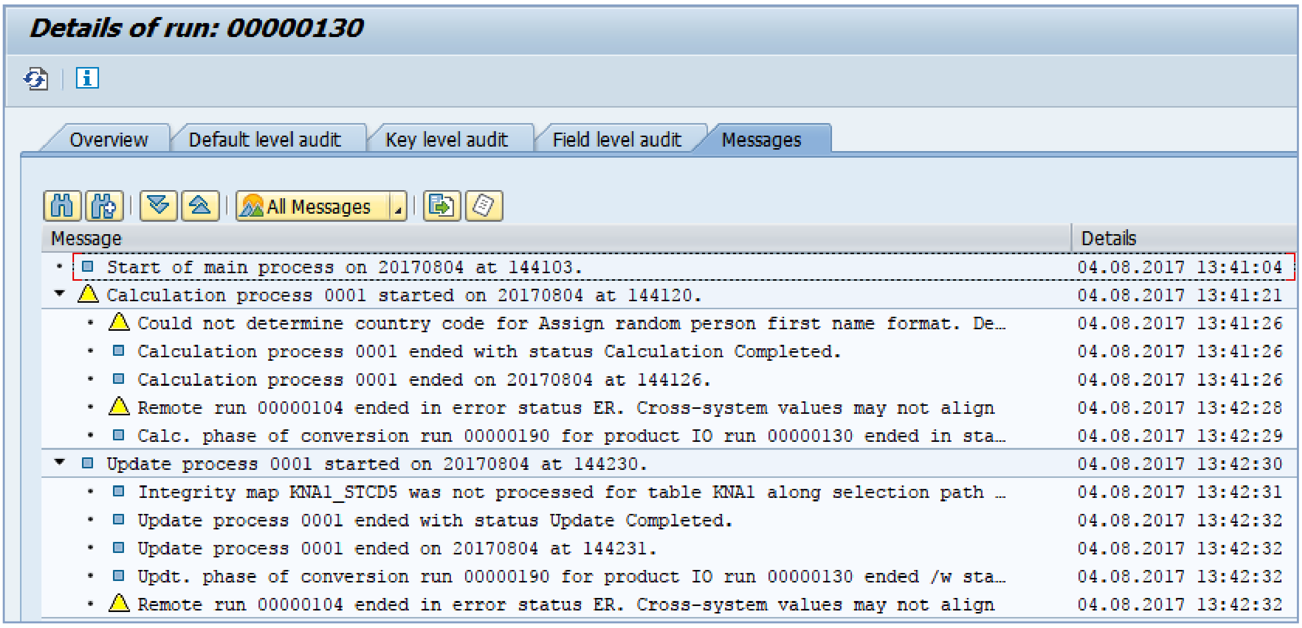
If active, the ‘Update audit (field level)’ details the behavior of the masking Run down to the field level when the masking Run is executed. The ‘Calculation audit (key level)’ and ‘Update audit (field level)’ tabs do not show content if the calculation audit or the update audit is not enabled on the Policy level. Also, content is not displayed, even if active, if the current user does not have auditing authorizations. The information detail starts from the System where the masking occurred on the left down to the assigned values and applicable table records on the right. The details provided are as follows:

Heading	Function
System	The system and client where the value assignment occurred.
Old Value	The original value of the field.
New Value	The masked value assigned to replace the original value in the field.
Integrity Map	The Integrity Map grouping for the affected field. (The Transformation Function assigned to this Integrity Map in a Rule produced the New value).
Table Name	The name of the table where the affected field occurs.
Field name	The name of the field affected.
Table Key	The table key of the record where the field was affected.
Deleted	If checked, indicates that the record was flagged for removal.

If a record or records are flagged for removal, the behavior depends on the execution context. When masking occurs as part of a data transfer (Client Sync or Object Sync) the data will not be exported from the original system. If the masking occurs ‘in-place’, the existing data record will be removed.

The update audit details may differ from the calculation audit details in some cases. This is due to the calculation audit details being written when the masking values are initially calculated on every system whereas the update level details are captured when the assigned masking values are written to the records. Because multiple masking rules may apply to the same table field and assigned values may be shared between systems, the final assigned value in the update field may differ from the initial masking value determined in the calculation phase.

4.3.5 Messages



```
Message                                                                      Details
• □ Start of main process on 20170804 at 144103.                             04.08.2017 13:41:04
▼ ⚠ Calculation process 0001 started on 20170804 at 144120.                  04.08.2017 13:41:21
   • ⚠ Could not determine country code for Assign random person first name format. De…   04.08.2017 13:41:26
   • □ Calculation process 0001 ended with status Calculation Completed.     04.08.2017 13:41:26
   • □ Calculation process 0001 ended on 20170804 at 144126.                 04.08.2017 13:41:26
   • ⚠ Remote run 00000104 ended in error status ER. Cross-system values may not align   04.08.2017 13:42:28
   • □ Calc. phase of conversion run 00000190 for product IO run 00000130 ended in sta…   04.08.2017 13:42:29
▼ □ Update process 0001 started on 20170804 at 144230.                       04.08.2017 13:42:30
   • □ Integrity map KNA1_STCD5 was not processed for table KNA1 along selection path …   04.08.2017 13:42:31
   • □ Update process 0001 ended with status Update Completed.               04.08.2017 13:42:32
   • □ Update process 0001 ended on 20170804 at 144231.                      04.08.2017 13:42:32
   • □ Updt. phase of conversion run 00000190 for product IO run 00000130 ended /w sta…   04.08.2017 13:42:32
   • ⚠ Remote run 00000104 ended in error status ER. Cross-system values may not align   04.08.2017 13:42:32
```

The 'Messages' tab displays a combined trace of all the messages that were logged by data-masking processes in the execution of the Run. The following options are available for processing the messages:

Icon	Meaning	Function
	Find/Find Next	Finds the specified term in the trace messages.
	Collapse	Collapses all trace messages in the selected tree node or collapses to the highest level node if none selected.
	Expand	Expands all trace messages in the selected tree node or expands all nodes if none selected.
All Messages	Message Type Filter	By clicking on the 'Messages' button, you can toggle between displaying one of the following message categories: All Messages Errors and Warnings Only Errors

	Download Trace	Exports the Message trace information to a DSM trace file (.trx extension). This trace information will automatically be included as part of the (Diagnostic Log) information when you select ‘Diagnostic Log’ on the Run List toolbar.
	Display as a report:	Displays the Message trace as a report output. This is useful if the Message trace is very long.

5. Policies

You will use the Data Secure Policy editor to create and manage Policies.

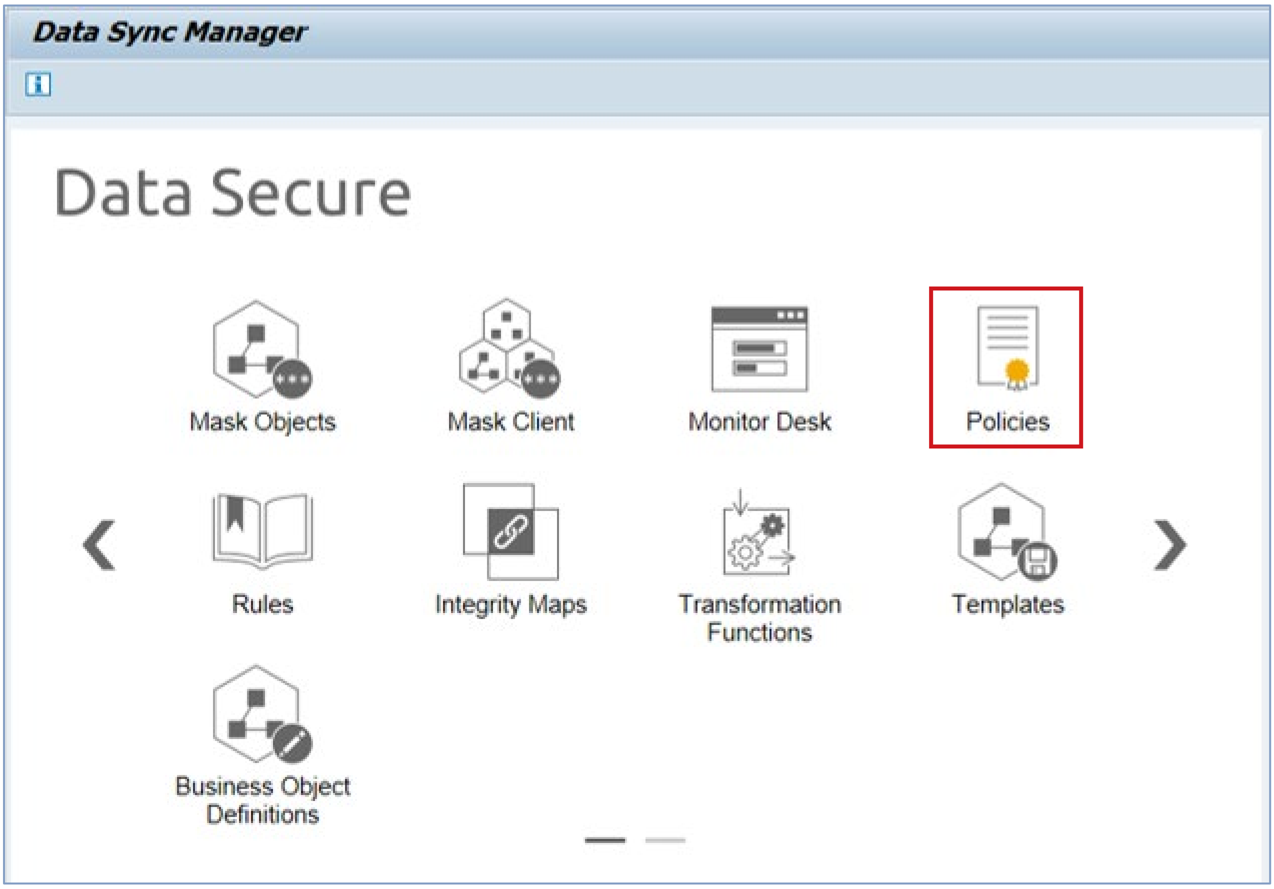
> ★ It is best practice for the security team to give functional teams access to this transaction so that they can define the policies.

5.1 Access the Policy Editor

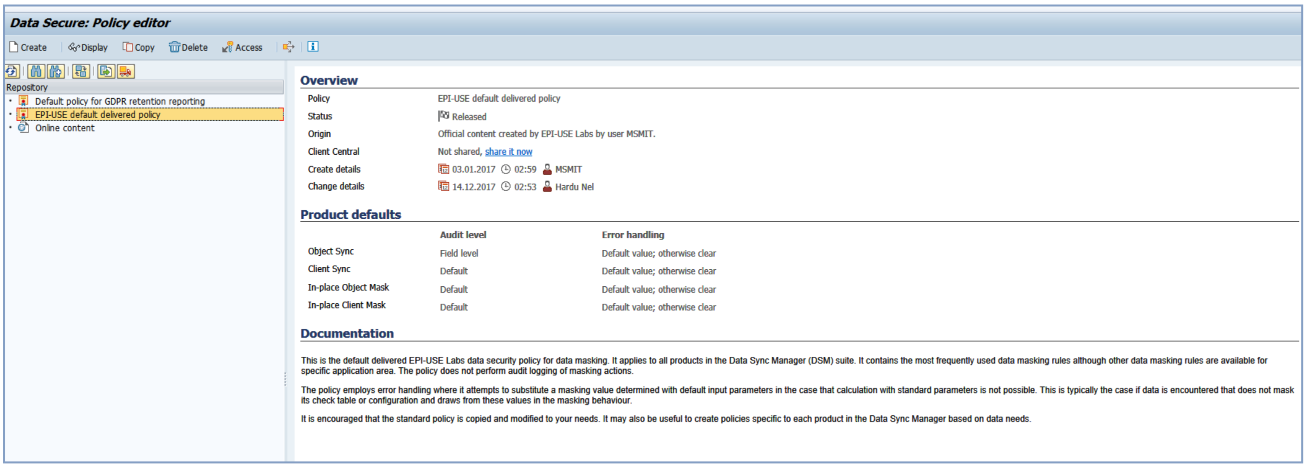
To access the Policy Editor:

Step 1: Enter the transaction code **/n/use/ds**. The Data Secure launchpad is displayed.

Step 2: Select the 'Policies' icon to display the Data Secure Run Monitor Desk screen.



The Policy editor shows the list of defined policies in the tree on the left. The list includes EPI-USE Labs delivered policies and custom policies.


Data Secure: Policy editor
Create
Display
Copy
Delete
Access
Repository
Default policy for GDPR retention reporting
EPI-USE default delivered policy
Online content

Overview

Policy	EPI-USE default delivered policy
Status	Released
Origin	Official content created by EPI-USE Labs by user MSMIT.
Client Central	Not shared, share it now
Create details	03.01.2017 02:59 MSMIT
Change details	14.12.2017 02:53 Hardu Nel

Product defaults

	Audit level	Error handling
Object Sync	Field level	Default value; otherwise clear
Client Sync	Default	Default value; otherwise clear
In-place Object Mask	Default	Default value; otherwise clear
In-place Client Mask	Default	Default value; otherwise clear

Documentation

This is the default delivered EPI-USE Labs data security policy for data masking. It applies to all products in the Data Sync Manager (DSM) suite. It contains the most frequently used data masking rules although other data masking rules are available for specific application area. The policy does not perform audit logging of masking actions.

The policy employs error handling where it attempts to substitute a masking value determined with default input parameters in the case that calculation with standard parameters is not possible. This is typically the case if data is encountered that does not mask its check table or configuration and draws from these values in the masking behaviour.

It is encouraged that the standard policy is copied and modified to your needs. It may also be useful to create policies specific to each product in the Data Sync Manager based on data needs.

Policies can be downloaded from Client Central either as delivered content from EPI-USE Labs or shared content from other community users.

Existing policies can be copied and modified to meet specific business requirements or new policies can be created. The ‘Default’ Policy, shipped with the product, can be copied and used as a starting point for custom policies. The ‘Default’ policy contains the data-masking Rules recommended by EPI-USE Labs.

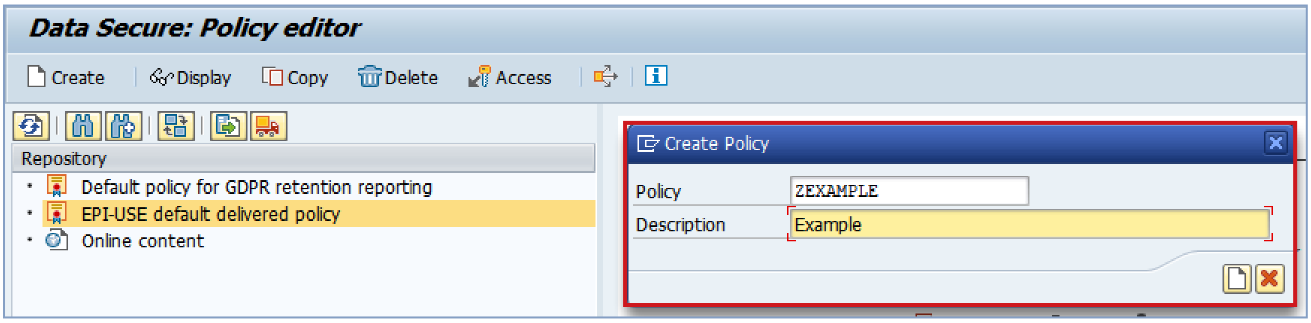
The Default policy option acts as a template for other policies. For this reason, you cannot edit this Policy.

The following options are available in the Data Secure Policy editor:

Icon	Name	Function
Create	Create	Creates a new Policy.
Display	Display	Displays a Policy from the list of available policies.
Change	Change	Changes the selected Policy.
Copy	Copy	Copies an existing Policy (to use it as a template for a new one).
Delete	Delete	Deletes the selected Policy.
Access	Access	Define access to the Policy via User Groups.
	Where-Used	Lists the templates where this Policy is used.

ℹ	Information	Displays the in-product help for the Policy editor.
	Find/ Find Next	Finds the specified Policy.
	Toggle Display	Switches between displaying the Policy descriptions, the technical names of Policies or a combination of both.

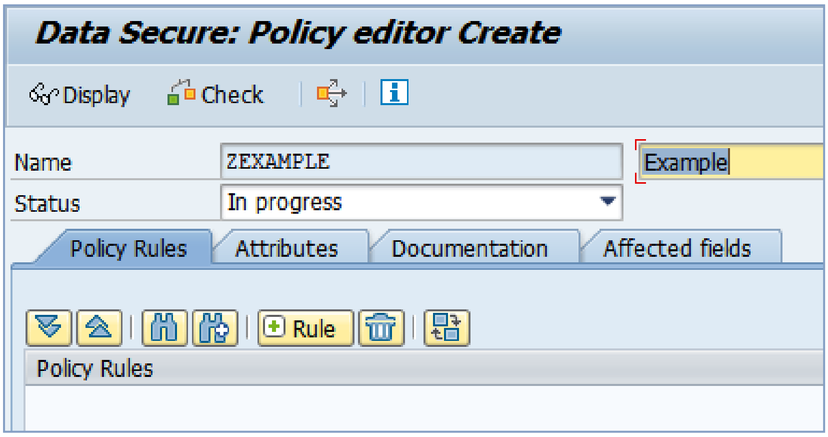
5.2 Create a new policy


Data Secure: Policy editor
Create
Display
Copy
Delete
Access
Repository
Default policy for GDPR retention reporting
EPI-USE default delivered policy
Online content
Create Policy

Policy: ZEXAMPLE
Description: Example

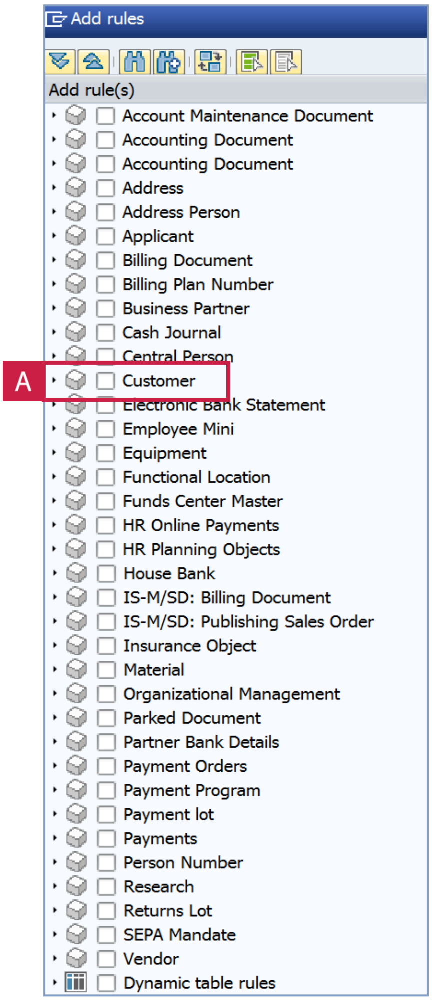
To create a new policy, click on the Create Create button, specify the technical name for the Policy and a description and then confirm the Create Policy dialog box. New custom policies should have a technical name starting with a Z or Y to match with SAP customizing naming conventions.

The Policy editor will open in the ‘Create’ mode:



Name: ZEXAMPLE Example
Status: In progress

To add data-masking rules to the policy, click the 'Add Rule' Rule button and select the rules from the list displayed below:



Add rules

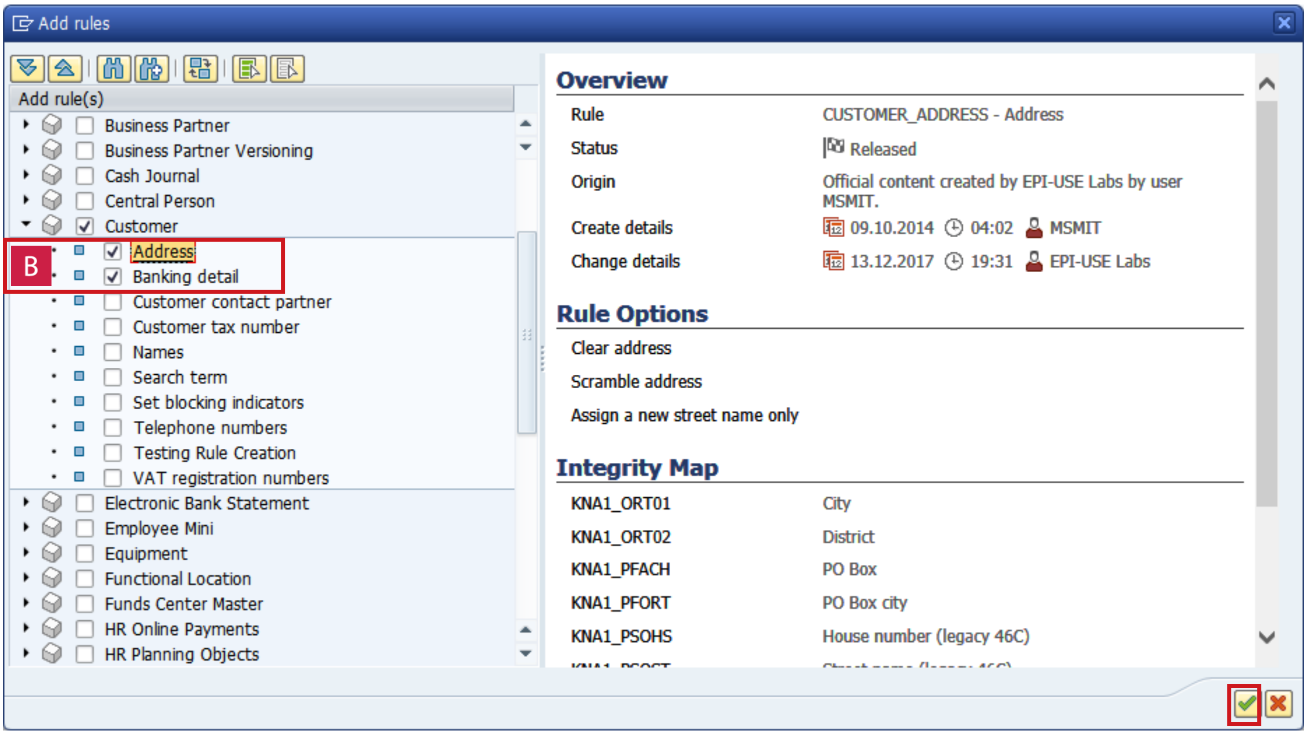
Add rule(s)

- □ Account Maintenance Document
- □ Accounting Document
- □ Accounting Document
- □ Address
- □ Address Person
- □ Applicant
- □ Billing Document
- □ Billing Plan Number
- □ Business Partner
- □ Cash Journal
- □ Central Person
- □ Customer
- □ Electronic Bank Statement
- □ Employee Mini
- □ Equipment
- □ Functional Location
- □ Funds Center Master
- □ HR Online Payments
- □ HR Planning Objects
- □ House Bank
- □ IS-M/SD: Billing Document
- □ IS-M/SD: Publishing Sales Order
- □ Insurance Object
- □ Material
- □ Organizational Management
- □ Parked Document
- □ Partner Bank Details
- □ Payment Orders
- □ Payment Program
- □ Payment lot
- □ Payments
- □ Person Number
- □ Research
- □ Returns Lot
- □ SEPA Mandate
- □ Vendor
- □ Dynamic table rules

Only rules that are in 'Released' or 'Testing only' status will be displayed.

Each Business Object displayed in the 'Add rules' dialog has several rules. To see what rules exist for each Business Object, expand the Object node. If you want to add all of the data-masking Rules corresponding to a Business Object, select the Business Object's node in the tree (A). To add any specific data-masking Rule, select its checkbox from the expanded node (see B on the next page).

Note: Conflicting rules that update the same data (same Integrity Map) will be flagged as invalid when the Policy is checked. The conflict will need to be resolved before the Policy can be used.



Add rules

Add rule(s)

- □ Business Partner
- □ Business Partner Versioning
- □ Cash Journal
- □ Central Person
- ☑ Customer
  - ☑ Address
  - ☑ Banking detail
  - □ Customer contact partner
  - □ Customer tax number
  - □ Names
  - □ Search term
  - □ Set blocking indicators
  - □ Telephone numbers
  - □ Testing Rule Creation
  - □ VAT registration numbers
- □ Electronic Bank Statement
- □ Employee Mini
- □ Equipment
- □ Functional Location
- □ Funds Center Master
- □ HR Online Payments
- □ HR Planning Objects

Overview

Rule	CUSTOMER_ADDRESS - Address
Status	Released
Origin	Official content created by EPI-USE Labs by user MSMIT.
Create details	09.10.2014 04:02 MSMIT
Change details	13.12.2017 19:31 EPI-USE Labs

Rule Options

Clear address

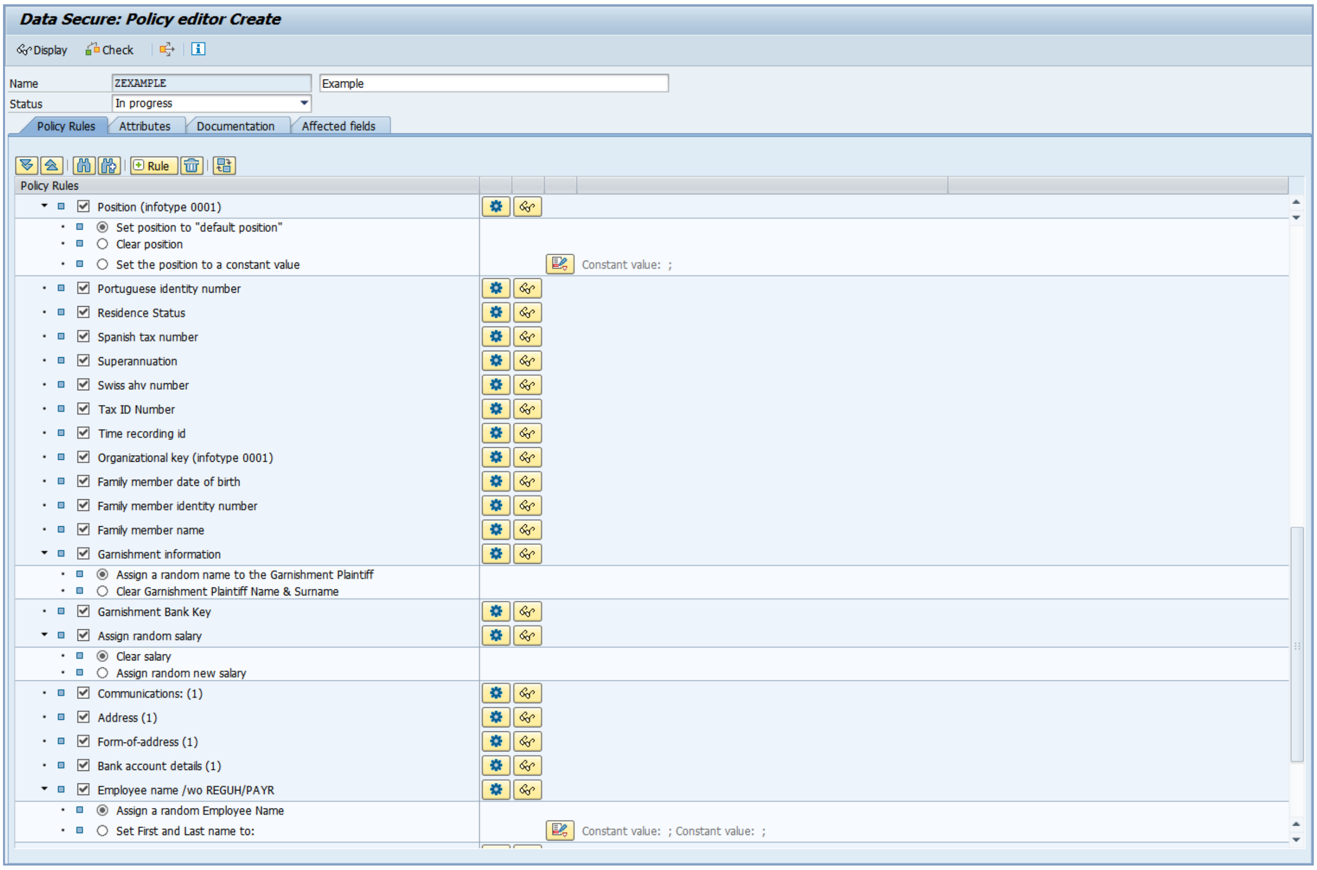
Scramble address

Assign a new street name only

Integrity Map

KNA1_ORT01	City
KNA1_ORT02	District
KNA1_PFACH	PO Box
KNA1_PFORT	PO Box city
KNA1_PSOHS	House number (legacy 46C)

Confirming the selections will add the selected Rules to the Policy. The Rules are then displayed as a tree providing the Business Object context and the options that are available to each one.



