One Identity Manager 9.2.1

Administration Guide for the SAP R/3 Compliance Add-on

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

One Identity Manager Administration Guide for the SAP R/3 Compliance Add-on
Updated - 16 May 2024, 04:09

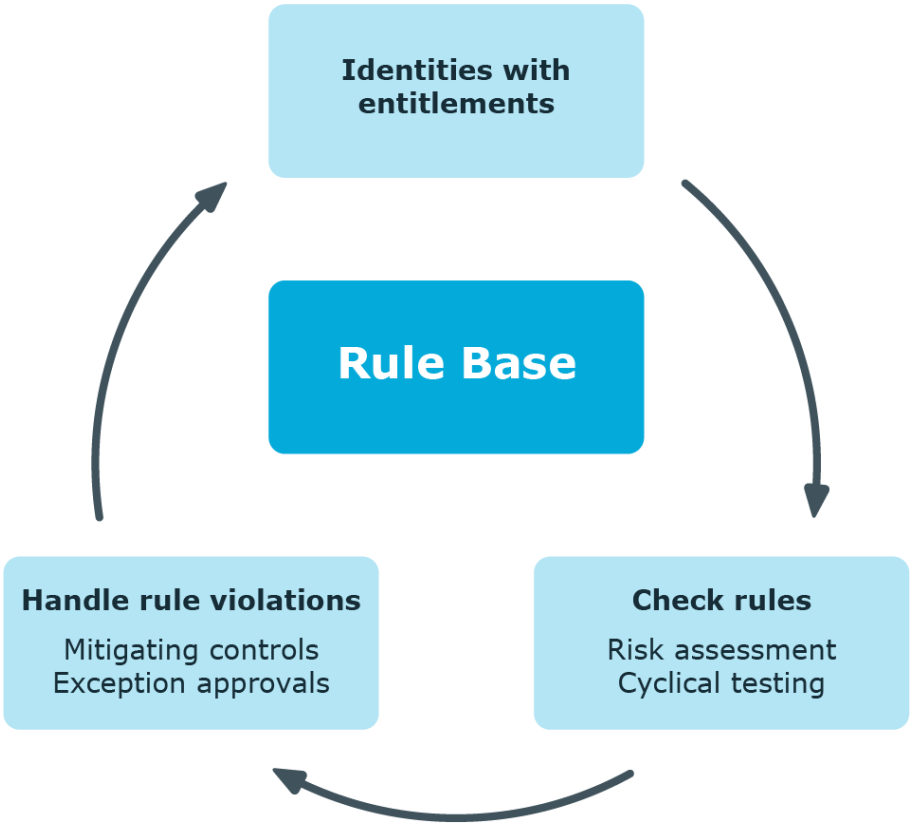
For the most recent documents and product information, see Online product documentation.

Contents

SAP functions and identity audit

One Identity Manager can be used to define rules that maintain and monitor regulatory requirements and automatically deal with rule violations. Define compliance rules to test entitlements or combinations of entitlements in the context of identity audit for identities in the company. On the one hand, existing rule violations can be found by checking rules. On the other hand, possible rule violations can be preemptively identified and thus prevented.

Figure 1: Identity audit in One Identity Manager



In addition to rule checking, One Identity Manager offers a very detailed examination of effective authorization for SAP R/3 target systems for SAP user accounts. By linking SAP user accounts to identities, combinations of SAP authorizations that an identity obtains through different SAP user accounts can be checked. Potentially dangerous authorizations

and combinations of them can easily be recognized this way and the necessary action taken.

SAP authorizations are verified on the basis of the SAP applications permitted for an user account and the associated authorization objects. To do this, in One Identity Manager, you define SAP functions that group together the SAP applications and authorization objects. One Identity Manager finds all the SAP roles and profiles that have exactly these authorization objects assigned to them. User accounts match the SAP functions if they are a member in the SAP roles and profiles that have been found.

In order to check whether there are potentially dangerous SAP authorizations in the company, define SAP functions that are critical for these authorizations. Find out which identities match these SAP functions by using compliance rules.

If identities are granted SAP authorizations through IT Shop requests, the authorizations that are not permitted can be detected and handled respectively when the request is made with the appropriate approval processes. For more information about approval processes in the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Based on this information, you can made corrections to data in One Identity Manager and transfer them to the connected SAP R/3 systems. The integrated report function in One Identity Manager can be used to provide information for the appropriate tests.

NOTE: Compliance Rules Module and SAP R/3 Compliance Add-on Module must be installed in order to set up and analyze SAP functions.

NOTE: You cannot use SAP functions to check the authorizations in the child systems of a central user administration.

One Identity Manager users for managing SAP functions

The following users are used for the administration of SAP functions.

Table 1: Users

Users	Tasks
Compliance rules administrators	Administrators must be assigned to the **Identity & Access Governance | Identity Audit | Administrators** application role. Users with this application role: • Enter base data for setting up company policies. • Create compliance rules and assign rule supervisors to them. • Can start rule checking and view rule violations as required.

Users	Tasks
	• Create reports about rule violations. • Define SAP functions and assign these to managers. • Define function instances and variables sets for SAP functions. • Enter mitigating controls. • Create and edit risk index functions. • Monitor Identity Audit functions. • Administer application roles for rule supervisors, exception approvers and attestors. • Set up other application roles as required.
Responsible for maintaining SAP functions.	Administrators must be assigned to the **Identity & Access Governance | Identity Audit | Maintain SAP functions** application role or a child application role. Users with this application role: • Are responsible for SAP function contents. • Edit working copies of function definitions for which they are responsible. • Define function instances and variables sets for SAP functions. • Assign mitigating controls.
One Identity Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles. One Identity Manager administrators: • Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required. • Create system users and permissions groups for non role-based login to administration tools in the Designer as required. • Enable or disable additional configuration parameters in the Designer as required. • Create custom processes in the Designer as required. • Create and configure schedules as required.
Compliance and security officer	Compliance and security officers must be assigned to the **Identity & Access Governance | Compliance & Security**

Users	Tasks
	Officer application role. Users with this application role: • View all compliance relevant information and other analysis in the Web Portal. This includes attestation policies, company policies and policy violations, compliance rules, and rule violations, critical SAP functions and risk index functions. • Edit attestation polices.

Prerequisites for setting up SAP functions

All the information regarding SAP authorizations, SAP users, SAP roles, and SAP profiles must be transferred to the One Identity Manager database so that One Identity Manager can test the effective SAP authorizations based on SAP functions.

Setting Up SAP Functions

1. In the Designer, set the **QER | ComplianceCheck** and the **TargetSystem | SAPR3 | SAPRights** configuration parameters.

   NOTE: If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

2. Set up a synchronization project for synchronizing the necessary SAP schema types and start synchronization.

Detailed information about this topic

- Setting up a synchronization project for synchronizing SAP authorization objects on page 10

Configuration parameters for SAP functions

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for various configuration parameters.

Check the configuration parameters and modify them as necessary to suit your requirements.

Configuration parameters are defined in the One Identity Manager modules. Each One Identity Manager module can also install configuration parameters. In the Designer, you can find an overview of all configuration parameters in the **Base data > General > Configuration parameters** category.

For more information, see Configuration parameters for SAP functions on page 61.

2

Setting up a synchronization project for synchronizing SAP authorization objects

SAP authorizations are verified on the basis of the SAP applications permitted for an SAP user account and the associated authorization objects. Authorization objects and SAP applications must be loaded into the One Identity Manager database first before you can create SAP functions. For each client, create a synchronization project for synchronizing the necessary schema types. A separate project template is required for this.

Use the Synchronization Editor to configure synchronization between the One Identity Manager database and SAP R/3 environment.

NOTE: Just one synchronization project can be created per target system and default project template used.

To set up a synchronization project for SAP authorization objects.

1. Set up an initial synchronization project as described in the One Identity Manager Administration Guide for Connecting to SAP R/3. The following special features apply:

   NOTE: You cannot use SAP functions to check the authorizations in the child systems of a central user administration. Set up the synchronization project for one client only, which is not a CUA system.

   a. In the project wizard on the **Select project template** page, select the **SAP R/3 authorization objects** project template.

   b. The **Restrict target system access** page is not displayed. The target system is only loaded.

   For more information, see the *One Identity Manager Administration Guide for Connecting to SAP R/3*.

2. Configure and set a schedule to run synchronization regularly.

   For more information, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Default project template for the SAP R/3 Compliance Add-on Module on page 63
- Referenced SAP R/3 tables and BAPI calls on page 65
- Synchronizing SAP authorizations with overlapping values on page 11
- Synchronizing very large numbers of SAP authorizations on page 12

Synchronizing SAP authorizations with overlapping values

In SAP R/3, if the same authorization is assigned to an SAP profile several times with overlapping value ranges, only one authorization assignment is read in by the synchronization. Therefore, the authorization check does not include all the values that user accounts with this profile can actually use.

Probable reason

When synchronizing the `ProfileHasAuthObjectField` schema type, the complete object list is loaded straight away. Only one data set is selected for each authorization assignment to an SAP profile. Other data sets are ignored.

Solution

If several authorization assignments with overlapping value ranges exist for one profile, the lowest lower value and the highest upper value must be read in by synchronization. To do this, the value ranges are evaluated separately by the synchronization. The objects must be loaded by single record access.

To enable single record access

1. In the Synchronization Editor, edit the properties of the **profileHasAuthObjectField** synchronization step.
2. Select the **Extended** tab.
3. Select the **Reload threshold** property and disable **Use start up configuration settings**.
4. Enter a value between **4** and **7**.
5. Save the changes.

NOTE: Changing the reload threshold may affect synchronization performance for this synchronization step.

