One Identity Manager 8.0.4

Compliance Rules Administration Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

One Identity Manager Compliance Rules Administration Guide
Updated - September 2019
Version - 8.0.4

Contents

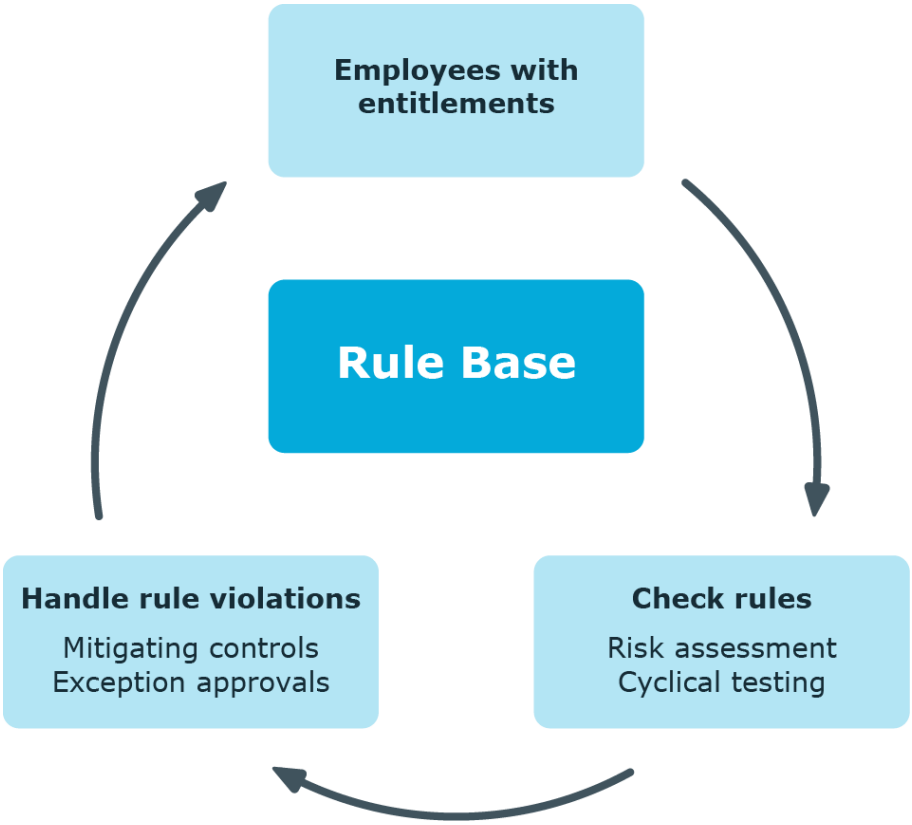
Compliance Rules and Identity Audit

Table 1: Configuration Parameters for Identity Audit

Configuration parameter	Meaning
QER\ComplianceCheck	Preprocessor relevant configuration parameter to control component parts for Identity Audit. Changes to the parameter require recompiling the database. If the parameter is set the components can be used.

The 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



Simple rule examples are:

- An employee may not obtain two entitlements A and B at the same time.
- Only employees with a particular department can have a particular entitlement.
- Every user account has to have a manager assigned to it.

You can use the identity audit function of the One Identity Manager to:

- Define rules for any employee assignments
- Evaluate the risk of possible rule violations
- Specify mitigating controls
- Initiate regular or spontaneous rule checks
- Detailed testing of edit permissions for employees within an SAP client (using SAP functions)
- Evaluate rule violations with differing criteria
- Create reports about rules and rule violations

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

To use the identity audit function

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

One Identity Manager Users for the Identity Audit

The following users are included in managing the rule base and editing rule violations.

Table 2: User

User	Task
Administrators for Identity Audit	Administrators must be assigned to the application role **Identity & Access Governance | Identity Audit | Administrators**. Users with this application role: • Enter base data for 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. • 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.
Rule supervisors	Rule supervisors must be assigned to the application role **Identity & Access Governance | Identity Audit | Rule supervisors** or to a child role. Users with this application role: • Are responsible for compliance rule content, for example, an auditor or a auditing department. • Edit the compliance rule working copies, which are assigned to the application role. • Enable and disable compliance rules. • Can start rule checking and view rule violations as required. • Assign mitigating controls.
One Identity	• Create customized permissions groups for application roles for

User	Task
Manager administrators	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, as required. • Enable or disable additional configuration parameters in the Designer, as required. • Create custom processes in the Designer, as required. • Create and configures schedules, as required. • Create and configure password policies, as required.
Exception approvers	Administrators must be assigned to the application role **Identity & Access Governance | Identity Audit | Exception approvers** or to a child role. Users with this application role: • Edit rule violations in the Web Portal. • Can grant exception approval or revoke it in the Web Portal.
Compliance rules attestors	Attestors must be assigned to the application role **Identity & Access Governance | Identity Audit | Attestors**. Users with this application role: • Attest compliance rules and exception approvals in the Web Portal for which they are responsible. • Can view master data for these compliance rules but not edit them. NOTE: This application role is available if the module Attestation Module is installed.
Compliance & Security officers	Compliance and security officers must be assigned to the application role **Identity & Access Governance | Compliance & Security Officer.** 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 and risk index functions. • Edit attestation polices
Auditors	Auditors are assigned to the application role **Identity & Access Governance | Auditors**. Users with this application role: • See the Web Portal all the relevant data for an audit.

Base Data for Setting up Rules

Various basic data is required to create rules, run rule checks and handle rule violation.

Rule groups:	Rule groups on page 10
Compliance frameworks:	Compliance Frameworks on page 12
Extended properties:	Extended Properties and Property Groups on page 17
Schedules:	Schedules for Checking Rules on page 13
Functional areas:	Functional Areas on page 21
Attestors:	Attestors on page 22
Rule supervisors:	Rule supervisor on page 23
Exception approvers:	Exception approver on page 25
Standard reasons:	Standard Reasons on page 26
Mail templates:	Creating Custom Mail Templates for Notifications on page 68

Rule groups

Use rule groups to group rules by functionality, for example, to group account policies or separate functions ("Segregation of duties").

To edit a rule group

1. Select the category **Identity Audit | Basic configuration data | Rule groups**.
2. Select a rule group in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Edit the master data for the rule group.
4. Save the changes.