Data Secure: Policy editor Create

Name ZEXAMPLE Example

Status In progress

Policy Rules | Attributes | Documentation | Affected fields

Policy Rules

- ☑ Position (infotype 0001)
  - ● Set position to "default position"
  - ○ Clear position
  - ○ Set the position to a constant value — Constant value: ;
- ☑ Portuguese identity number
- ☑ Residence Status
- ☑ Spanish tax number
- ☑ Superannuation
- ☑ Swiss ahv number
- ☑ Tax ID Number
- ☑ Time recording id
- ☑ Organizational key (infotype 0001)
- ☑ Family member date of birth
- ☑ Family member identity number
- ☑ Family member name
- ☑ Garnishment information
  - ● Assign a random name to the Garnishment Plaintiff
  - ○ Clear Garnishment Plaintiff Name & Surname
- ☑ Garnishment Bank Key
- ☑ Assign random salary
  - ● Clear salary
  - ○ Assign random new salary
- ☑ Communications: (1)
- ☑ Address (1)
- ☑ Form-of-address (1)
- ☑ Bank account details (1)
- ☑ Employee name /wo REGUH/PAYR
  - ● Assign a random Employee Name
  - ○ Set First and Last name to: — Constant value: ; Constant value: ;

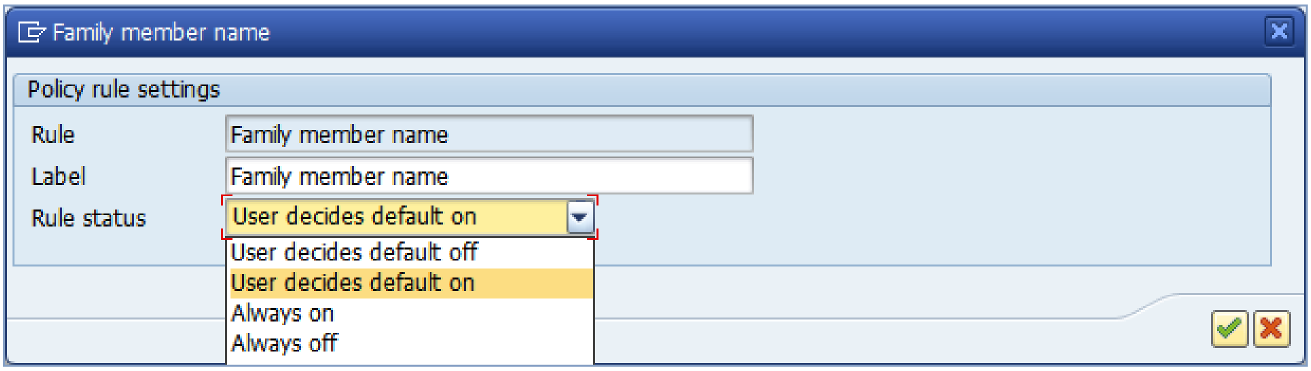
The following settings options are available for each Rule in the Policy editor (although the first four are relevant to Policies in general):

Icon	Name	Function
Change Display	Change/ Display	Toggles between 'Display' and 'Edit' mode.
Check	Check	Checks whether the current Policy configuration is valid.
⇄	Where-Used	Lists the Templates where this Policy is used.
i	Information	Displays the online help for the Policy editor.
⏬	Expand All	Fully expands the object tree.
⏫	Collapse All	Collapses the object tree.
Rule	Rule	Adds data-masking Rules to the Policy.
🔍 🔍	Find/ Find Next	Finds the specified Rule or rule option.
🗑	Delete	Removes the selected Rule(s) from the Policy.
⇅	Toggle Display	Switches between displaying the Rule descriptions, the technical names of Rules or a combination of both.
☑	Rule Active/ Inactive	Indicates that the Masking Rule will be active/inactive by default.
● ○	Option Selection	Indicates the default option for the Rule.
⚙	Rule Settings	Changes the default behavior settings for the Rule.
👓	Display Rule	Displays the Rule definition and allows you to display a different description for the rule to the User making use of the specific Policy.

Configure your rule options and selections based on your particular data-masking requirements. For example, for the Customer Address masking rule (see earlier screenshot B), you can choose between the following masking options:

- Clear address
- Scramble address
- Assign a new street name only

Some rules include options that require an input. The user will be able to input values (e.g. a constant for a name) but the policy can provide a default value for each input parameter.

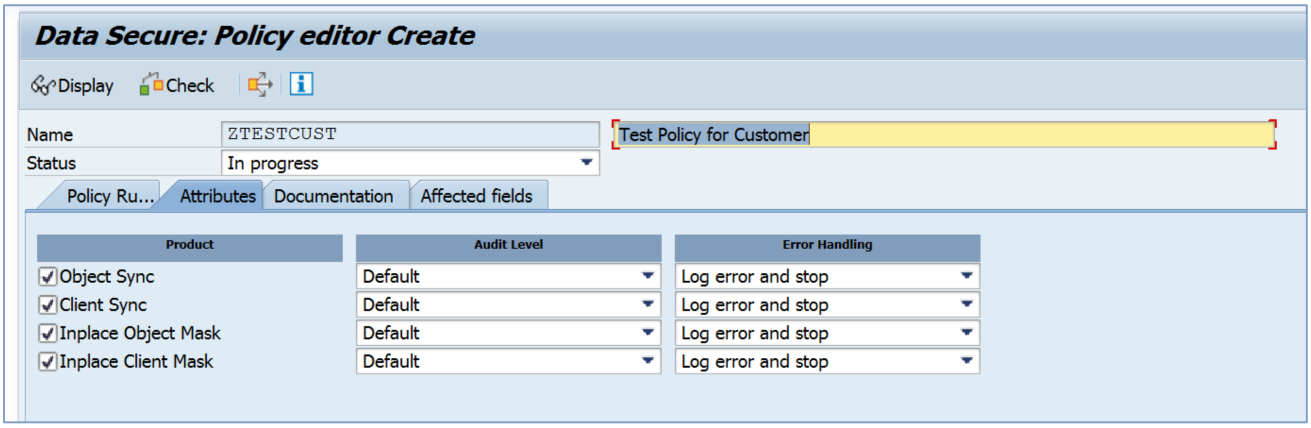


Rule	Family member name
Label	Family member name
Rule status	User decides default on

Specify if a rule should be active or inactive by default and/or mandatory in the Policy by using the Rule settings button. The available Rule settings are as follows:

Rule Behaviors	Description
User decides default on	The selected Rule is On (active) by default, but you can decide at execution time to switch it Off (inactive).
User decides default off	The selected Rule is Off (inactive) by default, but you can decide at execution time to switch it On (active).
Always on	The Rule will always be On (active). You won't be able to change this at execution time.
Always off	The Rule will always be Off (inactive). You won't be able to change this at execution time.

Once the Rule settings have been specified, select the Attributes page to associate the Policy with EPI-USE Labs products and specify their product-specific behavior. The product-specific settings are explained in the tables below:



Name	ZTESTCUST	Test Policy for Customer
Status	In progress	

Product	Audit Level	Error Handling
☑ Object Sync	Default	Log error and stop
☑ Client Sync	Default	Log error and stop
☑ Inplace Object Mask	Default	Log error and stop
☑ Inplace Client Mask	Default	Log error and stop

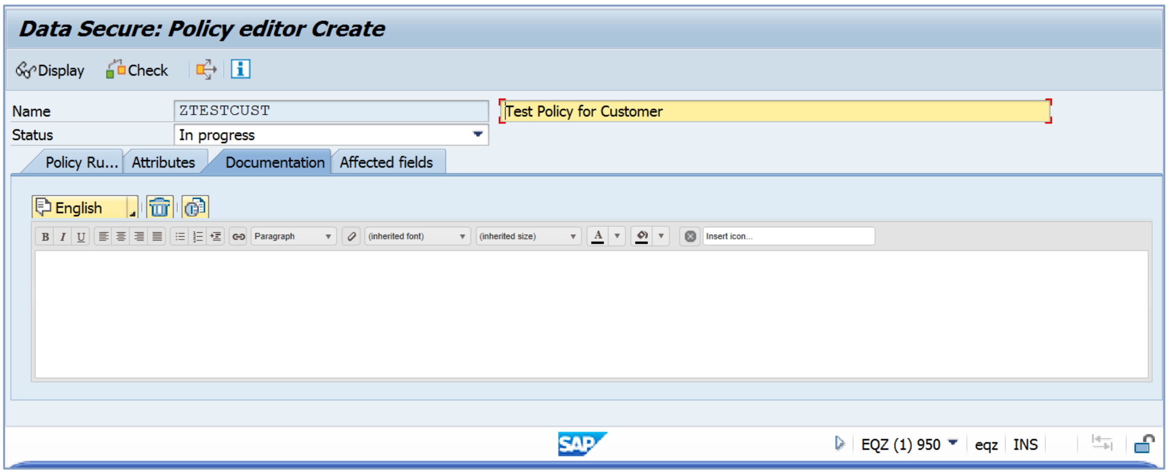
There are two groups of settings, namely for Audit Level and Error Handling. These are described in separate tables:

Audit Level	Description
Default	Lists the configuration of the rules that are used, the options and conditions, the parameters that were given in order to see what happened and why it happened. It provides an audit of the configuration at the time of execution.
Calculation (key level)	For each original value – in the context of a Business Object instance (key) – the original and calculated masked values are listed. This will not include all the tables and fields where the masking took place.
Update (field level)	For every original value that was masked, the corresponding masked value is listed with the context in which the value was determined.

And:

Error Handling	Description
Log error and continue	Will log the error and continue executing the Run. For more information on the error or errors, see the Messages tab in the Run details.
Log error and stop	This is the strictest option for Error Handling. This option will log the error and stop the Run. For more information on the error or errors, see the section on the Messages tab in the Run details in Section 4.3.5.
Default value; otherwise clear	This is the most flexible Error handling option. In case of an error, this will call the selected Transformation function using the default parameters defined for that function. If this Transformation Function still cannot determine a new value, the original value will be cleared. A warning message will appear in the Messages tab of the Run details. See Section 4.3.5.

Once the product-specific settings for the Policy have been set, you can document the Policy by selecting the 'Documentation' tab.

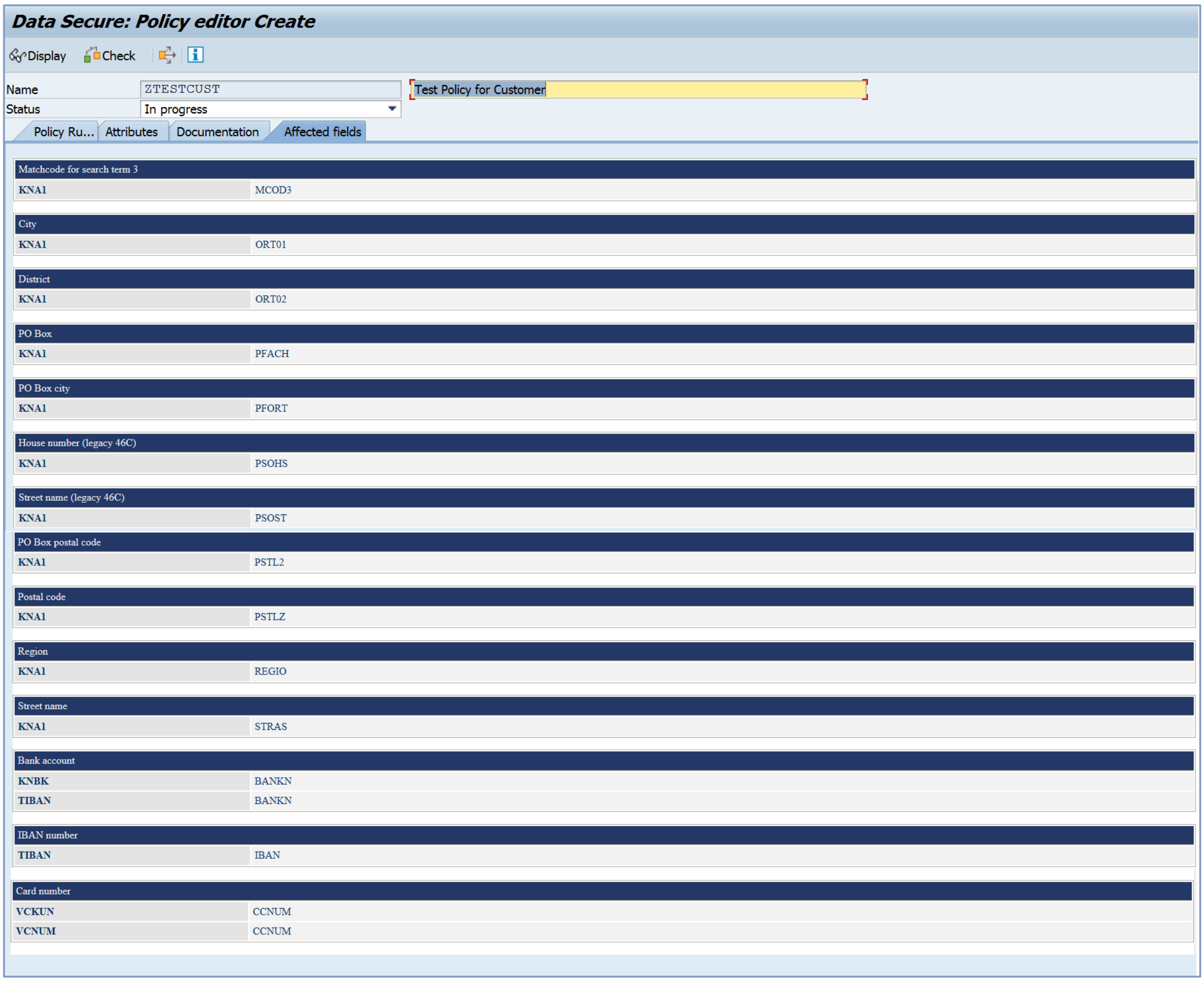


Data Secure: Policy editor Create

Name ZTESTCUST Test Policy for Customer

Status In progress

The ‘Affected fields’ tab lists all of the tables and fields affected by the data-masking rules contained in the Policy. The tables and fields are grouped by the Integrity Map concept (refer to Section 8).



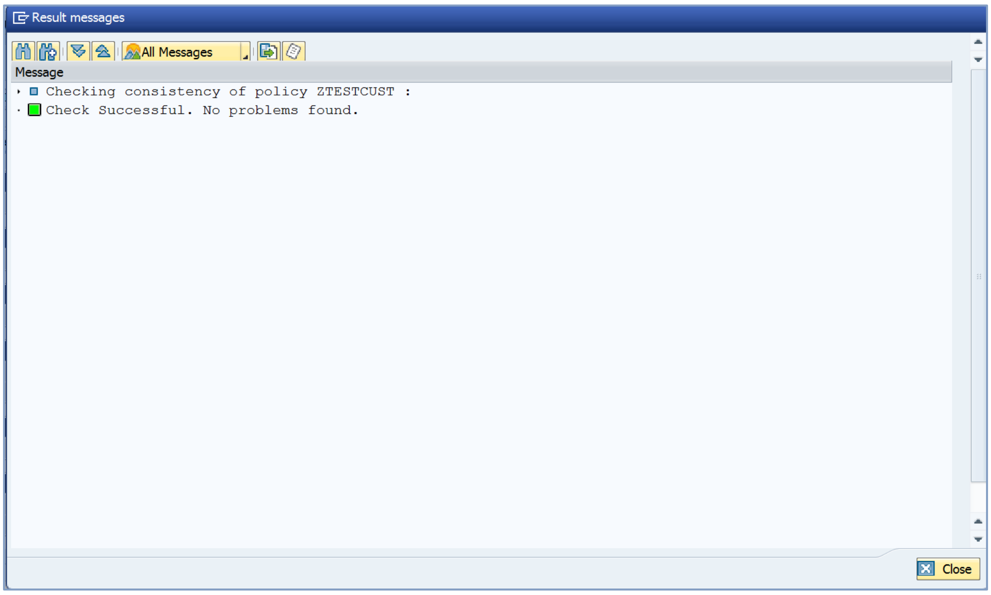
Data Secure: Policy editor Create

Name ZTESTCUST Test Policy for Customer

Status In progress

Matchcode for search term 3	
KNA1	MCOD3
City	
KNA1	ORT01
District	
KNA1	ORT02
PO Box	
KNA1	PFACH
PO Box city	
KNA1	PFORT
House number (legacy 46C)	
KNA1	PSOHS
Street name (legacy 46C)	
KNA1	PSOST
PO Box postal code	
KNA1	PSTL2
Postal code	
KNA1	PSTLZ
Region	
KNA1	REGIO
Street name	
KNA1	STRAS
Bank account	
KNBK	BANKN
TIBAN	BANKN
IBAN number	
TIBAN	IBAN
Card number	
VCKUN	CCNUM
VCNUM	CCNUM

Once the Policy settings have been updated, it is recommended that you run a check to ensure that the policy is consistent with no errors. This can be done by clicking on the Check Check button. A dialog box will display a trace of the check results in the ‘Result messages’ pop-up window.

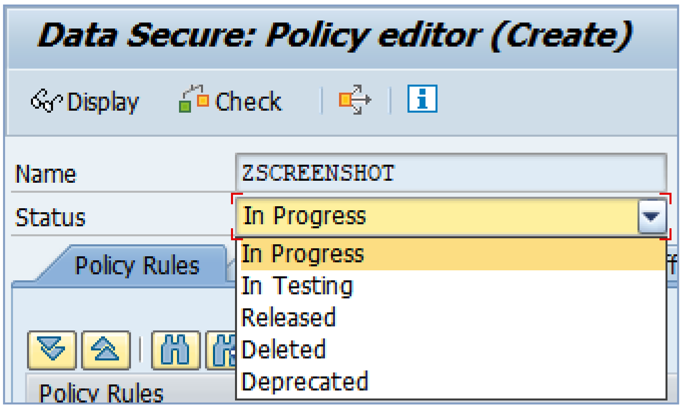


Result messages

Message

```
· ▫ Checking consistency of policy ZTESTCUST :
· 🟩 Check Successful. No problems found.
```

Before the policy can be made available to other users to use in masking runs, the Policy status needs to be updated.



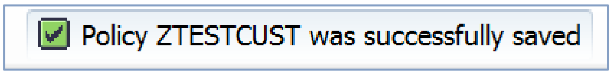
Name ZSCREENSHOT

Status In Progress

In Progress
In Testing
Released
Deleted
Deprecated

Status	Description
In Progress	The policy is still being created and it cannot be used.
In Testing	Policy can be used on the current system (and client), but cannot be distributed to other systems (or clients). This status is used when the Policy is being tested.
Released	The policy is available and can be actively used and distributed.
Deleted	Policy can no longer be used and will be deleted if distributed to another system/client.
Deprecated	The policy was previously shipped as a delivered Policy but is no longer supported and cannot be used by products and users. The Policy can be copied to be used as a template for custom Policies.

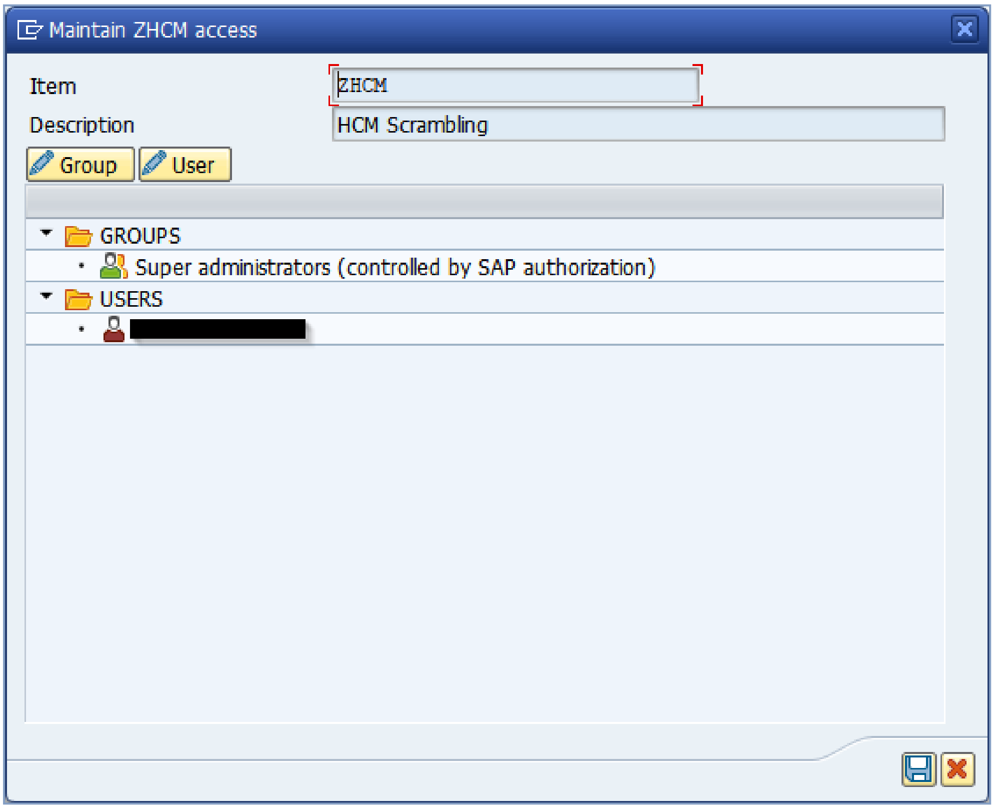
Once the status is selected and set, save the Policy by clicking on the 'Save' button.



Policy ZTESTCUST was successfully saved

The new Policy is available in the Policy Editor and its Overview is displayed on the right side of the screen.

The Policy can now be assigned to User Groups or specific users by selecting the Policy and clicking on the Access Access button. The following section details the User Group assignment screen.



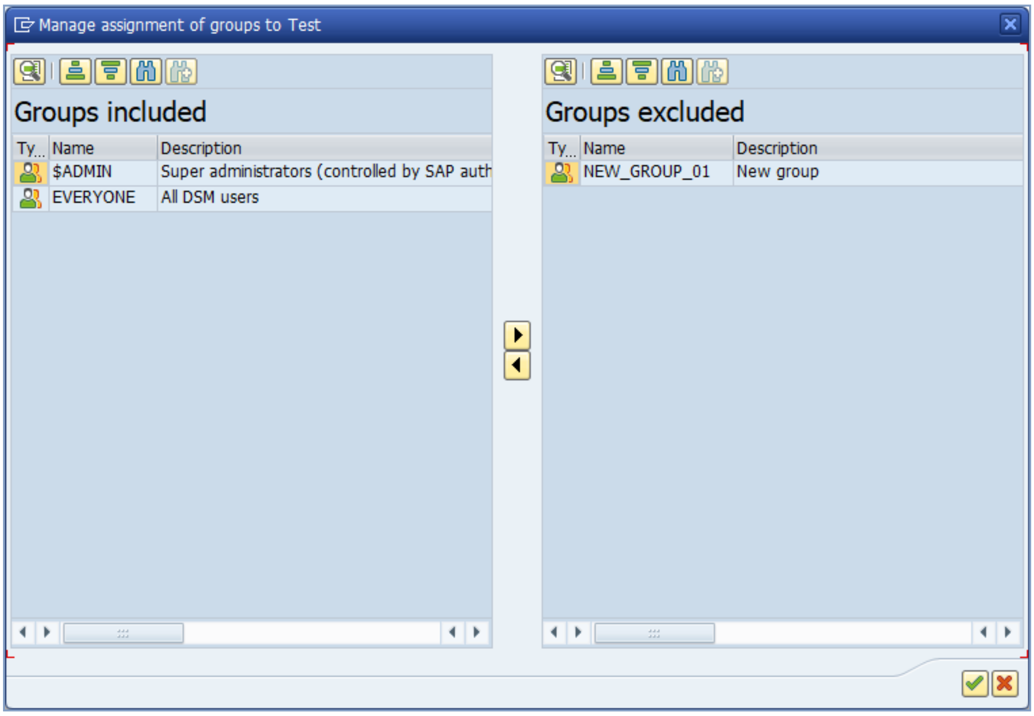
Maintain ZHCM access

Item	ZHCM
Description	HCM Scrambling

- GROUPS
  - Super administrators (controlled by SAP authorization)
- USERS
  - [redacted]

5.2.1 User Group access for Policy

The User Group assignment screen lists the User Groups and the specific users that are assigned to the current policy. User Groups can be assigned to the Policy by clicking on the Group Group button, while specific Users can be assigned by clicking on the User User button.



Manage assignment of groups to Test

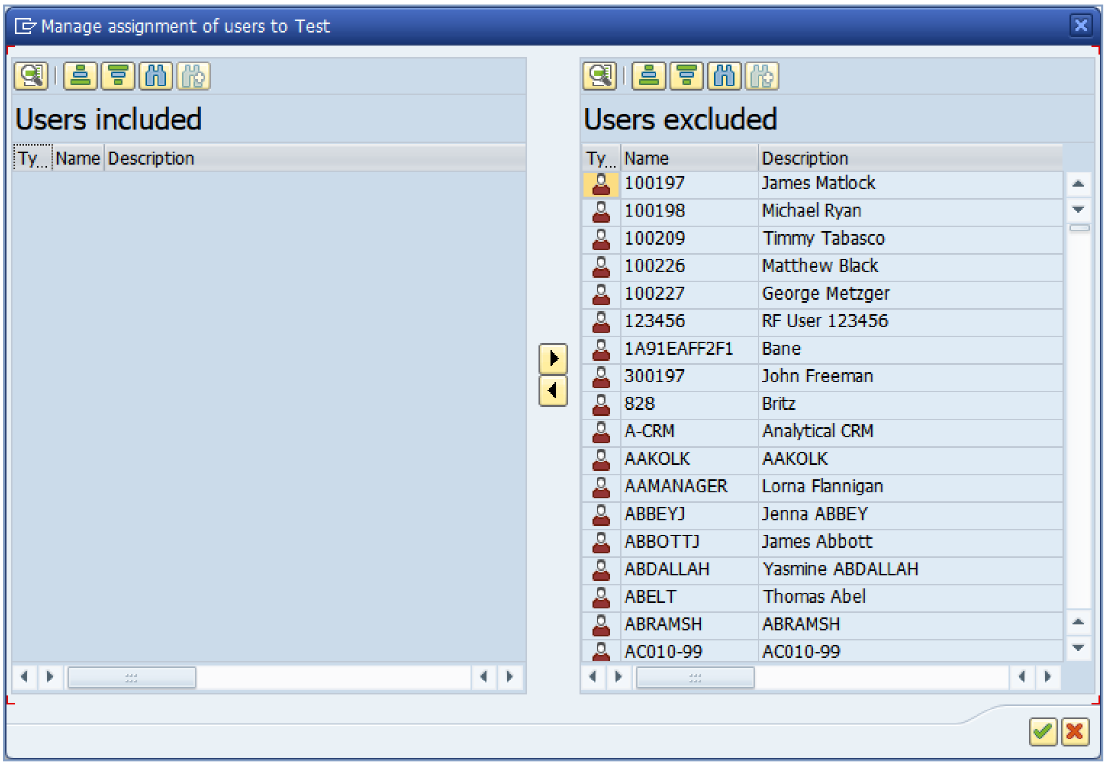
Groups included

Ty...	Name	Description
	$ADMIN	Super administrators (controlled by SAP auth
	EVERYONE	All DSM users

Groups excluded

Ty...	Name	Description
	NEW_GROUP_01	New group

User Groups listed on the left will have access to the Policy while User Groups listed on the right will not. User Groups can be moved between the two categories with the ◀ and ▶ buttons. Details for a specific User Group can be displayed by clicking on the Details 🔍 button.