For more about configuring the reload threshold, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- Setting up a synchronization project for synchronizing SAP authorization objects on page 10
- Synchronizing very large numbers of SAP authorizations on page 12

Objects in USOBHASH table not completely loaded

When synchronizing SAP authorization objects, not all objects in the USOBHASH table are loaded into the One Identity Manager database.

Probable reason

Changed implementation of the ABAP function AUTH_TRACE_GET_USOBHASH as of SAP BASIS version 7.57 (SAP S/4HANA 2022).

Solution

- Import the current SAPTRANSPORT_70.ZIP transport into the SAP R/3 system you want to synchronize.

  One Identity Manager version 9.1.3 or later provides an updated BAPI transport SAPTRANSPORT_70.ZIP. This uses the /VIAENET/LISTUSOBHASH function module instead of the AUTH_TRACE_GET_USOBHASH SAP module. When it accesses an SAP R/3 system, the SAP R/3 connector checks whether the /VIAENET/LISTUSOBHASH function module exists and uses that. This synchronizes all objects in the USOBHASH table.

If the function module is not available, the connector uses the AUTH_TRACE_GET_USOBHASH SAP module.

The synchronization log records whether the /VIAENET/LISTUSOBHASH function module is used.

Synchronizing very large numbers of SAP authorizations

If your SAP R/3 environment contains a very large number of ProfileHasAuthObjectField authorizations (several million), synchronization might quit unexpectedly or just not complete.

Solution

If the total number of authorizations is too large for processing, synchronization can be divided into several synchronization steps.

To split synchronization of `ProfileHasAuthObjectField` into several steps

1. In the Synchronization Editor, edit the synchronization workflow for synchronizing SAP authorization objects (default: **Initial Synchronization**).
2. Enable the **profileHasAuthObjectFieldPart1**, **profileHasAuthObjectFieldPart2**, **profileHasAuthObjectFieldPart3**, and **profileHasAuthObjectFieldPart4** synchronization steps.
    - If these synchronization steps are not available, first apply the VPR#37380 patch.

      This patch creates the synchronization steps in synchronization projects that were set up in versions of One Identity Manager older than 9.2.
3. Disable the **profileHasAuthObjectField** synchronization step.
4. Save the changes.

In subsequent synchronizations, all `ProfileHasAuthObjectField` objects are divided into four blocks and processed independently of each other.

For more information about editing synchronization steps and applying patches, see *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

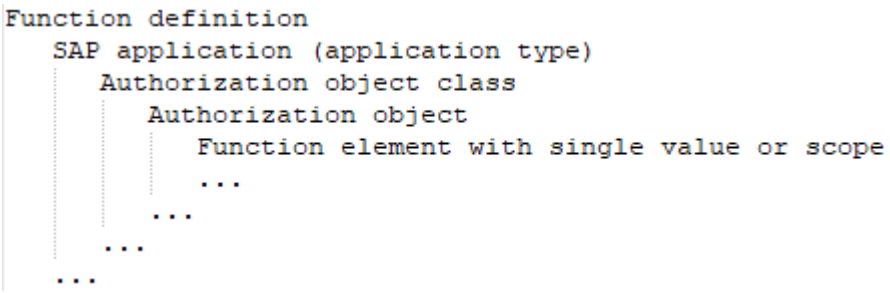
- Setting up a synchronization project for synchronizing SAP authorization objects on page 10
- Synchronizing SAP authorizations with overlapping values on page 11

Setting up SAP functions

You can create function definitions, function instances, and variable sets for SAP functions. A function definition contains the authorization definition as well as general main data. An authorization definition contains at least one SAP application. Each SAP application belongs to at least one authorization object. Each authorization object consists of at least one function element (activity or authorization field) with concrete instances. Instances are given as single values or as upper and lower scope limits. Function elements can be listed more than once per authorization object.

You can use an SAP function for different instances. To do this, use variables in the authorization definition. Fixed variable values are grouped in variable sets and used in the function instances.

Figure 2: Structure of an authorization definition



To set up an SAP function

1. Create a function definition.
    - (Optional) If necessary, assign a function category or functional area to the managers.
2. Create the authorization definition.
    - Consider the explanations for determining invalid authorizations.
    - Take the notes on authorization definitions into account.
    - Use variables for the values or scope limits if needed.
3. Check the completeness of the authorization objects.

4. (Optional) Assign mitigating controls to the function definition to be implemented when invalid authorizations are detected by the SAP function.
5. To be able to use the function definition for authorization checking, enable the working copy of this function definition.
6. Create at least one function instance for this function definition.

To find all the identities that match this SAP function through their SAP user accounts, apply the SAP function in compliance rules.

Detailed information about this topic

- Creating function definitions on page 15
- Base data for SAP functions on page 46
- Creating authorization definitions in the Authorization Editor on page 17
- Finding invalid authorizations on page 23
- Notes on authorization definitions on page 18
- Using variables on page 21
- Checking authorization objects for completeness on page 22
- Assigning mitigating controls to SAP functions on page 44
- Enabling working copies on page 23
- Defining function instances on page 39
- Compliance rules for SAP functions on page 54

Creating function definitions

A working copy is added to the database for every new function definition. The changes are not passed on to the production function definition until the working copy is enabled. SAP authorizations are only checked on the basis of active function definitions.

To create a new function definition

1. In the Manager, select the **Identity Audit > SAP functions > Function definitions** category.
2. Click in the result list.
3. Enter the function definition main data.
4. Save the changes.

   This adds a working copy.
5. Select the **Authorization Editor** task and set up the authorization definition.
6. Select the **Enable working copy** task and confirm the security prompt with **Yes**.

This adds an enabled function definition in the database. The working copy is retained and can be used to make changes later.

Related topics

- General main data of a function definition on page 16
- Creating authorization definitions in the Authorization Editor on page 17
- Enabling working copies on page 23

General main data of a function definition

Enter the following main data of a function category.

Table 2: Main data for a function definition

Property	Description
Function definition	Name of the SAP function.
Functional area	The SAP function is valid for this functional area.
Function category	Grouping criteria for the SAP function. To create a new function categories, click . Enter the name and a description of the function category.
Manager/supervisor	Application role whose members are responsible for the function definition in terms of content. To create a new application role, click . Enter the application role name and assign a parent application role.
Authorization objects	Spare text field for entering information about the authorization objects that are used in the function definitions.
Risk index	Defines the risk for the company if an SAP user account matches this SAP function. Use the slider to enter a value between **0** and **1**. **0**: No risk. **1**: Every SAP user account that matches the SAP function poses a problem. This field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set.
Risk index (reduced)	Show the risk index taking mitigating controls into account. An SAP function's risk index is reduced by the significance reduction of all mitigating controls assigned to it. The risk index (reduced) is calculated for the original SAP function. To copy the value to a working copy, run the **Create working copy** task.

Property	Description
	This field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. The value is calculated by One Identity Manager and cannot be edited.
Severity code	Specifies what it means to the company or the assigned functional area when an SAP user matches this SAP function. Enter a value between **0** and **1**. **0**: Just for information **1**: Any SAP user account that matches the SAP function requires changes to the affected SAP authorizations.
Significance	Specifies a verbal description of the effects on the company (or the functional area) when an SAP user account matches this SAP function. In the default installation, the value list displays {**low**, **average**, **high**, **critical**}.
Description	Text field for additional explanation.
working copy	Specifies whether this is a working copy of the function definition.

For more information about risk assessment, see the *One Identity Manager Risk Assessment Administration Guide*.

Detailed information about this topic

- SAP function categories on page 47
- Maintaining SAP functions on page 49
- Mitigating controls for SAP functions on page 57

Creating authorization definitions in the Authorization Editor

Use the Authorization Editor to set up the SAP function authorization definition. To do this, group SAP applications and authorization objects together that should be covered by the SAP function.

To compile an authorization definition

1. In the Manager, select the **Identity Audit > SAP functions > Function definition working copies** category.
2. Select the function definition in the result list.
3. Select the **Authorization Editor** task.
4. Select one of the following tasks.

- **1. Add via menu template**

  Select from which menu you want to select the menu items and the SAP system whose menu tree should be displayed. Then select a menu item from the menu tree. Transaction codes that are linked to a menu item are shown in brackets in the menu tree as additional information.

  All the transactions and their authorization objects are loaded that can be called from the selected menu item or its submenu items.

- **2. Add using SAP application**

  Select the type of SAP application and the SAP application whose authorization objects should be loaded into the Authorization Editor. All authorization object are added that are linked with the selected SAP application. You can define a filter to list the limit the number of SAP applications available.

- **3. Add using existing function definition**

  Select an existing function definition whose authorization definition is to be loaded into the Authorization Editor.

  Only enabled function definitions can be selected.

5. Specify details for each element in the Authorization Editor.
6. Save the changes.

Detailed information about this topic

- Authorization definition properties and their values on page 19
- Notes on authorization definitions on page 18
- Using variables on page 21

Notes on authorization definitions

Take the following advice into account when you create an authorization definition in the authorization editor.

- To add an additional activity value to an authorization object, click **+**. You can enter more than one activity value by `OR`-ing them together.
- To add an additional value for an authorization field to an authorization object, click **C** next to the authorization field.
- The same authorization object cannot be added more than once to an authorization definition.

Detailed information about this topic

- Creating authorization definitions in the Authorization Editor on page 17
- Finding invalid authorizations on page 23

Related topics

- Examples of SAP functions on page 29
- Rule conditions for SAP functions on page 54

Authorization definition properties and their values

The functionality of the Authorization Editor is based on the SAPGUI Authorization Editor. The columns in the Authorization Editor have the following meaning.