Enter the following data for a rule group

Table 3: Rule Group Properties

Property	Description
Group name	Name of the rule group.
Description	Spare text box for additional explanation.

Property	Description
Parent group	Rule group above this one in a hierarchy. To organize rule groups hierarchically, select the parent rule group in the menu.

Additional Tasks for Rule Groups

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

In the report **Rule violation overview** you can get an overview of all rule violations for a rule group.

Overview of Rule Groups

You can see the most important information about a rule group on the overview form.

To obtain an overview of a rule group

1. Select the category **Identity Audit | Basic configuration data | Rule groups**.
2. Select the rule group in the result list.
3. Select **Rule group overview** in the task view.

Assign Rules

Use this task to specify which compliance rules belong to the selected rule group.

To assign compliance rules to a rule group

1. Select the category **Identity Audit | Basic configuration data | Rule groups**.
2. Select the rule group in the result list.
3. Select the task **Assign rules**.
4. Double-click in **Add assignments** on the compliance rules to be assigned.

   – OR –

   Double-click in **Remove assignments** on the compliance rule assignments to be removed.
5. Save the changes.

Compliance Frameworks

Compliance frameworks are used for classifying attestation policies, compliance rules and company policies according to regulatory requirements.

Compliance frameworks can be organized hierarchically. To do this, assign a parent framework to the compliance frameworks.

To edit compliance frameworks

1. Select the category **Identity Audit | Basic configuration data | Compliance frameworks**.
2. Select the compliance framework from the result list. Select **Change master data** in the task view.

   – OR –

   Click **New** in the result list toolbar.

   This opens a master data form for a compliance framework.
3. Edit the compliance framework master data.
4. Save the changes.

Enter the following properties for compliance frameworks.

Table 4: Compliance Framework Properties

Property	Description
Compliance framework	Name of the compliance framework.
Parent framework	Parent compliance framework in the framework hierarchy. Select an existing compliance framework in the menu to organize compliance frameworks hierarchically.
Managers	Application role whose members are allowed to edit all compliance rules assigned to this compliance framework.
Description	Spare text box for additional explanation.

Additional Tasks for Compliance Frameworks

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

In the report **Rule violation overview** you can get an overview of all rule violations for a compliance framework.

The Compliance Framework Overview

You can see the most important information about a compliance framework on the overview form.

To obtain an overview of a compliance framework

1. Select the category **Identity Audit | Basic configuration data | Compliance frameworks**.
2. Select the compliance framework from the result list.
3. Select **Compliance framework overview** in the task view.

Assign Rules

Use this task to specify which compliance rules are included by the selected compliance framework.

To assign a compliance rule to compliance frameworks

1. Select the category **Identity Audit | Basic configuration data | Compliance frameworks**.
2. Select the compliance framework from the result list.
3. Select the task **Assign rules**.
4. Double-click in **Add assignments** on the compliance rules to be assigned.

   – OR –

   Double-click in **Remove assignments** on the compliance rule assignments to be removed.
5. Save the changes.

Schedules for Checking Rules

Cyclical checking of all rules is controlled through schedules. One Identity Manager provides two default schedules for rule checking. This ensures that the auxiliary table for object assignments are regularly updated and that rule checking is started. You can set up more schedules to do this. Ensure that the schedules are assigned to the rules.

To edit schedules

1. Select the category **Identity Audit | Basic configuration data | Schedules**.

   The result list shows exactly those schedules configured for the table `ComplianceRule`.
2. Select a schedule in the result list. Select **Change master data** in the task view.

   – OR –

Click in the result list toolbar.

3. Edit the schedule's master data.
4. Save the changes.

Enter the following properties for a schedule.

Table 5: Schedule Properties

Property	Meaning
Name	Schedule ID. Translate the given text using the button.
Description	Detailed description of the schedule. Translate the given text using the button.
Enabled	Specifies whether the schedule is enabled or not. NOTE: Only active schedules are executed.
Time zones	Unique identifier for the time zone that is used for executing the schedule. Select either "Universal Time Code" or one of the time zones. NOTE: When you add a new schedule, the time zone is preset to that of the client from which you started the Manager.
Start (date)	The day on which the schedule should be run for the first time.
Validity period	Period within which the schedule is executed. • If the schedule will be run for an unlimited period, select the option **Unlimited duration**. • To set a validity period, select the option **Limited duration** and enter the day the schedule will be run for the last time in **End (date)**.
Occurs	Interval in which the task is executed. Valid interval types are "Every minute", "Hourly", "Daily", "Weekly", "Monthly" and "Yearly". Specify the exact weekday for the interval type "Weekly". Specify the day of the month (1st - 31st) for the interval type "Monthly". Specify the day of the year (1 - 366) for the interval type "Yearly". NOTE: Schedules that have the sub-interval "31" and interval type "monthly" are run on the "31st of the month". The task is, therefore, only run in months with 31 days. The same is true of the interval type "yearly" and the sub-interval "366".
Start time	Fixed start time for the interval types "daily", "weekly", "monthly" and "yearly". Enter the time in local format for the chosen time zone. The start time for interval types "Every minute" and "Hourly" is calculated from the rate of occurrence and the interval type.
Repeat every	Rate of occurrence for executing the schedule within the selected time interval. Select at least one weekday for the interval type "Weekly".

Property	Meaning
Last planned run/Next planned run	Execution time calculated by the DBQueue Processor. They are recalculated each time a schedule is run. The time of the next run is calculated from the interval type, rate of occurrence and the start time. NOTE: The One Identity Manager provides the start information in the time zone of the client where the program was started. Changes due to daylight saving are taken into account.

Default Schedules

The One Identity Manager provides the following schedules for Identity Audit.

Table 6: Default Schedules

Calculation schedule	Description
default schedule compliance rule check	Default schedule for checking rules. This schedule generates a DBQueue Processor processing task for each rule for checking rules at regular intervals.
default schedule compliance rule fill	Default schedule for filling auxiliary tables. Auxiliary table for object assignments are evaluated to determine potential rule violations in the Web Portal. These auxiliary tables are regularly updated by the DBQueue Processor. This task generates processing tasks, on a cyclical basis, for updating the auxiliary table.

Related Topics

- Checking a Rule on page 55
- Determining Potential Rule Violations on page 67

Additional Tasks for Schedules

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

The Schedule Overview

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

To obtain an overview of a schedule

1. Select the category **Identity Audit | Basic configuration data | Schedules**.
2. Select the schedule in the result list.
3. Select **Schedule overview** in the task view.