Manage assignment of users to Test

Users included

Ty..	Name	Description

Users excluded

Ty..	Name	Description
👤	100197	James Matlock
👤	100198	Michael Ryan
👤	100209	Timmy Tabasco
👤	100226	Matthew Black
👤	100227	George Metzger
👤	123456	RF User 123456
👤	1A91EAFF2F1	Bane
👤	300197	John Freeman
👤	828	Britz
👤	A-CRM	Analytical CRM
👤	AAKOLK	AAKOLK
👤	AAMANAGER	Lorna Flannigan
👤	ABBEYJ	Jenna ABBEY
👤	ABBOTTJ	James Abbott
👤	ABDALLAH	Yasmine ABDALLAH
👤	ABELT	Thomas Abel
👤	ABRAMSH	ABRAMSH
👤	AC010-99	AC010-99

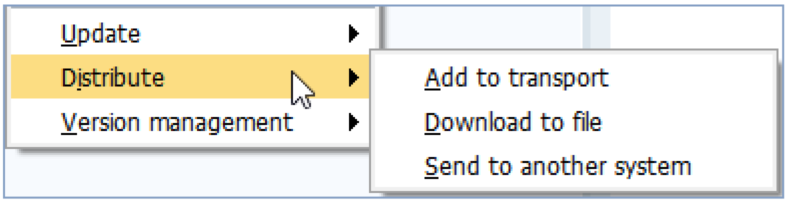
Similarly, by selecting the User icon a specific user can be associated with the Policy. Users on the left of the screen displayed have access to the Policy while users listed on the right do not. Users can be moved between the two categories by using the ◀ and ▶ buttons. Details about a user can be displayed by clicking on the Details 🔍 button.

Once a Policy is assigned to a User Group or a User, that Policy is available to that user for all of the Data Sync Manager products that the Policy relates to. If only one of the products is used, this or another policy applicable to the user will need to be applied to the DSM product's processing.

The EVERYONE User Group is shipped with Data Sync Manager and includes all users with access to the DSM software on the current client. This is the default group that Policies are assigned to, to make a policy available to all users. The Default policies delivered with DSM are assigned to this user Group by default but the assignment can be changed as necessary.

Now that the Policy is assigned to its designated Users or User Groups, the Policy should also be distributed to other systems and clients it should be available on. The next section details the available distribution options.

5.2.2 Distribution options



To access the distribution options for a Policy, right-click on the Policy and select the ‘Distribute’ option in the displayed menu. The available options are:

Name	Functions
Add to transport	Adds the selected Policy to a Transport for distribution using the standard SAP Transport mechanisms.
Download to file	Creates a file in the specified location that can later be ‘Uploaded’ into Data Secure using the matching ‘Import from file’ function from the ‘Update’ context menu.
Send to another system	Distributes the selected Policy to another DSM5 system client using an RFC destination. RFC destinations can either be specified Ad-hoc or pre-configured in the Control Center. Please see the Data Sync Manager Installation Guide, Control Center and Configuration Guide for details on using the Control Center.

With the policy created and distributed, a version can now be maintained. The next section discusses version management options.

5.2.3 Version management

There are two options in the Version management sub-menu that are accessed by right-clicking on a selected Policy. The options are:

- Create a new version of a Policy.
- Restore a saved version and make it the active version.

6. Rules

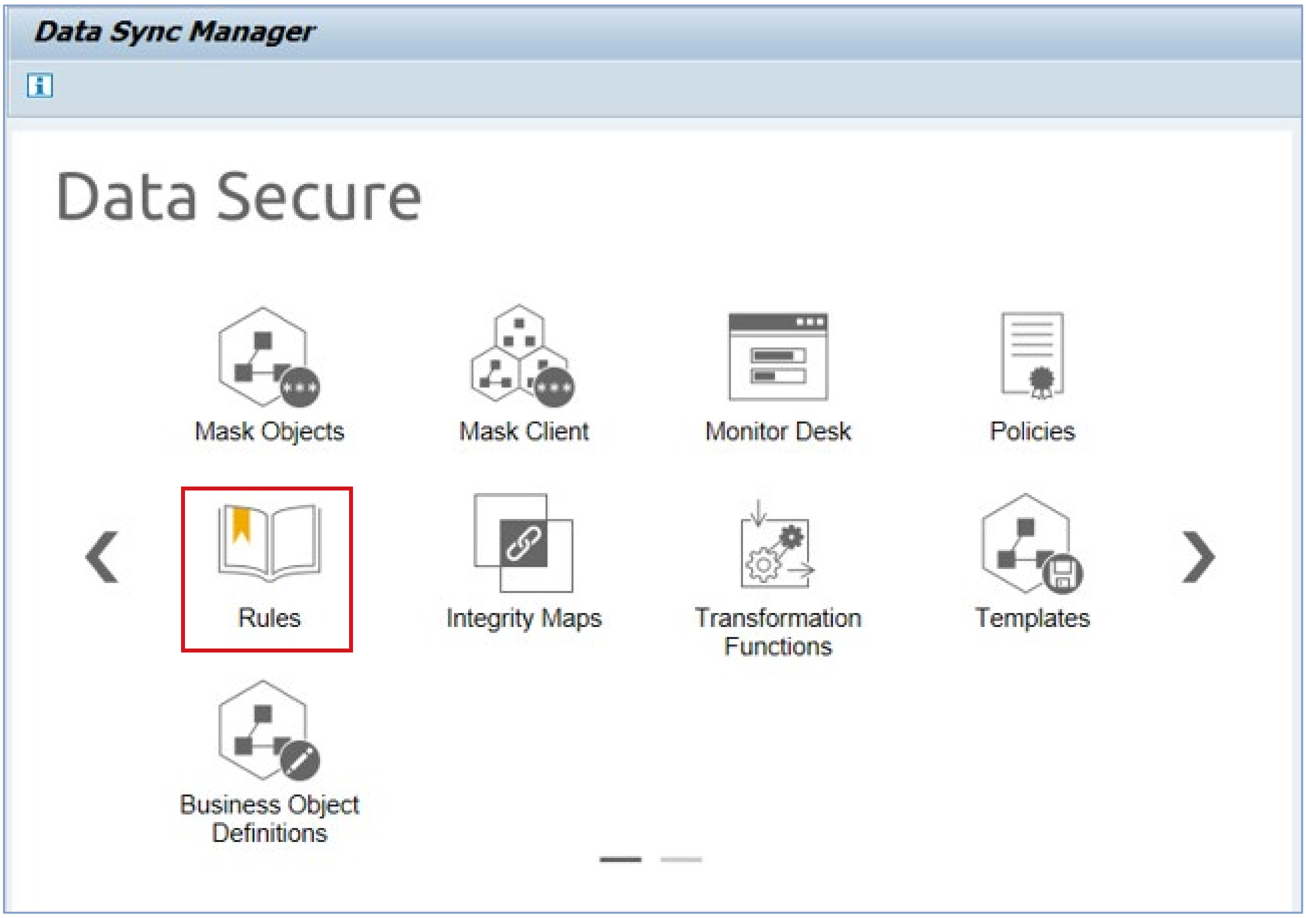
Rules define the Masking behavior by specifying the data to be masked (Integrity Maps) and the masking values to be assigned (Transformation Functions). To create and maintain masking Rules, visit the Rule editor as follows:

6.1 Access the Rule Editor and create a Rule

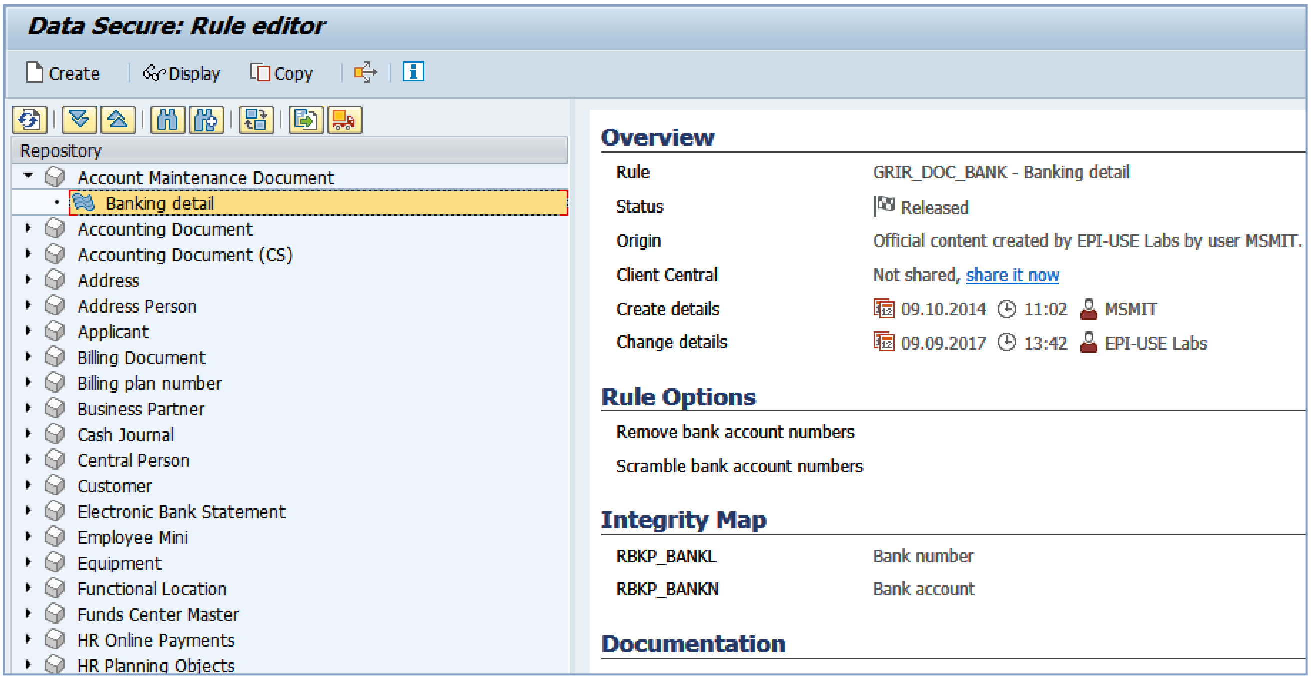
To access the Rule editor:

Step 1: Enter the transaction code **/n/use/ds**. The Data Secure launchpad is displayed.

Step 2: Select the 'Rules' icon to open the Rule editor.



The Rule editor displays a list of the data-masking Rules available on the current client. The Rules are grouped by their Business Object contexts. A special category titled 'Table rules' contains those rules that are not linked to a specific Business Object context and are instead defined directly in the context of a single database table.



Data Secure: Rule editor

Create | Display | Copy

Repository
- Account Maintenance Document
  - Banking detail
- Accounting Document
- Accounting Document (CS)
- Address
- Address Person
- Applicant
- Billing Document
- Billing plan number
- Business Partner
- Cash Journal
- Central Person
- Customer
- Electronic Bank Statement
- Employee Mini
- Equipment
- Functional Location
- Funds Center Master
- HR Online Payments
- HR Planning Objects

Overview

Rule	GRIR_DOC_BANK - Banking detail
Status	Released
Origin	Official content created by EPI-USE Labs by user MSMIT.
Client Central	Not shared, share it now
Create details	09.10.2014 11:02 MSMIT
Change details	09.09.2017 13:42 EPI-USE Labs

Rule Options

Remove bank account numbers

Scramble bank account numbers

Integrity Map

RBKP_BANKL	Bank number
RBKP_BANKN	Bank account

Documentation

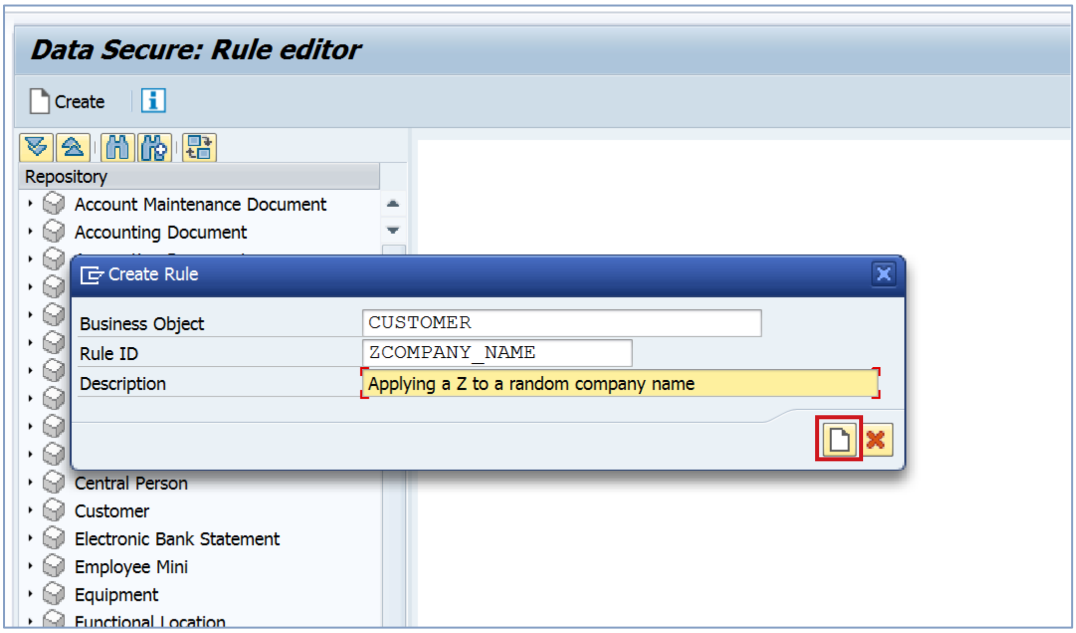
6.1.1 Create a new Rule

Click on the Create Create button to start creating a new rule.

> Selecting a Business Object will set the Business Object context of the rule to the selected Business Object. Selecting the Table rules node will create a Table rule.

When prompted to do so in the ‘Create Rule’ pop-up window, enter the following information:

- A Business Object context that the rule will execute in (e.g. CUSTOMER).
- A technical name (beginning with Z or Y) for the Rule.
- A description of what the Rule is intended to do.



Data Secure: Rule editor

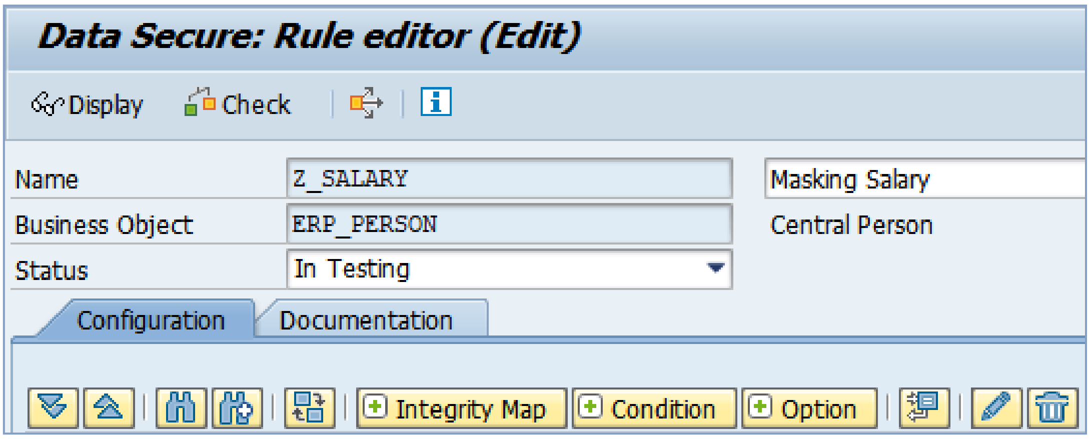
Create

Repository
- Account Maintenance Document
- Accounting Document
- Central Person
- Customer
- Electronic Bank Statement
- Employee Mini
- Equipment
- Functional Location

Create Rule

Business Object	CUSTOMER
Rule ID	ZCOMPANY_NAME
Description	Applying a Z to a random company name

Click on the 🗋 button to verify the inputs and proceed. The Rule editor details screen is displayed:



Data Secure: Rule editor (Edit)

Name	Z_SALARY	Masking Salary
Business Object	ERP_PERSON	Central Person
Status	In Testing	

The Overview portion of the Rule editor displays the following fields of which the Description and Status are editable.

Field	Description
Name	The technical name of the rule.
Business Object	The Business Object context for the Rule.
Status	The release status of the rule.
Description field (located next to the Name on the previous page)	The natural language description of the rule.

The Rule may be in one of the following statuses, each with its own implication for its use:

Status	Description
In Progress	The rule is still being created and it cannot be used in Policies yet.
In Testing	The rule can be used in Policies on the current system (and client), but cannot be distributed to other systems(and clients). This status is used when the Rule is being tested.
Released	The rule is available and can be actively used in Policies.
Deleted	The rule can no longer be used and will be deleted if distributed to another system/client.
Deprecated	The rule was previously shipped as standard but is no longer supported and cannot be used by products and users. The Rule can be copied and used as a template for custom Rules.

Use the Toggle Descriptions icon to switch between the functional descriptions and the technical names of Integrity Maps, Transformation Functions, Options and Conditions.

To define the Rule, the applicable Integrity Maps need to be added and Transformation functions assigned to mask the fields included in the Integrity Maps. The Integrity Maps define what data is to be masked and the Transformation functions define how that data is to be masked in each case.

Conditions can be placed on the Integrity Map to Transformation Function assignments and Options for Rule behavior can be specified. The Rule editor screen contains the following options:

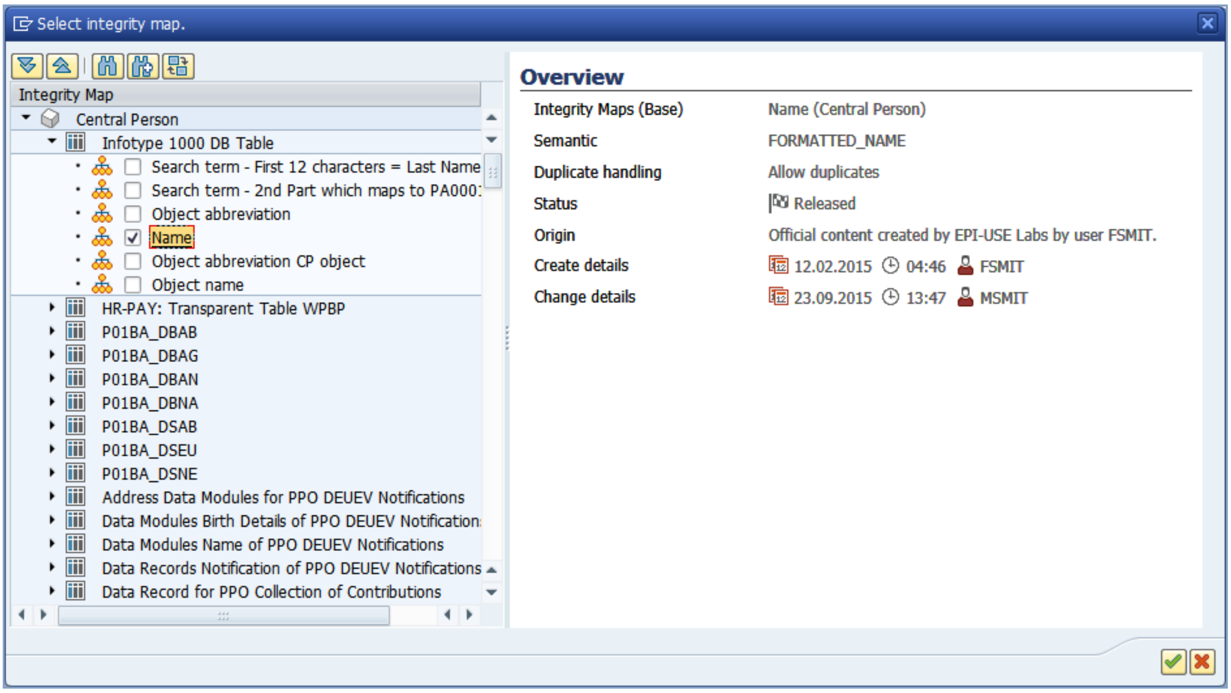
Icon	Name	Functions
Display ✎ Change	Display/ Change	Toggles between the Display and Edit modes of the current Rule.
Check	Check	Checks the configuration of the Rule for correctness. If an invalid configuration is found, a log of Rule configuration issues is displayed.
	Where-Used	Lists the Policies where the Rule is used.
i	Information	Displays the in-product help for the Rule editor.
⏷ ⏶	Expand/ Collapse	Expands/collapses all levels of the Rule configuration (Options/Conditions/Integrity Maps).
🔍 🔍+	Find/ Find Next	Finds the specified term in the Rule configuration.
	Toggle Display	Switches between displaying the Rule descriptions, the technical names of a Rule or a combination of both.
+ Integrity Map	Add Integrity Map	Adds the fields grouped by an Integrity Map to the scope of the Rule. Refer to Section 6.1.1.a for more details on Integrity Maps in Rules.
+ Condition	Add Condition	Makes a set of Integrity Map<->Transformation Function assignments conditional. Refer to Section 6.1.1.b on Rule conditions.
+ Option	Add Option	Adds optional behavior to the Rule. Integrity Maps added will need to be mapped to Transformation Functions to specify the optional behavior. Refer to Section 6.1.1.c for more details on Rule options.
	Assign Function	Assigns a Transformation Function to the Integrity Map that is different from the default. Refer to Section 6.1.1d for more information.
✎	Edit	Edits the assigned input parameters for the assigned Transformation Function. Refer to Section 6.1.1.e for more details.
🗑	Delete	Deletes the selected Integrity Map, Condition or Option from the Rule.

The ‘Assign Function’, ‘Edit’ and ‘Delete’ options only show when an Integrity Map is selected.

To start, click on the ‘Add Integrity Map’ Integrity Map button to add an Integrity Map to the scope of the rule.

a. Integrity Maps

When adding an Integrity Map to a Rule, the Business Object context is evaluated to determine all Integrity Maps created in the same Business Object context. These are listed for selection as the Integrity Maps that can be added to the Rule. The display groups the Integrity Maps according to the first table included in the Integrity map. This first table field serves as a reference for all the fields grouped under it as storing the same data in a redundant fashion. Refer to Section 8 for more information on Integrity Maps.



Select integrity map.

Integrity Map

- Central Person
  - Infotype 1000 DB Table
    - □ Search term - First 12 characters = Last Name
    - □ Search term - 2nd Part which maps to PA000:
    - □ Object abbreviation
    - ☑ Name
    - □ Object abbreviation CP object
    - □ Object name
  - HR-PAY: Transparent Table WPBP
  - P01BA_DBAB
  - P01BA_DBAG
  - P01BA_DBAN
  - P01BA_DBNA
  - P01BA_DSAB
  - P01BA_DSEU
  - P01BA_DSNE
  - Address Data Modules for PPO DEUEV Notifications
  - Data Modules Birth Details of PPO DEUEV Notification:
  - Data Modules Name of PPO DEUEV Notifications
  - Data Records Notification of PPO DEUEV Notifications
  - Data Record for PPO Collection of Contributions

Overview

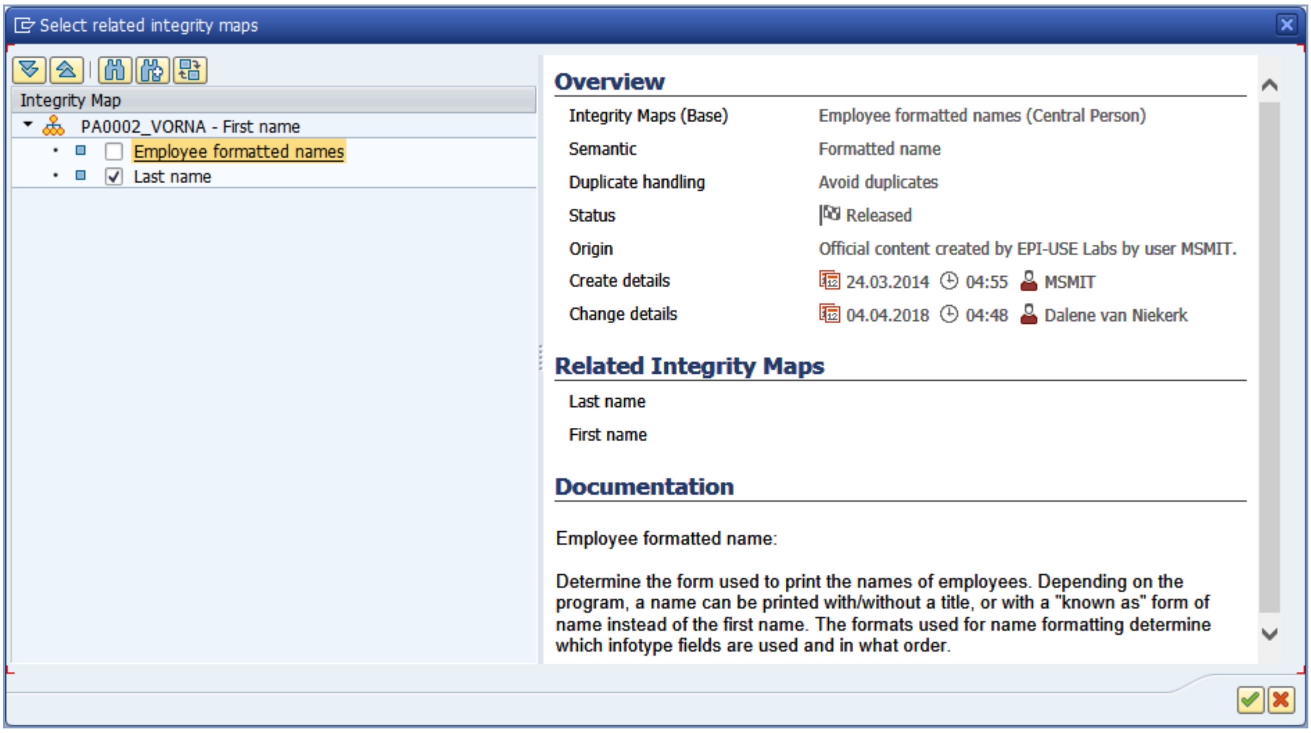
Integrity Maps (Base)	Name (Central Person)
Semantic	FORMATTED_NAME
Duplicate handling	Allow duplicates
Status	Released
Origin	Official content created by EPI-USE Labs by user FSMIT.
Create details	12.02.2015 04:46 FSMIT
Change details	23.09.2015 13:47 MSMIT

Click on the Continue ✓ button when you have selected the Integrity Map(s) you wish to include.

Most rules will include multiple Integrity Maps from the same table or different tables, all in the same Business Object context. If a table is in a different Business Object context, create a separate rule for it or extend the Business Object context to include the table.

More information on Business Objects and the Business Object Workbench can be accessed in the ‘BOW Extensions User Guide'.

Some Integrity Maps are enriched with metadata to suggest complementary Integrity Maps that make sense to update at the same time. If such an Integrity Map is selected, the suggested Integrity Maps to add will be shown in a subsequent step. The user can then decide whether to include them or not. Refer to Section 8.1.2 for more information on related Integrity Maps.



Integrity Map
- PA0002_VORNA - First name
  - □ Employee formatted names
  - ☑ Last name

Overview

Integrity Maps (Base)	Employee formatted names (Central Person)
Semantic	Formatted name
Duplicate handling	Avoid duplicates
Status	Released
Origin	Official content created by EPI-USE Labs by user MSMIT.
Create details	24.03.2014 04:55 MSMIT
Change details	04.04.2018 04:48 Dalene van Niekerk

Related Integrity Maps

Last name

First name

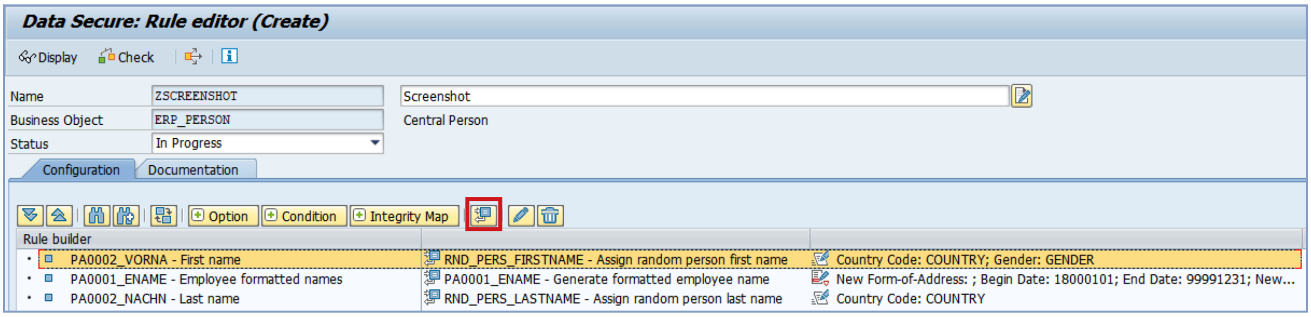
Documentation

Employee formatted name:

Determine the form used to print the names of employees. Depending on the program, a name can be printed with/without a title, or with a "known as" form of name instead of the first name. The formats used for name formatting determine which infotype fields are used and in what order.