Table 3: Properties of an authorization definition

Property	Description
Function definition / SAP application / authorization / function element	Function definition hierarchy. SAP applications, their associated authorization objects and function elements are mapped in a hierarchy.
Processing status	Processing status of hierarchy objects. : No value is specified for the function element. : A value is specified for the function element.
Add	Click **+**, to add more objects to the authorization definition. This adds a sub object. Click **C**, to copy the function element.
Remove	Click **-**, to remove objects from the authorization definition.
Description	Object description.
Any	Click *, to define the value of a function element as * (any value).
Value / lower limit	Values permitted for the function element. For example, you can limit SAP authorizations to specific SAP groups. When you specify a range, enter the lower limit here. Values can be added as variables. System variables can also be used. Wildcards can be used in the values. For more information, see Syntax examples for values on page 20.
Upper scope limit	Upper limit for the range of a function element Values can be added as variables. Values concatenated with **,** and * are not permitted. If **Lower limit** contains values concatenated with **,** or *, you cannot enter an upper limit.

Table 4: Syntax examples for values

Syntax (example)	SAP authorization is tested for	Input value examples
*	Any value Can only be used as a single value. An upper scope limit cannot be specified.	ab or 1234
Any string (from)	Exact given value	abc
[*]	The value *	*
String[*] (abc[*])	Values that contain exactly this string and *.	from*
String* (abc[*])	Values beginning with the given string and ending with any string Can only be used as a single value. An upper scope limit cannot be specified.	abcd or ab*
OR (01,02,78)	One of the values contained in the list ORing cannot be used for the upper scope limit. Can only be used as a single value. An upper scope limit cannot be specified.	01 or 02 or 78
[*],[,],[+] (FM[+]7)	Values that contain special characters	FM+7
Variable (Var)	Value stored in the variable	
System variable ($var)	Value stored in the system variable	

All function elements in an SAP application that are defined in a separate row must be fulfilled for the SAP function to match. If the SAP function can only match when an SAP profile has one of several possible characteristics of a function element, define these instances by ORing them.

To edit the properties of the selected object

- Double-click on a function element in the Authorization Editor.

  You can edit the description of the function element and the upper and lower limits.

Table 5: Function element properties

Property	Description
Type	Specifies whether the selected function element is an activity or a authorization field.

Property	Description
Name	Name of the function element.
Lower limit, upper limit	Values permitted for the function element. When you specify a range, enter a lower and an upper limit. Values can be added as variables. Click to select variables from the variable definitions available.
Description	Detailed description of the function elements.

Detailed information about this topic

- Notes on authorization definitions on page 18
- Using variables on page 21
- Creating and editing variable sets for authorization definitions on page 41
- Creating authorization definitions in the Authorization Editor on page 17

Using variables

You can set fixed values for function elements in authorization definitions. Otherwise, you can implement variables to use a function definition for different function instances. For this, the following is valid:

- Variable name
  - Begins with a letter
  - Only contains letters, numbers, and underscore
  - Is enclosed in $ signs

  Example: Var_01

  NOTE: Variable names cannot begin with system variable names.
- Value

Syntax (example)	SAP authorization is tested for	Input value examples
*	Any value Can only be used as a single value. An upper scope limit cannot be specified.	ab or 1234
Any string (from)	Exact given value	abc
[*]	The value *	*
String[*]	Values that contain exactly this string and *.	from*

Syntax (example)	SAP authorization is tested for	Input value examples
(abc[*])		
String* (abc [*])	Values beginning with the given string and ending with any string Can only be used as a single value. An upper scope limit cannot be specified.	abcd or ab*
OR (01,02,78)	One of the values contained in the list ORing cannot be used for the upper scope limit. Can only be used as a single value. An upper scope limit cannot be specified.	01 or 02 or 78
[*],[,],[+] (FM[+]7)	Values that contain special characters	FM+7

You can also use system variables as well as self-defined variables in the authorization definition. System variables have the following syntax: `${character}+` (example: $AUFART).

Variables must be uniquely identifiable by the authorization check. Therefore, names of self-defined variables may not match system variables or begin with system variable name.

Related topics

- Creating authorization definitions in the Authorization Editor on page 17
- Main data for a variable set on page 42

Checking authorization objects for completeness

One Identity Manager uses this task to test whether all authorization objects that belong to an SAP application occur in the authorization definition.

To test an authorization definition for completeness

1. In the Manager, select the **Identity Audit > SAP functions > Function definition working copies** category.
2. Select the function definition in the result list.
3. Select the **Authorization Editor** task.
4. Select the **Check authorization objects for completeness** task.

   Missing authorization objects are displayed in a separate window.

5. Enable the **Add** option on the authorization object you want to add to the authorization definition.
6. When all missing authorization objects are edited, click **OK**.

   The authorization objects can now be edited in the authorizations editor.

Related topics

- Creating authorization definitions in the Authorization Editor on page 17

Enabling working copies

SAP authorizations are only checked on the basis of active SAP functions. When you enable the working copy, the changes are transferred to the function definition. An active function definition is added to a new working copy.

To transfer changes from a working copy to a function definition

1. In the Manager, select the **Identity Audit > SAP functions > Function definition working copies** category.
2. Select the function definition in the result list.
3. Select the **Enable working copy** task.
4. Confirm the security prompt with **OK**.

Related topics

- Creating working copies on page 36
- Creating function definitions on page 15

Finding invalid authorizations

SAP authorizations are verified on the basis of the SAP applications permitted for an SAP user account and the associated authorization objects. To determine whether potentially dangerous authorizations are assigned within the company, define SAP functions that group together the SAP applications and authorization objects to be checked.
One Identity Manager compares all authorization objects assigned to single profiles with the authorization definition in the SAP function. This way, it determines all SAP roles and profiles that have exactly these authorization objects assigned via the sum of their single profiles.

The **TargetSystem | SAPR3 | SAPRights | TestWithoutTCD** configuration parameter is evaluated by authorization checks. The configuration parameter specifies whether SAP application are ignored and only authorization objects taken into account during the authorization check.

The TestWithoutTCD configuration parameter is not set (default)

The following rules apply to the authorization check:

An SAP role or SAP profile matches an SAP function when

1. It has at least one of the SAP applications defined in the SAP function.

```
Function definition
   CHIP_CATALOG_GET_LIST (RFC function module)   OR
      ...
   SE16 (Transaction)                            OR
      ...
   SU01 (Transaction)
      ...
```

2. It has all the authorization objects of this SAP application that are defined in the SAP function.

```
Function definition
   SAP application (application type)
      ...
         S_TCODE                              AND
            ...
         S_TABU_DIS                           AND
            ...
         S_TABU_NAM
            ...
```

3. It has all the different function elements of an authorization object that are defined in the SAP function.

```
Function definition
   SAP application (application type)
      ...
         Authorization object
            ACTVT                             AND
            TABLE
```

4. At least one or all of the values of one and the same function element defined in the SAP function are available.

```
Function definition
   SAP application (application type)
      ...
         Authorization object
            TABLE = USR10                     OR
            TABLE = USR11
         Authorization object
            ACTVT = 01,02,03                  01 OR 02 OR 03
```

An SAP role matches an SAP function if an SAP profile of this SAP role matches the SAP function.

An SAP profile matches an SAP function if it contains at least one of the SAP applications defined in the SAP function. The SAP profile must have all this SAP application's authorization objects to do this. If a function element with different values is defined for an authorization object, the SAP profile matches the SAP function if it has at least one of these values.

The TestWithoutTCD configuration parameter is set

SAP applications are not taken into account during the authorization check. The following rules apply to the authorization check:

An SAP role or SAP profile matches an SAP function when

1. It has all the authorization objects of all SAP applications defined in the SAP function, except for the authorization objects needed to identify the SAP applications.

```
Function definition
   SAP application (application type)
      ...
         S_CTS_ADMI                        AND
            ...
   SAP application (application type)
      ...
         S_TABU_DIS                        AND
            ...
         S_TABU_NAM
            ...
```

2. It has all the different function elements of an authorization object that are defined in the SAP function.

```
Function definition
   SAP application (application type)
      ...
         Authorization object
            ACTVT                          AND
            TABLE
```

3. At least one or all of the values of one and the same function element defined in the

SAP function are available.

```
Function definition
   SAP application (application type)
      ...
         Authorization object
            TABLE = USR10                    OR
            TABLE = USR11
         Authorization object
            ACTVT = 01,02,03                 01 OR 02 OR 03
```

Only the authorization objects and their values are of interest for the authorization check. It is irrelevant to which SAP applications these authorization objects belong. That means the authorization objects that are only used to identify the applications are ignored. The following authorization objects and function elements are therefore disregarded:

- External service: S_SERVICE with SRV_NAME and SRV_TYPE
- TADIR object: S_START with AUTHOBJNAM, AUTHOBJTYP, and AUTHPGMID
- RFC function module: S_RFC with RFC_NAME and RFC_TYPE
- Transaction: S_TCODE with TCD

Examples of authorization checking

An SAP function is defined with the following SAP applications, authorization objects, and function elements.