Assign Rules

Use this task to assign compliance rules to the selected schedule, which will check them. By default, the schedules "default schedule compliance rule file" and "default schedule compliance rule check" are assigned to a rule. You can use the assignments form to assign any rule to the selected schedule.

To assign the schedule to rules

1. Select the category **Identity Audit | Basic configuration data | Schedules**.
2. Select the schedule in the result list.
3. Select **Assign rules (for filling)** in the task view.

   - OR -

   Select **Assign rules (for testing)** in the task view.
4. Double-click on the rule you want to assign in **Add assignments**.
5. Save the changes.

To change an assignment

1. Select the category **Identity Audit | Basic configuration data | Schedules**.
2. Select the schedule in the result list.
3. Select **Assign rules (for filling)** in the task view.

   - OR -

   Select **Assign rules (for testing)** in the task view.
4. Select **Show objects already assigned to other objects** in the assignment form context menu.

   This shows rules that are already assigned in other schedules.
5. Double-click on one of these rules in **Add assignments**.

   The rule is assigned to the currently selected schedule.
6. Save the changes.
7. To put the changes into effect, enable the working copy.

NOTE: Assignments cannot be removed. Schedule assignments are compulsory for rules.

Related Topics

- Enabling Working Copies on page 38
- Default Schedules on page 15
- Extended Rule Input on page 32

Starting Schedules Immediately

To start a schedule immediately

1. Select the category **Identity Audit | Basic configuration data | Schedules**.
2. Select the schedule in the result list.
3. Select **Start immediately** from the task view.

   A message appears confirming that the schedule was started.

Extended Properties and Property Groups

You can use extended properties to access properties in rule conditions that are not mapped in the One Identity Manager data model. It may be necessary, depending on the range of rule base, to maintain a large number of extended properties. Therefore, you can group properties into property groups.

To assign extended properties

1. First, set up a property group, under which the extended properties will be grouped.
2. Set up the extended properties in the property group.
3. Assign the extended properties to the objects.

   There can be any number of objects of different object types assigned to an extended property at this point.

Create Property Groups

Property groups are used to group extended properties. Each extended property must be assigned to at least one property group. Furthermore, you can assign the extended properties to any other property groups.

To create a property group

1. Select the category **Identity Audit | Basic configuration data | Extended properties**.
2. Click in the result list toolbar.

3. Enter a name and description for the property group.
4. Save the changes.

To assign extended properties to a property group

1. Select the category **Identity Audit | Basic configuration | Extended properties**.
2. Select a property group in the result list.
3. Select **Assign extended properties** in the task view.
4. Assign extended properties in **Add assignments**.

   - OR -

   Remove extended properties from **Remove assignments**.
5. Save the changes.

Edit Extended Properties

To edit an extended property

1. Select the category **Identity Audit | Basic configuration data | Extended properties | <property group>**.
2. Select the extended property in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Edit the extended property's master data.
4. Save the changes.

Extended Property Master Data

Enter the following data for an extended property.

Table 7: Extended Property Master Data

Property	Description
Extended property name	Name of the extended property.
Property group	The property group for structuring extended properties. You can assign a primary property group to a property on the master data form. Extended properties are grouped by this property group in navigation. If an extended property needs to be assigned to several property groups,

Property	Description
	then you can use the task **Assign property groups** to assign additional property groups.
Lower scope boundary	Lower scope boundary for further subdivision.
Upper scope boundary	Upper scope boundary for further subdivision.
Description	Spare text box for additional explanation.
Spare fields no. 01.....spare field no. 10	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Detailed information about this topic

- Specifying Scoped Boundaries on page 19

Specifying Scoped Boundaries

You can subdivide extended properties by specifying scoped boundaries. You are not obliged to enter scoped boundaries. If you do enter a lower boundary you are not required to enter an upper one. However, if you specify an upper boundary, you have to enter a lower one.

Take note of the following when defining scoped boundaries:

- Basically, any string is permitted as a lower or upper scoped boundary.
- You can use * as a wildcard for any number of characters (even null).
- Wild cards can only be added to the end of a string, for example, AB*. Strings such as *AB or A*B are not allowed, for example.
- If you enter a lower boundary without a wildcard, you cannot use a wildcard in the upper boundary.

The following restrictions apply for the length of the string:

- If you enter a lower and upper boundary without a wildcard, the strings have to be the same length, for example, lower boundary 123/upper boundary 456. A lower boundary of 123 and an upper of 45, for example, is not permitted or a lower boundary 123/upper boundary 4567 is also not allowed.
- If you use a wildcard in the lower boundary but none in the upper boundary, then the length of the upper boundary string needs to be the same as or bigger than the string in the lower boundary.
- If you use a wildcard in the lower and upper boundary, they have to be the same length, for example, lower boundary 123*/upper boundary 456*. A lower boundary

of 123* and an upper of 45*, for example, is not permitted or a lower boundary 123*/upper boundary 4567* is also not allowed.

Additional Tasks for Extended Properties

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Extended Property Overview

Use this task to obtain an overview of the most important information about an extended property. For this you need to take into account the affiliation of the extended property to the different One Identity Manager objects.

To obtain an overview of an extended property

1. Select the category **Identity Audit | Basic configuration data | Extended properties | <property group>**.
2. Select the extended property in the result list.
3. Select **Extended property overview** in the task view.

To obtain an overview of a property group

1. Select the category **Identity Audit | Basic configuration data | Extended properties**.
2. Select a property group in the result list.
3. Select the task **Property group overview** in the task view.

Assign Objects

You can assign extended properties to company resources, hierarchical roles and employees.

To assign objects to an extended property

1. Select the category **Identity Audit | Basic configuration data | Extended properties | <property group>**.
2. Select the extended property in the result list.
3. Select **Assign objects** in the task view.
4. Select the desired object type in **Select object type**.

   The object belonging to the object types are displayed on the form.

5. Assign objects in **Add assignments**.

   - OR -

   Remove objects in **Remove assignments**.
6. Save the changes.

Assign Property Groups

Each extended property must be assigned to at least one property group. Furthermore, you can assign the extended properties to any other property groups.

To assign an extended property to a property group

1. Select the category **Identity Audit | Basic configuration data | Extended properties | <property group>**.
2. Select the extended property in the result list.
3. Select **Assign property groups** in the task view.
4. Assign property groups in **Add assignments**.

