One Identity Manager 8.1.2

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

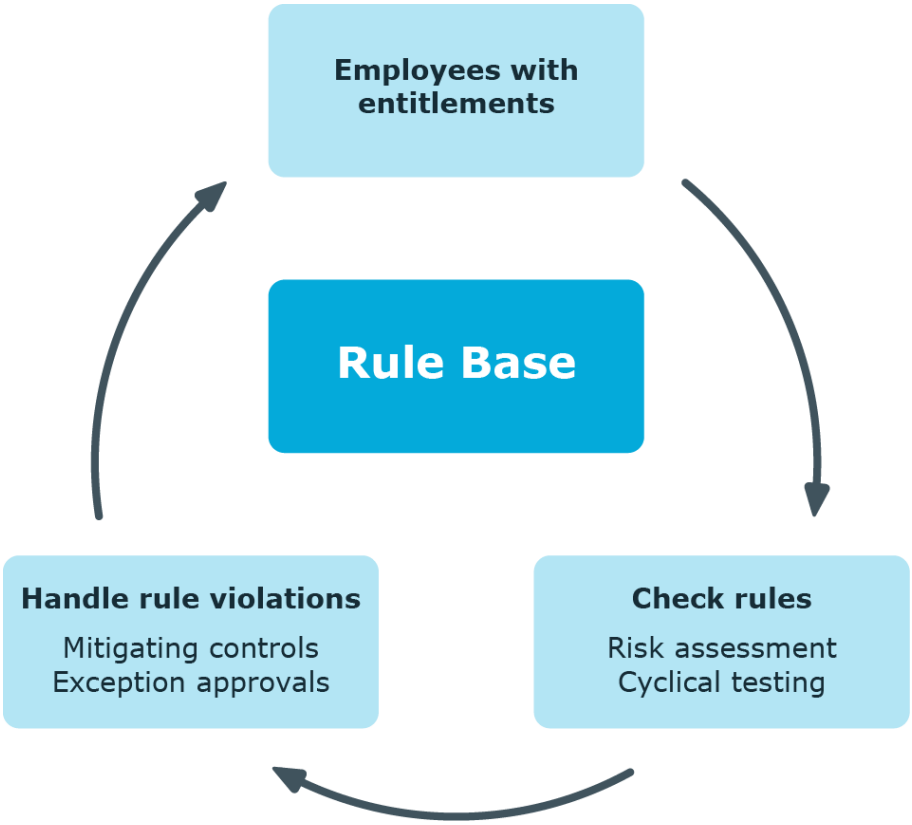
One Identity Manager Administration Guide for the SAP R/3 Compliance Add-on
Updated - January 2020
Version - 8.1.2

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 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 transactions permitted for a user account and the associated authorization objects. To do this you have to define the transactions and authorization objects you want to verify to be such SAP functions in the One Identity Manager. The SAP finds all the One Identity Manager roles and profiles that have exactly these authorization objects and transactions 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 detailed information about approval procedures in the IT Shop, see the One Identity Manager IT Shop Administration Guide.

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

NOTE: SAP R/3 Compliance Add-on Module and Compliance Rules Module must be 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 managing SAP functions.

Table 1: User

User	Task
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.

User	Task
	• 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	• 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. • Create and configure password policies as required.
Compliance & 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 polices.

Prerequisites for setting up SAP functions

Table 2: Configuration parameters for handling SAP functions

Configuration parameter	Meaning
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.
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.

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. Check in Designer that "QER\ComplianceCheck" and "TargetSystem\SAPR3\SAPRights" are set. Otherwise, set the configuration parameters and compile the database.
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

2

Setting up a synchronization project for synchronizing SAP authorization objects

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

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

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.

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

Detailed information about this topic

- One Identity Manager Administration Guide for Connecting to SAP R/3
- One Identity Manager Target System Synchronization Reference Guide

Related topics

- Appendix: Default project template for the SAP R/3 Compliance Add-on Module on page 51
- Appendix: Referenced SAP R/3 tables and BAPI calls on page 53

3

Basic data for SAP functions

The following base data is relevant for SAP Functions:

- Configuration parameter

  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 Appendix: Configuration parameters for SAP functions on page 50.