Figure 3: Authorization definition with transactions

Function definition / SAP application / authorization / element	E	A	R	Description	A	Lower limit	Upper limit
SAP Function Doc Sample A					*		
SE16 (Transaction)		+	-	Data Browser	*		
AAAB			-	Cross-application Authorization Objects	*		
S_TCODE		+	-	Transaction Code Check at Transaction Start	*		
ACTVT			-	Activity			
TCD		C	-	Transaction Code	*	SE16	
HR			-	Human Resources	*		
P_TCODE		+	-	HR: Transaction codes	*		
TCD		C	-	Transaction Code	*	[*]	
SU01 (Transaction)		+	-	User Maintenance	*		
AAAB			-	Cross-application Authorization Objects	*		
S_TCODE		+	-	Transaction Code Check at Transaction Start	*		
ACTVT			-	Activity			
TCD		C	-	Transaction Code	*	SU01	
BC_A			-	Basis: Administration	*		
S_USER_GRP		+	-	User Master Maintenance: User Groups	*		
ACTVT			-	Activity			
ACTVT			-	Create or generate		01	
ACTVT			-	Change		02	
ACTVT			-	Display		03	
CLASS		C	-	User group in user master maintenance	*	SUPER,AK_GR	

If the configuration parameter is not set, all SAP roles and SAP profiles with the authorizations found by the SAP function shown are listed here:

SAP application **SE16** with:
Authorization object **S_TCODE** with
Function element **ACTVT**
AND
Function element **TCD** with the value **SE16**

AND

Authorization object **P_TCODE** with
Function element **TCD** with exactly the value *****

OR

SAP application **SU01** with:
Authorization object **S_TCODE** with
Function element **ACTVT**
AND
Function element **TCD** with at least the value **SU01**

AND

Authorization object **S_USER_GRP** with
Function element **ACTVT** with at least one of the values **01** OR **02** OR **03**
AND
Function element **CLASS** with at least one of the values **SUPER** OR **AK_GR**

If the configuration parameter is set, all SAP roles and SAP profiles with the authorizations found by the SAP function are listed here:

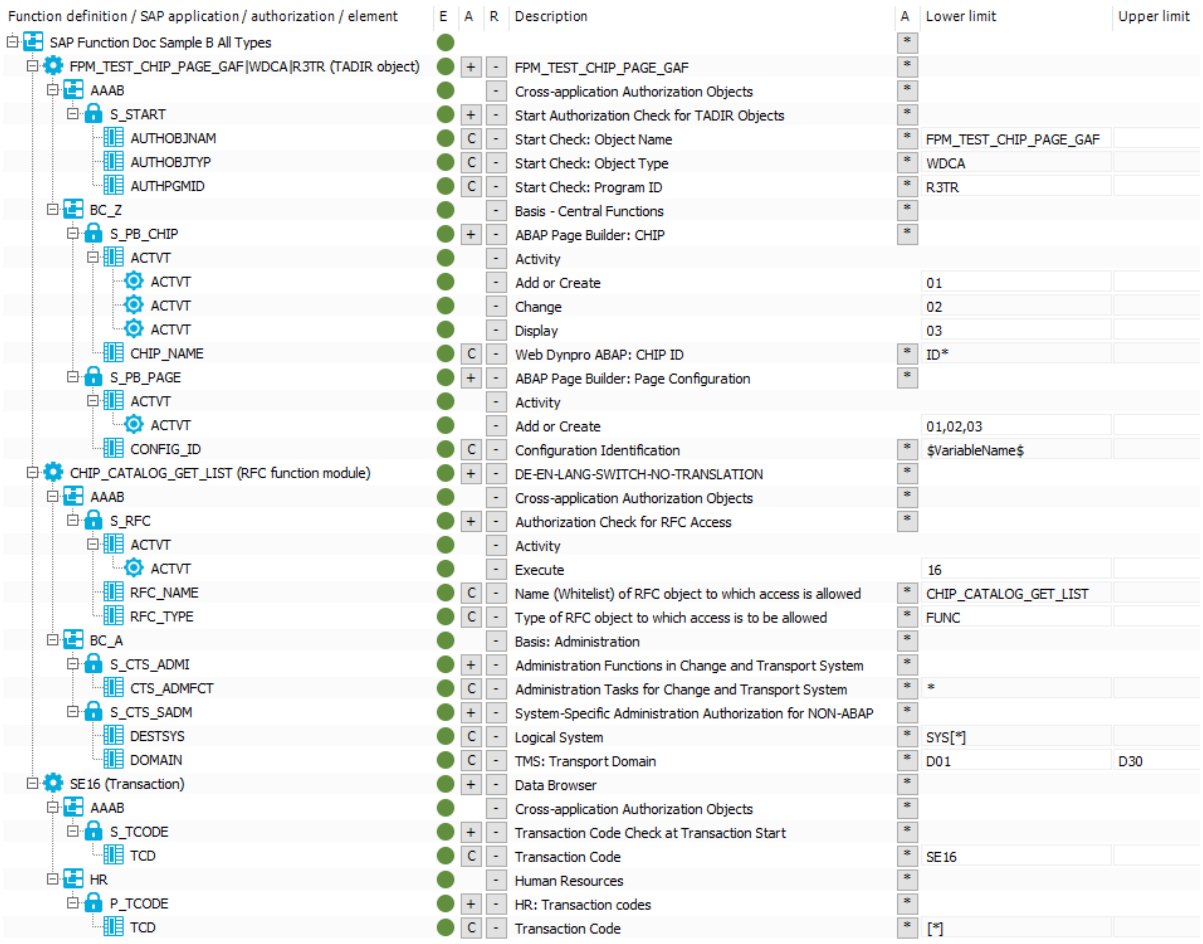
Authorization object **P_TCODE** with
Function element **TCD** with exactly the value *****

AND

Authorization object **S_USER_GRP** with
Function element **ACTVT** with at least one of the values **01** OR **02** OR **03**
AND
Function element **CLASS** with at least one of the values **SUPER** OR **AK_GR**

The following function definition contains various SAP applications with different application types.

Figure 4: Authorization definition with different application types



Function definition / SAP application / authorization / element	E	A	R	Description	A	Lower limit	Upper limit
SAP Function Doc Sample B All Types					*		
FPM_TEST_CHIP_PAGE_GAF|WDCA|R3TR (TADIR object)		+	-	FPM_TEST_CHIP_PAGE_GAF	*		
AAAB			-	Cross-application Authorization Objects	*		
S_START		+	-	Start Authorization Check for TADIR Objects	*		
AUTHOBJNAM		C	-	Start Check: Object Name	*	FPM_TEST_CHIP_PAGE_GAF	
AUTHOBJTYP		C	-	Start Check: Object Type	*	WDCA	
AUTHPGMID		C	-	Start Check: Program ID	*	R3TR	
BC_Z			-	Basis - Central Functions	*		
S_PB_CHIP		+	-	ABAP Page Builder: CHIP	*		
ACTVT			-	Activity			
ACTVT			-	Add or Create		01	
ACTVT			-	Change		02	
ACTVT			-	Display		03	
CHIP_NAME		C	-	Web Dynpro ABAP: CHIP ID	*	ID*	
S_PB_PAGE		+	-	ABAP Page Builder: Page Configuration	*		
ACTVT			-	Activity			
ACTVT			-	Add or Create		01,02,03	
CONFIG_ID		C	-	Configuration Identification	*	$VariableName$	
CHIP_CATALOG_GET_LIST (RFC function module)		+	-	DE-EN-LANG-SWITCH-NO-TRANSLATION	*		
AAAB			-	Cross-application Authorization Objects	*		
S_RFC		+	-	Authorization Check for RFC Access	*		
ACTVT			-	Activity			
ACTVT			-	Execute		16	
RFC_NAME		C	-	Name (Whitelist) of RFC object to which access is allowed	*	CHIP_CATALOG_GET_LIST	
RFC_TYPE		C	-	Type of RFC object to which access is to be allowed	*	FUNC	
BC_A			-	Basis: Administration	*		
S_CTS_ADMI		+	-	Administration Functions in Change and Transport System	*		
CTS_ADMFCT		C	-	Administration Tasks for Change and Transport System	*	*	
S_CTS_SADM		+	-	System-Specific Administration Authorization for NON-ABAP	*		
DESTSYS		C	-	Logical System	*	SYS[*]	
DOMAIN		C	-	TMS: Transport Domain	*	D01	D30
SE16 (Transaction)		+	-	Data Browser	*		
AAAB			-	Cross-application Authorization Objects	*		
S_TCODE		+	-	Transaction Code Check at Transaction Start	*		
TCD		C	-	Transaction Code	*	SE16	
HR			-	Human Resources	*		
P_TCODE		+	-	HR: Transaction codes	*		
TCD		C	-	Transaction Code	*	[*]	

If the configuration parameter is set and without taking the SAP applications into account, the SAP function shown will determine all SAP roles and SAP profiles that have the following authorizations:

Authorization object **S_PB_CHIP** with
Function element **ACTVT** with at least one of the values **01** OR **02** OR **03**
AND
Function element **CHIP_NAME** with an value that starts with **ID**

AND

Authorization object **S_PB_PAGE** with
Function element **ACTVT** with at least one of the values **01** OR **02** OR **03**
AND
Function element **CONFIG_ID** with the instance that is specified as a value in the **$VariableName$** variable

AND

Authorization object **S_CTS_ADMI** with
Function element **CTS_ADMFCT** with any value

AND

Authorization object **S_CTS_SADM** with

Function element **DESTSYS** with at least the value of exactly **SYS***
AND
Function element **DOMAIN** with at least one value in a range from **D01** to **D30**

AND

Authorization object **P_TCODE** with
Function element **TCD** with exactly the value *

If the configuration parameter is not set, the SAP function shown will determine all SAP roles and SAP profiles with the authorizations. The evaluation at the level of the function elements is identical to the evaluation when the configuration parameter is set and is therefore not shown again.