   - OR -

   Remove property groups in **Remove assignments**.
5. Save the changes.

Functional Areas

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

The risk of rule violation should be analyzed 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. Define assessment criteria for the functional areas.
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. Select the category **Identity Audit | Basic configuration data | Functional areas**.
2. Select the functional area in the result list. Select **Change master data** in the task view.

   - OR -

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

Enter the following data for a functional area.

Table 8: 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 text box for additional explanation.

Attestors

Installed Module: Attestation Module

Employees that can be used to attest attestation procedures can be assigned to compliance rules. Assign an application role for attestors to the compliance rules. Assign employees to this application role that are authorized to attest compliance rules.

A default application role for attestors is available in One Identity Manager. You may create other application roles as required. For more information about application roles, see One Identity Manager Application Roles Administration Guide.

Table 9: Default Application Roles for Attestors

User	Task
Attestors for Identity Audit	Attestors must be assigned to the application role **Identity & Access Governance	Identity Audit	Attestors**. Users with this application role:

User	Task
	• Attest compliance rules and exception approvals in the Web Portal for which they are responsible. • Can view master data for these compliance rules but not edit them. NOTE: This application role is available if the module Attestation Module is installed.

To edit attestors

1. Select the category **Identity Audit | Basic configuration data | Attestors**.
2. Select **Change master data** in the task view.

   - OR -

   Select an application role in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Edit the application role's master data.

Property	Value
Parent application role	Assign the application role **Identity & Access Governance | Identity Audit | Attestors** or a child application role.

4. Save the changes.
5. Select the task **Assign employees**, to add members to the application role.
6. Assign employees in **Add assignments**.

   - OR -

   Remove employees from **Remove assignments**.
7. Save the changes.

Rule supervisor

You can assign compliance rules to employees that are responsible for rule content. This may be an auditor or a auditing department, for example. To do this, assign compliance rules to an application role for rule supervisors. Assign employees to this application role, who are authorized to edit working copies of compliance rules.

A default application role for target system managers is available in One Identity Manager. You may create other application roles as required. For more information about application roles, see the One Identity Manager Application Roles Administration Guide.

Table 10: Default Application Role for Rule Supervisors

User	Task
Rule Supervisors	Rule supervisors must be assigned to the application role **Identity & Access Governance | Identity Audit | Rule supervisors** or to a child role. Users with this application role: • Are responsible for compliance rule content, for example, an auditor or a auditing department. • Edit the compliance rule working copies, which are assigned to the application role. • Enable and disable compliance rules. • Can start rule checking and view rule violations as required. • Assign mitigating controls.

To edit a rule supervisor

1. Select the category **Identity Audit | Basic configuration data | Rule supervisors**.
2. Select **Change master data** in the task view.

   - OR -

   Select an application role in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Edit the application role's master data.

Property	Value
Parent application role	Assign the application role **Identity & Access Governance | Identity Audit | Rule supervisors** or a child application role.

4. Save the changes.
5. Select the task **Assign employees**, to add members to the application role.
6. Assign employees in **Add assignments**.

   - OR -

   Remove employees from **Remove assignments**.

7. Save the changes.

Exception approver

Employees who can issue exception approvals for rule violations can be assigned to compliance rules. To do this, assign an application role for exception approvers to the compliance rule. Assign those employees who are entitled to approve rule violation exceptions to this application role.

A default application role for exception approvers is available in One Identity Manager. You may create other application roles as required. For more information about application roles, see the One Identity Manager Application Roles Administration Guide.

Table 11: Default Application Role for Exception Approvers

User	Task
Exception Approvers	Administrators must be assigned to the application role **Identity & Access Governance | Identity Audit | Exception approvers** or to a child role. Users with this application role: • Edit rule violations in the Web Portal. • Can grant exception approval or revoke it in the Web Portal.

To edit an exception approver

1. Select the category **Identity Audit | Basic configuration data | Exception approvers**.
2. Select **Change master data** in the task view.

   - OR -

   Select an application role in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
3. Edit the application role's master data.

Property	Value
Parent application role	Assign the application role**Identity & Access Governance | Identity Audit | Exception approvers** or a child application.

4. Save the changes.
5. Select the task **Assign employees**, to add members to the application role.

6. Assign employees in **Add assignments**.

   - OR -

   Remove employees from **Remove assignments**.
7. Save the changes.

Related Topics

- Granting Exception Approval on page 61

Standard Reasons

In the Web Portal, you can enter reasons, which provide explanations for individual approval decisions of the exception approvals. You can freely formulate this text. You also have the option to predefine reasons. The exception approver selects the most suitable text from these standards reasons in the Web Portal and stores it with the rule violation.

To edit standard reasons

1. Select the category **Identity Audit | Basic configuration data | Standard reasons**.
2. Select a standard reason in the result list. Select **Change master data** in the task view.

   – OR –

   Click in the result list toolbar.
3. Edit the master data for a standard reason.
4. Save the changes.

Enter the following properties for the standard reason.

Table 12: General Master Data for a Standard Reason

Property	Description
Standard reason	Reason text as displayed in the Web Portal.
Description	Spare text box for additional explanation.
Automatic Approval	Specifies whether the reason text is entered automatically by One Identity Manager into the rule violation. Do not set this option if the you want to select the standard reason in the Web Portal.
Additional text required	Specifies whether an additional reason should be entered in freely formatted text for the exception approval.

Predefined Standard Reasons

The One Identity Manager supplies predefined standard reasons. These standard reasons are added to the rule violations by One Identity Manager, if approval is automatic.

To display predefined standard reasons

- Select the category **Identity Audit | Basic configuration data | Standard reasons | Predefined**.

Setting up a Rule Base

You can define rules for maintaining and monitoring regulatory requirements in a rule base. A rule in the One Identity Manager not only contains a technical description but also properties such as rule violation level, owner, manager or audit information. The rules can be also classified into categories ("compliance framework") and rule groups.

Once you have added a rule, an associated object for rule violations is added in the database. Everyone who violates the rule is added to this object.

Creating Rules

A working copy is added to the database for every rule. Edit the working copies to create rule and change them. Changes to the rule do not take effect until the working copy is enabled.