- 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. For more information, see Functional areas on page 12.

- Maintaining SAP functions

  An SAP function can be assigned to employees that manage the SAP functions and there for can edit the working copies. For more information, see Maintenance SAP functions on page 13.

SAP Function categories

Use function categories to group SAP functions by specific criteria.

To edit function categories

1. Select **Identity Audit | Basic configuration data | SAP Function categories**.
2. Select a function category in the result list. Select the **Change master data** task.

   - OR -

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

Enter the following master data for a function category.

Table 3: SAP function category properties

Property	Description
Category	The category item’s name.
Parent category	Parent category for organizing function categories hierarchically.
Description	Spare 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.

Example for using functional areas are:

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 edit functional areas

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 master data** task.

   - OR -

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

Enter the following data for a functional area.

Table 4: 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 in order to organize 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	Spare 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 on page 47

Maintenance SAP functions

You can assign SAP functions to employees that are responsible for the content of those SAP functions. A default application role exists for maintaining SAP functions in One Identity Manager. Assign the employees that are authorized to enable and edit working copies of this SAP function and to define function instances to this application role. 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 5: Default application roles for maintaining SAP functions

User	Task
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 specify a supervisor for maintaining SAP functions.

1. Select the category **Identity Audit | SAP functions | Function definition working copies**.
2. Select the function definition in the result list.
3. Select the **Change master data** task.
4. In the **Manager/supervisor** menu, select the application role.

   - OR -

   To create a new application role, click next to the **Manager/supervisor** menu.
   - Enter the application role name and assign the parent application role **Identity & Access Governance | Identity Audit | Maintain SAP functions**.
   - Click **OK** to add the new application role.
5. Save the changes.
6. Assign employees to this application role who are permitted to edit the function definition.

To add employees to an application role

1. Select the application role in **Identity Audit | Basic configuration data | Maintain SAP functions**.
2. Select **Assign employees**.
3. Assign the employees you want and save the changes.

Related topics

- General master data for a function definition on page 24

4

Finding non-compliant authorizations

Table 6: Configuration parameters for authorization checks

Configuration parameter	Description
TargetSystem\SAPR3\SAPRights\TestWithoutTCD	Checks SAP authorizations without taking SAP transactions into account.

SAP authorizations are verified on the basis of the transactions permitted for an SAP user account and the associated authorization objects. Authorization objects and transactions are grouped into single profiles. In order to check whether there are potentially dangerous authorizations in the company, define authorization objects and transactions as SAP functions. The One Identity Manager compares all authorization objects and transactions 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 and transactions assigned through single roles.

"TargetSystem\SAPR3\SAPRights\TestWithoutTCD" is evaluated by authorization checks. If the configuration parameter is not set (default case), the following rules apply to the authorization checks:

An SAP role or SAP profile matches an SAP function, when

1. It contains at least one of the transaction defined in the SAP function
2. It has all the authorization objects for this transaction
3. It has all the different authorization object function elements
4. At least one of the instances is defined exactly same function element.

An SAP role matches an SAP function if the SAP profile of this SAP role contains one the transactions defined in the SAP function. The SAP profile must have all this transaction'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.

These transactions are not taken into accounts during authorizations check if "TargetSystem\SAPR3\SAPRights\TestWithoutTCD" is set. In this case, the following rules apply for authorization checking:

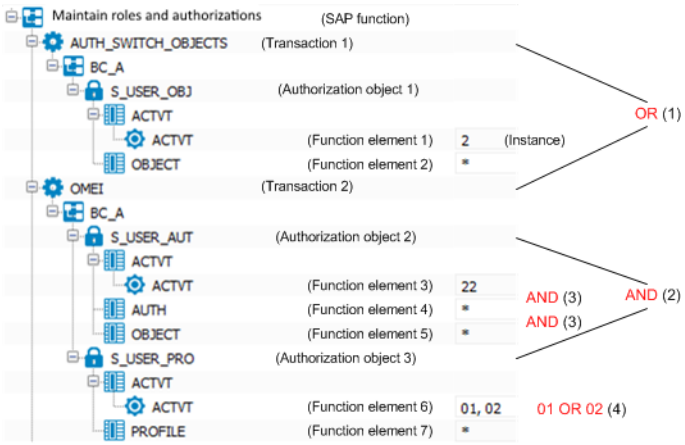
An SAP role or SAP profile matches an SAP function when

1. It has all the authorization objects for all transactions
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 transactions, authorization objects, and function elements.