SAP application **FPM_TEST_CHIP_PAGE_GAF** with:
Authorization object **S_START**
AND
Authorization object **S_PB_CHIP**
AND
Authorization object **S_PB_PAGE**

OR

SAP application **CHIP_CATALOG_GET_LIST** with:
Authorization object **S_RFC**
AND
Authorization object **S_CTS_ADMI**
AND
Authorization object **S_CTS_SADM**

OR

SAP application **SE16** with:
Authorization object **S_TCODE**
AND
Authorization object **P_TCODE**

Related topics

- Notes on authorization definitions on page 18
- Examples of SAP functions on page 29
- Authorization definition properties and their values on page 19

Examples of SAP functions

If you create an authorization definition, you need to think about which authorization combinations are not compliant. You can differentiate between two use cases:

1. Find all SAP roles and profiles with invalid combinations of authorizations.

Create an SAP function for authorizations that cannot occur together with an SAP role or an SAP profile. The authorization check identifies all SAP roles and profiles whose authorizations in total have this invalid combination of authorizations.

2. Find all identities that have obtain invalid combinations of authorizations through their SAP user accounts.

   Create different SAP functions for authorizations that in combination are invalid. Create compliance rules that combine these SAP functions. The compliance check finds all identities that have such invalid authorization combinations over the sum of all authorizations of their SAP user accounts.

Example for use case 1

A company has changed its policies on compliant SAP authorizations. Now the new policies must be checked to see if existing authorizations comply. SAP roles and profiles with invalid combinations of authorizations must be identified so that they can be modified to meet the new requirements.

An SAP function is created for each invalid authorization combination.

Table 6: Example of an authorization definition

SAP function	SAP application	Authorization objects	Field	Value
F-A	TR1	AO2	ACTVT	*
	TR1	AO2	Class	*
	TR1	AO3	ACTVT	02
	TR1	S_TCODE	TCD	TR1
	RF	AO5	ACTVT	*
	RF	AO5	RLTYP	R*
	RF	S_RFC	RFC_NAME	RF
F-B	TR1	AO3	ACTVT	*
	TR1	AO4	ACTVT	02,03,07
	TR1	AO4	Class	DEF[*]
	TR1	S_TCODE	TCD	TR1

The following SAP profiles are available:

Table 7: Defined SAP profiles

SAP profile	SAP application	Authorization objects	Field	Value
P1	TR1	AO1	ACTVT	*
	TR1	AO1	Class	*
	TR1	AO3	ACTVT	*
	TR1	AO4	ACTVT	01, 02
	TR1	AO4	Class	DEF*
	TR1	S_TCODE	TCD	TR1
P2	TR1	AO2	ACTVT	*
	TR1	AO2	Class	*
	TR1	AO3	ACTVT	01
	TR1	S_TCODE	TCD	TR1
P3	TR1	AO3	ACTVT	01, 02
	TR1	AO4	Class	*
	TR1	AO4	ACTVT	03, 07
P4	RF	AO5	ACTVT	03
	RF	AO5	RLTYP	*
	RF	S_RFC	RFC_NAME	RF

SAP profiles are found that match the SAP function during authorization checking.

Results of the authorization check: **TestWithoutTCD** is not set.

- SAP function: F-A

  SAP profile affected: P4

  The profile P4 has all the authorization objects, fields, and values named in SAP application RF.

  The profile P1 is missing authorization objects AO2, S_TCODE, AO5, and S_RFC. Therefore it does not match the SAP function.

  The profile P2 is missing the value 02 for the authorization object AO3 as well as the authorization objects AO5 and S_RFC. Therefore it does not match the SAP function.

  The profile P3 is missing authorization objects AO2, S_TCODE, AO5, and S_RFC. Therefore it does not match the SAP function.

- SAP function: F-B

  SAP profile affected: P1

The profile P1 has all the authorization objects and fields named in the SAP function and at least one of the values.

The profile P2 is missing authorization object AO4. Therefore it does not match the SAP function.

The profile P3 is missing authorization object S_TCODE. Therefore it does not match the SAP function.

Profile P4 is missing the authorization objects AO3, AO4, and S_TCODE. Therefore it does not match the SAP function.

If the **TestWithoutTCD** configuration parameter is set for authorization checking, then the SAP profiles P2 and P3 comply with the new guidelines and can continue to be used. The profiles P1 and P4 must be modified to comply with the new policies.

Results of the authorization check: **TestWithoutTCD** is set.

- SAP function: F-A

  The authorization objects S_TCODE and S_RFC are ignored during the check.

  SAP profile affected: none

  The profile P1 is missing authorization objects AO2 and AO5. Therefore it does not match the SAP function.

  Profile P2 is missing authorization object AO5 and value 02 for authorization object AO3. Therefore it does not match the SAP function.

  The profile P3 is missing authorization objects AO2 and AO5. Therefore it does not match the SAP function.

  The profile P4 is missing authorization objects AO2 and AO3. Therefore it does not match the SAP function.

- SAP function: F-B

  The authorization object S_TCODE is ignored during the check.

  SAP profiles affected: P1, P3

  The profile P1 has all the authorization objects and fields named in the SAP function and at least one of the values.

  The profile P3 has all the authorization objects and fields named in the SAP function and at least one of the values.

  The profile P2 is missing authorization object AO4. Therefore it does not match the SAP function.

  The profile P4 is missing authorization objects AO3 and AO4. Therefore it does not match the SAP function.

If the **TestWithoutTCD** configuration parameter is set for authorization checking, then the SAP profiles P2 and P4 comply with the new guidelines and can continue to be used. The P1 and P3 profiles must be adjusted.

Example for use case 2

SAP user accounts must be checked for guidelines violations. The following user accounts and identities are available:

- User A with user account AC1 with the SAP profile P1
- User B with user account AC2 with the SAP profiles P2 and P3
- User C with user account AC3 with the SAP profile P2 and user account AC4 with the SAP profile P3

The SAP profiles have the following authorizations:

- P1 with AO1 and AO2
- P2 with AO1
- P3 with AO2

An identity cannot have the two authorizations AO1 and AO2 at the same time. The SAP function SF-A is created for the check. A compliance rule CR-X finds all identities that match this SAP function.

- SF-A checks AO1 AND AO2
- CR-X: The identity has at least the SAP SF-A function.

Only the SAP profile P1 matches the SAP function. Therefore, the compliance rule finds a rule violation for just User A. To ensure that the combination of the SAP profiles P2 and P3 is also recognized as invalid, additional SAP functions and compliance rules must be created.

- SF-B checks AO1
- SF-C checks AO2
- CR-Y: The identity has at least the SAP function SF-B AND they have at least the SAP function SF-C.

The SAP profiles P1 and P2 match the SAP function SF-B. The SAP profiles P1 and P3 match the SAP function SF-C. Thus, the compliance rule CR-Y can be used to determine all identities who are assigned the SAP profiles P1 or P2 and P3 though their user accounts and therefore have both authorizations AO1 and AO2.

Table 8: Result of the rule check

Rule	Rule condition	Identity that violate rules
CR-X	The identity has at least the SAP function SF-A.	User A
CR-Y	The identity has at least the SAP function SF-B AND they have at least the SAP function SF-C.	User A User B User C

Related topics

- Finding invalid authorizations on page 23
- Rule conditions for SAP functions on page 54

Editing function definitions

A working copy is added to the database for every function definition. You can edit the working copies to change the function definitions. The changes are not passed on to the production function definition until the working copy is enabled. SAP authorizations are only checked on the basis of active function definitions.

NOTE: One Identity Manager users with the **Identity & Access Governance | Identity Audit | Maintain SAP functions** application role can edit existing working copies if they are entered as the manager in the main data.

To edit an existing function definition

1. In the Manager, select the **Identity Audit > SAP functions > Function definitions** category.
   a. Select the function definition in the result list.
   b. Select the **Create working copy** task.

      The data from the existing working copy are overwritten with the data from the active function definition, after prompting. The working copy is opened and can be edited.

   - OR -

   In the Manager, select the **Identity Audit > SAP functions > Function definition working copies** category.
   a. Select a working copy in the result list.
   b. Select the **Change main data** task.
2. Edit the working copy's main data.
3. Save the changes.
4. Select the **Enable working copy** task and confirm the security prompt with **Yes**.

   The changes to the working copy are transferred to the active function definition.

Related topics

- Creating working copies on page 36
- General main data of a function definition on page 16
- Enabling working copies on page 23

Function definition overview

You can display the most important information about a function definition on the overview form.

To obtain an overview of a function definition

1. In the Manager, select the **Identity Audit > SAP functions > Function definitions** category.
2. Select the function definition in the result list.
3. Select the **Function definition** task.

To obtain an overview of a working copy

1. In the Manager, select the **Identity Audit > SAP functions > Function definition working copies** category.
2. Select the function definition in the result list.
3. Select the **Function definition** task.

Authorization overview

Function elements are displayed in a flat structure in the authorization overview.

To display an overview of all function elements for an active function definition

1. In the Manager, select the **Identity Audit > SAP functions > Function definitions** category.
2. Select the function definition in the result list.
3. Select the **Authorization overview** task.

To display an overview of all function elements for a working copy

1. In the Manager, select the **Identity Audit > SAP functions > Function definition working copies** category.
2. Select the function definition in the result list.
3. Select the **Authorization overview** task.

   You can edit all the object properties here.

Related topics

- Creating authorization definitions in the Authorization Editor on page 17

Creating working copies

To modify an existing function definition, you require a working copy of the function definition. You can create a working copy from the active function definition. After confirming the prompt, the data of an existing working copy is overwritten with the data from the active function definition.

To create a working copy

1. In the Manager, select the **Identity Audit > SAP functions > Function definitions** category.
2. Select the function definition in the result list.
3. Select the **Create working copy** task.
4. Confirm the security prompt with **Yes**.

Related topics

- Enabling working copies on page 23

Exporting function definitions

To transfer SAP functions from a development environment to a production environment, for example, you can export function definitions to CSV files. These CSV files can be imported into other databases.