NOTE: One Identity Manager users with the application role **Identity & Access Governance | Identity Audit | Rule supervisors** can edit existing rules if they are entered as a rule supervisor in the general data.

To create a new rule

1. Select the category **Identity Audit | Rules**.
2. Click in the result list toolbar.
3. Enter the master data for the rule.
4. Save the changes.

   This adds a working copy.
5. Select **Enable working copy** from the task view. 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.

To edit an existing rule

1. Select the category **Identity Audit | Rules**.
   a. Select the rule in the result list.
   b. Select **Create copy** in the task view.

      The data from the existing working copy are overwritten by the data from the original rule after a security prompt. The working copy is opened and can be edited.

   - OR -

   Select the category **Identity Audit | Rules | Working copies of rules**.
   a. Select the working copy in the result list.
   b. Select **Change master data** in the task view.
2. Edit the working copy's master data.
3. Save the changes.
4. Select **Enable working copy** from the task view. Confirm the security prompt with **OK**.

   The changes to the working copy are transferred to the rule. This reenables a disabled rule on demand.

Setting Up a Rule

Enter the following master data for a rule.

Table 13: Setting Up a Rule

Property	Description
Rule	Name for the rule. A new objects for rule violations is added automatically with this name when a new rule is created. NOTE: If you rename compliance rules, the name of the associated rule violation is not changed.
Description	Spare text box for additional explanation.
Main version number	Current revision of the rule as a version number. The version number is incremented in the One Identity Manager default installation each time you make a change to the rule condition.
Working copy	Specifies whether this is a working copy.
Disabled	Specifies whether the rule is disabled. Only enabled rules are taken into account by rule checking. Use the

Property	Description
	tasks **Enable rule** or **Disable rule** to enable or disable a rule. The working copy rule is always disabled.
Rule group	Rule group to which the rule belongs in terms of content. Select a role group from the menu. To create a new rule group, click . Enter a name and description for the rule group.
Rule supervisor	Application role whose members are responsible for the rule in terms of content. To create a new application role, click . Enter the application role name and assign a parent application role.
Exception approval allowed	Specifies whether exception approval is permitted when the rule is violated. Assignments or requests that cause the rule to be violated can be approved and issued anyway with this.
Exception approver	Application role, whose members are entitled to grant exception approval for violations to this rule. To create a new application role, click . Enter the application role name and assign a parent application role.
Exception approvers info	Information, which the exception approver may require for making a decision. This advice should describe the risks and side effects of an exception.
Validity period	Time period for limiting exception approvals. Enter the number for which days the exception approval applies. When the validity period expires, the exception approvals are automatically lifted.
Attestors	Applications role whose members are authorized to approve attestation cases for compliance rules and rule violations. To create a new application role, click . Enter the application role name and assign a parent application role. NOTE: This property is available if the Attestation Module is installed.
Functional area	Functional area relevant to the rule.
Department	Department relevant to the rule.
Rule for cyclic testing and risk assessment in the IT Shop.	Specifies whether the rule is taken into account by risk assessment of IT Shop requests. This option is only visible if the configuration parameter "QER\ComplianceCheck\SimpleMode\NonSimpleAllowed" is set.
Rule only for cyclical testing	Specifies whether the rule is only taken into account by cyclical testing.

Property	Description
	This option is only visible if the configuration parameter "QER\ComplianceCheck\SimpleMode\NonSimpleAllowed" is set.
Condition	Conditions, which result in a rule violation. Use the Rule Editor to enter the conditions.

Detailed information about this topic

- Creating Rule Conditions on page 43
- Enabling and Disabling Rules on page 41
- Rule groups on page 10
- Rule supervisor on page 23
- Exception approver on page 25
- Exception Approval over a Limited Period on page 62
- Attestors on page 22
- Functional Areas on page 21
- Creating Rule Conditions on page 43
- Rule Conditions in Advanced Mode on page 52

Related Topics

- Rule Check Analysis on page 58
- Granting Exception Approval on page 61

Risk Assessment

Table 14: Configuration Parameter for Risk Assessment

Configuration parameter	Active Meaning
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 set, a value for the risk index can be entered and calculated.

You can use the One Identity Manager to evaluate the risk of rule violations. To do this, enter a risk index for the rule. The risk index specifies the risk involved for the company if the rule is violated. The risk index is given as a number in the range 0-1. By doing this you specify whether a rule violation is not considered a risk for the company (risk index = 0) or whether every rule violation poses a problem (risk index = 1).

When a rule condition is created, system entitlement risk indexes can already be included as an object property. By using rules of this type you can prevent system entitlements that exceed a specified risk index from being requested in the IT Shop.

You can create several reports with the Report Editor to evaluate objects, assignments and rule violations depending on the risk index.

To evaluate the risk of a rule violation in the context of identity audit, you can enter values for grading rules on the **Assessment criteria** tab.

Table 15: Assessment Criteria for a Rule

Property	Description
Severity	Specifies the impact on the company of violations to this rule. Use the slider to enter a value between 0 and 1. 0 ... no impact 1 ... every rule violation is a problem.
Significance	Provides a verbal description of the significance for the company of violations to this rule. In the default installation value list is displayed with the entries {NONE, 'low', 'average', 'high', 'critical'}.
Risk index	Specifies the risk for the company of violations to this rule. The template is given a risk index depending on the value of the effect. **Table 16: Risk index in connection with significance** **Significance** / **Risk index** Low / 0,0 Average / 0,33 High / 0,66 Critical / 1,0 Risk index in connection with significanc Use the slider to enter a value between 0 and 1. 0 ... no risk 1 ... every rule violation is a problem. The template adjusts the risk index when the significance is changed. This property is only visible if the configuration parameter "QER\CalculateRiskIndex" is set.
Risk index (reduced)	Show the risk index taking mitigating controls into account. A rule'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 rule. To copy the value to a working copy, run the task **Create working copy**.

Property	Description
	This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. The value is calculated by One Identity Manager and cannot be edited.
Transparency index	Specifies how traceable assignments are that are checked by this rule. Use the slider to enter a value between 0 and 1. 0 ... no transparency 1 ... full transparency
Max. number of rule violations	Number of rule violation permitted for this rule.

Detailed information about this topic

- One Identity Manager Risk Assessment Administration Guide
- Report Editor in the One Identity Manager Configuration Guide
- Mitigating Controls on page 74

Related Topics

- Creating Rule Conditions on page 43
- Creating a Working Copy on page 41

Extended Rule Input

You can enter additional comments about the rule and revision data on the **Extended** tab..