Figure 2: Authorization definition



All SAP roles and SAP profiles with the authorizations listed below are found with the SAP function shown if the configuration parameter is not set.

- Transaction 1 with authorization object 1 and function element 1 with "02" OR "07" OR "21" AND Function elements 2

  - OR -

- Transaction 2 with authorization object 2 and function element 3, 4, AND 5

  - AND -

  with authorization object 3 and function element 6 with the instance "01" OR "02"AND function element 7 with instance "SLH" OR "SLN"

All SAP roles and SAP profiles with the authorizations listed below are found through SAP functions when the configuration parameter is set.

- Authorization object 1 and function element 1 with the instance "02" OR "07" OR "21" AND Function elements 2

  - AND -

- Authorization object 2 and function element 3, 4, AND 5

  - AND -

- Authorization object 3 and function element 6 with the instance "01" OR "02"AND function element 7 with 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 7: Example of an authorization definition

SAP function	Transaction	Authorization objects	Field	Value
A	T1	BO2	ACTVT	*
	T1	BO2	Class	*
	T1	BO3	ACTVT	01, 02
	T2	BO5	ACTVT	*
	T2	BO5	Class	RST*
B	T1	BO3	ACTVT	*
	T1	BO4	ACTVT	02, 03, 07
	T1	BO4	Class	*

The following SAP roles are available:

Table 8: Defined SAP roles

SAP role	Transaction	Authorization objects	Field	Value
R1	T1	BO1	ACTVT	*
	T1	BO1	Class	*
	T1	BO3	ACTVT	*
	T1	BO4	ACTVT	01, 02
	T1	BO4	Class	DEF*
R2	T1	BO2	ACTVT	*
	T1	BO2	Class	*
	T1	BO3	ACTVT	*
R3	T1	BO4	ACTVT	03, 07
	T1	BO4	Class	*
R4	T2	BO5	ACTVT	03
	T2	BO5	Class	*

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

Table 9: Authorization test results

SAP function	SAP role	"TestWithoutTCD"	Reason
B	R1	disabled | enabled	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. The configuration parameter does not affect the result of the authorization test because only one transaction is used in the SAP function.
A	R2, R4	Disabled	The role R2 has all the authorization objects, fields and characteristics named in transaction T1. The role R4 has all the authorization objects,

SAP function	SAP role	"TestWithoutTCD"	Reason
			fields and characteristics named in transaction T2. 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.
A		enabled	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 is compliant without taking the authorization test 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 10: 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 {*}

Employees	SAP user accounts	SAP roles	Permissions
			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 11: More SAP functions

SAP function	Transaction	Authorization objects	Field	Value
B	T1	BO3	ACTVT	*
	T1	BO4	ACTVT	02, 03, 07
	T1	BO4	Class	*
C	T1	BO3	ACTVT	*
D	T1	BO4	ACTVT	02, 03, 07
	T1	BO4	Class	*

Table 12: 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	Clara Harris

Rule	Rule condition	Employee who violate rules
	own the SAP function D.	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 44

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

- Authorization Editor on page 26
- Finding non-compliant authorizations on page 15

Related topics

- Examples of SAP functions on page 17
- Rule conditions for SAP functions on page 44

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 master data. An authorization definition consists of at least one transaction. A least one authorization object belongs to a transaction. 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 boundaries. 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.

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:

Table 13: Variables specification

Property	Specification
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.