To export the function definition to a CSV file

1. In the Manager, select the **Identity Audit > SAP functions > Function definitions** category.
2. Select the function definition in the result list.
3. Select the **Change main data** task.
4. Select the **Export** task.
5. Specify the file name and storage location for the CSV file.
6. Click **Save**.

The following properties are exported:

Table 9: Exported main data of a function definition

Property	Data field in the CSV file.
Name of the function definition	Function
Assigned function category	Process

Property	Data field in the CSV file.
Description	Function Description
Significance	Risk Level
Suggested authorization value	TransactionType
Transaction code	Transaction
TADIR program ID	AUTHPGMID
TADIR object type	AUTHOBJTYP
TADIR object name	AUTHOBJNAM
Type of external service	SRV_TYPE
Name of external service	SRV_NAME
RFC object type	RFC_TYPE
RFC object name	RFC_NAME
Hash value	SAPHashValue
Authorization objects	Object
Authorization fields	Field
Description of authorization field.	Field Description
Value/lower scope limit	Value From
Upper scope limit	Value To

The import status (`State`) is included with each data record in the CSV file as additional information. The import status is set to **1** by default on export. This data is evaluated when function definitions are imported.

Related topics

- Importing function definitions on page 51
- Exporting working copies on page 37
- Exporting function definitions on page 50

Exporting working copies

To transfer SAP functions from a development environment to a production environment, for example, you can export function definitions to CSV files. These CSV files can be imported into other databases.

To export the function definition of a working copy to a CSV file

1. In the Manager, select the **Identity Audit > SAP functions > Function definition working copies** category.
2. Select the function definition in the result list.
3. Select the **Change main data** task.
4. Select the **Export** task.
5. Specify the file name and storage location for the CSV file.
6. Click **Save**.

The following properties are exported:

Table 10: Exported main data of a function definition

Property	Data field in the CSV file.
Name of the function definition	Function
Assigned function category	Process
Description	Function Description
Significance	Risk Level
Suggested authorization value	TransactionType
Transaction code	Transaction
TADIR program ID	AUTHPGMID
TADIR object type	AUTHOBJTYP
TADIR object name	AUTHOBJNAM
Type of external service	SRV_TYPE
Name of external service	SRV_NAME
RFC object type	RFC_TYPE
RFC object name	RFC_NAME
Hash value	SAPHashValue
Authorization objects	Object
Authorization fields	Field
Description of authorization field.	Field Description
Value/lower scope limit	Value From
Upper scope limit	Value To

The import status (`State`) is included with each data record in the CSV file as additional information. The import status is set to **1** by default on export. This data is evaluated when function definitions are imported.

Related topics

- Importing function definitions on page 51
- Exporting function definitions on page 36
- Exporting function definitions on page 50

Defining function instances

One and the same function definition can be used for different concrete instances. A specific SAP client that the SAP function will be used in is given in the function instance. In addition, the variables that are assigned to the authorization fields are given specific values. Function instances can only be created for SAP functions that are enabled.

To create a function instance

1. In the Manager, select the **Identity Audit > SAP functions > Function instances** category.
2. Click in the result list.
3. Edit the function instance's main data.
4. Save the changes.

To edit a function instance

1. In the Manager, select the **Identity Audit > SAP functions > Function instances** category.
2. In the result list, select a function instance and run the **Change main data** task.
3. Edit the function instance's main data.
4. Save the changes.

NOTE: One Identity Manager users with the **Identity & Access Governance | Identity Audit | Maintain SAP functions** application role can create and edit function instances for the SAP functions if they are listed as the manager.

Detailed information about this topic

- Main data for function instances on page 40
- Checking field variable definitions on page 40
- Function instance overview on page 41

Main data for function instances

Enter the following main data of a function instance.

Table 11: Function instance properties

Property	Description
Function definition	The function instance is created for this function definition.
Client	SAP client to which the SAP function should be applied.
Variable set	Variable set with functions defined, which are used in the function definition. The variable set and the function instance must be assigned to the same SAP client.
Manager/supervisor	Application role whose members are responsible for the function instance and variable sets in terms of content. To create a new application role, click . Enter the application role name and assign a parent application role.
Display name	Function instance display name. This is formatted from the function definition name, the assigned client and variable set.
Description	Text field for additional explanation. The function definition description is copied to a new function instance.
Function Instance Elements	Displays SAP applications, approval objects, and function elements of the SAP function with specified values that are determined from the assigned variable set. Changes to the variables or variable set are displayed as soon as the DBQueue Processor has processed the corresponding authorization tasks.

Related topics

- Creating and editing variable sets for authorization definitions on page 41
- Maintaining SAP functions on page 49
- Checking field variable definitions on page 40

Checking field variable definitions

Before you use function instances in compliance rules, check whether all variable which are used in the function definition are defined in the variable set. If there is no function definition or variable set assigned to the function instance, the check-in fails with an error message. Variables that are not defined in the associated variable set are listed in the error message.

To check variable definitions

1. In the Manager, select the **Identity Audit > SAP functions > Function instances** category.
2. Select the function instance in the result list.
3. Select the **Change main data** task.
4. Select the **Check variable definitions** task.

Related topics

- Main data for function instances on page 40
- Main data for a variable set on page 42

Function instance overview

You can display the most important information about a function instance on the overview form.

To obtain an overview of a function instance

1. In the Manager, select the **Identity Audit > SAP functions > Function instances** category.
2. Select the function instance in the result list.
3. Select the **Function instance** task.

Creating and editing variable sets for authorization definitions

Use variable sets to group variables together that are used in an authorization definition and give then fixed values.

To create a variable set

1. In the Manager, select the **Identity Audit > SAP Functions > Variable sets** category.
2. Click in the result list.
3. Edit the variable set's main data.
4. Save the changes.

To edit a variable set

1. In the Manager, select the **Identity Audit > SAP Functions > Variable sets** category.
2. In the result list, select the variable set and run the **Change main data** task.
3. Edit the variable set's main data.
4. Save the changes.

Detailed information about this topic

- Main data for a variable set on page 42
- Adding variables used in SAP functions on page 43

Related topics

- Creating authorization definitions in the Authorization Editor on page 17
- Variable set overview on page 44
- Copying variable sets on page 44

Main data for a variable set

Enter the following main data of variable sets.

Table 12: Main data for a variable set

Property	Description
Variable set	Unique variable set identifier.
Client	Valid SAP client for the variable set.
Department	Relevant department for the variable set.
Functional area	Functional area relevant to the variable set.
Description	Text field for additional explanation.
SAP field variables	List of defined variables.

To create a field variable in the variable set

- Click **Add** and enter the following properties.
  - **Variable**: Name of the variable in `${alphanum}+$` notation.

    NOTE: Variable names cannot begin with system variable names. Variable sets with variables like this cannot be saved.

- **Value**: Concrete instances for the variable to be copied to the function instance.
- **Description**: Text field for additional explanation.
- **Authorization object**: Reference to the authorization object to use in the variable in.

There is help for your selected on the form. On the form, there is help available for selecting authorization fields for an authorization object to be used for defining variables.

To delete a field variable from the variable set

1. Select a line in the list of field variables.
2. Click **Remove selected**.

TIP: You can add variable sets without defining variables. Use these variables set for function definitions that do not have variables entered as values.

Detailed information about this topic

- Using variables on page 21

Related topics

- Adding variables used in SAP functions on page 43

Adding variables used in SAP functions

Variables used in authorization definitions of SAP functions can be added to variable sets.

To transfer variables to a variable set

1. Select the **Identity Audit > SAP Functions > Variable sets** category.
2. Select the variable set in the result list.
3. Select the **Change main data** task.
4. Select the **Apply chosen variables** task.
5. Mark all function definitions or working copies from which you want to copy the variables into the variable set.

   Multi-select is possible.
6. Click **OK** to transfer the variables.

   All variables from the selected function definitions are add to the list of field variables.
7. Edit the variables' properties.
8. Save the changes.

Related topics

- Main data for a variable set on page 42

Copying variable sets

To copy a variable set

1. In the Manager, select the **Identity Audit > SAP Functions > Variable sets** category.
2. In the result list, select the variable set and run the **Change main data** task.
3. Select the **Copy variable set** task.
4. Click **Yes** to immediately edit the copy's main data.
5. Edit the copy's main data.
6. Save the changes.

Related topics

- Main data for a variable set on page 42

Variable set overview

You can display the most important information about a variable set on the overview form.

To obtain an overview of a variable set

1. In the Manager, select the **Identity Audit > SAP Functions > Variable sets** category.
2. Select the variable set in the result list.
3. Select the **Variable set overview** task.

Assigning mitigating controls to SAP functions

Mitigating controls can be stored with SAP functions. These reduce the effects on the company when SAP users match with SAP functions. At the same time, you specify how to deal with SAP users or SAP groups that match the SAP function. For example, changing a user assignment to an SAP role in the SAP system can be used as a mitigating control for an SAP function.

Mitigating controls can also be used as controlling measures for compliance rules. Mitigating controls assigned to the SAP functions for testing are automatically transferred into compliance rules about SAP functions.

Prerequisites:

- Enabled compliance rules are assigned to a functional area and a department.
- The SAP functions for testing are assigned to the same functional area and then associated variable set of the same department.

To edit mitigating controls

- In the Designer, enable the **QER | CalculateRiskIndex** configuration parameter.

Detailed information about this topic

- Assigning mitigating controls to a function definition on page 45
- Creating mitigating controls for SAP functions on page 46
- Mitigating controls for SAP functions on page 57

Assigning mitigating controls to a function definition

To assign mitigating controls to a function definition

1. In the Manager, select the **Identity Audit > SAP functions > Function definition working copies** category.
2. Select the working copy in the result list.
3. Select the **Assign mitigating controls** task.

