



One Identity Manager 8.2.1

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

Copyright 2022 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC.

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

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 - 27 April 2022, 03:09
Version - 8.2.1

Contents

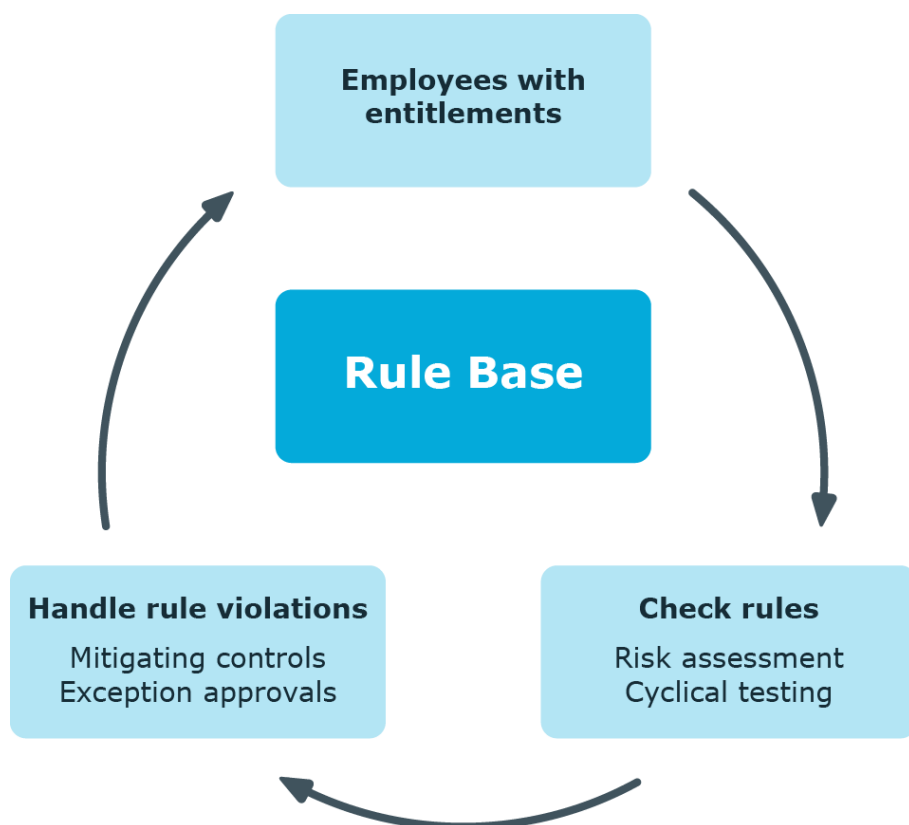
SAP functions and identity audit	5
One Identity Manager users for managing SAP functions	6
Prerequisites for setting up SAP functions	8
Setting up a synchronization project for synchronizing SAP authorization objects	9
Base data for SAP functions	11
SAP function categories	11
Functional areas	12
Maintaining SAP functions	14
Finding non-compliant authorizations	15
Examples of SAP functions	17
Setting up SAP functions	22
Notes on authorization definitions	22
Using variables	23
Creating and editing function definitions	24
General main data of a function definition	25
Function definition overview	26
Creating authorization definitions in the Authorization Editor	27
Checking authorization objects for completeness	30
Authorization overview	30
Creating working copy	31
Enabling working copies	31
Exporting function definitions	32
Exporting working copies	33
Assigning mitigating controls to SAP functions	35
Assigning mitigating controls to a function definition	35
Creating mitigating controls for SAP functions	36
Defining function instances	36
Main data for a function instance	37
Function instance overview	38

Checking field variable definitions	38
Adding variable set for authorization objects	38
Main data for a variable set	39
Variable set overview	40
Copying variable sets	41
Adding variables used in SAP functions	41
Exporting function definitions	42
Importing function definitions	43
Compliance rules for SAP functions	46
Rule conditions for SAP functions	46
More rule violation reports	47
Mitigating controls for compliance rules with SAP functions	48
Mitigating controls for SAP functions	49
Entering main data for mitigating controls	49
Mitigating controls overview	50
Assigning function definitions to mitigating controls	50
Calculating mitigating controls for SAP functions	51
Appendix: Configuration parameters for SAP functions	52
Appendix: Default project template for the SAP R/3 Compliance Add-on Module	54
Appendix: Referenced SAP R/3 tables and BAPI calls	56
About us	57
Contacting us	57
Technical support resources	57
Index	58

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 employees 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 this 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 employees, combinations of SAP authorizations that an employee 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 employees match these SAP functions by using compliance rules.