The related Integrity Maps may be storing the same values but perhaps in a different format – e.g. upper case vs lower case formats. Consider carefully whether you should also include these Integrity Maps in your rule.

In cases like these, it is recommended that users rather copy and change a rule since they need to consider all fields when building their own rule.



Name	ZSCREENSHOT	Screenshot
Business Object	ERP_PERSON	Central Person
Status	In Progress	

Rule builder

PA0002_VORNA - First name	RND_PERS_FIRSTNAME - Assign random person first name	Country Code: COUNTRY; Gender: GENDER
PA0001_ENAME - Employee formatted names	PA0001_ENAME - Generate formatted employee name	New Form-of-Address: ; Begin Date: 18000101; End Date: 99991231; New...
PA0002_NACHN - Last name	RND_PERS_LASTNAME - Assign random person last name	Country Code: COUNTRY

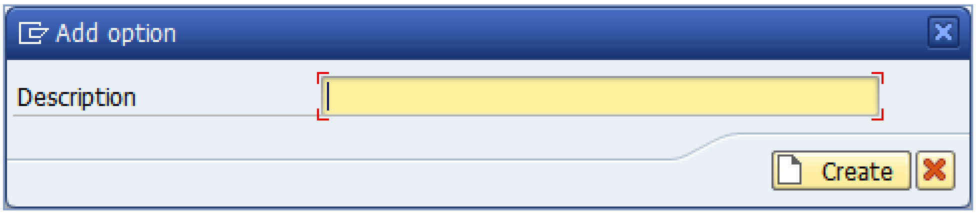
Once the selected Integrity Maps have been added to the Rule, they are assigned a default Transformation Function. This default Transformation Function is specified when the Integrity Map is defined. Refer to Section 8 for more details. If the Transformation Function receives input parameters, the default input parameters are mapped if possible. Refer to Section 7 for more information on Transformation Functions.

The user may want to change the Transformation Function assigned to the Integrity Map from the default. To do so, select the Assign Function button. Refer to Section 6.1.1.e for more information. The user may also wish to retain the assigned function but change the input parameters. To do so. select the Edit button. Refer to Section 6.1.1.f for more details.

The next section discusses adding optional behavior to the Rule.

b. Options

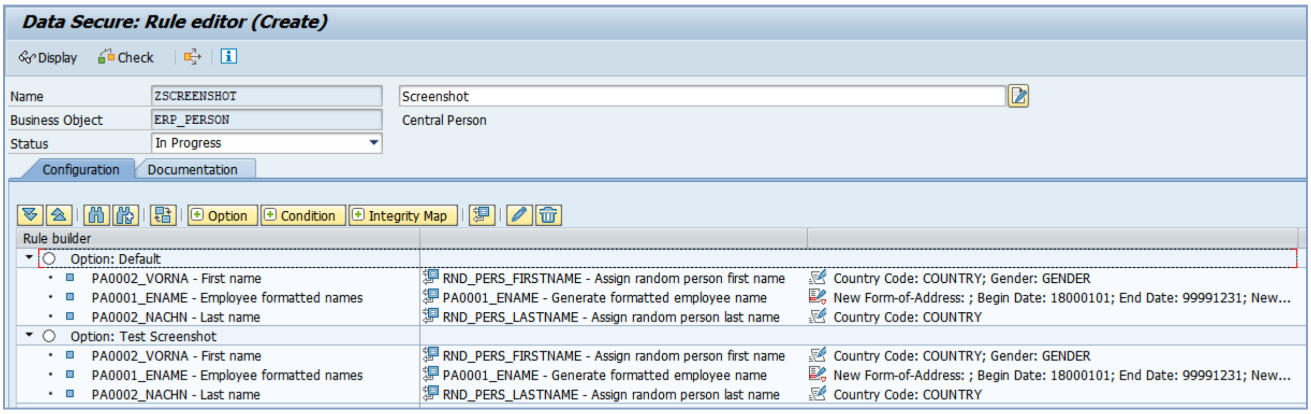
When adding optional behavior to a Rule, you first need to provide a description of the optional behavior.



Description:

Confirm the description and add the Option to the Rule by clicking on the Create button. All Integrity Maps added to the Rule will need to be mapped to the Transformation Functions for the Option according to the desired behavior.

The behavior executed by the Rule will depend on the Option selected. The rule option selection is either fixed when the Rule is added to a Data Security Policy (Section 5.2) or the user can select the option to be used when making selections for a masking run (refer to Section 3).



Data Secure: Rule editor (Create)

Name: ZSCREENSHOT — Screenshot

Business Object: ERP_PERSON — Central Person

Status: In Progress

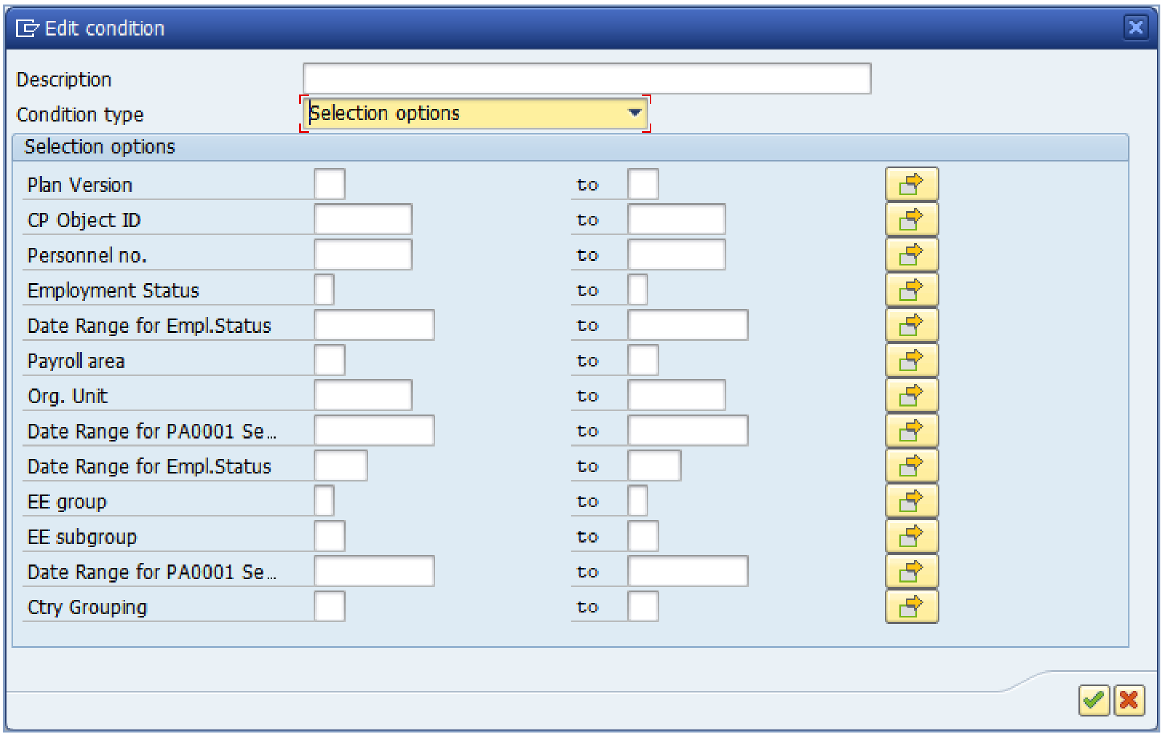
Rule builder		
○ Option: Default		
PA0002_VORNA - First name	RND_PERS_FIRSTNAME - Assign random person first name	Country Code: COUNTRY; Gender: GENDER
PA0001_ENAME - Employee formatted names	PA0001_ENAME - Generate formatted employee name	New Form-of-Address: ; Begin Date: 18000101; End Date: 99991231; New...
PA0002_NACHN - Last name	RND_PERS_LASTNAME - Assign random person last name	Country Code: COUNTRY
○ Option: Test Screenshot		
PA0002_VORNA - First name	RND_PERS_FIRSTNAME - Assign random person first name	Country Code: COUNTRY; Gender: GENDER
PA0001_ENAME - Employee formatted names	PA0001_ENAME - Generate formatted employee name	New Form-of-Address: ; Begin Date: 18000101; End Date: 99991231; New...
PA0002_NACHN - Last name	RND_PERS_LASTNAME - Assign random person last name	Country Code: COUNTRY

The next section discusses adding conditional behavior to the Rule.

c. Condition

When conditional behavior is added to a Rule, a description of the conditional behavior is required. A condition type needs to be selected, which determines the technique used to match the data processed by the masking engine to its associated masking behavior. All Integrity Maps added to the Rule need to be mapped to Transformation Functions to define the masking behavior for the corresponding data.

Condition types can either be based on Business Object selection option or Business Object context parameters. A condition type based on Business Object selection option considers data valid for the associated behavior if the data falls within the selection criteria specified. Refer to the Business Object Workbench user and extensions guide for more information on extending the Business Object selection options.



Edit condition

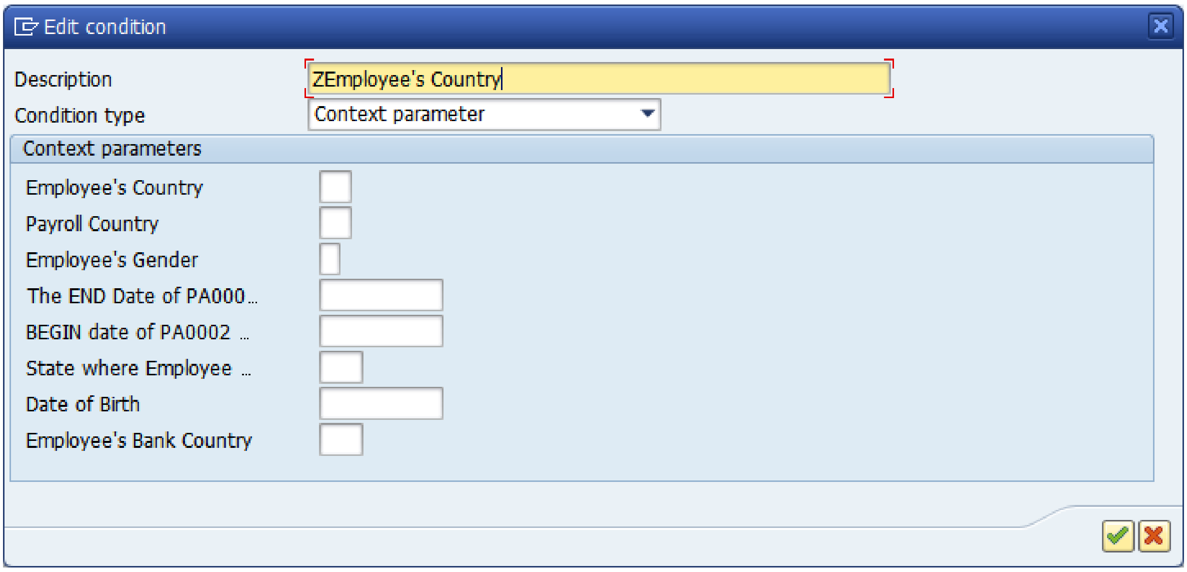
Description	
Condition type	Selection options

Selection options

Plan Version		to		
CP Object ID		to		
Personnel no.		to		
Employment Status		to		
Date Range for Empl.Status		to		
Payroll area		to		
Org. Unit		to		
Date Range for PA0001 Se...		to		
Date Range for Empl.Status		to		
EE group		to		
EE subgroup		to		
Date Range for PA0001 Se...		to		
Ctry Grouping		to		

A condition type based on a Context parameter is considered valid for data only if the data matches the value of the Context parameter specified.

Each instance of a Business Object holds a single value for a Context parameter. Refer to the Business Object Workbench user and extensions guide for more details on extending the available Context parameters.



Edit condition

Description: ZEmployee's Country

Condition type: Context parameter

Context parameters

Employee's Country:

Payroll Country:

Employee's Gender:

The END Date of PA000...:

BEGIN date of PA0002 ...:

State where Employee ...:

Date of Birth:

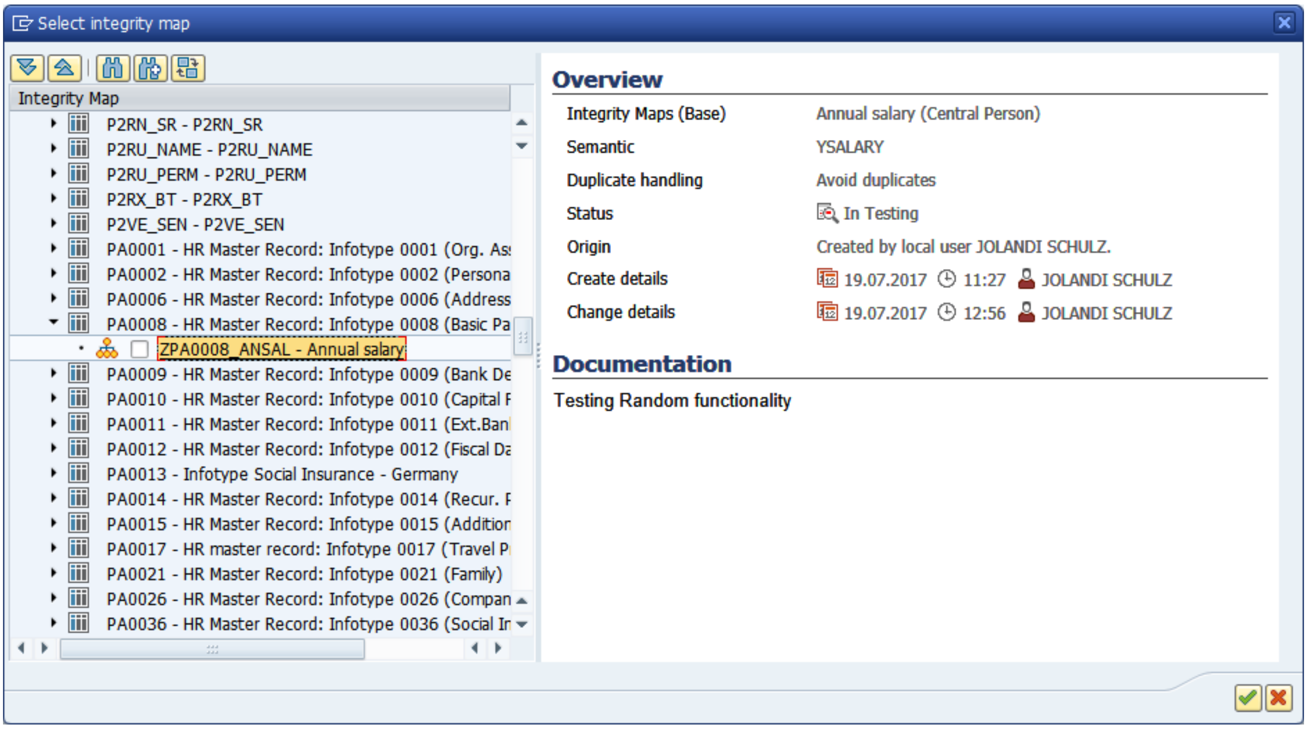
Employee's Bank Country:

After selecting a Condition type and specifying a matching value(s), create the condition by clicking on the Continue ✓ button. Conditions are grouped into the Options selected when they are created (if Options on the Rule exist).

Conditions will be evaluated top to bottom by the masking engine and the first Condition matching data will have its associated masking behavior applied. Conditional behaviors for a Rule are evaluated in order when the masked value for a field in a record is determined. The first Conditional behavior to match the record is used. By default, every Rule has at least one Condition that is always considered a match for any record. This condition is the fallback behavior should the current record not be a match for other conditions evaluated first.

The next section discusses the assignment of a Transformation Function to the currently selected Integrity Map in the context of the current Option and Condition (if any).

d. Integrity Map



Select integrity map

Integrity Map

- P2RN_SR - P2RN_SR
- P2RU_NAME - P2RU_NAME
- P2RU_PERM - P2RU_PERM
- P2RX_BT - P2RX_BT
- P2VE_SEN - P2VE_SEN
- PA0001 - HR Master Record: Infotype 0001 (Org. As
- PA0002 - HR Master Record: Infotype 0002 (Persona
- PA0006 - HR Master Record: Infotype 0006 (Address
- PA0008 - HR Master Record: Infotype 0008 (Basic Pa
  - □ ZPA0008_ANSAL - Annual salary
- PA0009 - HR Master Record: Infotype 0009 (Bank De
- PA0010 - HR Master Record: Infotype 0010 (Capital F
- PA0011 - HR Master Record: Infotype 0011 (Ext.Banl
- PA0012 - HR Master Record: Infotype 0012 (Fiscal Da
- PA0013 - Infotype Social Insurance - Germany
- PA0014 - HR Master Record: Infotype 0014 (Recur. F
- PA0015 - HR Master Record: Infotype 0015 (Addition
- PA0017 - HR master record: Infotype 0017 (Travel P
- PA0021 - HR Master Record: Infotype 0021 (Family)
- PA0026 - HR Master Record: Infotype 0026 (Compan
- PA0036 - HR Master Record: Infotype 0036 (Social Ir

Overview

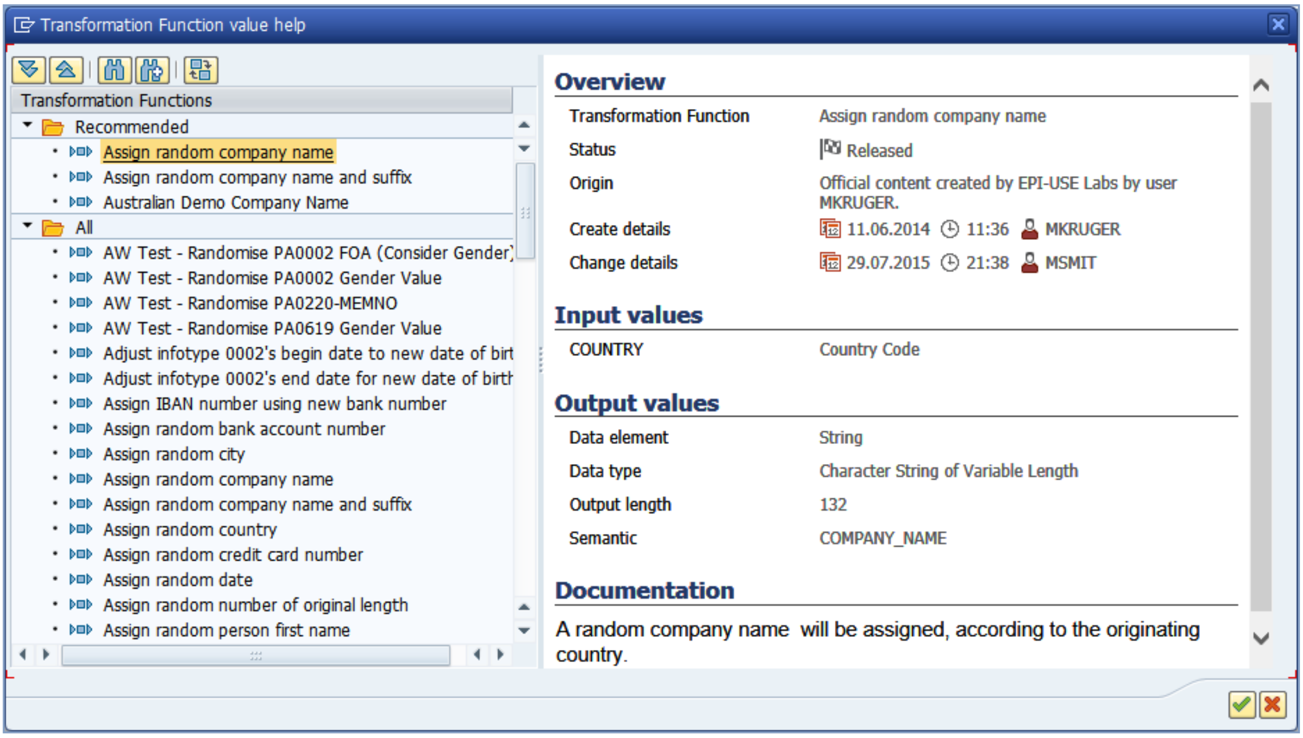
Integrity Maps (Base)	Annual salary (Central Person)
Semantic	YSALARY
Duplicate handling	Avoid duplicates
Status	In Testing
Origin	Created by local user JOLANDI SCHULZ.
Create details	19.07.2017 11:27 JOLANDI SCHULZ
Change details	19.07.2017 12:56 JOLANDI SCHULZ

Documentation

Testing Random functionality

e. Assign Function

When assigning a Transformation Function to an Integrity Map, a list of Transformation Functions is provided. The list is divided into two sub-folders, namely Recommended and All. The first section lists the Recommended Transformation Functions.



Transformation Function value help

Transformation Functions

- Recommended
  - Assign random company name
  - Assign random company name and suffix
  - Australian Demo Company Name
- All
  - AW Test - Randomise PA0002 FOA (Consider Gender)
  - AW Test - Randomise PA0002 Gender Value
  - AW Test - Randomise PA0220-MEMNO
  - AW Test - Randomise PA0619 Gender Value
  - Adjust infotype 0002's begin date to new date of birt
  - Adjust infotype 0002's end date for new date of birth
  - Assign IBAN number using new bank number
  - Assign random bank account number
  - Assign random city
  - Assign random company name
  - Assign random company name and suffix
  - Assign random country
  - Assign random credit card number
  - Assign random date
  - Assign random number of original length
  - Assign random person first name

Overview

Transformation Function	Assign random company name
Status	Released
Origin	Official content created by EPI-USE Labs by user MKRUGER.
Create details	11.06.2014 11:36 MKRUGER
Change details	29.07.2015 21:38 MSMIT

Input values

COUNTRY	Country Code

Output values

Data element	String
Data type	Character String of Variable Length
Output length	132
Semantic	COMPANY_NAME

Documentation

A random company name will be assigned, according to the originating country.

The Recommended section is determined by matching the Semantic tag associated with the Integrity Map with that of the Transformation Functions. If a match is found the Transformation Function is recommended. For more information on key concepts and definitions, please refer to Appendix A.

The next section lists all other Transformation Functions.

Although all Transformation Functions are listed, not every Transformation Function may be compatible with the current Integrity Map based on its output value type. The Rule Editor will check that the assigned Transformation Function is compatible with the Integrity Map before allowing you to proceed. See Section 8 for more details.

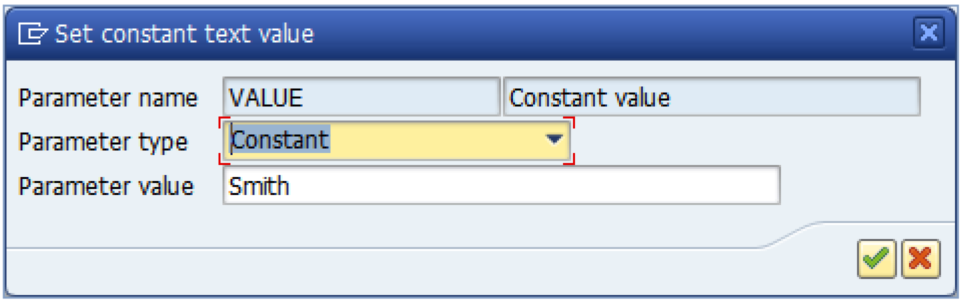
The right-hand side of the screen provides details on the definition of the selected Transformation Function, including a listing of its input parameters and a description of its behavior.

Select either a Recommended or other Transformation Function to assign to the current Integrity Map based on your functional requirements and click on the Continue ✓ button to proceed. For example, the Integrity Map PA0002_VORNA representing the First name field of an Employee is assigned the 'Assign random first name' function in order to assign random first names to replace the current names. The functional requirement is what the customer wants to do when they change the values from their original to scramble/mask them. If the Transformation Function has input parameters, the next section will describe how to assign them.

This is performed either when the Transformation Function is first assigned or when the input parameters are updated with the Change/Edit ✎ button.

f. Edit Function Parameters

When the parameters for a Transformation Function are changed, the parameters are listed in order with the technical names and descriptions. The parameters are defined when the Transformation Function is created. Refer to Section 7 for more details.



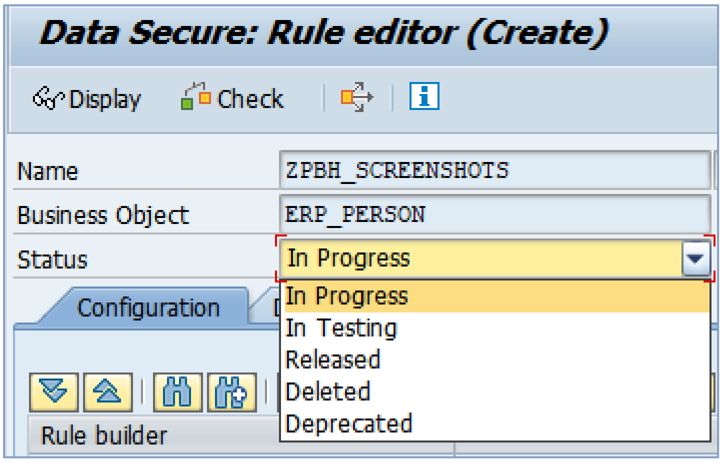
Set constant text value

Parameter name	VALUE	Constant value
Parameter type	Constant	
Parameter value	Smith	

Each parameter is assigned a valid value of a specific type as follows:

Parameter	Behavior
Context-specific	A parameter value that is determined by the Business Object instance context. { } For example, if the Business Object is Customer, the parameter Country will vary according to the Country code associated with the specific Customer whose records are processed.
Old value	The original value(s) of another Integrity Map that is processed before the values of the associated fields are changed by the masking engine.
Constant	A fixed value as specified is assigned to the parameter.
System field	A system field value SY- is assigned to the parameter. A specific value INITIAL is available for assigning INITIAL values to parameters.
User-specified	The value of the parameter is specified via the execution screen of the product that is using the masking rule. (See Section 3 for more details).
New value	If the value of the specified Integrity Map is changed, the New value of the field is provided as in input parameter This parameter allows one masking behavior/rule to influence another. { } For example, a Rule may use a name randomization function for an Integrity map to calculate a new value for the first name field and similarly use a different function to calculate a new surname or last name for the last name field. To update full name fields, it can pass the 'new value' of these fields as input parameters to a function to produce the new full name.
Field value	A value from a field of the current record. Since values are calculated based on the main field of an Integrity Map and distributed to other tables and fields, only values from that table will be available.

When the rule is ready to be used, you need to select its correct status (same process as per Policy status).