   In the **Add assignments** pane, assign the mitigating controls.

   TIP: In the **Remove assignments** pane, you can remove mitigating control assignments.

   To remove an assignment

   - Select the mitigating control and double-click .
4. Save the changes.

Creating mitigating controls for SAP functions

To create a mitigating control for SAP functions

1. In the Manager, select the **Identity Audit > SAP functions > Function definition working copies** category.
2. Select a working copy in the result list.
3. Select the **Assign mitigating controls** task.
4. Select the **Create mitigating controls** task.
5. Enter the main data of the mitigating control.
6. Save the changes.
7. Select the **Assign function definitions** task.
8. In the **Add assignments** pane, double-click the function definitions you want to assign.
9. Save the changes.

Detailed information about this topic

- Mitigating controls for SAP functions on page 57

Base data for SAP functions

The following base data is relevant for SAP Functions:

- SAP function categories

  Use SAP function categories to group SAP functions by specific criteria.

  For more information, see SAP function categories on page 47.

- Functional areas

  Functional areas can be used as an additional group characteristic for SAP functions. Furthermore, you can use functional areas to analyze rule violations in context of Identity Audit for different SAP functions and to approve requests in the IT Shop or attestation cases by peer group analysis.

  For more information, see Functional areas on page 47.

- Maintaining SAP functions

  SAP functions can be assigned identities that manage the SAP functions and therefore can edit the working copies.

  For more information, see Maintaining SAP functions on page 49.

SAP function categories

Use function categories to group SAP functions by specific criteria.

To create or edit a function category

1. In the Manager, select the **Identity Audit > Basic configuration data > SAP function categories** category.
2. In the result list, select a function category and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the function category's main data.
4. Save the changes.

Enter the following main data of a function category.

Table 13: SAP function category properties

Property	Description
Category	The function category’s name.
Parent category	Parent category for organizing function categories hierarchically.
Description	Text field for additional explanation.

Related topics

- General main data of a function definition on page 16

Functional areas

You can use functional areas to analyze rule violations in context of Identity Audit for different SAP functions. You can enter criteria that provide information about risks from rule violations for functional areas and SAP functions.

To analyze rule checks for different areas of your company in the context of identity audit, you can set up functional areas. Functional areas can be assigned to hierarchical roles and service items. You can enter criteria that provide information about risks from rule violations for functional areas and hierarchical roles. To do this, you specify how many rule violations are permitted in a functional area or a role. You can enter separate assessment criteria for each role, such as a risk index or transparency index.

Moreover, functional areas can be replaced by peer group analysis during request approvals or attestation cases.

Example: Use of functional areas

To assess the risk of rule violations for cost centers. Proceed as follows:

1. Set up functional areas.
2. Assign cost centers to the functional areas.
3. Define assessment criteria for the cost centers.
4. Specify the number of rule violations allowed for the functional area.
5. Assign compliance rules required for the analysis to the functional area.
6. Use the One Identity Manager report function to create a report that prepares the result of rule checking for the functional area by any criteria.

To create or edit a functional area

1. In the Manager, select the **Identity Audit > Basic configuration data > Functional areas** category.
2. In the result list, select a function area and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the function area main data.
4. Save the changes.

Enter the following data for a functional area.

Table 14: Functional area properties

Property	Description
Functional area	Description of the functional area
Parent Functional area	Parent functional area in a hierarchy. Select a parent functional area from the list for organizing your functional areas hierarchically.
Max. number of rule violations	List of rule violation valid for this functional area. This value can be evaluated during the rule check.
Description	Text field for additional explanation.

Mitigating controls assigned to the function definitions to be tested are automatically copied to rules about SAP functions. Conditions:

- Active rules are assigned to a functional area and a department.
- The function definitions to be tested are assigned to the same functional area and to the variable set associated with the same department.

Related topics

- Mitigating controls for SAP functions on page 57
- General main data of a function definition on page 16

Maintaining SAP functions

You can assign SAP functions to identities that are responsible for the content of those SAP functions. To do this, assign the an application for maintaining SAP functions to an application role. Assign to this application role, the identities that are authorized to enable and edit working copies of this function definition and can define function instances.

A default application role exists for maintaining One Identity Manager functions in SAP. Create more application roles if required. For more information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 15: Default application roles for maintaining SAP functions

User	Tasks
Responsible for maintaining SAP functions.	Administrators must be assigned to the **Identity & Access Governance | Identity Audit | Maintain SAP functions** application role or a child application role. Users with this application role: • Are responsible for SAP function contents. • Edit working copies of function definitions for which they are responsible. • Define function instances and variables sets for SAP functions. • Assign mitigating controls.

To add identities to the default application role for maintaining SAP functions

1. In the Manager, select the **Identity Audit > Basic configuration data > Maintain SAP functions** category.
2. Select the **Assign identities** task.
3. In the **Add assignments** pane, add identities.

   TIP: In the **Remove assignments** pane, you can remove assigned identities.

   To remove an assignment

   - Select the identity and double-click .
4. Save the changes.

Related topics

- General main data of a function definition on page 16

Exporting function definitions

To transfer SAP functions from a development environment to a production environment, for example, you can export function definitions to CSV files. These CSV files can be imported into other databases.

To export all function definitions to a CSV file

1. In the Manager, select the **Identity Audit** category.
2. Select the **Plugins > Export all SAP function definitions** menu item.
3. To only export working copies, click **Yes**.

   - OR -

   To only export enabled SAP functions, click **No**.
4. Specify the file name and storage location for the CSV file.
5. Click **Save**.

   All function definitions are written to file in sequence.

The following properties are exported:

Table 16: Exported main data of a function definition

Property	Data field in the CSV file.
Name of the function definition	Function
Assigned function category	Process
Description	Function Description
Significance	Risk Level
Suggested authorization value	TransactionType
Transaction code	Transaction
TADIR program ID	AUTHPGMID
TADIR object type	AUTHOBJTYP
TADIR object name	AUTHOBJNAM
Type of external service	SRV_TYPE
Name of external service	SRV_NAME

Property	Data field in the CSV file.
RFC object type	RFC_TYPE
RFC object name	RFC_NAME
Hash value	SAPHashValue
Authorization objects	Object
Authorization fields	Field
Description of authorization field.	Field Description
Value/lower scope limit	Value From
Upper scope limit	Value To

The import status (`State`) is included with each data record in the CSV file as additional information. The import status is set to **1** by default on export. This data is evaluated when function definitions are imported.

NOTE: SAP function managers can only export those function definitions for which they are responsible, as entered in the main data.

Related topics

- Importing function definitions on page 51
- Exporting working copies on page 37
- Exporting function definitions on page 36

Importing function definitions

To transfer SAP functions from a development environment to a production environment, for example, you can export function definitions to CSV files. These CSV files can be imported into other databases.

When importing SAP functions from an existing CSV file, the function definitions contained in the CSV file are transferred to the database as working copies. The following data fields must be in the CSV file so that function definitions can be imported.

Table 17: Data fields for importing function definitions

Data field in the CSV file. (header)	Object properties in One Identity Manager
Function	Function definition

Data field in the CSV file. (header)	Object properties in One Identity Manager
TransactionType	Suggested authorization value
Object	Authorization objects
Field	Authorization field
Value From	Value/lower scope limit
Value To	Upper scope limit
State	No equivalent. The import status controls which data records are imported into One Identity Manager. **1**: Import
Process (optional)	Category
Function description (optional)	Description of the function definition.
Risk level (optional)	Significance Possible values are {**Low**|**Medium**|**High**|**Critical**}.
Transaction (optional)	Transaction code
AUTHPGMID (optional)	TADIR program ID
AUTHOBJTYP (optional)	TADIR object type
AUTHOBJNAM (optional)	TADIR object name
SRV_TYPE (optional)	Type of external service
SRV_NAME (optional)	Name of external service
RFC_TYPE (optional)	RFC object type
RFC_NAME (optional)	RFC object name
SAPHashValue (optional)	Hash value
Field description (optional)	Describes the authorization fields, authorization objects and SAP applications.

NOTE:

- The order of the data fields is arbitrary.
- All required data fields must be defined in the header and must be present in the data sets.
- Mark data fields without values with two sequential delimiters.
- Data sets with empty mandatory fields are not imported.

To import function definitions

1. In the Manager, select the **Identity Audit** category.
2. Select the **Plugins > Import SAP function definitions** menu item.
3. Select the CSV file you want to import and click **Open**.
4. Confirm the security prompt with **Yes**.

   The functions definitions are transferred to the database as working copies. If there is already a working copy with the same name in the database, it is overwritten by the import.

Related topics

- Exporting function definitions on page 50
- Exporting working copies on page 37
- Exporting function definitions on page 36

Compliance rules for SAP functions

Compliance rules can be checked through effective authorizations as well as through authorizations, which an identity has in an SAP R/3 system due to their user accounts and group and role memberships. Effective write permissions are tested through SAP functions. To do this, SAP functions are added to rule conditions.

The validity period of role assignments is taken into account in the rule check.

For more information about compliance rules, see the *One Identity Manager Compliance Rules Administration Guide*.