If employees 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 procedures. For more information about approval procedures in the IT Shop, see the *One Identity Manager IT Shop Administration Guide*.

Based on this information, you can make 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. • Create reports about rule violations. • Define SAP functions and assign these to managers.

Users	Tasks
	• 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 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 policies.

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 not 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 9](#)

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 54
- [Referenced SAP R/3 tables and BAPI calls](#) on page 56

Base data for SAP functions

The following base data is relevant for SAP Functions:

- Configuration parameters

Use configuration parameters to configure the behavior of the system's basic settings. One Identity Manager provides default settings for different 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 52.

- SAP function categories

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

For more information, see [SAP function categories](#) on page 11.

- 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 12.

- Maintaining SAP functions

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

For more information, see [Maintaining SAP functions](#) on page 14.

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 2: 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.

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 3: 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 49

Maintaining SAP functions

You can assign SAP functions to employees 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 employees 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 detailed information about implementing and editing application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 4: 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 employees 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 employees** task.
3. In the **Add assignments** pane, add employees.
TIP: In the **Remove assignments** pane, you can remove assigned employees.

To remove an assignment

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

Related topics

- [General main data of a function definition](#) on page 25

Finding non-compliant 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 through the single profiles.

The **TargetSystem | SAPR3 | SAPRights | TestWithoutTCD** configuration parameter is evaluated by authorization checks. The configuration parameter defines whether only the authorization objects or also the SAP applications are to be 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.
2. It has all the authorization objects for this SAP application.
3. It has all the different authorization object function elements.
4. At least one of the instances is defined exactly the same function element.

An SAP role matches an SAP function if the SAP profile of this SAP role contains one 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 list of different instances is defined for the authorization object, the SAP profile matches the SAP function if it has at least one of these instances.

The TestWithoutTCD configuration parameter is set

SAP applications are not taken into account during the authorization check. In this case, the following rules apply for authorization checking:

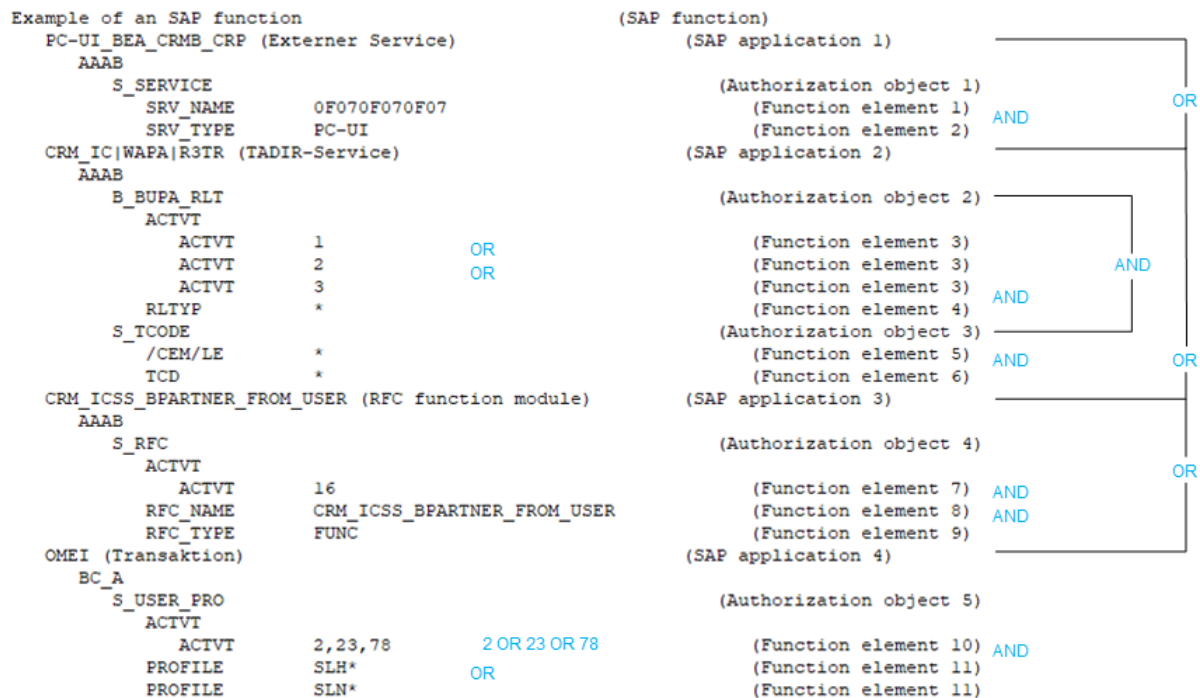
An SAP role or SAP profile matches an SAP function when