Data Secure: Rule editor (Create)

Name ZPBH_SCREENSHOTS

Business Object ERP_PERSON

Status In Progress

In Progress
In Testing
Released
Deleted
Deprecated

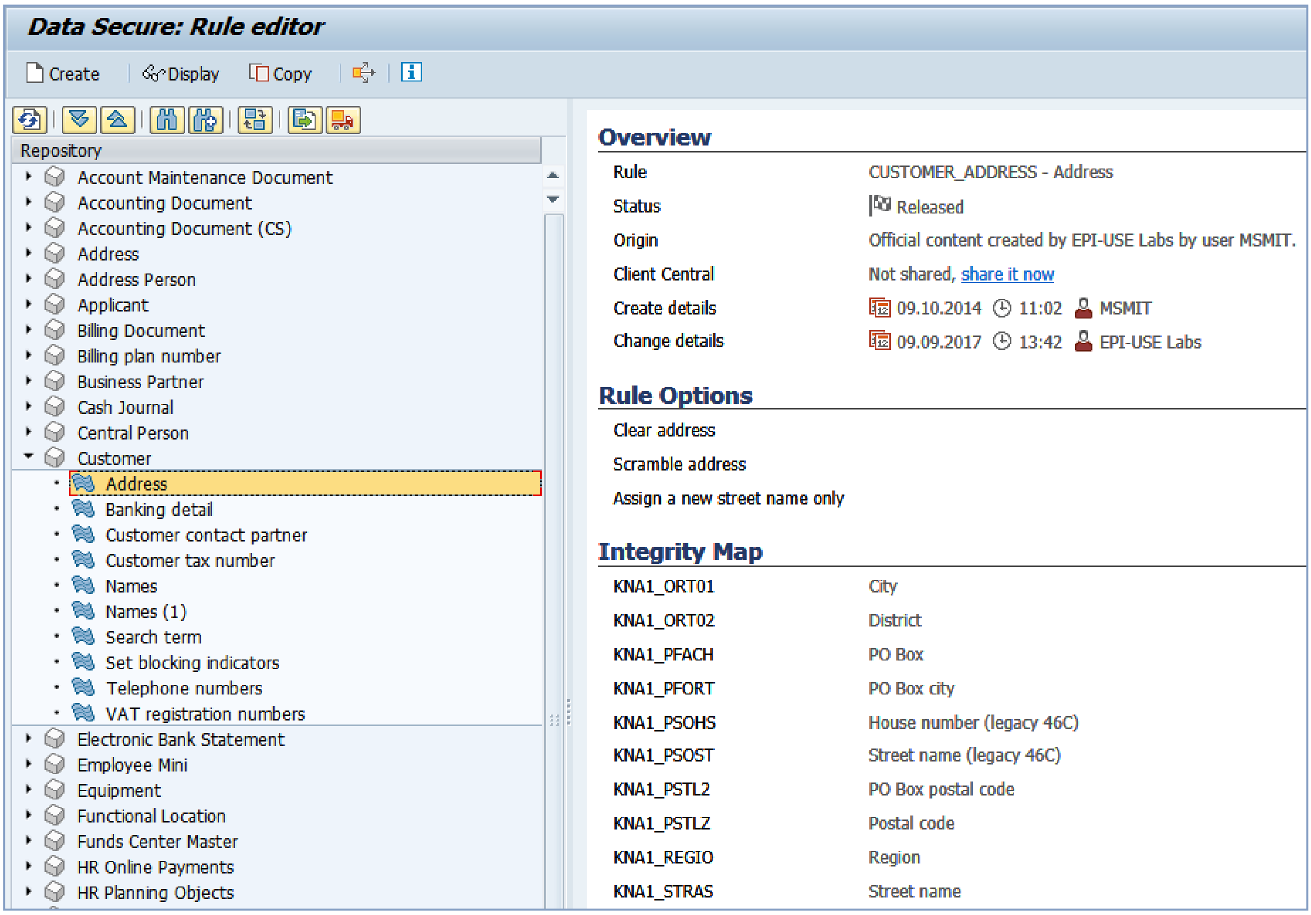
The statuses and their effects are as follows:

Status	Description
In Progress	The rule is still being created and it cannot be used.
In Testing	The rule can be used by on the current system (and client), but cannot be distributed to other systems(and clients). This setting is used when the Rule is being tested.
Released	The rule is available and can be actively used.
Deleted	The rule can no longer be used and will be deleted if distributed to another system/client.
Deprecated	The rule was previously shipped as standard but is no longer supported and cannot be used by products and users. The Rule can be copied to use as a template for custom Rules.

6.2 Maintain an existing Rule

6.2.1 Display or Change Rule

Custom rules are maintained in the Rule editor. To open the Rule editor, select the Rules button in the Data Secure Launchpad. Select the Rule to be maintained and select the Change button to change the rule or the Display button to display the rule information.



Data Secure: Rule editor

Repository
- Account Maintenance Document
- Accounting Document
- Accounting Document (CS)
- Address
- Address Person
- Applicant
- Billing Document
- Billing plan number
- Business Partner
- Cash Journal
- Central Person
- Customer
  - Address
  - Banking detail
  - Customer contact partner
  - Customer tax number
  - Names
  - Names (1)
  - Search term
  - Set blocking indicators
  - Telephone numbers
  - VAT registration numbers
- Electronic Bank Statement
- Employee Mini
- Equipment
- Functional Location
- Funds Center Master
- HR Online Payments
- HR Planning Objects

Overview

Rule	CUSTOMER_ADDRESS - Address
Status	Released
Origin	Official content created by EPI-USE Labs by user MSMIT.
Client Central	Not shared, share it now
Create details	09.10.2014 11:02 MSMIT
Change details	09.09.2017 13:42 EPI-USE Labs

Rule Options

Clear address
Scramble address
Assign a new street name only

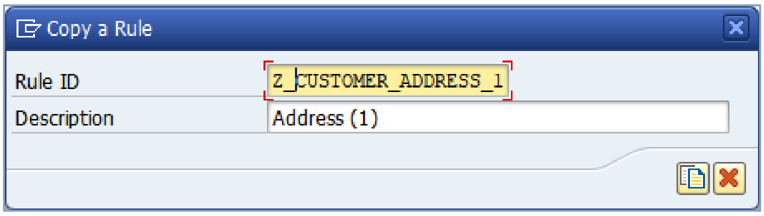
Integrity Map

KNA1_ORT01	City
KNA1_ORT02	District
KNA1_PFACH	PO Box
KNA1_PFORT	PO Box city
KNA1_PSOHS	House number (legacy 46C)
KNA1_PSOST	Street name (legacy 46C)
KNA1_PSTL2	PO Box postal code
KNA1_PSTLZ	Postal code
KNA1_REGIO	Region
KNA1_STRAS	Street name

When editing a Rule, all the same options are available as when creating a new Rule. Please refer to Section 6.1.1 for more details.

6.2.2 Copy Rule

To copy an existing Rule, select the Rule and Click on the Copy button. You will need to provide a Rule ID (that should start with a Z or Y) and name for this new rule in the dialog.



Copy a Rule

Rule ID	Z_CUSTOMER_ADDRESS_1
Description	Address (1)

All the features of the original Rule are copied to the new Rule. This is especially useful when you want to customize the behavior of standard delivered Rules.

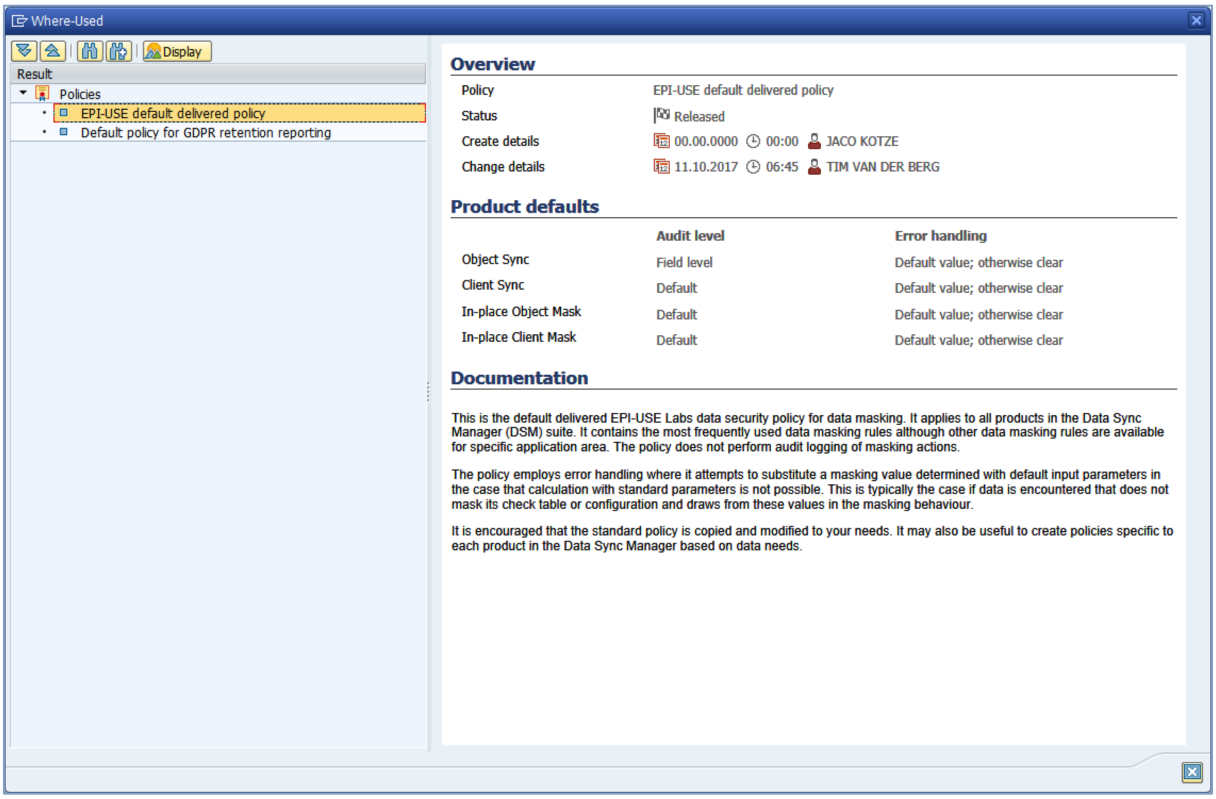
6.2.3 Delete Rule

To delete a Rule, select the Rule and click on the Delete button.

> Standard delivered Rules can be restored if deleted by using the 'Check for updates' option available on the 'Utilities' menu. Please refer to Section 6.5 on the next page for more details.

6.2.4 Where-used

Select a Rule and then the Where-used list button to display all Policies where the selected rule is used. You can also right-click and select Where-used on the context menu


Where-Used
Display
Result
Policies
EPI-USE default delivered policy
Default policy for GDPR retention reporting

Overview

Policy	EPI-USE default delivered policy
Status	Released
Create details	00.00.0000 00:00 JACO KOTZE
Change details	11.10.2017 06:45 TIM VAN DER BERG

Product defaults

	Audit level	Error handling
Object Sync	Field level	Default value; otherwise clear
Client Sync	Default	Default value; otherwise clear
In-place Object Mask	Default	Default value; otherwise clear
In-place Client Mask	Default	Default value; otherwise clear

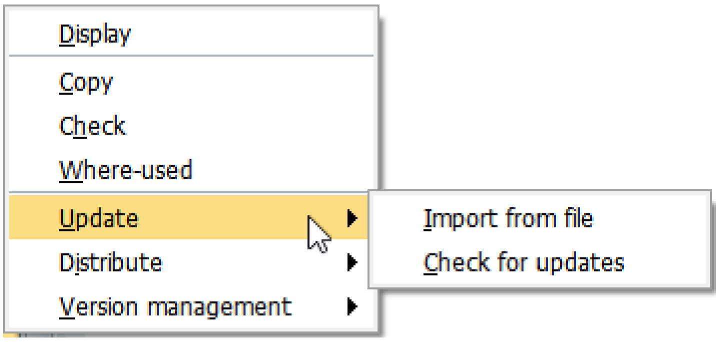
Documentation

This is the default delivered EPI-USE Labs data security policy for data masking. It applies to all products in the Data Sync Manager (DSM) suite. It contains the most frequently used data masking rules although other data masking rules are available for specific application area. The policy does not perform audit logging of masking actions.

The policy employs error handling where it attempts to substitute a masking value determined with default input parameters in the case that calculation with standard parameters is not possible. This is typically the case if data is encountered that does not mask its check table or configuration and draws from these values in the masking behaviour.

It is encouraged that the standard policy is copied and modified to your needs. It may also be useful to create policies specific to each product in the Data Sync Manager based on data needs.

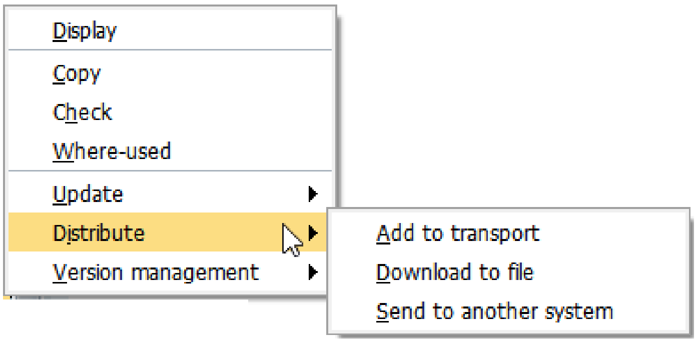
6.3 Update



The Update menu allows Rules to be updated either by uploading an updated definition from a file or by checking for an updated version delivered in the latest Data Sync Manager transport. Selecting either option will prompt for the Rule(s) to be updated. Upon confirmation, the definition is updated to the specified version.

If a standard delivered Rule is deleted, it can be retrieved by using the ‘Check for Updates’ function that will import the rule version included with the latest DSM transport.

6.4 Distribute

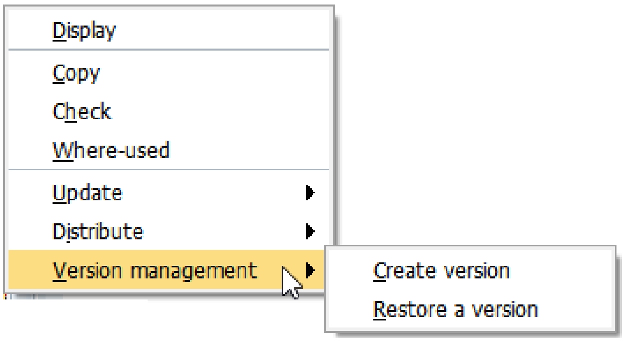


The distribution options for a Rule are accessed from the context menu. This is obtained by right-clicking on a Rule and navigating to a specific ’Distribute’ option in the displayed drop-down menu. The options available are:

Name	Function
Add to transport	Adds the selected Rule to a Transport for distribution using the SAP standard Transport mechanisms.
Download to file	Creates a file at the specified destination that can later be ‘imported’ into Data Secure using the matching function from the ‘Update’ context menu.
Send to another system	Distribute the selected Rule to another system (where DSM5 is installed) by means of an RFC destination. RFC destinations can either be specified Ad-hoc or are configured in the Control Center. Please see the Data Sync Manager Installation Guide for further details.

With the Rule created and distributed, a version can now be maintained. The next section discusses version management options.

6.5 Version Management



There are two options in the Version management sub-menu that are accessed by right-clicking on a selected Rule. They are:

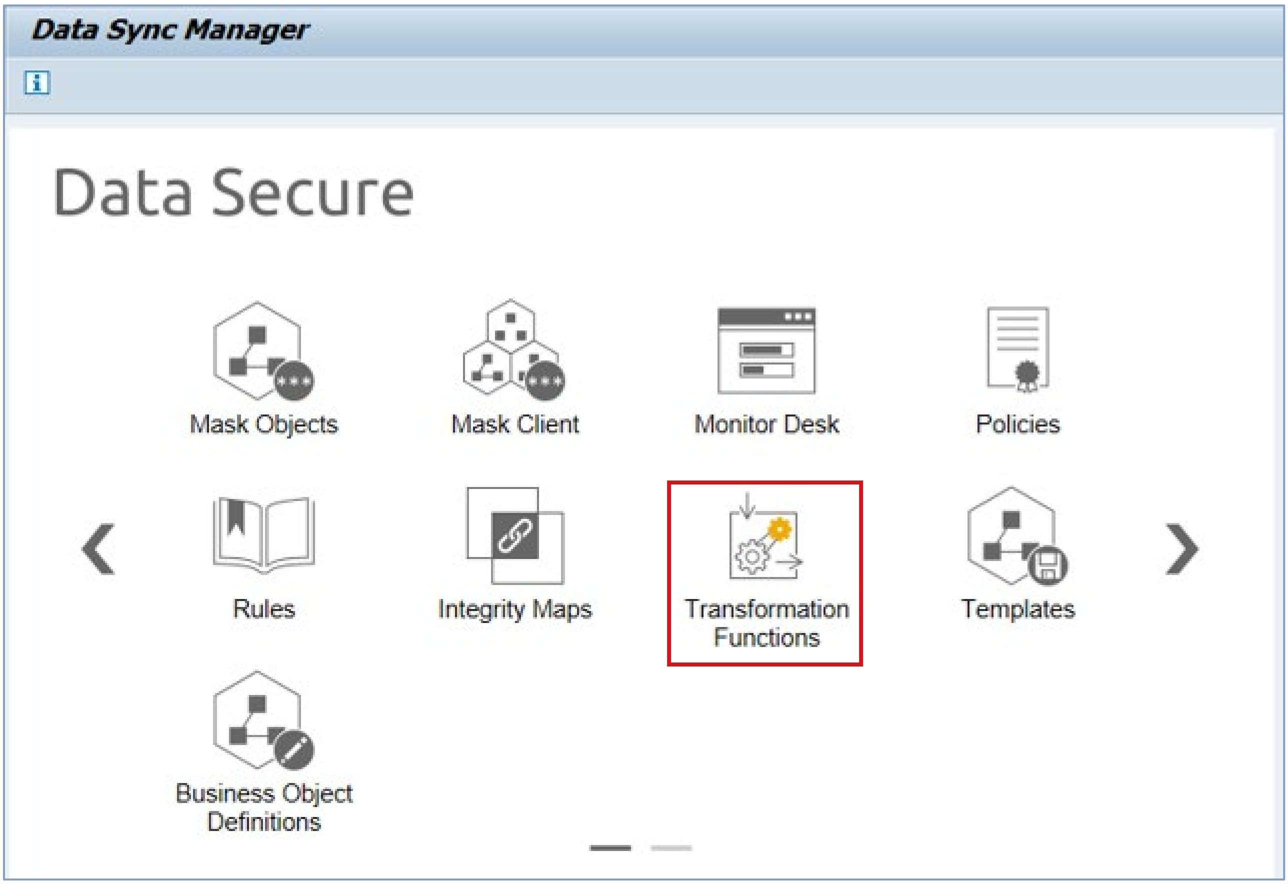
- To store a specific version of a Rule.
- To restore a saved version and make it current at a later time.

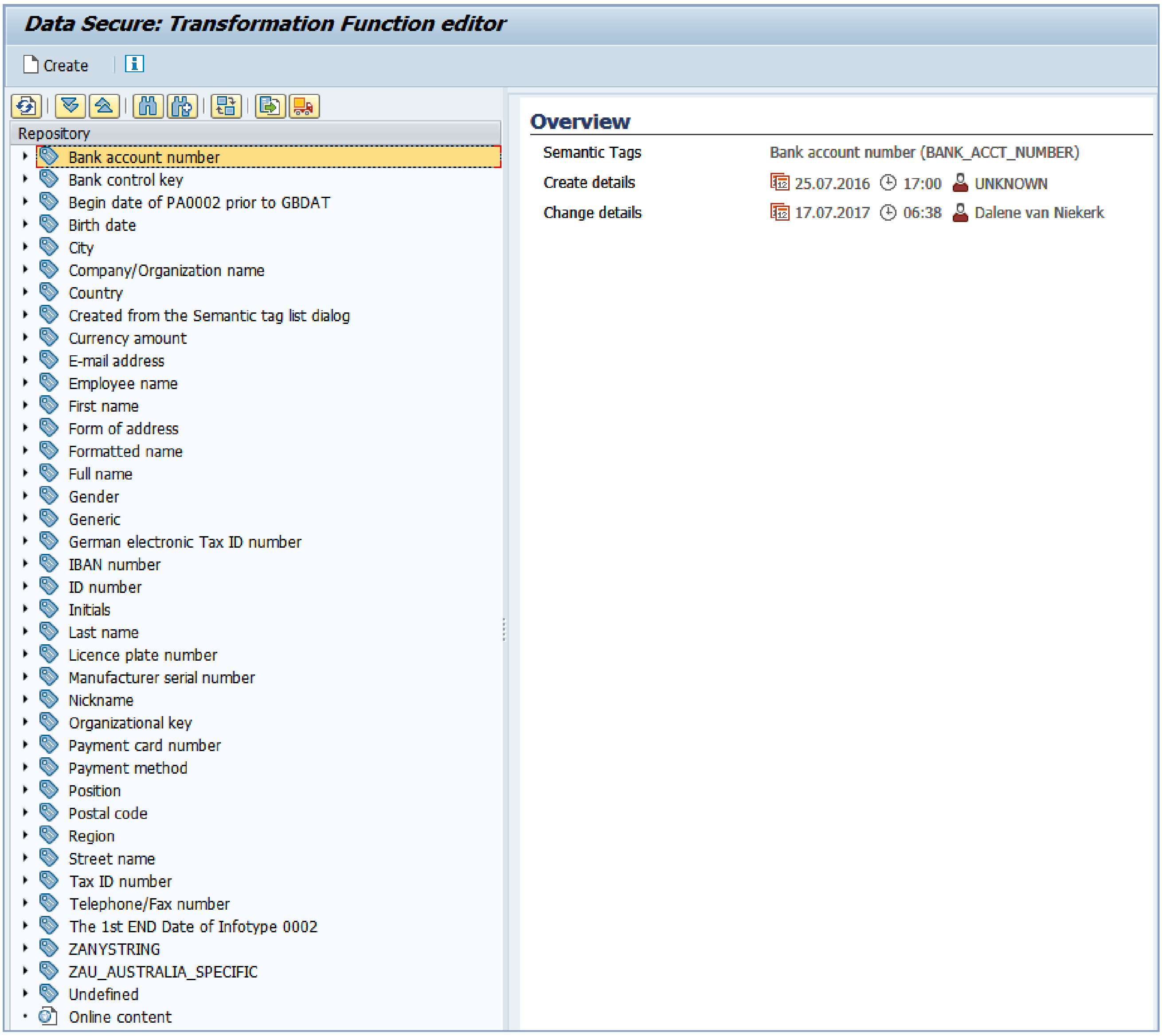
PLEASE NOTE:

**THIS GUIDE IS DIVIDED INTO TWO MAIN PARTS.
THE FIRST PART, UP TO AND INCLUDING SECTION 6 IS MAINLY AIMED AT USERS OF DATA SECURE WHILE THE SECOND PART, SECTIONS 7 AND 8, IS AIMED AT CONTENT DEVELOPERS TO DEFINE DATA MASKING BEHAVIORS.**

7. Transformation Functions

Transformation Functions produce output values according to input parameters. In the context of Data Secure, this determines how a particular value is masked. Transformation Functions are maintained through transaction code '**/n/use/ds**'. From the Data Secure launchpad, select the icon to enter the Transformation Function editor.





Data Secure: Transformation Function editor

Repository

- Bank account number
- Bank control key
- Begin date of PA0002 prior to GBDAT
- Birth date
- City
- Company/Organization name
- Country
- Created from the Semantic tag list dialog
- Currency amount
- E-mail address
- Employee name
- First name
- Form of address
- Formatted name
- Full name
- Gender
- Generic
- German electronic Tax ID number
- IBAN number
- ID number
- Initials
- Last name
- Licence plate number
- Manufacturer serial number
- Nickname
- Organizational key
- Payment card number
- Payment method
- Position
- Postal code
- Region
- Street name
- Tax ID number
- Telephone/Fax number
- The 1st END Date of Infotype 0002
- ZANYSTRING
- ZAU_AUSTRALIA_SPECIFIC
- Undefined
- Online content

Overview

Semantic Tags	Bank account number (BANK_ACCT_NUMBER)
Create details	25.07.2016 17:00 UNKNOWN
Change details	17.07.2017 06:38 Dalene van Niekerk

The Transformation Function editor lists all the Transformation Functions present on the system, grouping them by the Semantic Tag assigned to the Transformation Function in its definition. The Semantic Tags allow functions producing similar output value types to be grouped and paired with compatible Integrity Maps in the context of data masking Rules. Refer to Appendix A for more information on Semantic tags and the relevant section of the Installation and Administration Guide for more details on how to maintain Semantic tags.

The following actions are available in the Transformation Function editor when a Transformation Function is selected:

Icon	Name	Function
Display Change	Display/Change	Display/Edit the selected Transformation Function. Note that 'Change' is only available for custom functions. You cannot change a delivered function.
Check	Check	Checks the validity of the configuration of the selected Transformation Function. Inconsistencies in the configuration are displayed in a log for review.
⇄	Where-Used List	Lists the Rules where the Transformation Function is used.
Create	Create	Allows you to create a new Transformation Function.
ℹ	Information	Display the on-line help for the Transformation Function editor.
▼ ▲	Expand/Collapse	Expand/collapse the Transformation Function editor tree.
🔍 🔍+	Find/Find Next	Finds the Transformation Function matching the specified term.
	Toggle Display	Switches the tree display between the Transformation Function descriptions, technical names or a combination of both.
	Export definition	Export the Transformation Function definition to .elp file.
	Add to transport	Add the Transformation Function definition to a transport.

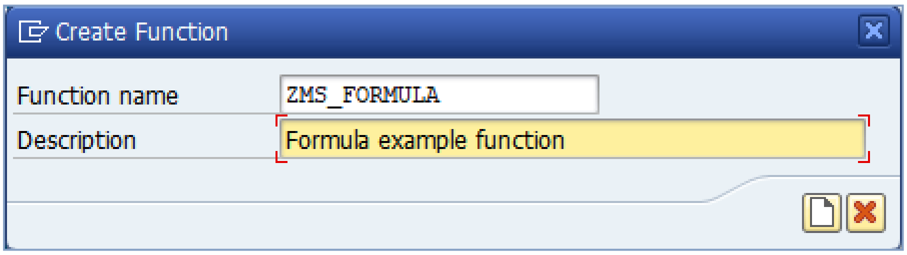
7.1 Creating a Transformation Function

There are two different ways to create a Transformation Function. You can create a Transformation Function manually by selecting the Create button or copy an existing custom or delivered Transformation Function by selecting the Copy button.

If there is an existing Transformation Function that is close to satisfying the masking requirements, the best practice would be to copy and change the existing Transformation Function. Once the pre-existing Transformation Function is copied into a custom namespace, it can be changed to satisfy the masking requirements.

Please note that before any custom Transformation Function logic can be specified, a package needs to be specified wherein code generation will take place. To do so, Select > Utilities > Environment > Transformation Functions from the main menu. Please specify a package in the customer (Z* or Y*) namespace for the generation of Transformation Function logic.

To create a new Transformation Function, select the 🗋 Create button. A pop-up is displayed requiring you to provide the technical name and description to be used for the Transformation Function.

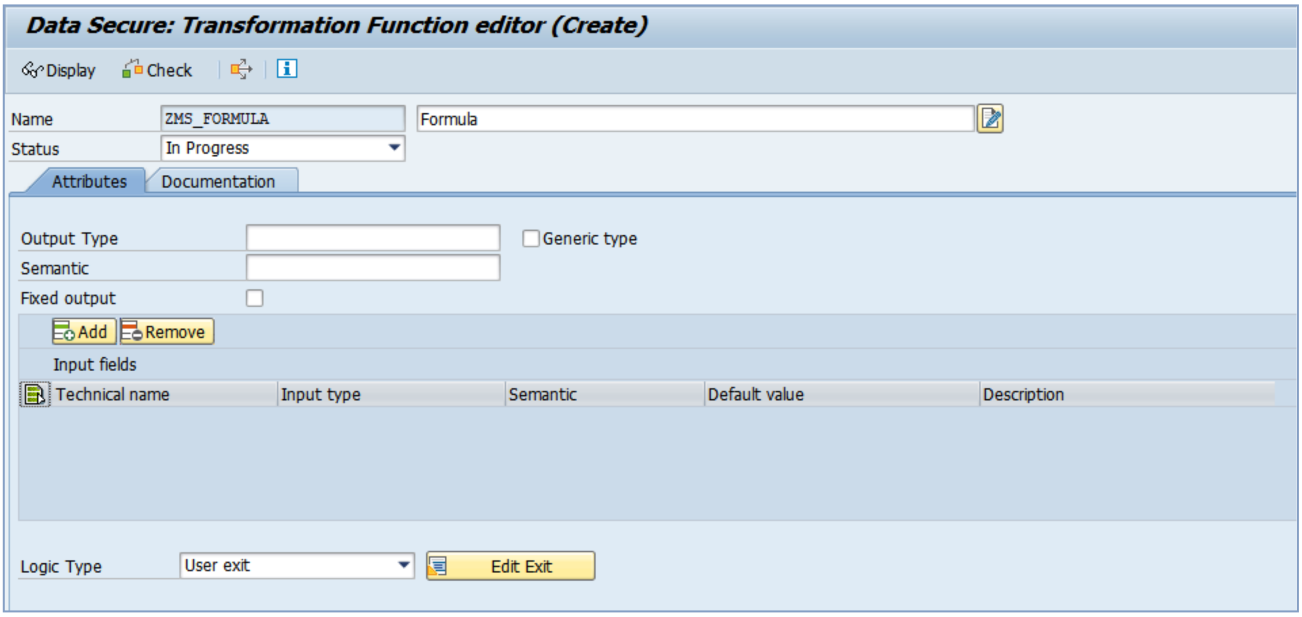


Create Function

Function name: ZMS_FORMULA

Description: Formula example function

Specify the Function name, that must start with a Z or Y, and Description and then select the Create 🗋 button to confirm. The Transformation Function details screen is displayed:



Data Secure: Transformation Function editor (Create)

Name: ZMS_FORMULA Formula

Status: In Progress

Output Type:

□ Generic type

Semantic:

Fixed output: □

Technical name	Input type	Semantic	Default value	Description

Logic Type: User exit

The following functions are available in the Transformation Function editor:

Name	Description
Name and Description	The technical name and description of the function. The description can be maintained in multiple languages. The technical name should always start with a Z or Y.
Status	The technical status of the function. Assign the status according to the desired availability of the Transformation Function. The available statuses are as follows: - **In Progress (default for new rules)**: Transformation Function is still being created. It cannot be used by Rules. - **In Testing**: Transformation Function can be used by on the current system (and client) but cannot be distributed to other systems (and clients). This status is used while the Transformation Function is being tested.