<table>
<tr><th>Property</th><th>Specification</th></tr>
<tr><td>Value</td><td>
<table>
<tr><th>Syntax (example)</th><th>SAP authorization is tested for</th><th>Example for value in the SAP system</th></tr>
<tr><td>*</td><td>Any value</td><td>abc | 1234</td></tr>
<tr><td>Any string (from)</td><td>Exact given value</td><td>abc</td></tr>
<tr><td>[*]</td><td>The value *</td><td>*</td></tr>
<tr><td>String[*] (abc[*])</td><td>Value</td><td>from*</td></tr>
<tr><td>String* (abc[*])</td><td>Values beginning with the given string and ending with any string</td><td>abc* | abcd</td></tr>
<tr><td>Comma delimited list (abc, 1234, d*)</td><td>A value contained in the list</td><td>ab | 1234 | c* | cde</td></tr>
</table>
</td></tr>
</table>

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

- Authorization Editor on page 26
- Master data for a variable set on page 38

Creating 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 application role **Identity & Access Governance | Identity Audit | Maintain SAP functions** can edit existing working copies for which they are listed as responsible in the master data.

To create a new function definition

1. Select the category **Identity Audit | SAP functions | Function definitions**.
2. Click in the result list.
3. Enter the function definition master data.
4. Save the changes.

   This adds a working copy.
5. Select the **Activate working copy** task. Confirm the security prompt with **OK**.

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

To edit an existing function definition

1. Select the category **Identity Audit | SAP functions | Function definitions**.
   a. Select the function definition in the result list.
   b. Select **Create working copy** in the task view.

      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 -

   Select the category **Identity Audit | SAP functions | Function definition working copies**.
   a. Select a working copy in the result list.
   b. Select the **Change master data** task.
2. Edit the working copy's master data.
3. Save the changes.
4. Select the **Activate working copy** task. Confirm the security prompt with **OK**.

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

General master data for a function definition

Table 14: Configuration parameters for risk assessment of SAP functions

Configuration parameter	Effect when set
QER\CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is enabled, values for the risk index can be entered and calculated.

Enter the following master data for a function category.

Table 15: Master 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. The input 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 task **Create working copy**. The input field is only visible if the "QER\CalculateRiskIndex" configuration parameter is set. The value is calculated by the 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 ... only information 1 ... Every SAP user account that matches the SAP function requires changes to the affected SAP authorizations.
Significance	Enter a verbal description of the effects on the company (or the functional area) when an SAP user matches this SAP function. In the default installation value list is displayed with the entries {NONE, 'low', 'average', 'high', 'critical'}.

Property	Description
Description	Spare field for additional explanation.
Working copy	Specifies whether this is a working copy of the function definition.

Detailed information about this topic

- SAP Function categories on page 11
- Maintenance SAP functions on page 13
- Mitigating controls on page 47
- One Identity Manager Risk Assessment Administration Guide

Additional tasks for working copies

After you have entered the master data, you can run the following tasks.

Function definition overview

You can see the most important information about a working copy on the overview form.

To obtain an overview of a working copy

1. Select the category **Identity Audit | SAP functions | Function definition working copies**.
2. Select the function definition in the result list.
3. Select **Function definition**.

Authorization Editor

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

To compile an authorization definition

1. Select **Identity Audit | SAP Functions | Function definition working copies**.
2. Select the function definition in the result list.
3. Select **Authorization Editor**.

4. Select one of the following tasks.
   - **1. Add by menu template...**

     Table 16: Menu template properties

Property	Description
SAP Menu display	Menu items from the SAP GUI's SAP menu
All other menus	Menu items from all other SAP menus
System	SAP system to be used to display the menu tree
Menu	Menu tree for selecting menu items All the transaction and authorization objects are loaded that can be called from the selected menu items. Transaction codes that are linked to a menu item are shown in brackets in the menu tree as additional information.

   - OR -
   - **2. Add by transaction...**.

     Table 17: Properties of a transaction

Property	Description
Filter	Filter for list of available transactions
Transaction	Transactions whose authorization objects are to be loaded into the Authorization Editor All authorization object are added that are linked with the selected transaction.

   - OR -
   - **3. Add via authorization object...**.