1. It has all the authorization objects for all SAP applications.
2. It has all the different authorization object function elements.
3. At least one of the instances is defined exactly same function element.

Example of authorization checking

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

Figure 2: Authorization definition



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 1 with authorization object 1 and function element 1 AND 2
- OR -
- SAP application 2 with authorization object 2 and function element 3 with the instance **1 OR 2 OR 3** AND function element 4
- AND -
with authorization object 3 and function element 5 AND 6
- OR -
- SAP application 3 with authorization object 4 and function element 7 AND 8 AND 9
- OR -
- SAP application 4 with authorization object 5 and function element 10 with the instance **2 OR 23 OR 78** AND function element 11 with the instance **SLH* OR SLN***.

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 1 and function element 1 AND 2
- AND -
- Authorization object 2 and function element 3 with the instance **1** OR **2** OR **3** AND function element 4
- AND -
- Authorization object 3 and function element 5 AND 6
- AND -
- Authorization object 4 and function element 7 AND 8 AND 9
- AND -
- Authorization object 5 and function element 10 with the instance **2** OR **23** OR **78** AND function element 11 with the instance **SLH*** OR **SLN***.

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 test identifies all SAP roles and profiles that have this non-compliant combination of authorizations.
2. Find all employees that have obtain non-compliant combinations of authorizations through their SAP user accounts.
Create SAP functions for compliant authorizations or combinations of authorizations. Create compliance rules for mutually exclusive SAP functions. The compliance check finds all employees that combine such non-compliant authorization combinations through 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 tested to see if existing authorizations (SAP roles and profiles) comply. SAP roles and profiles with non-compliant combinations of authorizations must be identified so that they can be modified to meet the new requirements.

An SAP function is created for each non-compliant authorization combination.

Table 5: Example of an authorization definition

SAP function	SAP application	Authorization objects	Field	Value
A	TR	BO2	ACTVT	*
	TR	BO2	Class	*
	TR	BO3	ACTVT	01, 02
	RF	BO5	ACTVT	*
	RF	BO5	RLTYP	R*
B	TR	BO3	ACTVT	*
	TR	BO4	ACTVT	02, 03, 07
	TR	BO4	Class	*

The following SAP roles are available:

Table 6: Defined SAP roles

SAP role	SAP application	Authorization objects	Field	Value
R1	TR	BO1	ACTVT	*
	TR	BO1	Class	*
	TR	BO3	ACTVT	*
	TR	BO4	ACTVT	01, 02
	TR	BO4	Class	DEF*
R2	TR	BO2	ACTVT	*
	TR	BO2	Class	*
	TR	BO3	ACTVT	*
R3	TR	BO4	ACTVT	03, 07
	TR	BO4	Class	*
R4	RF	BO5	ACTVT	03
	RF	BO5	RLTYP	*

SAP roles are found that match the SAP function during authorization testing.

Authorization test results:

- SAP function: B

Configuration parameter **TestWithoutTCD**: set or not set

The configuration parameter does not affect the result of the authorization test because only one SAP application is used in the SAP function.

Open SAP role: R1

The role R1 has all the authorization objects and fields named in the SAP function and at least one field characteristic.

Role R2 is missing authorization object BO4. Therefore it does not match the SAP function.

Role R3 is missing authorization object BO3. Therefore it does not match the SAP function.

The role R4 is missing authorization object BO3 and BO4. Therefore it does not match the SAP function.

- SAP function: A

Configuration parameter **TestWithoutTCD**: not set

Open SAP roles: R2, R4

The role R2 has all the authorization objects, fields, and characteristics named in SAP application TR.