Table 17: Extended Master Data for a Rule

Property	Description
Rule number	Additional name for the rule.
Implementation notes	Spare text box for additional explanation. You can use implementation notes to enter explanations about the content of the rule condition, for example.
Test schedule	Schedule for starting rule checks on a regular basis. The schedule "default schedule compliance rule check" is assigned by default. You can assign your own schedule.
Fill schedule	Schedule, which starts recalculation of the auxiliary tables for rule checking.

Property	Description
	The schedule "default schedule compliance rule fill" is assigned by default. You can assign your own schedule.
Status	Rule status with respect to its audit status.
Auditor	Person that audited the rule the last time.
Date of Audit	Date of last rule audit.
Audit remarks	Remarks referring to the audit, for example, results that might be important for the next audit.

Related Topics

- Checking a Rule on page 55
- Determining Potential Rule Violations on page 67

Rule Comparison

You can compare the results of a working copy with the original rule. The comparison values are then displayed on the **Rule comparison** tab on the master data form.

Table 18: Results of a Rule Comparison

Rule violations	Lists all employees for whom the rule, due to the change is
Newly added	violated for the first time
Identical	still being violated
No longer included	no longer violated

TIP: All working copies with a different condition to that of the original rule are displayed in **Identity audit | Rules | Working copies of rules | Modified working copies**.

Detailed information about this topic

- Comparing a Rule Working Copy with the Original on page 38

IT Shop Properties for a Rule

Table 19: Configuration Parameter for IT Shop Relevant Properties

Configuration Parameter	Meaning if Set
QER\ComplianceCheck\EnableITSettingsForRule	IT Shop properties for the compliance rule are visible and can be edited.

You can integrate checking of requests for rule compliance into approval workflows in IT Shop. On the **IT Shop properties** tab, specify how violations of this rule should be handled within an approval process for IT Shop requests.

NOTE: This tab is only shown when the rule condition is created in the simplified version. For more information, see Creating Rule Conditions on page 43.

To enter IT Shop properties for a rule

1. Set the configuration parameter "QER\ComplianceCheck\EnableITSettingsForRule" in the Designer.
2. Enable the option **Rule for cyclical testing and risk analysis** on the rule's master data form on the **General** tab in the IT Shop.
3. Select the tab **IT Shop properties**.
4. Edit the master data.
5. Save the changes.

Table 20: IT Shop Properties

Property	Description
Identifying a Rule Violation	Specify which rule violations are logged. **Table 21: Permitted Value** **Value** / **Description** New rule violation due to a request — Only rule violations that are added through approval of the current request are logged. Unapproved exception — Rule violations that are added through approval of the current request are logged. Already known rule violations that have not yet been granted an exception are also logged. Any compliance violation — All rule violations are logged, independent of whether an exception approval has already been granted or not. This value is automatically set when the option **Explicit exception approval** is enabled.
Explicit Exception Approval	Specifies whether exception approvals are presented again or whether existing exception approvals should be reused. **Table 22: Permitted Value** **Option is** / **Description** Enabled — A known rule violation must always be presented for exception approval, even if there is an exception approval from a previous violation of the rule. Disabled — A known rule violation is not presented again for exception approval, if there is an exception approval from a previous violation of the rule. This exception approval is reused and the known rule violation is automatically granted exception.

Additional Tasks for Working Copies

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of Working Copies

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 | Rules | Working copies of rules**.
2. Select the rule in the result list.
3. Select **Shelf overview** in the task view.

Assigning Compliance Frameworks

Use this task to specify, which compliance frameworks are relevant for the selected rule. Compliance frameworks are used for classifying attestation policies, compliance rules and company policies according to regulatory requirements.

To assign compliance frameworks to a rule

1. Select the category **Identity Audit | Rules | Working copies of rules**.
2. Select the working copy in the result list.
3. Select **Assign compliance frameworks** from the task list.
4. Double-click on a compliance framework in **Add assignments** to assign it.

   – OR –

   Double-click on a compliance framework in **Remove assignments** to remove the approver.
5. Save the changes.

Mitigating Controls

Mitigating controls describe controls that are implemented if a compliance rule was violated. The next rule check should not find any rule violations once the controls have been applied.

To edit mitigating controls

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

Detailed information about this topic

- Mitigating Controls on page 74
- Assigning Mitigating Controls on page 37
- Creating Mitigating Controls on page 37

Assigning Mitigating Controls

Specify which mitigating controls apply to the selected role.

To assign mitigating controls to a rule

1. Select the category **Identity Audit | Rules | Working copies of rules**.
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 –

   Double-click on a mitigating control in **Remove assignments** to remove the assignment.
5. Save the changes.

NOTE: 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.

For more detailed information, see the One Identity Manager Administration Guide for the SAP R/3 Compliance Add-on.

Creating Mitigating Controls

To create a mitigating control for rules

1. Select the category **Identity Audit | Rules | Working copies of rules**.
2. Select a working copy in the result list.
3. Select **Assign mitigating controls** from the task list.
4. Select **Create mitigating controls** from the task list.
5. Enter the master data for the mitigating control.
6. Save the changes.
7. Select the task **Assign rules**.
8. Double-click on the rule you want to assign in **Add assignments**.
9. Save the changes.

Detailed information about this topic

- Mitigating Controls on page 74

Enabling Working Copies

When you enable the working copy, the changes are transferred to the original rule. A rule is added to a new working copy. Only original rules are taken into account by rule checking.

To enable a working copy

1. Select the category **Identity Audit | Rules | Working copies of rules**.
2. Select the working copy in the result list.
3. Select **Enable working copy** in the task view.
4. Confirm the security prompt with **OK**.

TIP: All working copies with a different condition to that of the original rule are displayed in **Identity audit | Rules | Working copies of rules | Modified working copies**.

Recalculate

There are several tasks available for a working copy, which immediately perform a rule check. For more information, see Checking a Rule on page 55.

Copy Rule

Rules can be copied to reuse complex rule conditions, for example. Working copies as well as active rules can be used as copy templates.

To copy a working copy

1. Select the category **Identity Audit | Rules | Working copies of rules**.
2. Select the working copy in the result list.
3. Select **Change master data** in the task view.
4. Select **Copy rule...** in the task view.
5. Enter a name for the copy and click **OK**.