     Table 18: Authorization object properties

Property	Description
Filter	Filter for list of available authorization objects
Authorization objects	Authorization objects to be loaded to the Authorization Editor All transactions that are linked to the authorization object are added.

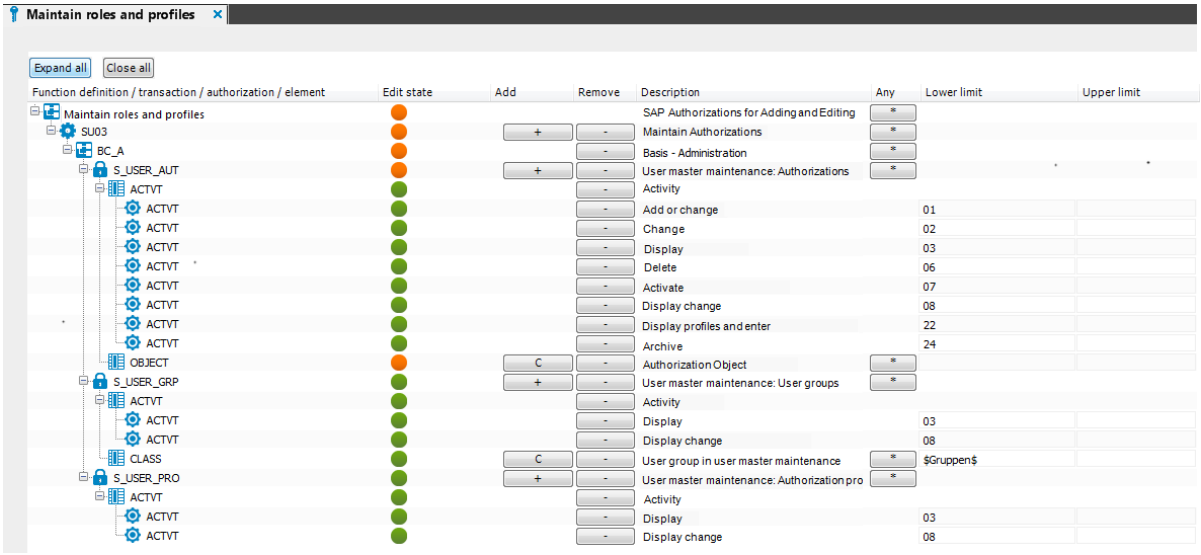
   - OR -

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

  Select an existing function definition whose authorization definition you want to load into the Authorization Editor.

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

Figure 3: Authorization Editor for SAP functions



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

Table 19: Properties of an authorization definition

Property	Description
Function definition / transaction / authorization / function element	Function definition hierarchy. Transactions, their associated authorization objects and function elements are mapped in a tree structure.
Processing status	Processing status of tree structure 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

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td></td><td>value).</td></tr>
<tr><td>Value / lower limit</td><td>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.
<table><tr><th>Syntax (example)</th><th>SAP authorization is tested for</th><th>Example for value in the SAP system</th></tr><tr><td>*</td><td>Any value</td><td>abc | 1234</td></tr><tr><td>Any string (from)</td><td>Exact given value</td><td>abc</td></tr><tr><td>[*]</td><td>The value *</td><td>*</td></tr><tr><td>String[*] (abc[*])</td><td>Value</td><td>from*</td></tr><tr><td>String* (abc[*])</td><td>Values beginning with the given string and ending with any string</td><td>abc* | abcd</td></tr><tr><td>Comma delimited list (abc, 1234, d*)</td><td>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.</td><td>ab | 1234 | c* | cde</td></tr><tr><td>Variable (Var)</td><td>Value stored in the variable</td><td></td></tr><tr><td>System variable ($var)</td><td>Value stored in the system variable</td><td></td></tr></table></td></tr>
<tr><td>Upper scope boundary</td><td>Upper limit for the range of a function element Values can be added as variables.</td></tr>
</table>

All function elements in a transaction 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 20: 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 22
- Creating variable sets on page 38

Related topics

- Notes on authorization definitions on page 21

Checking authorization objects for completeness

One Identity Manager uses this task to test whether all authorization objects that belong to a transaction occur in the authorization definition.