The role R4 has all the authorization objects, fields, and characteristics named in SAP application RF.

The role R1 is missing the authorization object BO2 or BO5. Therefore it does not match the SAP function.

The role R3 does not have any of the named authorization objects. Therefore it does not match the SAP function.

- SAP function: A

Configuration parameter **TestWithoutTCD**: set

Open SAP roles: R2, R4

The role R1 is missing authorization object BO2 and BO5. Therefore it does not match the SAP function.

Role 2 is missing authorization object BO5. Therefore it does not match the SAP function.

The role R3 does not have any of the named authorization objects. Therefore it does not match the SAP function.

The role R4 is missing authorization object BO2 and BO3. Therefore it does not match the SAP function.

The SAP role R3 complies with the new policies and can still be used. The roles R1, R2, and R4 must be modified to comply to the new policies. If an authorization test is compliant without taking the SAP applications into account, only role R1 must be modified.

Example for use case 2

Now you need to run a test to ascertain which SAP user accounts do not conform to the new policies. To do this, you have to create compliance rules for the SAP functions.

Table 7: SAP user accounts used

Employees	SAP user accounts	SAP roles	Permissions
Clara Harris	K1	R1	BO1 ACTVT {*} BO1 CLASS {*} BO3 ACTVT {*} BO4 ACTVT {01, 02} BO4 CLASS {DEF*}
Ben King	K2	R2, R3	BO2 ACTVT {*} BO2 CLASS {*} BO3 ACTVT {*} BO4 ACTVT {03, 07} BO4 CLASS {*}
Jenny Basset	K3	R2	BO2 ACTVT {*} BO2 CLASS {*} BO3 ACTVT {*}
Jenny Basset	K4	R3	BO4 ACTVT {03, 07} BO4 CLASS {*}
Jan Bloggs	K5	R3	BO4 ACTVT {03, 07} BO4 CLASS {*}

The SAP roles R2 and R3 are assigned to user account K2. The user account obtains all the authorizations from both these roles. However, according to the new policies, an employee cannot own the authorizations BO3 and BO4 (SAP function B) at the same time. A compliance rule is created for this, which finds all employees matching the SAP function B (rule C1). Since neither role R2 nor role R3 matches this SAP function, a rule violation is not found.

In order for One Identity Manager to acknowledge the rule violation, SAP functions must be created for the conflicting authorization objects. As a result, the SAP functions that cause a rule violation are combined into a compliance rule.

Table 8: More SAP functions

SAP function	SAP application	Authorization objects	Field	Value
B	TR	BO3	ACTVT	*
	TR	BO4	ACTVT	02, 03, 07
	TR	BO4	Class	*
C	TR	BO3	ACTVT	*
D	TR	BO4	ACTVT	02, 03, 07
	TR	BO4	Class	*

Table 9: Compliance rules

Rule	Rule condition	Employee who violate rules
CR1	Employee owns SAP function B.	Clara Harris
CR2	The employee owns the SAP function C AND the employee own the SAP function D.	Clara Harris Ben King Jenny Basset

Jan Bloggs does not violate the compliance rule. The SAP role R3 matches the SAP function D but this only leads to a rule violation in combination with the SAP function C.

Related topics

- [Finding non-compliant authorizations](#) on page 15
- [Rule conditions for SAP functions](#) on page 46

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 consists of at least one SAP application. A least one authorization object belongs to an SAP application. 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. Use variables in the authorization definition to do this. Fixed variable values are grouped in variable sets and used in the function instances.

Notes on authorization definitions

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

- Click **+** to add an additional value for the ACTVT element to an authorization object. You can also write several permitted values for ACTVT elements as a comma delimited list.
- To add an additional value for another function element (for example, CLASS) to an authorization object, click **C** next to this function element. The permitted values of this function element cannot be entered as a comma delimited list. They must always appear as separate entries in the authorization definition.
- Authorization objects cannot be added more than once to an authorization definition. if you want to run a function test on the same authorization object with different instances, create a separate SAP function for each instance. Combine these SAP function in a compliance rule.