	■ **Released**: Transformation Function definition is complete and it can be actively used in Policies and distributed. ■ **Deleted**: Transformation Function can no longer be used and will be deleted if distributed to another system/client. ■ **Deprecated**: Transformation Function was previously shipped as delivered but is no longer supported and cannot be used by products and users. The Transformation Function can be copied to be used as a template for custom functions. A rule containing Transformation Functions or Integrity Maps in 'In Testing' status cannot be set to Released status. Any Policy containing a Rule in 'In Testing' status cannot be set to 'Released' status. This is so that the unreleased artifacts cannot be distributed as a component of another.
Output Type	A data element describing the type of output the function produces.
Generic Type	An indicator that the function produces output matching any field type. This function will not be checked for field type compatibility when assigned to an Integrity Map in a Rule.
Semantic	Associate the Transformation Function with a Semantic Tag. The tag is used to group the function for display in the TF Editor and to match the function to compatible Integrity Maps. Refer to Appendix A for more details on Integrity Map semantic tags. The search help for Semantic tags allows you to create a new Semantic tag. Once a tag has been created it can be used for other Transformation Functions as well. You can also maintain Semantic tags in the Maintain Semantic option under Business Object Maintenance in the Administration section.
Fixed Output	The function will be evaluated once only during a Data Secure run and the output value will be assigned to the fields of the associated Integrity Map in a rule. This option is selected as an optimization when only a single new value over all assigned fields is desired. An example would be a function that assigns a constant value such as 'Scrambled' or a function that sets a field to its initial value.
Documentation	Detailed documentation of the Transformation Function behavior. Language-specific documentation is available.

A Transformation Function may receive parameters so that its behavior can be determined by context. To specify parameters, add them to the Transformation Function by selecting the Add button or remove a parameter by selecting the Remove button. The following 'Input fields' details are specified for each parameter that is added to the Transformation Function:

Input field	Description
Technical Name	The technical name of the input parameter.
Input Type	A data element specifying the value type required by the input parameter.
Semantic Tag	Attach a Semantic tag to the parameter. The parameter is used to pair the input parameter with a Business Object context parameter from an object definition.
Default Value	The default value that will be used for the parameter if no input is specified.
Description	The on-screen label for the parameter when used elsewhere (Rule editor).

With the header details and parameters of the Transformation Function specified, the Transformation Function still requires its Transformation logic. Select the Logic type as either 'User exit' or 'Formula'. Please refer to Section 7.1.1 and 7.1.2 for details on each of these.

7.1.1 User-exit based Transformation Functions

User-exit based Transformation Function logic generates an 'SAP-program include' in the format '<package_name>_CF_<technical_function_name>' where '<package_name>' is the name of the package specified in the environmental settings for Transformation Functions and '<technical_function_name>' is the unique technical name specified for the function during creation.

Selecting the Edit Exit button will navigate to the 'EXIT_EXECUTE' method of a generated class that serves as the API for custom Transformation Function logic.

To edit the logic the editing user will require an SAP developer key and the system and client where the action is performed will need to be open to repository changes (see transaction SCC4 for the client).

We recommended that the code changes are reviewed according to your organization's security and change control practices and that Transformation Functions are moved through your landscape using Transports to adhere to SAP standard change control practices for ABAP code.

The 'EXIT_EXECUTE' method represents the API for specifying Transformation Function logic compatible with the Data Secure masking engine. The original value of a masked field is received through an input parameter called 'I_OLD_VALUE'. The new value that the field should receive is specified in an exporting parameter with the name 'E_NEW_VALUE'.

To read the additional parameter values that may be supplied to a Transformation Function in a Rule (refer to Section 6.1.1c), use the API methods 'GET_PARAM_VALUE' to read a single parameter value and ‘GET_PARAM_VALUES’ to read all the possible values of a defined parameter. The name of the parameter is specified in the input ‘I_PARAM_NAME’ parameter and the value of the parameter is returned in the parameters shown as ‘E_VALUE’ and ‘ET_VALUES’.

An optional ‘IIF_TRACE’ parameter, which is a reference to the interface ‘/USE/IF_USL2_TRACE’, is provided to write trace messages via the Data Secure masking engine. The ‘IIF_TRACE’ parameter can also be passed to calls of ‘GET_PARAM_VALUE’ and ‘GET_PARAM_VALUES’ to trace messages written when attempting to obtain parameter values. Trace message can be written through a variety of method calls declared in the ‘/USE/IF_USL2_TRACE’ interface.

An optional ‘I_USE_NEW’ parameter can be used to force a parameter of type ‘Old value’ to obtain the ‘New value’ masked value if a masked value has been determined; otherwise, the parameter value is based on the parameter type used during the rule creation.

Some parameter types may have multiple values such as those of the type ‘Old value’ and ‘New value’. To match one of the multiple parameter values to the current record, a reference to the currently processed record, called ‘MSR_RECORD’, can be used. The reference is typed according to the DDIC type of the currently processed record.

The remaining content of the class is generated. Except for class (DATA), static (CLASS-DATA) attributes, and methods specified in the PUBLIC, PROTECTED or PRIVATE sections of the class declarations, other content may be lost when the Transformation Function is saved or distributed.

7.1.2 Formula-based Transformation Functions (LabsScript)

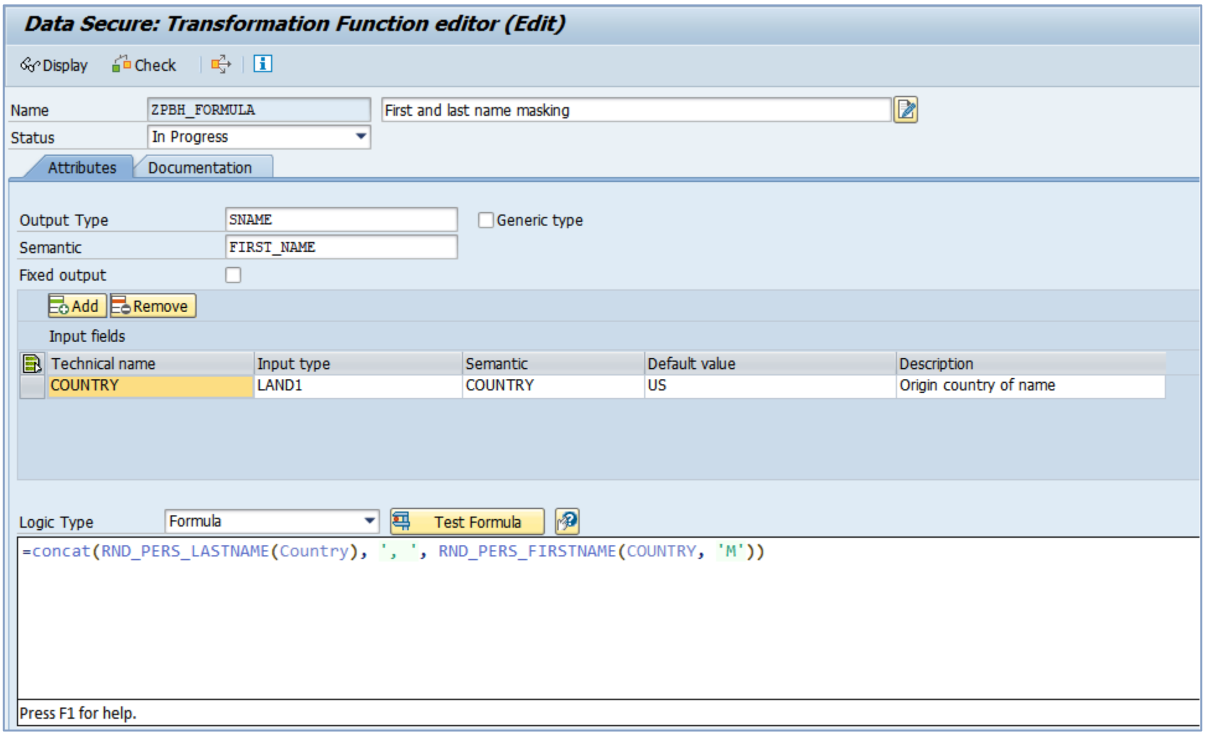
To eliminate the need for a developer key and to reduce the risk of dangerous ABAP statements being used in the Transformation Function logic, we provide the LabsScript scripting language for specifying Transformation Function logic.

LabsScript uses functional syntax familiar to users of Spreadsheet software with a variety of standard logical, text and mathematical functions available. For more information on the language, select ‘Formula’ from the drop-down for field Logic type, select within the editable area displayed and press the F1 key or click on the ? button. In-product help is displayed with detailed information on language syntax.

In the context of Data Secure, LabsScript is enhanced by recording every Transformation Function present on the current system as a function that can be called directly within the language. The input parameters of a function are also available to be specified as part of the function call. The parameters are documented in the in-product help as for standard LabsScript functions.

The parameters of the current function are available in the LabsScript syntax and are accessed by specifying their technical name. Please refer to Section 7.1 for more details on Transformation Function parameters.

Below is a sample function that calls delivered Transformation Functions (RND_PERS_FIRSTNAME, RND_PERS_LASTNAME) to produce a randomized male full name in a <last name>, <first name> format according to the country provided as an input parameter for the function. The function ‘CONCAT’ is a standard ‘concatenate’ function in the LabsScript language.



Name: ZPBH_FORMULA — First and last name masking
Status: In Progress

Output Type: SNAME □ Generic type
Semantic: FIRST_NAME
Fixed output: □

Input fields

Technical name	Input type	Semantic	Default value	Description
COUNTRY	LAND1	COUNTRY	US	Origin country of name

Logic Type: Formula

```
=concat(RND_PERS_LASTNAME(Country), ', ', RND_PERS_FIRSTNAME(COUNTRY, 'M'))
```

Press F1 for help.

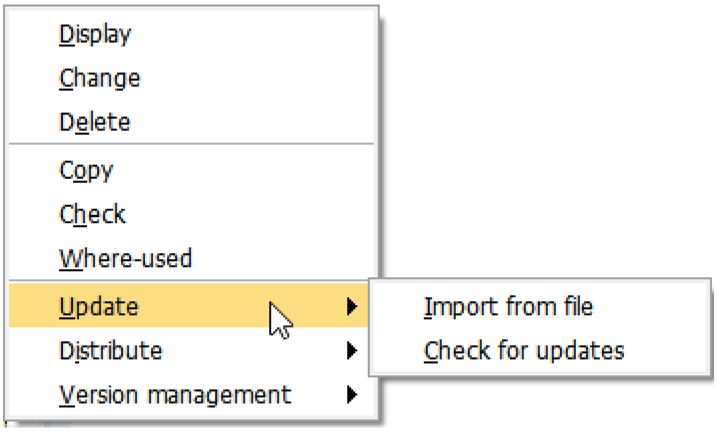
To test the validity of the formula, click on the Test Formula button. The syntax of the function is checked for validity and the function is called using the default parameter value assigned. A sample of the resulting value is displayed.

With the Transformation Function logic specified either by User exit or by a LabsScript formula, the Transformation Function is ready to be saved. First, check the configuration by selecting the Check button. A trace is displayed listing any error in the configuration.

If there are no errors in the configuration, proceed to save the Transformation by selecting the ‘Save’ 💾 button. The Transformation Function is checked once again and the configuration is saved.

Click the ‘Back’ button to return to the list of available Transformation functions. The new function will be available under the function’s Semantic Tag folder.

You can now use the Update, Distribution and Versioning functions described in the following sections. To access these functions, select the specific Transformation Function and right-click to access the context menu.

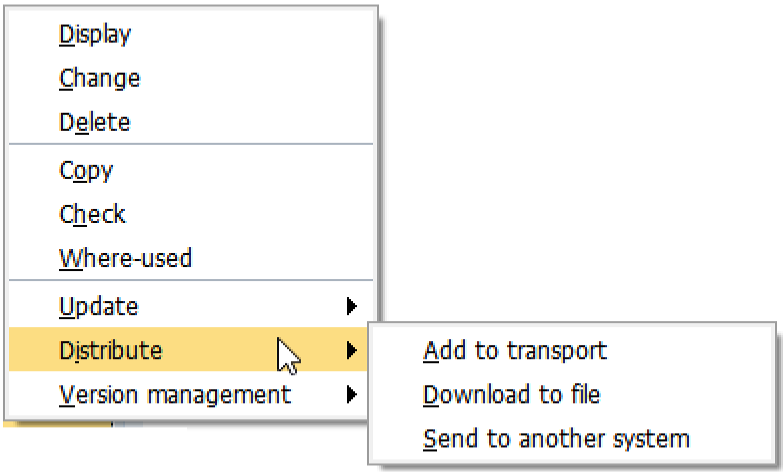


7.1.3 Update

The Update menu allows Transformation Functions to be updated either by uploading an updated definition from a file or by checking for an updated version as delivered in the latest Data Sync Manager transport. Selecting either option will prompt for the Transformation Function(s) to be updated. Upon confirmation, the definition is updated to the specified version.

If EPI-USE Labs delivered Transformation Functions are deleted, they can be retrieved by using the 'Check for Updates' function to restore the EPI-USE Labs delivered versions.

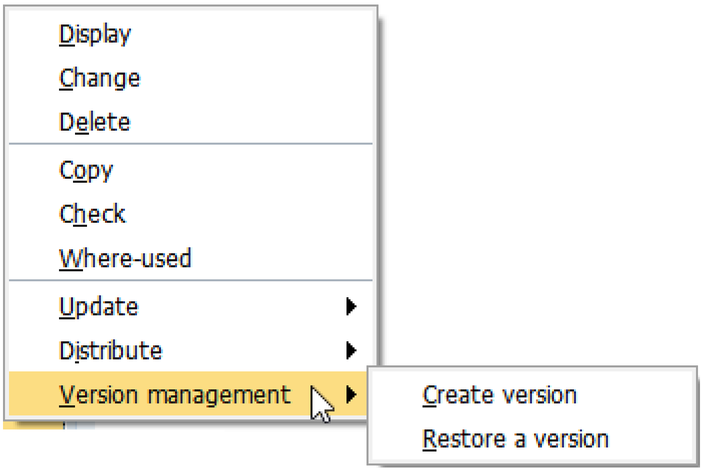
7.1.4 Distribute



The distribution options for Transformation Functions are accessed from the context menu obtained by right-clicking a Transformation Function and browsing to the 'Distribute' option in the displayed menu. The options available are:

Name	Function
Add to transport	Adds the selected Transformation Function to a Transport for distribution using the SAP standard Transport mechanisms.
Download to file	Creates a file at the specified destination that can later be 'Imported' into Data Secure using the matching function from the 'Update' right-click context menu.
Send to another system	Distributes the selected Transformation Function to another system (where DSM5 is installed) by means of an RFC destination. RFC destinations can either be specified ad-hoc or are determined by the Control Center. Please see the Data Sync Manager Installation Guide for further details.

7.1.5 Version Management



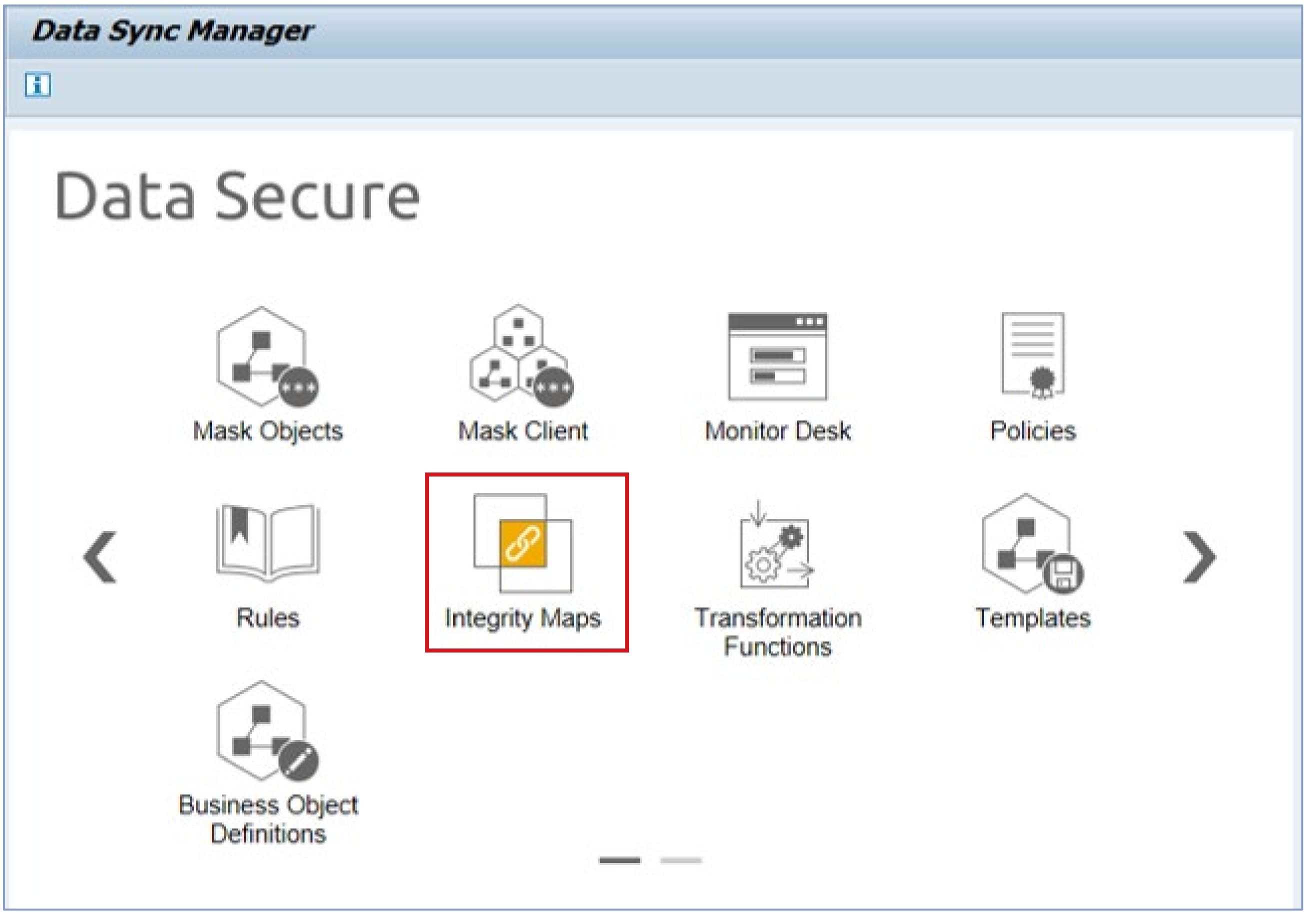
There are two options in the Version management sub-menu that are accessed by right-clicking on a selected Transformation Function:

- Store a specific version of a Transformation Function (Create version)
- Restore a saved version and make it current at a later time (Restore a version).

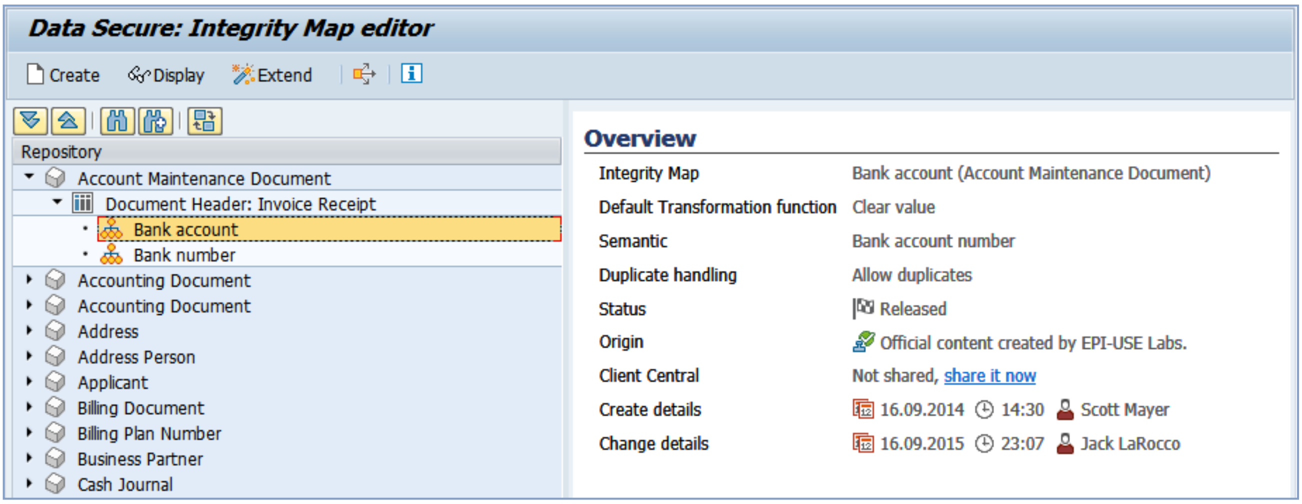
8. Integrity Maps

Integrity Maps are defined within a Business Object Context as a set of fields that store the same or similar information in a redundant fashion and therefore needs to be updated with the same/similar values when masked in order to retain semantic data integrity.

Integrity Maps are maintained through transaction code **/n/use/ds**. From the Data Secure launchpad, select ‘Integrity Maps’ to enter the Integrity Map editor.



The Integrity Map editor lists all Integrity Maps present on the system, grouped by Business Object context and reference table.



Data Secure: Integrity Map editor

Repository
- Account Maintenance Document
  - Document Header: Invoice Receipt
    - Bank account
    - Bank number
- Accounting Document
- Accounting Document
- Address
- Address Person
- Applicant
- Billing Document
- Billing Plan Number
- Business Partner
- Cash Journal

Overview

Integrity Map	Bank account (Account Maintenance Document)
Default Transformation function	Clear value
Semantic	Bank account number
Duplicate handling	Allow duplicates
Status	Released
Origin	Official content created by EPI-USE Labs.
Client Central	Not shared, share it now
Create details	16.09.2014 14:30 Scott Mayer
Change details	16.09.2015 23:07 Jack LaRocco

The following actions are available in the Integrity Maps editor when a delivered Integrity Map is selected:

Button	Name	Description
Create	Create	Creates a new Integrity Map.
Extend	Extend	Extends an existing Integrity Map with additional tables, fields and/or links to other Integrity Maps.
Delete	Delete	Deletes the selected the Integrity Map. Note that this function is only available for custom functions. You cannot delete a delivered function.
⇨	Where-Used List	Lists the Rules where the Integrity Map is used.
i	Information	Displays the In-product help for the Integrity Map editor.
⟳	Refresh	Refreshes the Integrity Map editor tree.
▽	Expand tree	Expands the tree or selected tree node.
△	Collapse tree	Collapses the tree or selected tree node.
🔍 🔍	Find/Find Next	Finds a specific Integrity Map.
⇄	Toggle names	Switches the tree display between the Integrity Map descriptions, technical names or a combination of both.

	Download to file	Allows a selection of Integrity Maps to download to a specified file destination. The file can later be 'Imported' into Data Secure using the matching function from the 'Update' context menu.
	Add to Transport	Allows selection of Integrity Maps to add to SAP Transport for distribution using the SAP standard Transport mechanisms.

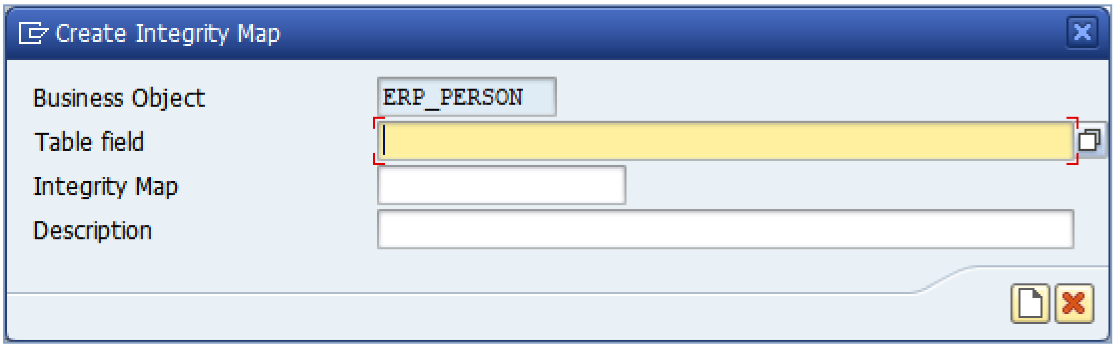
8.1 Creating an Integrity Map

A new Integrity Map is created by selecting the Create button.

To process only the records relevant to a single real-world entity such as a customer/ vendor/employee, an Integrity Map is defined in the context of a Business Object. Processing a single instance of this Business Object and updating the fields recorded in the Integrity Map produces the intended result of updating only the sensitive data belonging to the real-world entity.

8.1.1 Create the Integrity Map

To create a new Integrity Map, select the Create button and specify the Business Object context, the (reference) table field, the technical name of the Integrity Map and its description.



Create Integrity Map

Business Object: ERP_PERSON

Table field:

Integrity Map:

Description:

- **Business Object:** The Business Object context of the Integrity Map determines which records from the tables listed in the Integrity Map are transformed according to its assigned Transformation Function in a Rule (refer to Section 6.1.1 for more details).

  The record selection is based on the selection configuration of the table within the Business Object definition. Refer to the relevant section of the Business Object Workbench User and Extensions guide for more information on configuring the selection of tables in the context of a Business Object definition.

  Only tables that occur in the specified Business Object **A** or occur in another Business Object **B** that is related to **A** by an IS-A integration point can be added to the Integrity Map. IS-A integration points are created between Business Objects that should be masked 1-to-1 as they correspond to the same real-world entity. Refer to the Business Object Workbench User and Extensions guide for more information on adding IS-A relationships between Business Objects.

If an Integrity Map is set to 'Avoid duplicates', the masking engine will determine the current Business Object key that corresponds to a record and then group assigned values according to the Business Object key. If the record occurs in a table of a different Business Object **B**, the IS-A integration point from **B** to **A** is followed to determine the key of Business Object **A** to be used for grouping assigned masked values.