Detailed information about this topic

- Rule conditions for SAP functions on page 54
- Mitigating controls for compliance rules with SAP functions on page 55

Rule conditions for SAP functions

To define new rules for SAP functions

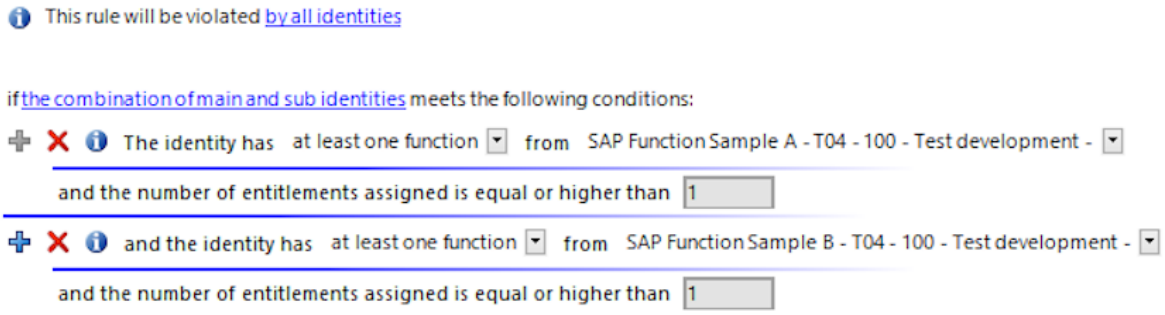
1. In the Manager, select the **Identity Audit > Rules** category.
2. Click in the result list.
3. Enter the main data of the rule.
4. Set the **Rule for cyclical testing and risk analysis in IT Shop** option.
5. Limit the affected permissions with the **at least one function** option and select the SAP functions to test.
    a. If you have selected more than one SAP functions, under **number of entitlements assigned**, specify how many SAP functions must be matched to violate the rule.
    b. If SAP authorizations in combination result in a rule violation, enter a rule block for each SAP function.
6. Save the changes.

This adds a working copy.

7. Select the **Enable working copy** task and confirm the security prompt with **Yes**.

   This adds an enabled rule in the database. The working copy is retained and can be used to make changes later.

Figure 5: Condition for SAP functions



When One Identity Manager tests rules, it finds all the identities whose assigned SAP users match the SAP functions that are given in the rule. An SAP user matches an SAP function when:

- An SAP role assigned to the SAP user account matches the SAP function

  - OR -

- An SAP role that is assigned a reference user matching an SAP function

  - AND -

- The SAP user account is assigned this reference user.

For more information about creating rule conditions, see the *One Identity Manager Compliance Rules Administration Guide*.

Related topics

- Examples of SAP functions on page 29

Mitigating controls for compliance rules with SAP functions

Mitigating controls assigned to the function definitions to be tested are automatically copied to rules about SAP functions. Conditions:

- Active rules are assigned to a functional area and a department.
- The function definitions to be tested are assigned to the same functional area and to the variable set associated with the same department.

Related topics

- Assigning mitigating controls to SAP functions on page 44

More rule violation reports

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. Additional reports can be created for enabled compliance rules for SAP functions.

Table 18: Reports about rule violations with SAP functions

Report	Description
Rule violations with SAP applications	This report groups together all rule violations for the selected rule. It supplies results for rules that verify SAP functions. All function instances are listed with their SAP applications for each identity through which they violated the rule. SAP profiles and their authorization objects that match the SAP function are displayed for each SAP function.
Rule violations with SAP roles	This report groups together all rule violations for the selected rule. It supplies results for rules that verify SAP functions. SAP groups, SAP roles, and SAP profiles with their authorization objects are listed for each identity through which they violated the rule.
SAP roles and profiles with rule violations	The report shows all SAP roles and profiles that match SAP functions and thereby violate the selected rule.

Mitigating controls for SAP functions

Violation of regulatory requirements can harbor different risks for companies. To evaluate these risks, you can apply risk indexes to SAP functions. These risk indexes provide information about the risk involved for the company if this particular SAP function is violated. Once the risks have been identified and evaluated, mitigating controls can be implemented.

Mitigating controls are independent on One Identity Manager's functionality. They are not monitored through One Identity Manager.

Mitigating controls describe controls that are implemented if an SAP function was violated. The next calculation should not find any invalid authorizations for this SAP function once the controls have been applied.

To edit mitigating controls

- In the Designer, set the **QER | CalculateRiskIndex** configuration parameter and compile the database.

If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

For more information about mitigating controls, see the *One Identity Manager Risk Assessment Administration Guide*.

Detailed information about this topic

- Entering main data for mitigating controls on page 58
- Mitigating controls overview on page 58
- Assigning function definitions to mitigating controls on page 59
- Calculating mitigating controls for SAP functions on page 59

Entering main data for mitigating controls

To create or edit mitigating controls

1. In the Manager, select the **Risk index functions > Mitigating controls** category.
2. Select a mitigating control in the result list and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the mitigating control main data.
4. Save the changes.

Enter the following main data of mitigating controls.

Table 19: General main data of a mitigating control

Property	Description
Measure	Unique identifier for the mitigating control.
Significance reduction	When the mitigating control is implemented, this value is used to reduce the risk of denied attestation cases. Enter a number between **0** and **1**.
Description	Detailed description of the mitigating control.
Functional area	Functional area in which the mitigating control may be applied.
Department	Department in which the mitigating control may be applied.

Related topics

- Mitigating controls for SAP functions on page 57

Mitigating controls overview

You can display the most important information about a mitigating control on the overview form.

To obtain an overview of a mitigating control

1. In the Manager, select the **Risk Index Functions** category.
2. Select the **Mitigating controls** category.

3. Select the mitigating control in the result list.
4. Select **Mitigating control overview** category.

Related topics

- Mitigating controls for SAP functions on page 57

Assigning function definitions to mitigating controls

Use this task to specify the function definitions for which a mitigating control is valid. You can only assign function definitions that are enabled on the assignment form.

To assign SAP function definitions to mitigating controls

1. In the Manager, select the **Risk index functions > Mitigating controls** category.
2. Select the mitigating control in the result list.
3. Select the **Assign function definitions** task.

   In the **Add assignments** pane, assign the function definitions.

   TIP: In the **Remove assignments** pane, you can remove function definitions assignments.

   To remove an assignment

   - Select the mitigating control and double-click .
4. Save the changes.

Related topics

- Assigning mitigating controls to SAP functions on page 44
- Mitigating controls for SAP functions on page 57

Calculating mitigating controls for SAP functions

The reduction in significance of a mitigating control supplies the value by which the risk index of an SAP function is reduced when the control is implemented. One Identity Manager calculates a reduced risk index based on the risk index and the significance reduction. One Identity Manager supplies default functions for calculating reduced risk indexes. These functions cannot be edited with One Identity Manager tools.

The reduced risk index is calculated from the SAP function and the significance reduced sum of all assigned mitigating controls.

```
Risk index (reduced) = Risk index - sum significance reductions
```

If the significance reduction sum is greater than the risk index, the reduced risk index is set to **0**.

Related topics

- Mitigating controls for SAP functions on page 57

Appendix A

Configuration parameters for SAP functions

The following configuration parameters are additionally available in One Identity Manager after the module has been installed.

Table 20: Configuration parameters for the module

Configuration parameter	Description
TargetSystem | SAPR3 | SAPRights	Preprocessor relevant configuration parameter for controlling component parts for testing authorizations in SAP R/3 using SAP functions. If the parameter is set, the components are available. Changes to the parameter require recompiling the database. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
TargetSystem | SAPR3 | SAPRights | TestWithoutTCD	Checks SAP authorizations without taking SAP applications into account.

The following configuration parameters are also required.

Table 21: Additional configuration parameters

Configuration parameter	Description
QER | CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating the risk index. Changes to the parameter require recompiling the database.

Configuration parameter	Description
	If the parameter is enabled, values for the risk index can be entered and calculated. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
QER | ComplianceCheck	Preprocessor relevant configuration parameter for controlling the database model components for checking the rule base. Changes to the parameter require recompiling the database. If the parameter is enabled, you can use the model components. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

Appendix B

Default project template for the SAP R/3 Compliance Add-on Module

A default project template ensures that all required information is added in One Identity Manager. This includes mappings, workflows, and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

Use the **SAP R/3 authorization objects** project template to synchronize authorization objects and transactions. The project template uses mappings for the following schema types.

Table 22: Mapping SAP R/3 schema types to tables in the One Identity Manager schema

Schema type in the target system	Table in the One Identity Manager Schema
TOBJ	SAPAuthObject
ObjectClass	SAPAuthObjectClass
AUTHX	SAPField
Transactions	SAPTransaction
TACT	SAPActivity
ObjectHasField	SAPAuthObjectHasField
ObjectHasActivity	SAPAuthObjectHasSapActivity
FieldHasRcTable	SAPFieldHasSAPRCTable
TMENU01	SAPMenu
MenuHasTransaction	SAPMenuHasSAPTransaction
ProfileHasAuthObjectField	SAPProfileHasAuthObjectElem

Schema type in the target system	Table in the One Identity Manager Schema
RcTable	SAPRCTable
Variable	SAPRCVariable
TRANSACTIONHASTOBJ	SAPTransactionHasSAPAuthObject
RFCFUNCTION	SAPTransaction
USOBHASH	SAPTransaction

Appendix C

Referenced SAP R/3 tables and BAPI calls

The following overview provides information about all the tables referenced by SAP authorization objects in an SAP R/3 system and the BAPI calls that are run. The tables and BAPIs accessed by the SAP R/3 connector when SAP R/3 basis administration is synchronized are listed in the One Identity Manager Administration Guide for Connecting to SAP R/3.

Table 23: Referenced tables and BAPIs

Tables	BAPI Calls
AUTHX	AUTH_TRACE_GET_USOBHASH
OBJCT	RFC_READ_TABLE or /VIAENET/READTABLE
TACT	AUTH_TRACE_GET_USOBHASH or /VIAENET/LISTUSOBHASH
TACTZ	
TFDIR	
TMENU01	
TMENU01R	
TMENU01T	
TOBJ	
TOBCT	
TSTCT	
USOBHASH	
USOBX_C	
USR10	
UST10S	
UST12	
USVART	

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

R

S

U

V

W