Detailed information about this topic

- [Creating authorization definitions in the Authorization Editor](#) on page 27
- [Finding non-compliant authorizations](#) on page 15

Related topics

- [Examples of SAP functions](#) on page 17
- [Rule conditions for SAP functions](#) on page 46

Using variables

You can set fixed values for function elements in authorization definitions. 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	Example for value in the SAP system
*	Any value	abc 1234
Any string (from)	Exact given value	abc
[*]	The value *	*
String[*] (abc[*])	Values beginning with the given string and ending with *	from*
String* (abc[*])	Values beginning with the given string and ending with any string	abc* abcd
Comma delimited list (abc, 1234, d*)	A value contained in the list	ab 1234 c* cde

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 27
- [Main data for a variable set](#) on page 39

Creating and editing function definitions

A working copy is added to the database for every function definition. Edit the working copies to create function definitions and change them. 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 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 **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.

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

- [General main data of a function definition](#) on page 25

General main data of a function definition

Enter the following main data of a function category.

Table 10: 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 calcu-

Property	Description
	lated for the original SAP function. To copy the value to a working copy, run the Create working copy task. 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 11
- [Maintaining SAP functions](#) on page 14
- [Mitigating controls for SAP functions](#) on page 49

Function definition overview

You can see 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.

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 by 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 by SAP application**

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

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

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

Only the enabled function definitions can be selected.

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

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

Table 11: 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 28.
Display value / lower limit	Display name for the function element's value, when a hash value is specified, for example.
Upper scope limit	Upper limit for the range of a function element Values can be added as variables.

Table 12: Syntax examples for values

Syntax (example)	SAP authorization is tested for	Example for value in the SAP system
*	Any value	abc 1234
Any string (from)	Exact given value	abc
[*]	The value *	*

Syntax (example)	SAP authorization is tested for	Example for value in the SAP system
String[*] (abc [*])	Values beginning with the given string and ending with *	from*
String* (abc [*])	Values beginning with the given string and ending with any string	from* abcd
Comma delimited list (abc, 1234, d*)	A value contained in the list Comma-delimited lists can only be used with ACTVT elements. This list is used like a string on other function elements.	abc 1234 c* cde
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 functions should only match when an SAP profile has one of several possible instances of one and the same function element, define this instance as a comma-delimited list of values for this function element.

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 13: Function element properties

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

- [Using variables](#) on page 23
- [Adding variable set for authorization objects](#) on page 38

Related topics

- [Notes on authorization definitions](#) on page 22

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 27

Authorization overview

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

To display an overview of all function elements

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

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 27

Creating working copi

To modify an existing function definition, you required a working copy of the function definition. The working copy can be created from the active function definition. The data of an existing working copy are overwritten with the data from the active function definition, after prompting.

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 31

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 copi](#) on page 31

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 14: 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

Property	Data field in the CSV file.
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 43
- [Exporting working copies](#) on page 33
- [Exporting function definitions](#) on page 42

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 15: 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 43
- [Exporting function definitions](#) on page 32
- [Exporting function definitions](#) on page 42

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 35
- [Creating mitigating controls for SAP functions](#) on page 36
- [Mitigating controls for SAP functions](#) on page 49

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 49

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 or 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.
- OR -
Click  in the result list.
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 a function instance](#) on page 37
- [Checking field variable definitions](#) on page 38
- [Function instance overview](#) on page 38

Main data for a function instance

Enter the following main data of a function instance:

Table 16: 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

- [Adding variable set for authorization objects](#) on page 38
- [Maintaining SAP functions](#) on page 14
- [Checking field variable definitions](#) on page 38

Function instance overview

You can see 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.

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 a function instance](#) on page 37

Adding variable set for authorization objects

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

To create or edit authorization objects

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.
- OR -
Click  in the result list.
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 39
- [Adding variables used in SAP functions](#) on page 41

Related topics

- [Creating authorization definitions in the Authorization Editor](#) on page 27
- [Variable set overview](#) on page 40
- [Copying variable sets](#) on page 41

Main data for a variable set

Enter the following main data of variable sets.

Table 17: 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 23

Related topics

- [Adding variables used in SAP functions](#) on page 41

Variable set overview

You can see 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.