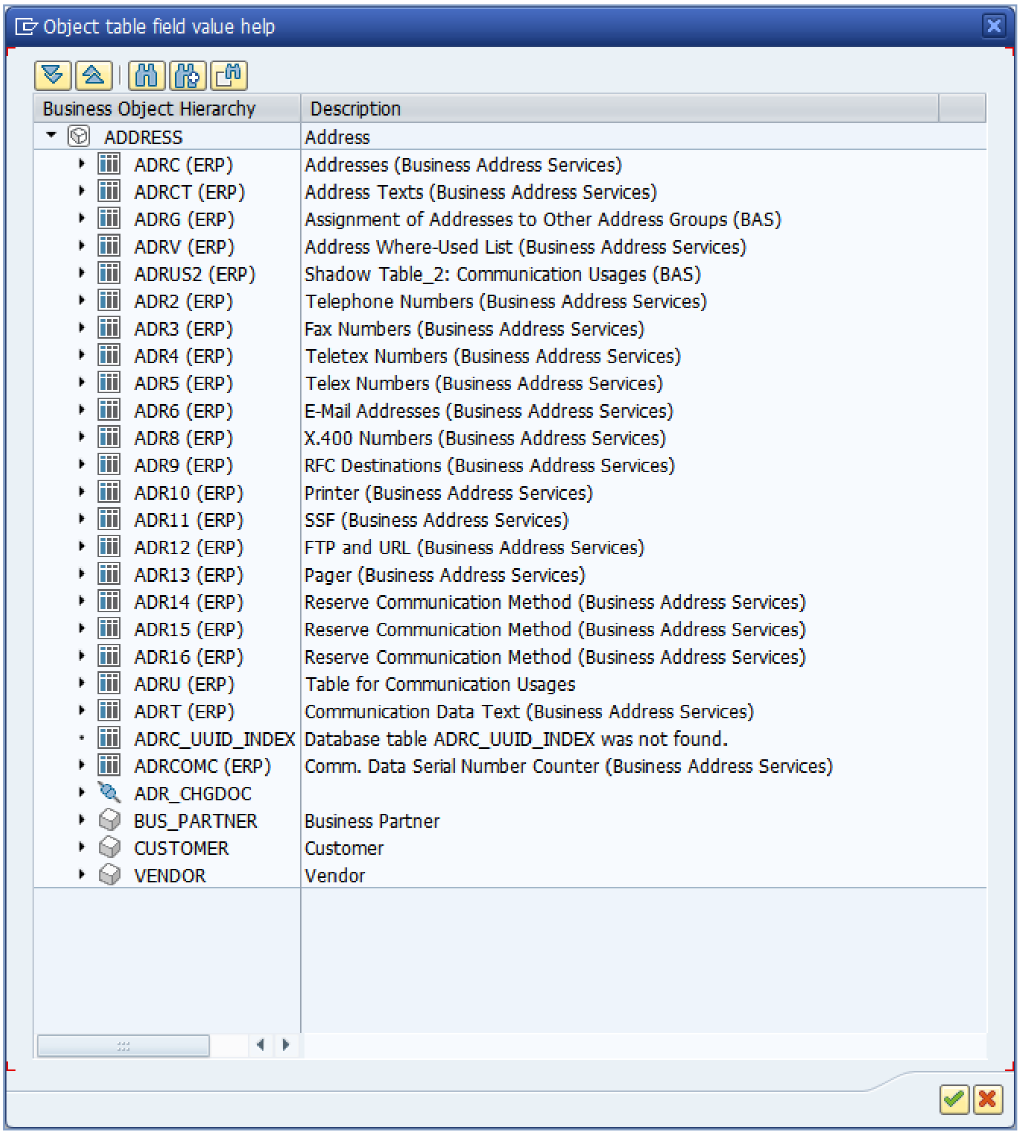
For example, a Vendor that is also an Employee will have occurrences of its first name masked in the same way across Vendor and Employee records. Other Vendors that are different Employees with the same first name will receive different masked values. This avoids traceable patterns in the masked data.

- **Table field**: The reference table field is read to determine the values that need to be masked. The new masked value assigned to this field will be used to convert all table fields grouped within the Integrity Map. Be sure to select a main table and field that is duplicated to the other table fields grouped in the Integrity Map.

To guide the user, a 'Search help' is provided listing the available table fields that may act as a reference table field.

If the engine encounters a value in another grouped table field that does not match the reference table field value, the engine will issue a warning and calculate a new masked value using the context of the record being processed. If an input value to the assigned Transformation Function (refer to Section 6.1.1) cannot be determined, the default values of the Transformation Function are used (refer to Section 7.1).

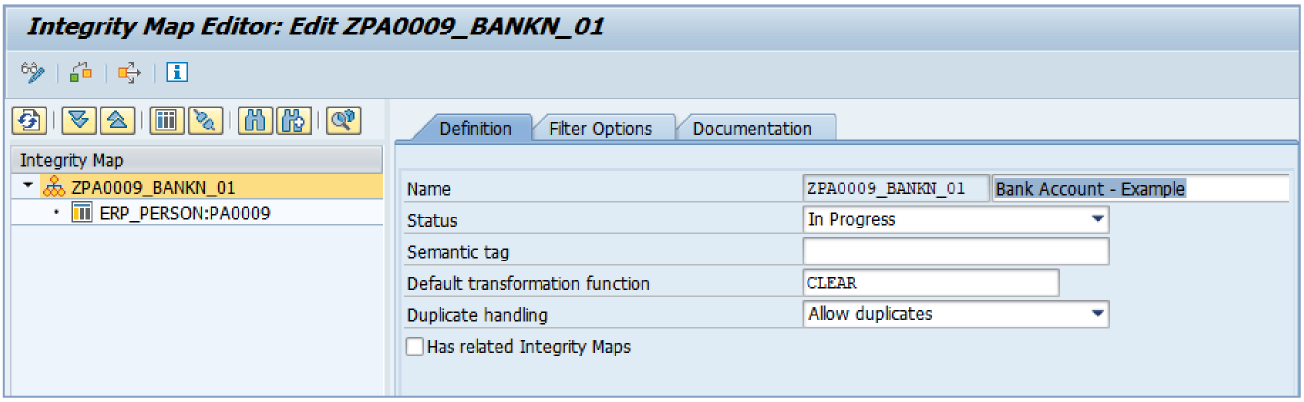
- **Technical name**: The technical name of the Integrity Map must start with a 'Z' or 'Y' to distinguish custom Integrity Maps from EPI-USE delivered ones. The technical name uniquely identifies the Integrity Map and the description provides more information with regard to its purpose.



Business Object Hierarchy	Description
ADDRESS	Address
ADRC (ERP)	Addresses (Business Address Services)
ADRCT (ERP)	Address Texts (Business Address Services)
ADRG (ERP)	Assignment of Addresses to Other Address Groups (BAS)
ADRV (ERP)	Address Where-Used List (Business Address Services)
ADRUS2 (ERP)	Shadow Table_2: Communication Usages (BAS)
ADR2 (ERP)	Telephone Numbers (Business Address Services)
ADR3 (ERP)	Fax Numbers (Business Address Services)
ADR4 (ERP)	Teletex Numbers (Business Address Services)
ADR5 (ERP)	Telex Numbers (Business Address Services)
ADR6 (ERP)	E-Mail Addresses (Business Address Services)
ADR8 (ERP)	X.400 Numbers (Business Address Services)
ADR9 (ERP)	RFC Destinations (Business Address Services)
ADR10 (ERP)	Printer (Business Address Services)
ADR11 (ERP)	SSF (Business Address Services)
ADR12 (ERP)	FTP and URL (Business Address Services)
ADR13 (ERP)	Pager (Business Address Services)
ADR14 (ERP)	Reserve Communication Method (Business Address Services)
ADR15 (ERP)	Reserve Communication Method (Business Address Services)
ADR16 (ERP)	Reserve Communication Method (Business Address Services)
ADRU (ERP)	Table for Communication Usages
ADRT (ERP)	Communication Data Text (Business Address Services)
ADRC_UUID_INDEX	Database table ADRC_UUID_INDEX was not found.
ADRCOMC (ERP)	Comm. Data Serial Number Counter (Business Address Services)
ADR_CHGDOC	
BUS_PARTNER	Business Partner
CUSTOMER	Customer
VENDOR	Vendor

Once all the details are specified, create the Integrity Map by selecting the ☑ 'Continue' button and complete the detailed Integrity Map configuration.

8.1.2 General settings


Integrity Map Editor: Edit ZPA0009_BANKN_01

Integrity Map
- ZPA0009_BANKN_01
  - ERP_PERSON:PA0009

Definition | Filter Options | Documentation

Name: ZPA0009_BANKN_01 Bank Account - Example
Status: In Progress
Semantic tag:
Default transformation function: CLEAR
Duplicate handling: Allow duplicates
□ Has related Integrity Maps

The following general field settings are available for the Integrity Map:

Name	Description
Name and Description	The technical name and description of the Integrity Map as specified during creation. The description can be maintained in multiple languages.
Status	The Integrity Map may have one of the following statuses: ▪ **In Progress**: Integrity Map is still being created. It cannot be used by Rules. ▪ **In Testing**: Integrity Map can be used on the current system (and client), but cannot be distributed to other systems. This status is used when the Integrity Map is being tested. ▪ **Released**: Integrity Map is available and can be actively used in Rules. ▪ **Deleted**: Integrity Map can no longer be used and will be deleted if distributed to another system. ▪ **Deprecated**: Integrity Map was previously shipped with the DSM transport but is no longer supported and cannot be used by products and users. The Integrity Map can be copied to be used as a template for custom Integrity Maps.
Semantic tag	A Semantic tag describing the fields grouped by the Integrity Map (Refer to the Installation, Control Center and Configuration Guide for more details on Semantic tags).
Default transformation function	The default Transformation function to be assigned when the Integrity Map is added to a Rule. (Refer to Section 6.1.1).
Duplicate handling	The following options are available to specify how the Data Secure engine should handle the assignment of duplicate masked field values to multiple instances of the Business Object: ▪ **Allow duplicates**: Duplicate masked values may be assigned to multiple occurrences of an original value in the field grouped by the Integrity Map.

	- **Avoid duplicates**: If it is determined that a masked value has already been assigned for an original field value for one Business Object instance, a new masked value will be assigned if the same original value occurs for a different Business Object instance (refer to Section 1.4.3 for more information). - **No duplicates allowed**: Every assigned masked value should be unique since it is expected that every original value that occurs in the fields grouped by the Integrity map is unique. The engine will assign values until it is determined that the assigned value is unique across all Business Object instances.
Related Integrity Maps	Indicates whether the Integrity Map has other related Integrity Maps that should be processed concurrently. If 'Has related Integrity Maps' is activated, you can specify a list of other Integrity Maps related to the current Integrity Map. The resulting behavior is that when the Integrity Map is added to a Rule (refer to Section 6.1.1), the related Integrity Maps will be suggested as additional Integrity Maps to add to the Rule to ensure that all the related data is masked consistently If the 'Technical' flag is set for a related Integrity Map, this Integrity Map will be selected by default in the list of related Integrity Maps suggested when the main Integrity Map is added to a Rule. It can, however, be deselected.

With the Integrity Map created and the general settings specified, the next section details the options available to expand the scope of the Integrity Map beyond the check table field.

8.1.3 Integrity Map content

The following buttons and functions are available in the Integrity Map Editor toolbar:

Button	Name	Function
✎	Display/edit	Toggles between display and edit mode for the Integrity Map.
	Check	Checks that the Integrity Map configuration is valid.
	Where-Used	Lists the Rules where this Integrity Map is used.
i	Information	Displays the online help for the Integrity Map Editor.
⟳	Refresh	Refreshes the Integrity Map details editor screen.

⏬	Expand tree	Fully expands the Integrity Map detail editor tree.
⏫	Collapse tree	Collapses the Integrity Map detail editor tree.
▦	Add Table	Adds a table to the Integrity Map. How to use it to extend the Integrity Map is discussed further below.
🔗	Include Integrity Map	Includes the scope of another Integrity Map within this Integrity Map. Refer to details on how to use it to extend the Integrity Map further below.
🔍 🔍	Find/Find Next	Finds a specific table or included Integrity Map.
🔍	Discovery	Executes a discovery search for the Integrity Map.

The two Toolbar options that can be used to extend the scope of the Integrity Map are discussed in more detail below:

- **Add table**: This adds the specified table to the scope of the Integrity Map directly. The same table selection dialog is displayed as the reference table and field selection when you create a new Integrity Map(refer to Section 8.1.1).

> When the Integrity Map is created, it automatically adds a direct mapping for the entire reference field in the reference table.

- **Include Integrity Map**: This extends the scope of the main Integrity Map to include the specified Integrity Map's fields as well. The selection of Integrity Maps that can be included in the current Integrity Map is limited to Integrity Maps of Business Objects related with IS-A integration points to the current Integrity Map's related Business Object.

  Tables added directly to an Integrity Map using the Add Table option are treated differently from tables added via the inclusion of another Integrity Map. If a table field is added directly in an Integrity Map, it is assumed that all the values that occur in it also occur in the reference table and field.

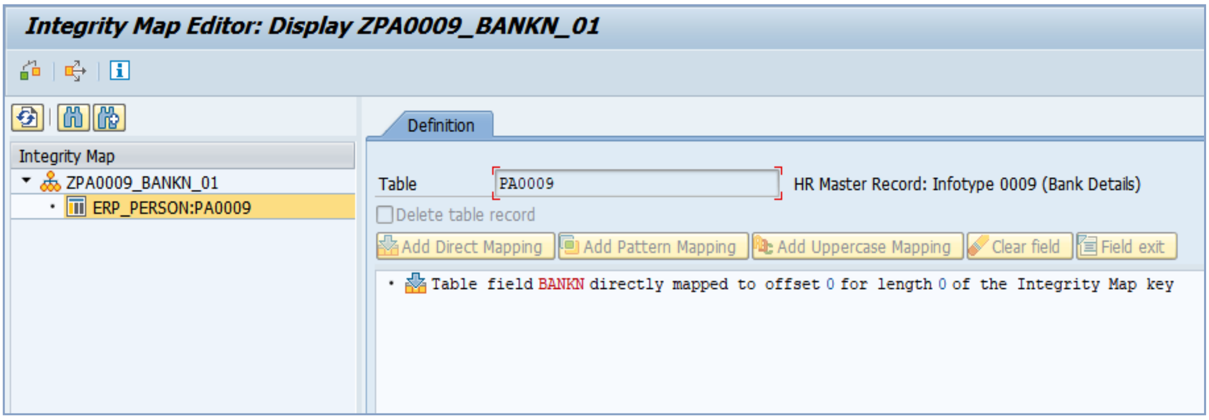
  If instead, a field occurs in another Integrity Map, which is included in the original Integrity Map, it is not assumed that every value of this field will occur in the reference field of the original Integrity Map. If the field value in the included Integrity Map matches a value found in the reference table and field of the included Integrity Map, the new value of the main table field is assigned to the included Integrity Map field. If it does not find a matching value, the value assigned to the included Integrity Map will be assigned during masking.

For example, the Integrity Map that contains the bank account number of an Employee in Infotype 0009 (PA0009) will also directly include the payroll cluster (table PCL2) bank account number as it is duplicated by payroll processing. If the same Employee is a Business Partner, it may have a bank account in the context of being a Business Partner (BUT0BK) that may or may not match with the bank account used by the Employee record in HCM. The Business Partner bank account Integrity Map is therefore included in the Employee bank account Integrity Map so that they are *assigned the same masked value if they were the same originally*.

Now that we have defined how to extend the scope of the Integrity Map to include additional tables and other Integrity Maps, the next section discusses the options available for mapping fields in the tables mentioned above to the main Integrity Map field.

8.1.4 Mapping options

To specify field mappings for a table included in an Integrity Map, select the table in the tree on the left-hand side of the screen.



Integrity Map Editor: Display ZPA0009_BANKN_01

Table PA0009 HR Master Record: Infotype 0009 (Bank Details)

☐ Delete table record

- Table field BANKN directly mapped to offset 0 for length 0 of the Integrity Map key

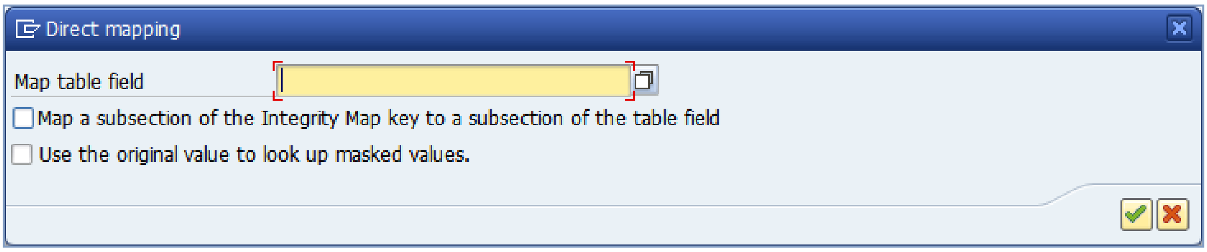
If the selected table is the reference table, an automatic mapping to the reference field will be displayed. It will be a Direct Mapping that maps the entirety of the reference field. If a new table is added to the scope of the Integrity Map, no field will be added by default and field mapping needs to be added through the following options:

Icons	Function
Add Direct Mapping	Maps directly to and from the specified offset and length of the designated field. This is the default mapping type.
Add Pattern Mapping	Maps a value matching the specified occurrence pattern in the designated field. Used for mapping long strings of text.
Add Uppercase Mapping	Similar to the direct mapping but converts any new value to upper case before assigning the new value to the field.

Clear field	Clears the specified field to its initial value instead of assigning a new value to it.
Field exit	Reads the entire field and then calls a User exit to determine how the new value is transformed before being assigned to the field. Used for binary/encrypted fields.
☐ Delete table record	Flags the entire record for deletion. When copied, the record is excluded and when masked in-place, the record is deleted.

The options identified in the table above are discussed in more detail in the list below:

- **Direct mapping**: On creating a direct mapping the user is prompted to specify whether the entire field or a subset of the field value will be read and written. Selecting the option "Map a subsection of the Integrity Map key to a subsection of the table field" allows the user to specify which portion of the key table field is read for processing and which portion of the newly calculated value should be written to the specified portion of the field.



Direct mapping

Map table field

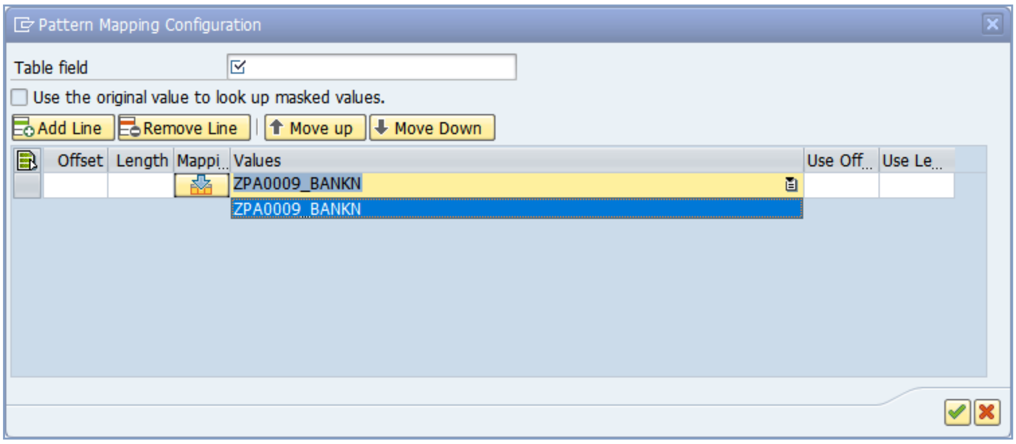
☐ Map a subsection of the Integrity Map key to a subsection of the table field

☐ Use the original value to look up masked values.

If selected, the option 'Use the original value to lookup masked values' instructs Data Secure to calculate a new value for the original value in the specified field. If the option is not selected, the field receives the same new value as determined for another field.

One field per table added to an Integrity Map must be designated for new value determination. If separate new values are desired over multiple fields in the same table, separate Integrity Maps are required.

- **Pattern mapping**: The pattern mapping allows a pattern to be specified using a sequence of symbol types.



Pattern Mapping Configuration

Table field ☑

☐ Use the original value to look up masked values.

Offset	Length	Mappi...	Values	Use Off...	Use Le...
			ZPA0009_BANKN		
			ZPA0009_BANKN		

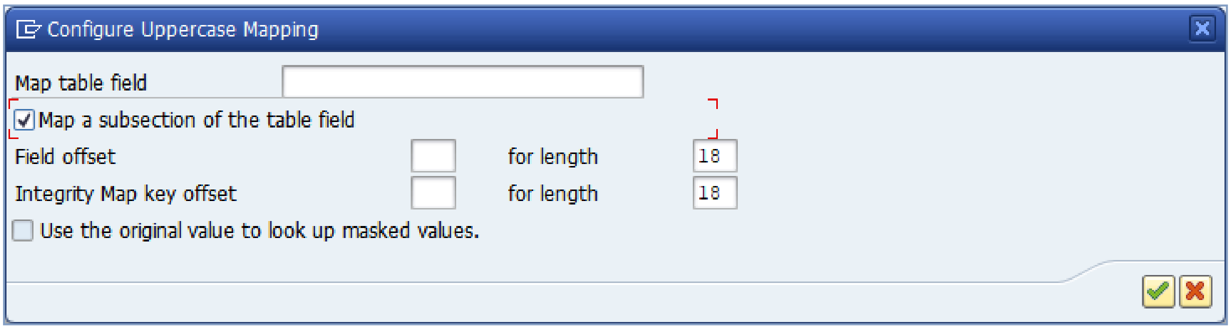
These symbol types are:

Buttons	Name	Description
	Direct Mapping	Adds a symbol to the pattern that will be matched to the extracted lookup value (Integrity map key). The portion matched to the symbol will be replaced when the new value is written.
	System Field	Adds the value of the system field as a symbol to the pattern. The system field value (if matched) will remain once the new value is written to the field
T	Literal Value	Adds the specified value as a symbol to the pattern matched. The value will remain once the new value is written to the field.

The symbols are combined into a pattern that is matched to the specified field value. Every match is processed for a value to be mapped by Data Secure. The option 'Use original value to look up masked values' functions the same as for the Direct mapping option.

Only the portion of the pattern that is mapped by a key mapping is replaced by the new key value. Other symbols in the pattern will retain their original value.

- **Uppercase mapping**: This option is the same as the Direct Mapping option, except all values are converted to Uppercase before being written back to the designated field. The 'Map a subsection…' and 'Use original value…' options function the same as for the direct mapping.



Configure Uppercase Mapping

Map table field

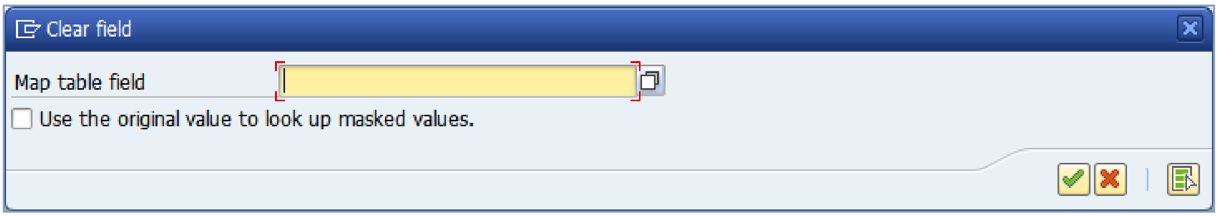
☑ Map a subsection of the table field

Field offset for length 18

Integrity Map key offset for length 18

☐ Use the original value to look up masked values.

- **Clear field**: The specified table field is initialized regardless of original content. Select the button to specify multiple fields to be processed this way. The 'Use the original value… ' option works the same as for the direct mapping option with the difference that the full original value of the field is used for matching to other fields, but the field is initialized instead of being assigned the new value.



Map table field

□ Use the original value to look up masked values.

- **Field exit**: When selected, a User exit is generated where the user can specify how values to the designated field are to be written. When using this option the entire field is read as-is and the assigned Transformation function needs to account for processing the original value's format.

  The generated method receives the importing 'IS_RECORD' parameter containing the original record values. The resulting value to be read/written is contained in the changing 'C_VALUE' parameter.

To generate the user-exit, appropriate developer authorization and access will be checked. It is recommended that the Integrity Map is created on a development system and distributed to other systems via the transport mechanism so that appropriate change control is applied for the user-exit code specified.

The package to be used for user-exit generation is specified on the Integrity Map overview screen by selecting the menu option Utilities > Environment > Mapping Functions.

- **Delete table record**: Instead of mapping individual fields, Data Secure will flag the entire record for deletion. Every record selected along the path specified when adding the table to the Integrity Map (refer to Section 8.1.3) and included by the filter option specified (refer to Section 8.1.5 below), is flagged for deletion.

  In the context of record transfers, the record is not transferred. In the context of in-place masking, the record will be deleted from the database table.

8.1.5 Filter options

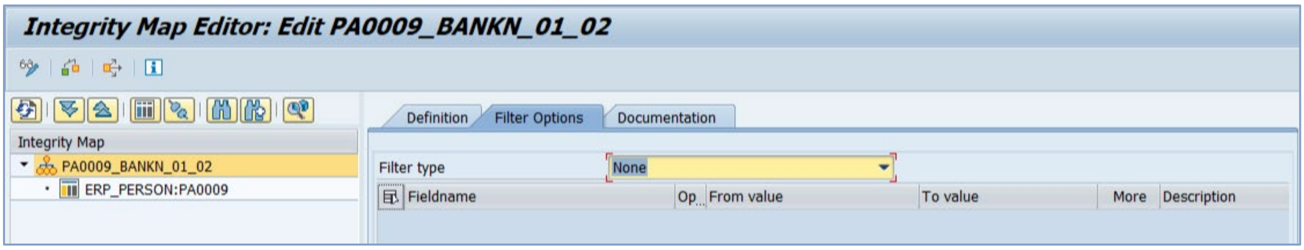
By default, Data Secure picks a data record based on the Business Object definition and it will return all the records based on that selection. The Filter Options allow you to filter down these records.

You can use one of the following qualifier types to filter the records to include in the Integrity Map:

- None
- Custom filter logic (user exit)
- Contextual Values
- Field value selection
- Object selection

To add a filter, select the Qualifier from the drop-down menu and complete the filter criteria as described in the screenshots below:

- **None**: All the records that match the selection path will be included.



Integrity Map Editor: Edit PA0009_BANKN_01_02

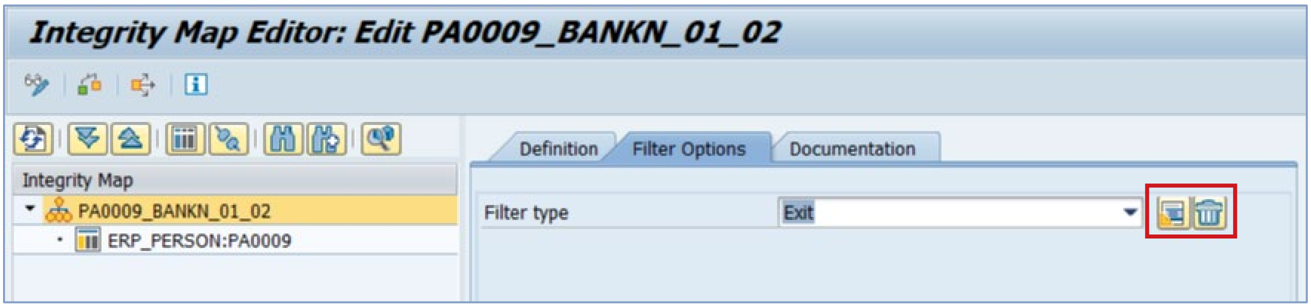
Integrity Map
- PA0009_BANKN_01_02
  - ERP_PERSON:PA0009

Filter type: None

Fieldname	Op.	From value	To value	More	Description

- **Exit**: An exit allows the user to write their own filter logic but requires developer access and ABAP knowledge. The exit receives all the records and evaluates whether it should be included in the Integrity Map or not. The row numbers that should be included are then exported.

> Please note that you can use the buttons as shown in the screenshot above in the following manner:
>
> - **Edit** a custom exit.
> - **Remove** an existing exit.

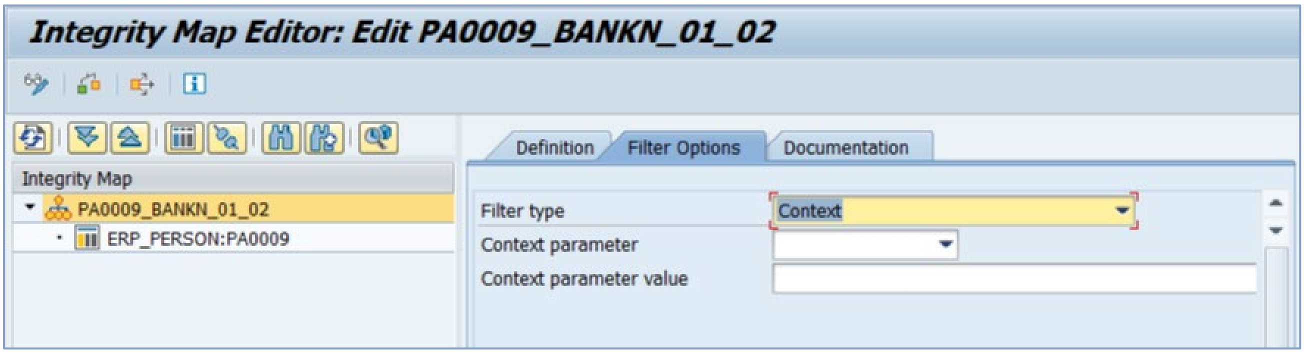


Integrity Map Editor: Edit PA0009_BANKN_01_02

Integrity Map
- PA0009_BANKN_01_02
  - ERP_PERSON:PA0009

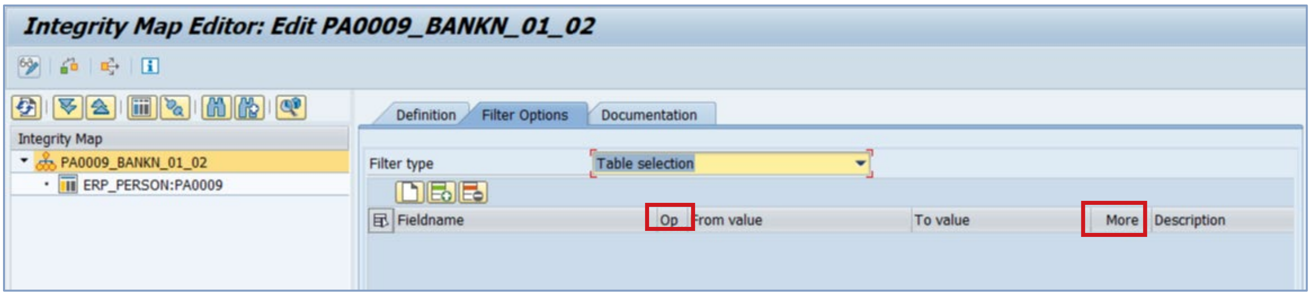
Filter type: Exit

- **Context**: This option is used to determine if records should be included based on the value of a context parameter. Refer to the BOW Extensions Guide for more information on context parameters.