To test an authorization definition for completeness

1. Select **Identity Audit | SAP Functions | Function definition working copies**.
2. Select the function definition in the result list.
3. Select **Authorization Editor**.
4. Select **Check authorization objects for completeness**.

   Missing authorization objects are displayed in a separate window.
5. Enable **Add** on the authorization object you want to add to the authorization definition.
6. Close the window using the **OK** button.

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

Authorization overview

Function elements are displayed in a flat structure in the authorization overview. You can edit all the object properties here.

To display an overview of all function elements

1. Select **Identity Audit | SAP Functions | Function definition working copies**.
2. Select the function definition in the result list.
3. Select **Authorization overview**.

Enabling a working copy

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. Select **Identity Audit | SAP Functions | Function definition working copies**.
2. Select the function definition in the result list.
3. Select **Enable working copy**.
4. Confirm the security prompt with **OK**.

Mitigating controls

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:

- Active 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

- Set the configuration parameter "QER\CalculateRiskIndex" in the Designer.

Detailed information about this topic

- Assigning mitigating controls on page 32
- Creating mitigating controls on page 32
- Mitigating controls on page 47

Assigning mitigating controls

To assign mitigating controls to a function definition

1. Select the category **Identity Audit | SAP functions | Function definition working copies**.
2. Select the working copy in the result list.
3. Select **Assign mitigating controls** from the task list.
4. Double-click on a mitigating control in **Add assignments** to assign it.

   – OR –

   In the **Remove assignments** view, double-click on the mitigating control for which you want to delete the assignment.
5. Save the changes.

Creating mitigating controls

To create a mitigating control for SAP functions

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

Detailed information about this topic

- Mitigating controls on page 47

Exporting a working copy

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. Select **Identity Audit | SAP Functions | Function definition working copies**.
2. Select the function definition in the result list.
3. Select the **Change master data** task.
4. Select **Export...**
5. Specify the file name and storage location for the CSV file.
6. Click **Save**.

The following properties are exported:

Table 21: Exported master data for 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
Transactions	Transaction
Authorization objects	Object
Authorization fields	Field
Description of authorization field.	Field Description
Value/lower scope boundary	Value From
Upper scope boundary	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 42
- Exporting function definitions on page 41
- Exporting a function definition on page 35

Additional tasks for function definitions

After you have entered the master data, you can run the following tasks.

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. Select the category **Identity Audit | SAP functions | Function definitions**.
2. Select the function definition in the result list.
3. Select **Function definition**.

Authorization overview

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

To display an overview of all function elements

1. Select **Identity Audit | SAP functions | Function definitions**.
2. Select the function definition in the result list.
3. Select **Authorization overview**.

Creating a working copy

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. Select the category **Identity Audit | SAP functions | Function definitions**.
2. Select the function definition in the result list.
3. Select **Create working copy** in the task view.
4. Confirm the security prompt with **Yes**.

Exporting a function definition

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. Select **Identity Audit | SAP functions | Function definitions**.
2. Select the function definition in the result list.
3. Select the **Change master data** task.
4. Select **Export...**
5. Specify the file name and storage location for the CSV file.
6. Click **Save**.

The following properties are exported:

Table 22: Exported master data for 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
Transactions	Transaction
Authorization objects	Object
Authorization fields	Field
Description of authorization field.	Field Description
Value/lower scope boundary	Value From
Upper scope boundary	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 42
- Exporting a working copy on page 33
- Exporting function definitions on page 41

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 edit function instances

1. Select **Identity Audit | SAP Functions | Function instances**.
2. Select a function instance in the result list. Select the **Change master data** task.

   - OR -

   Click in the result list.
3. Edit the function instance's master data.
4. Save the changes.

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

Master data for a function instance

Enter the following master data for a function instance:

Table 23: 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	Spare field for additional explanation. The function definition description is copied to a new function instance.