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 39

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 39

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 18: 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

Property	Data field in the CSV file.
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 43
- [Exporting working copies](#) on page 33
- [Exporting function definitions](#) on page 32

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 19: Data fields for importing function definitions

Data field in the CSV file. (header)	Object properties in One Identity Manager
Function	Function definition
TransactionType	Suggested authorization value
Object	Authorization objects
Field	Authorization field

**Data field in the CSV file.
(header)**

Object properties in One Identity Manager

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 42
- [Exporting working copies](#) on page 33
- [Exporting function definitions](#) on page 32

Compliance rules for SAP functions

Compliance rules can be checked through effective authorizations as well as through authorizations, which an employee 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*

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 function to test.
 - 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 3: Condition for SAP functions

Condition

This rule will be violated by all employees

if the combination of all the employee's identities meets the following conditions:

+ X i The employee has at least one function from Maintain roles and profiles - T01 - 120 - DOKU DE

and the number of entitlements assigned to the employee is equal or higher than 1

When One Identity Manager tests rules, it finds all the employees 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*.

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 20: 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 employee 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 employee through which they violated the rule.
SAP roles	The report shows all SAP roles and profiles that match SAP functions and

Report	Description
and profiles with rule violations	thereby violate the selected rule.

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 35

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 not 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 risk mitigation controls, see the *One Identity Manager Risk Assessment Administration Guide*.

Detailed information about this topic

- [Entering main data for mitigating controls](#) on page 49
- [Mitigating controls overview](#) on page 50
- [Assigning function definitions to mitigating controls](#) on page 50
- [Calculating mitigating controls for SAP functions](#) on page 51

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 21: 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.

Mitigating controls overview

You can see 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.

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 35

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**.

Configuration parameters for SAP functions

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

Table 22: 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 not 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 <i>One Identity Manager Configuration Guide</i> .
TargetSystem SAPR3 SAPRights TestWithoutTCD	Checks SAP authorizations without taking SAP applications into account.

The following configuration parameters are also required.

Table 23: Configuration parameters for the module

Configuration parameter	Description
QER CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's 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 not 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 <i>One Identity Manager Configuration Guide</i>.
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 not 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 <i>One Identity Manager Configuration Guide</i>.

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 24: 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

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 25: Referenced tables and BAPIs

Tables	BAPI Calls
AUTHX	/VIAENET/LISTMENU01
OBJCT	AUTH_TRACE_GET_USOBHASH
TACT	RFC_READ_TABLE
TACTZ	
TFDIR	
TMENU01	
TMENU01R	
TMENU01T	
TOBJ	
TOBCT	
TSTCT	
USOBHASH	
USOBX_C	
USR10	
UST10S	
UST12	
USVART	

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

A

- application role
 - maintain SAP function 14
- authorization definition 27
 - add variable to variable set 41
 - authorization field 27
 - example 17
 - export 32
 - processing status 27
 - value 27
 - variable 27, 38-39
- Authorization Editor 27
- authorization objects 27

C

- compliance rule 5, 46

F

- field variable 39
- function category 11
- function definition 22
 - create 24
 - edit 24
 - export
 - all 42
 - single 32
 - manager 25
 - severity level 25
 - significance 25
 - working copy 24

- function instance 22, 36
 - test variable 38
- functional area 12

I

- Identity Audit 5

M

- mitigating control
 - assign (SAP function definition) 35
 - assign SAP function 36, 50
 - create 36
 - log 49
 - overview 50
 - SAP function 49
 - significance reduction 49

O

- overview form
 - function definition 26
 - function instance 38

P

- permission
 - verify 5
- plugin
 - SAP function 42-43
- project template 54

R

risk assessment
 functional area 12

risk index
 calculate 51
 reduced
 calculate 51

rule condition
 function 46

rule violation
 example 17

S

SAP function
 compliance rule 46

SAP application 27

SAP function 5
 apply 17
 function definition 25
 import 43
 manager 36-37

SAP function category 11

significance reduction 49

synchronization
 configure 9
 start 9
 synchronization project
 create 9

synchronization project
 create 9
 project template 54

system variable 23

T

transaction 27

U

user account
 reference user 46

V

variable 22
 check usage 38
 system variable 23
variable name 23
variable set 38
 accept variable 41
 copy 41
 overview form 40
 SAP function 37

W

working copy
 assign mitigating control 35
 create 31
 enable 31
 export function definition 33
 export permissions definition 33
 overview form 26