   This creates a working copy with the given name.
6. To edit the copy's master data immediately, click **Yes**.

   -OR -

   To edit the copy's master data later, click **No**.

Comparing a Rule Working Copy with the Original

If you have made changes to the rule condition in a working copy, you can determine the effects of this using a comparison with the original rule. Rules can only be compared when

an original of the working copy exists. The result of the rule comparison is displayed on the tab **Rule comparison** of master data form.

To compare a rule with the working copy.

1. Select the category **Identity Audit | Rules | Working copies of rules**.
2. Select the working copy in the result list.
3. Select **Change master data** in the task view.
4. Select **Rule comparison** in the task view.

Table 23: Results of a Rule Comparison

Rule violations	Lists all employees for whom the rule, due to the change is
Newly added	violated for the first time
Identical	still being violated
No longer included	no longer violated

To display the rule comparison as report

- Select the report **Show rule comparison**.

Related Topics

- Rule Comparison on page 33

Maintain Exception Approver

Use this task to maintain exception approvers for the selected rule. You can assign employees to the application role for exception approvers on the master data form and remove them from it.

NOTE: Changes apply to all the rules assigned to this application role.

To authorize employees as exception approvers

1. Select the category **Identity Audit | Rules | Working copies of rules**.
2. Select the working copy in the result list.
3. Select **Maintain exception approvers** in the task view.
4. Double-click on the employees you want to assign be assigned to the application role in **Add Assignments**.

   – OR –

   Double-click on the employees you want to remove in **Remove Assignments**.
5. Save the changes.

Related Topics

- Setting Up a Rule on page 28
- Exception approver on page 25

Maintain Rule Supervisors

Use this task to maintain rule supervisors for the selected rule. You can assign employees to the application role for rule supervisors on the master data form and remove them from it.

NOTE: Changes apply to all the rules assigned to this application role.

To authorize employees as rule supervisors

1. Select the category **Identity Audit | Rules | Working copies of rules**.
2. Select the working copy in the result list.
3. Select **Maintain rule supervisors** in the task view.
4. Double-click on the employees you want to assign be assigned to the application role in **Add Assignments**.

   – OR –

   Double-click on the employees you want to remove in **Remove Assignments**.
5. Save the changes.

Related Topics

- Setting Up a Rule on page 28
- Rule supervisor on page 23

Enable SQL Definition

In certain cases, the rule condition can be formulated directly in SQL. For more information, see Rule Condition as SQL Query on page 54.

Additional Tasks for Rules

After you have entered the master data, you can apply different tasks to it. The task view contains different forms with which you can run the following tasks.

Overview of the Rule

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

To obtain an overview of a rule

1. Select the category **Identity Audit | Rules**.
2. Select the rule in the result list.
3. Select **Shelf overview** in the task view.

Creating a Working Copy

To modify an existing rule, you need to make a working copy. The working copy can be created from the existing rule. The working copy data can be used to overwrite the rule as required.

To create a working copy

1. Select the category **Identity Audit | Rules**.
2. Select the rule in the result list.
3. Select **Create working copy** in the task view.
4. Confirm the security prompt with **Yes**.

TIP: All working copies with a different condition to that of the original rule are displayed in **Identity audit | Rules | Working copies of rules | Modified working copies**.

Enabling and Disabling Rules

Enable the rule so that rule violation can be found. To exclude rules from testing, you can disable them. Any existing rule violations are removed by the DBQueue Processor. The working copy rule is always disabled.

To enable a rule

1. Select the category **Identity Audit | Rules**.
2. Select the rule in the result list.
3. Select **Enable rule** in the task view.

To display a rule

1. Select the category **Identity Audit | Rules**.
2. Select the rule in the result list.
3. Select **disable rule** in the task view.

Recalculate

There are several tasks available for a rule, which immediately perform a rule check. For more information, see Checking a Rule on page 55.

Copy Rule

Rules can be copied to reuse complex rule conditions, for example. Working copies as well as active rules can be used as copy templates.

To enable a rule

1. Select the category **Identity Audit | Rules**.
2. Select the rule in the result list.
3. Select **Change master data** in the task view.
4. Select **Copy rule...** in the task view.
5. Enter a name for the copy and click **OK**.

   This creates a working copy with the given name.
6. To edit the copy's master data immediately, click **Yes**.

   -OR -

   To edit the copy's master data later, click **No**.

Maintain Exception Approver

Use this task to maintain exception approvers for the selected rule. To do this, assign employees who are allowed to approve exceptions to this rule to the applications roles entered for exception approvers on the master data form.

NOTE: Changes apply to all the rules assigned to this application role.

To authorize employees as exception approvers

1. Select the category **Identity Audit | Rules**.
2. Select the rule in the result list.
3. Select **Maintain exception approvers** in the task view.
4. Double-click on the employees you want to assign be assigned to the application role in **Add Assignments**.

   – OR –

   Double-click on the employees you want to remove in **Remove Assignments**.
5. Save the changes.

Related Topics

- Setting Up a Rule on page 28
- Exception approver on page 25

Maintain Rule Supervisors

Use this task to maintain rule supervisors for the selected rule. To do this, assign employees who are allowed to edit this rule to the applications roles entered for exception approvers on the master data form.

NOTE: Changes apply to all the rules assigned to this application role.

To authorize employees as rule supervisors

1. Select the category **Identity Audit | Rules**.
2. Select the rule in the result list.
3. Select **Maintain rule supervisors** in the task view.
4. Double-click on the employees you want to assign be assigned to the application role in **Add Assignments**.

   – OR –

   Double-click on the employees you want to remove in **Remove Assignments**.
5. Save the changes.

Related Topics

- Setting Up a Rule on page 28
- Rule supervisor on page 23

Creating Rule Conditions

Table 24: General Configuration Parameters for Rule Compliance

Configuration parameter	Meaning if Set
QER\ComplianceCheck\SimpleMode	Preprocessor relevant configuration parameter for controlling the definition of rule conditions for compliance rules. Changes to the parameter require recompiling the database. If this parameter is set, you can set up rule conditions with a simplified definition.

In the rule condition, combine all the entitlements that lead to a rule violation. The affected employee group and entitlements are restricted separately in the rule condition. Employees and identities that the rule condition will be applied to, are determined by the employee group. The properties that result in a rule violation for the affected employees, are defined by the affected entitlements. The entitlements are determined through the object relations of the affected employees (table `PersonHasObject`).