Property	Description
Function Instance Elements	Displays transactions, 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 variable sets on page 38
- Maintenance SAP functions on page 13

Additional tasks for function instances

After you have entered the master data, you can run the following tasks.

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. Select **Identity Audit | SAP Functions | Function instances**.
2. Select the function instance in the result list.
3. Select **Function instance**.

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. Select **Identity Audit | SAP Functions | Function instances**.
2. Select the function instance in the result list.

3. Select the **Change master data** task.
4. Select **Check variable definitions**.

Creating variable sets

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

To edit variable sets

1. Select the category **Identity Audit | SAP functions | Variable sets**.
2. Select a variable set in the result list. Select the **Change master data** task.

   - OR -

   Click in the result list.
3. Edit the variable set's master data.
4. Save the changes.

Master data for a variable set

Enter the following master data for variable sets.

Table 24: Master 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	Spare field for additional explanation.
SAP field variables	List of defined variables.

To edit field variables

1. To add a line in the list, click **Add variable**.

Table 25: Variable Properties

Property	Description
Variable	Name of the variable in `${alphanum}+$`. 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	Spare field for additional explanation.
Authorization objects	Reference to the authorization object in which the variable will be used

2. To delete marked variable from the list, click **Remove selected**.

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.

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 22

Additional tasks for variable sets

After you have entered the master data, you can run the following tasks.

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. Select the category **Identity Audit | SAP functions | Variable sets**.
2. Select the variable set in the result list.
3. Select **Variable set overview**.

Copying a variable set

To copy a variable set

1. Select the category **Identity Audit | SAP functions | Variable sets**.
2. Select the variable set in the result list.
3. Select the **Change master data** task.
4. Select **Copy variable set**.
5. Click **Yes** to immediately edit the copy's master data.
6. Edit the copy's master data.
7. Save the changes.

Applying used variables

Variables used in SAP functions can be transferred to variable sets.

To transfer variables to a variable set

1. Select **Identity Audit | SAP Functions | Variable sets**.
2. Select the variable set in the result list.
3. Select the **Change master data** task.
4. Select **Apply chosen variables...**.
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 variable from the selected function definitions are add to the list of field variables.
7. Edit the variables.
8. Save the changes.

Plug-ins for SAP functions

There are two plugins available for SAP functions. Run **Plugins** from the menu bar. You can use the plugins to swap existing SAP functions in the One Identity Manager database between different One Identity Manager databases.

Exporting function definitions

To export all function definitions to a CSV file

1. Select **Identity Audit**.
2. Select **Plugins | Export all** SAP-
3. Click **Yes** to export only working copies.

   - OR -

   Click **No** to export only enabled SAP functions.
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 26: Exported master data for 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
Transactions	Transaction
Authorization objects	Object
Authorization fields	Field
Description of authorization field.	Field Description
Value/lower scope boundary	Value From
Upper scope boundary	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 supervisors can only export those function definitions for which they are responsible, as entered in the master data.

Related topics

- Importing function definitions on page 42
- Exporting a working copy on page 33
- Exporting a function definition on page 35

Importing function definitions

A plugin is available to import SAP functions from an existing CSV file. The functions 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 27: Data fields for importing function definitions

Data field in the CSV file. (header)	Object Properties in One Identity Manager
Compulsory fields:	
Function	Function definition
Transaction	Transaction
Object	Authorization objects
Field	Authorization field
Value From	Value/lower scope boundary
Value To	Upper scope boundary
State	No equivalent The import status controls which data records are imported into One Identity Manager. 1 ... import
Optional fields:	
Process	Category
Function Description	Description of the function definition.
Risk Level	Significance Possible values are {Low|Medium|High|Critical}.
Field Description	Describes the authorization fields, authorization objects and transactions.

NOTE: The order of the data fields is arbitrary. Ensure that all required data fields are defined in the header and exist 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. Select **Identity Audit**.
2. Select **Plugins | ImportSAP function definitions...**.
3. Select the CSV file to import. 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.

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 detailed information about compliance rules, see the One Identity Manager Compliance Rules Administration Guide.