Filter type: Context
Context parameter
Context parameter value

- **Table Selection**: Table Selection is used to filter rows based on the values of specific fields in the Integrity Map main table. The selection option is evaluated row by row.

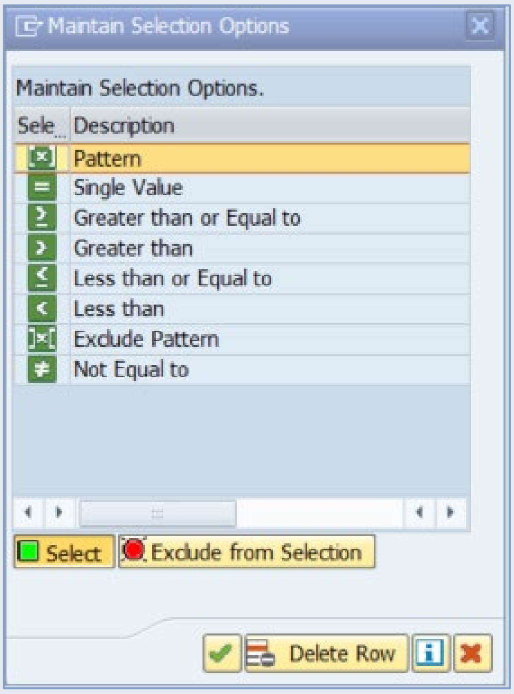


Filter type: Table selection

Fieldname	Op	From value	To value	More	Description

Please note that you can use the buttons as shown in the highlight above as follows:

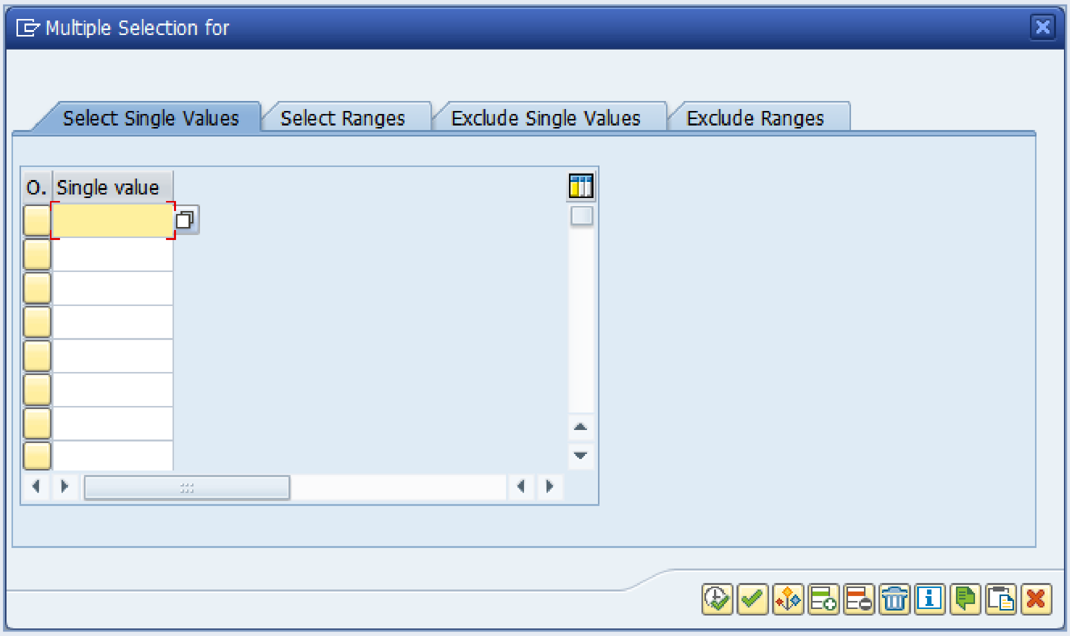
- **Maintain Selection Options**: This allows users to determine the selection option to apply to the specified table field values. as shown on the drop-down list displayed below:



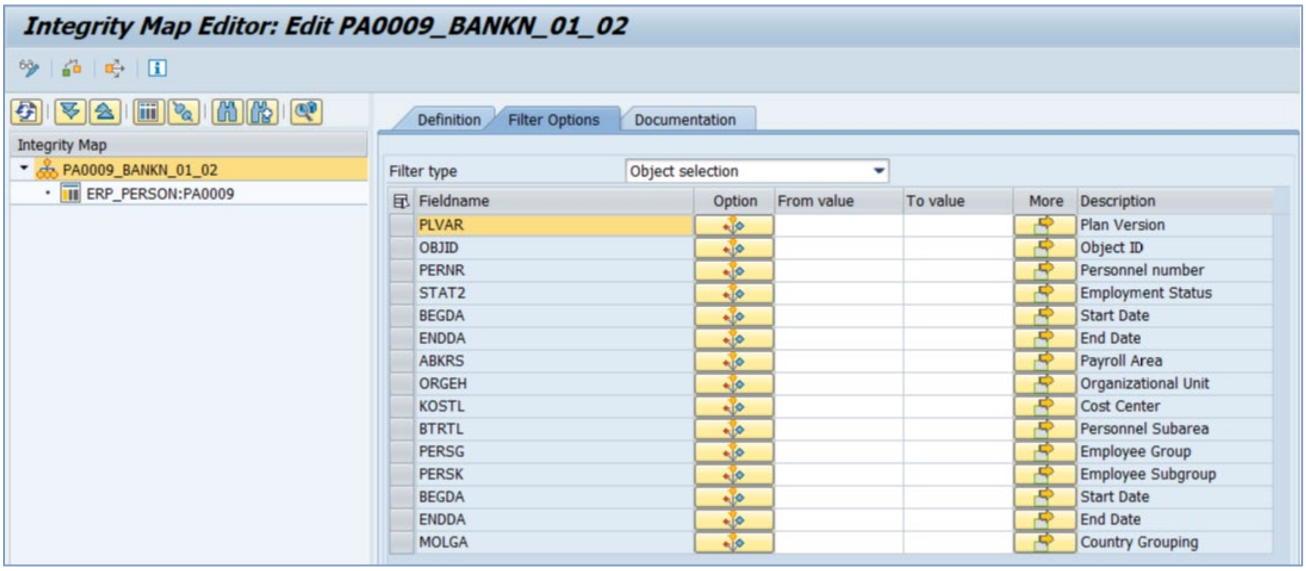
Maintain Selection Options.

Sele...	Description
[×]	Pattern
=	Single Value
≥	Greater than or Equal to
>	Greater than
≤	Less than or Equal to
<	Less than
]×[	Exclude Pattern
≠	Not Equal to

- **Multiple Selection for**: When you use the 'Multiple Selection for' button, you have the option to include or exclude multiple selections field values and/or value ranges.



- **Object selection**: This option allows you to filter the object instances included in the imap by specifying selection criteria for any of the selection fields defined for the Integrity Map's Business Object. The records of the Integrity Map will be processed if the current object instance falls within the selection options, otherwise, none of the object instance records will be processed.



Integrity Map Editor: Edit PA0009_BANKN_01_02

Filter type: Object selection

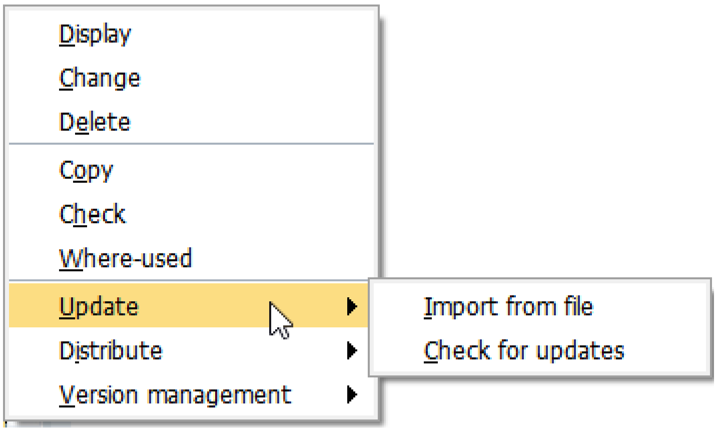
Fieldname	Option	From value	To value	More	Description
PLVAR					Plan Version
OBJID					Object ID
PERNR					Personnel number
STAT2					Employment Status
BEGDA					Start Date
ENDDA					End Date
ABKRS					Payroll Area
ORGEH					Organizational Unit
KOSTL					Cost Center
BTRTL					Personnel Subarea
PERSG					Employee Group
PERSK					Employee Subgroup
BEGDA					Start Date
ENDDA					End Date
MOLGA					Country Grouping

8.2 Extending an Integrity Map

The scope of an existing delivered Integrity Map can be extended by clicking the Extend button.

8.3 Other Menus

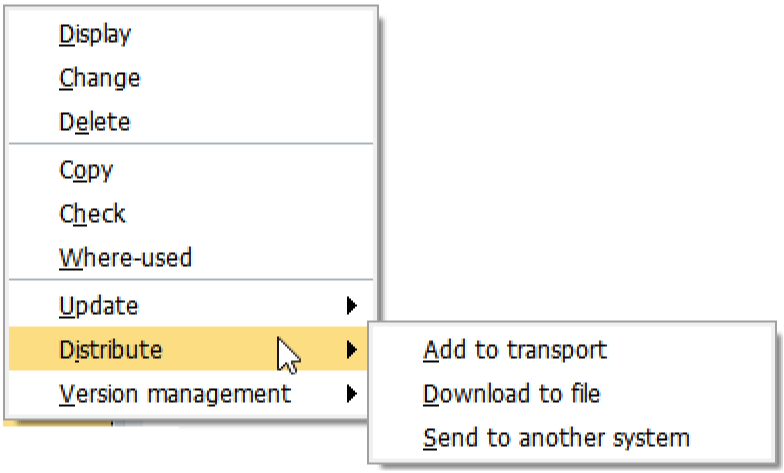
8.3.1 Update



The Update menu allows Integrity Maps to be updated either by uploading an updated definition from a file or by checking for an updated version delivered in the latest Data Sync Manager transport. Selecting either option will prompt for the Integrity Map(s) to be updated. Upon confirmation, the definition is updated to the specified version.

If EPI-USE Labs delivered Integrity Maps are deleted, they can be retrieved by using the 'Check for Updates' function to restore the EPI-USE Labs delivered versions.

8.3.2 Distribute

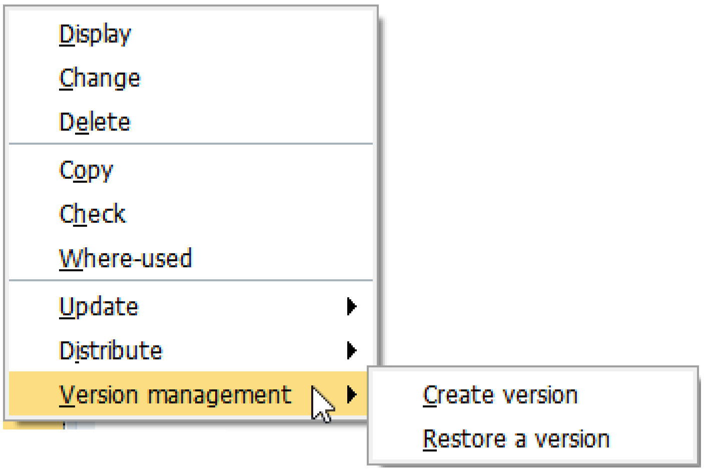


The distribution options for Integrity Maps are accessed from the context menu that is obtained by right-clicking an Integrity Map and browsing to the 'Distribute' option in the displayed menu.

The options available are:

Name	Function
Add to transport	Adds the selected Integrity Map to a Transport for distribution using the SAP standard Transport mechanisms.
Download to file	Creates a file at the specified destination that can later be 'Imported' into Data Secure using the matching function from the 'Update' context menu.
Send to another system	Distribute the selected Transformation Function to another system (where DSM5 is installed) by means of an RFC destination. RFC destinations can either be specified Ad-hoc or are determined by the Control Center. Please see the Installation, Control Center and Configuration Guide for further details.

8.3.3 Version Management



There are two options in the Version management sub-menu that are accessed by right-clicking on a selected Integrity Map. They allow you to:

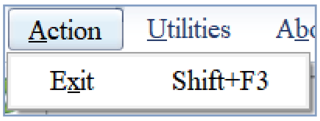
- Store a specific version of an Integrity Map (Create Version).
- Restore a saved version and make it current at a later time (Restore a version).

9. Menus

Each DSM product screen has three drop-down menus (Action, Utilities and About) in addition to the two SAP standard menus (System and Help):

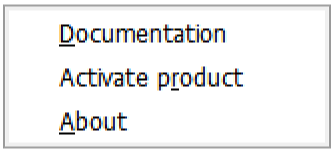
We will discuss the DSM-specific menus here.

9.1 Action



The 'Action' menu has the Exit function that will close the current screen and return you to the Data Secure page.

9.2 About



The 'About' menu allows you to view the transaction documentation, Activate the product and view the 'About' information box.

9.2.1 Documentation

You can view the general product documentation by selecting this menu option.

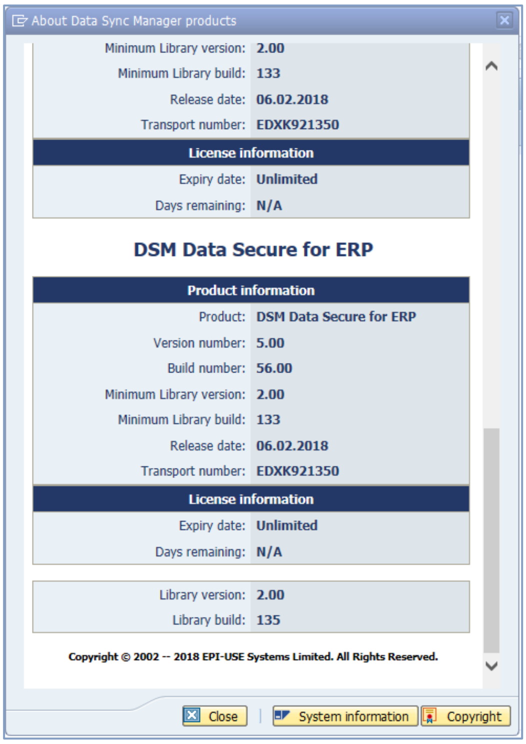
Clicking on the blue 'Documentation' button ℹ will show documentation relevant to a particular screen.

9.2.2 Activate Product

This functionality is available to all users. See the Installation, Control Center and Configuration Guide for a detailed description.

9.2.3 About

The pop-up window will display information on the product.



About Data Sync Manager products

Minimum Library version: 2.00
Minimum Library build: 133
Release date: 06.02.2018
Transport number: EDXK921350

License information

Expiry date: Unlimited
Days remaining: N/A

DSM Data Secure for ERP

Product information

Product: DSM Data Secure for ERP
Version number: 5.00
Build number: 56.00
Minimum Library version: 2.00
Minimum Library build: 133
Release date: 06.02.2018
Transport number: EDXK921350

License information

Expiry date: Unlimited
Days remaining: N/A

Library version: 2.00
Library build: 135

Copyright © 2002 -- 2018 EPI-USE Systems Limited. All Rights Reserved.

a. Product Information

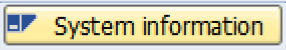
- Product: name of the EPI-USE Labs product.
- Version Number: version of the product that is installed on the current system.
- Builder Number: build number of the product transport installed on the system.
- Minimum Library version: The minimum version of the Library transport that the current build of the product transport requires.
- Minimum Library build: The minimum build number of the Library transport that the current build of the product transport requires.
- Release Date: date that the build was released.
- Transport Number: transport number of the shipped product.

b. License Information

- Expiry Date: date that the license will need to be renewed.
- Days Remaining: number of days remaining before the license will need to be renewed.

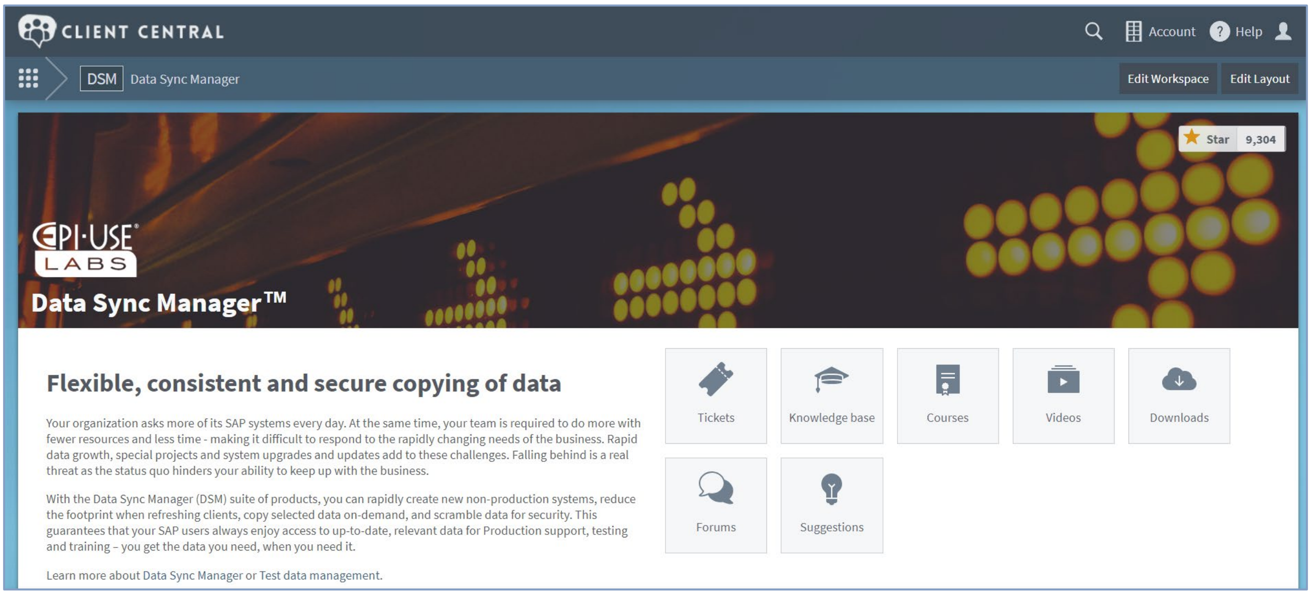
c. Library Information

- Library version: The current library version installed on this system.
- Library build: The current library build installed on this system.

Icon	Name	Functions
 System information	System information	Displays the SAP system information specific to the installation.
Copyright	Copyright	Displays the copyright text.

10. Accessing support through Client Central

EPI-USE Labs provides customers with solution and services support through Client Central for virtually 24 hours on working days. Among other services, you can log tickets, access knowledge base articles and tutorial videos, download the latest transports and user guides, post messages in the forums, and contribute to the improvement of our solutions with suggestions.



Flexible, consistent and secure copying of data

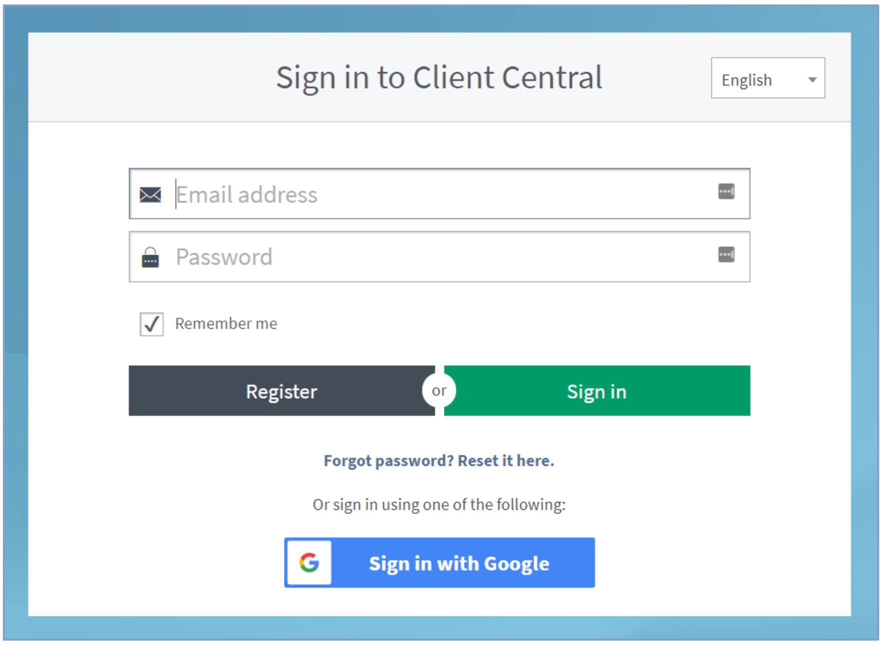
Your organization asks more of its SAP systems every day. At the same time, your team is required to do more with fewer resources and less time - making it difficult to respond to the rapidly changing needs of the business. Rapid data growth, special projects and system upgrades and updates add to these challenges. Falling behind is a real threat as the status quo hinders your ability to keep up with the business.

With the Data Sync Manager (DSM) suite of products, you can rapidly create new non-production systems, reduce the footprint when refreshing clients, copy selected data on-demand, and scramble data for security. This guarantees that your SAP users always enjoy access to up-to-date, relevant data for Production support, testing and training – you get the data you need, when you need it.

Learn more about Data Sync Manager or Test data management.

10.1 Requesting access to Client Central

If you do not have access to Client Central, click 'Register' and follow the prompts.


Sign in to Client Central
English
Email address
Password
☑ Remember me
Register
or
Sign in
Forgot password? Reset it here.
Or sign in using one of the following:
Sign in with Google

10.2Logging a ticket

If you encounter an error or need more specific help, log a ticket with our Support team:

1. Click Tickets > Log a ticket.
2. Complete the required fields.
   - To find out which version of DSM you are running, click About > About on the menu bar.
   - Under 'Description', provide a **short but detailed** description of the problem, including screenshots and the error message or unusual output that you received.
   - Exporting and attaching a diagnostic log (DL) to your ticket will save time and help the Support team assist you. Please create a zipped folder if you would like to attach multiple files.
3. Click 'Submit'.

The system will issue you a ticket number and send you an email acknowledging the ticket, and an EPI-USE Labs support representative will begin to assist you. You can view the status of your tickets on Client Central's homepage under 'Tickets'.

10.3Additional help and resources

10.3.1 Guides

View and download various DSM5 installation, configuration and user guides in the DSM5 Documentation folder.

10.3.2 Knowledge base articles

Visit the DSM knowledge base for articles about solution features, troubleshooting and best practices, FAQs, change logs, and more.

10.3.3 Videos

Browse the DSM video library for product overviews, demonstrations and tutorials.

10.3.4 Forums

Visit the forums to ask questions to or share your expertise with other members of Client Central's online community.

10.4Supported SAP releases and languages

DSM Object Sync is designed to be used with your existing SAP system. It is easily installed via a transport onto each client where it is needed.

Data Secure is available for the following SAP releases:

ERP (all modules including FI, HCM, LO)	SRM	CRM	BW	SCM
ECC 6.0 and above (including S/4 HANA)	7.x	7.x	7.x	7.x

Data Secure for SCM requires a Support Package level of 701 or higher.

Data Sync Manager 5 is only available for these versions and above. Any customers on lower versions will be using DSM4. For DSM4, please refer to the DSM4 Guides in Client Central: (https://cc.epiuse.com/support/home).

DSM Object Sync 5 is available in:

- English
- German (Pending translation)
- French (Pending translation)
- Spanish (Pending translation)

although support is available in many more languages.

10.5Contact us

You are welcome to send us comments and suggestions regarding our products, documents, services and support via:

- the Client Central support portal (for existing customers only) or support@labs.epiuse.com (if you do not have access to Client Central).
- the EPI-USE Labs website.

We are happy to incorporate suggestions that make our products more powerful and easier to use. In this way, we can contribute to making your work simpler and more efficient.

11. Appendix A: Key concepts and definitions

This section will provide a generic explanation of key concepts and definitions for DSM5 before looking at an overview of concepts specific to Data Secure.

Concept	Definition
DSM 5	DSM 5 is the latest version of the Data Sync Manager product.
Rule	A Rule defines tables and fields in the system that must be masked and the masking operation that should be applied in each case.
Policy	A Policy collects Data Security rules to be applied within a specified context. It allows for the specification of rule defaults and behaviors in DSM. There can be different Policies created and used across Data Secure and other DSM components.
Integrity Map	An Integrity Map is a group of fields that store the same or similar information in a redundant fashion. The fields can, therefore, be masked with the same value.
Transformation Function	A Transformation Function is a function that accepts inputs and produces an output value which is used as the masking value for an original value.
Run	A Run is an identifiable package that stores the data to be masked and the masking Policy applied. The results of applying the Policy to the specified data are stored against the Run as trace messages, key statistics and audit logs.
Audit Logs	Audit Logs list the masking settings and the original versus the masked field values. Audit Logs should be retained for review and auditing purposes and disposed of thereafter. Audit Log access should be restricted using the Auditor template role. For more information, refer to the DSM Authorizations Guide.
Diagnostic Log	The Diagnostic Log captures non-sensitive Run information for EPI-USE Labs diagnostic purposes.
Documentation button	ℹ The 'Documentation' button provides context-specific information.
Business Object selections	These are the selection options defined for the Business Object in the Business Object Workbench. Each allows a selection to be made on the data based on the populated values. In this case, a record is compared to this selection to determine if the record is valid for the condition or not. You can refer to the BOW Extensions User guide for more details.
Business Object context parameters	Context parameters are defined in the Business Object Workbench for a specific Business Object definition. Each object instance will have one context parameter value. For example, for the Business Object Employee, we have a parameter that lists the current gender of that Employee instance key where for Employee 1000 on IDES the context parameter value would be 'F' for female. Data Secure uses these variable values to make behavioral decisions. For example,

	it would assign a female first name to Employee 1000 because the Context Parameter value for said Employee is 'F' for female. The creation of Business Object Context Parameters is also done in the BOW Extensions User Guide.
Semantic Tag	A Semantic tag is metadata associated with a Content Item (Integrity Map, Transformation function or parameter) as a hint to the product to what other Artifacts it could be associated with. For example, if a Transformation Function is tagged in the same way as an Integrity Map that Transformation Function is recommended as a default to assign to that Integrity Map for masking. In future applications such as Data Disclose, we have also used this Semantic Tag metadata as a grouping mechanism for fields. For example, because all the Integrity Maps for name fields are tagged with a Semantic Tag for names we can search all those fields when searching for a person's name in the system for Data Disclose.

12. Appendix B: Icons

These are the icons that users might encounter in EPI-USE Labs documentation:

Functional icons

?	**Optional** You have the option to follow the suggestions provided or follow an alternative.
★	**Recommended** We strongly suggest that you follow the given guidelines.
✓	**Required** It is essential that you implement the given instructions.
📎	**Take note** This important information will help you use this solution more efficiently.
💣	**Warning** Be aware of possible dangers.
{ }	**Example** The example will assist you with the current section.
👣	**Step-by-step** Follow the systematic instructions to complete the process.