Rule conditions for SAP functions

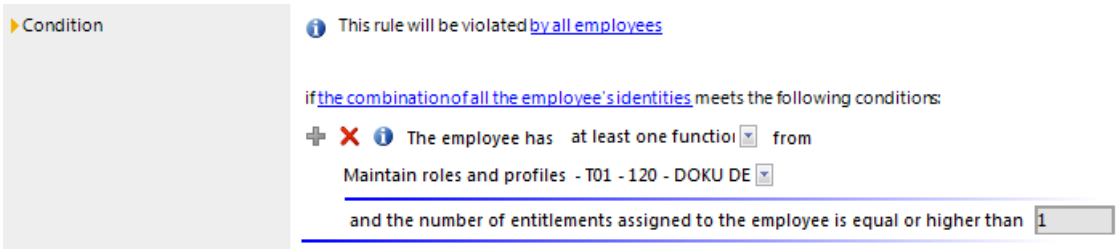
To define new rules for SAP functions

1. Select the category **Identity Audit | Rules**.
2. Click in the result list.
3. Enter the master data for the rule.
4. Set the option **Rule for cyclical testing and risk analysis in IT Shop**.
5. Limit the affected permissions with the option **at least one function** 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 **Enable working copy**. Confirm the security prompt with **OK**.

   This adds an enabled rule in the database. The working copy remains and can be used for making changes to the rule later.

Figure 4: Condition for SAP Functions



When the 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.

Detailed information about this topic

- One Identity Manager Compliance Rules Administration Guide

More rule violation reports

Table 28: Reports about Rule Violations

Report	Description
Rule violations with SAP transactions	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 transaction for each employee through which they violated the rule. SAP profiles and their authorization objects that match the SAP function are displayed for each transaction.
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.

Mitigating controls for compliance rules

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.

Mitigating controls

Table 29: Configuration parameter for risk assessment

Configuration parameter	Effect when set
QER\CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is enabled, values for the risk index can be entered and calculated.

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 compliance SAP compliance was violated, function is met. 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.

Detailed information about this topic

- One Identity Manager Risk Assessment Administration Guide

Entering master data

To 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 master data** task.

   - OR -

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

Enter the following master data for mitigating controls.

Table 30: General master data for 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.

Additional tasks for mitigating controls

After you have entered the master data, you can run the following tasks.

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. Select **Risk index functions**.
2. Open **Mitigating controls**.

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

Assigning function definitions

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. Select the **Risk index functions | Mitigating controls** category.
2. Select the mitigating control in the result list.
3. Select the **Assign function definitions** task.
4. In **Add assignments**, double-click the function definitions you want to assign.

   - OR -

   In **Remove assignments**, double-click the function definitions whose assignment is to be deleted.
5. Save the changes.

Calculating mitigation

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**.

Appendix: Configuration parameters for SAP functions

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

Table 31: 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.
TargetSystem\SAPR3\SAPRights\TestWithoutTCD	Checks SAP authorizations without taking SAP transactions into account.

Appendix: 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 packages and transactions. The template uses mappings for the following schema types.

Table 32: 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
Transaction	SAPTransaction
TACT	SAPActivity
objectHasField	SAPAuthObjectHasField
ObjectHasActivity	SAPAuthObjectHasSapActivity
FieldHasRcTable	SAPFieldHasSAPRCTable
tMenu01	SAPMenu

Schema Type in the Target System	Table in the One Identity Manager Schema
menuHasTransaction	SAPMenuHasSAPTransaction
ProfileHasAuthObjectField	SAPProfileHasAuthObjectElem
RcTable	SAPRCTable
RcVariable	SAPRCVariable
TRANSACTIONHASTOBJ	SAPTransactionHasSAPAuthObject

Appendix: 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 executed. 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 33: Referenced tables and BAPIs

Tables	BAPI Calls
• AUTHX • DD04L • DD07L • TACT • TACTZ • TMENU01 • TMENU01R • TOBJ • TOBCT • TSTCT • USOBT_C • USR10 • UST10S • UST12 • USVART	• RFC_READ_TABLE

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

S

T

U

V

W