NOTE: If the configuration parameter "QER\ComplianceCheck\SimpleMode\NonSimpleAllowed" is set, rule conditions can be created in advanced mode as well as in the simplified definition.

To use the simplified definition

- Enable the option **Rule for cyclical testing and risk analysis in IT Shop** on the rule's master data form.

For more information, see Rule Conditions in Advanced Mode on page 52.

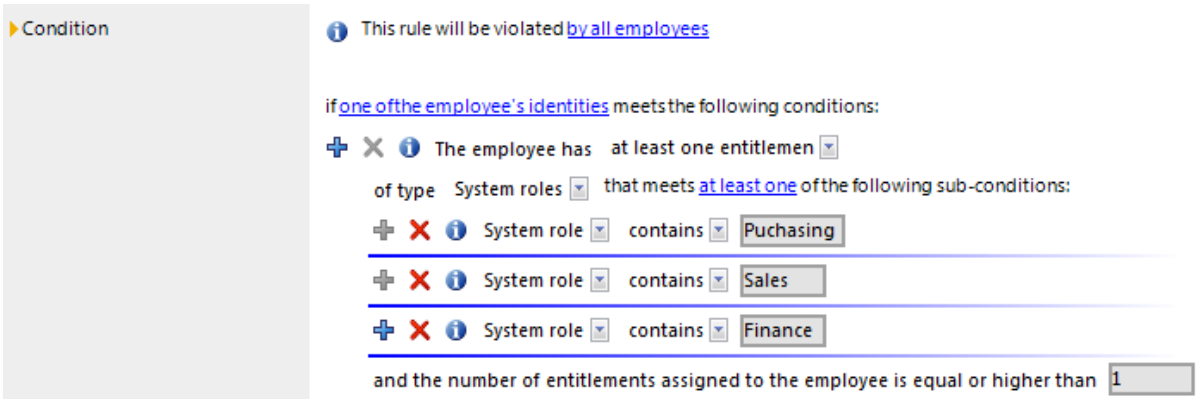
Basics for Using the Rule Editor

Table 25: Configuration Parameters for Entering Extended Rule Conditions

Configuration parameter	Meaning if Set
QER\ComplianceCheck\SimpleMode\ShowDescriptions	Displays additional input fields for describing the compliance rules in the Rule Editor.

The Rule Editor is there to help you formulate rule conditions. You can use predefined condition type and operator for this. The complete database query is composed internally. If the configuration parameter "QER\ComplianceCheck\SimpleMode\ShowDescriptions" is set, additional input fields are displayed in the simplified definition, providing a more detailed description of each rule block.

Figure 2: Rule Editor for Simple Definition of Rules



The Rule Editor control elements supply operators and properties that you need for formulating partial conditions. You can only select one entry from the drop-down menu. You can select more entries from extended drop-down menus, where the properties are displayed hierarchically and then added to the condition using an "or" operator. You may enter text directly into input fields. Pop-up menus and input fields are shown and hidden dynamically.

A rule condition is made up of several rule blocks. A rule violation is detected when an employee, with properties and assignments, can be matched to all the rule blocks.

There are two types of rule blocks:

- Affected groups of employees

  Each rule must obtain exactly one rule block that specifies the employee group that the rule should be applied to. By default, all employees with all identities are taken into account. You can, however, restrict the employee groups more.

- Entitlements affected

  You need to define at least one rule block that finds affected entitlements. The properties that result in a rule violation in the employee group affected are defined here. You can check the following entitlements in the rule block: roles, target system groups, system entitlements, system roles, applications, resources.

You can add any number of partial conditions within one rule block and link them with each other using the Rule Editor. Use the options **All** and **At least one** to specify whether one or all partial conditions in the block have to be fulfilled.

Table 26: Meaning of Icons in the Rule Editor

Icon	Meaning
	Add another partial condition or another rule block. A new line is displayed for entering the condition.
	Delete the partial condition or rule block. The line is removed.
	Opens the preview window. Affected objects are shown.
	The list of affected objects is shown in the preview window.

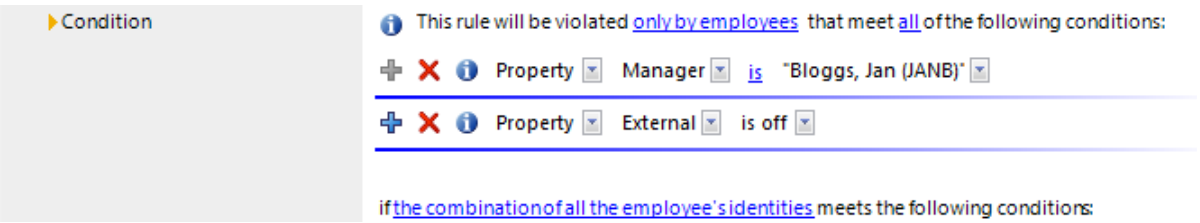
To display a preview of affected objects

1. Click the condition or partial condition in the Rule Editor.
2. Click in the preview window to display the list of affected objects.

Specifying the Affected Employee Group

Each rule has to contain exactly one rule block which specifies the employee group.

Figure 3: Rule Block for the Employee Group Affected



Use the following to options to limit the affected employee groups.

- From all employees

  All employees are taken into account
  .
- Only from employees that fulfill all/at least one of the following conditions

  You can limit the employee group with a condition, for example, "All employees in group A" or "All external employees". To determine the affected employee group, formulate the appropriate partial conditions.

  You can specify a condition type in the first pop-up menu of the partial condition which restricts the affected employee group.

Table 27: Permitted Condition Types in the Rule Editor

Condition Type	Meaning
Property	Employees' properties. The drop-down menu with permitted properties is already restricted to the most important employee properties.
For the user account with the target system type	User account properties of the employees with the selected target system type.
SQL query	Sql query (WHERE clause) input.

- A single identity

Table 28: Results of the Rule Check

The rule is ...	Condition
violated	An employee's sub or main identity fulfills the rule condition.
not violated	The main identity only fulfills the rule condition due to its subidentity.

- The combination of all identities

  The rule is violated:

  - If an employee's subidentity or the main identity fulfills the rule condition

    - OR -
  - the main identity only fulfills the rule condition due to its subidentity.

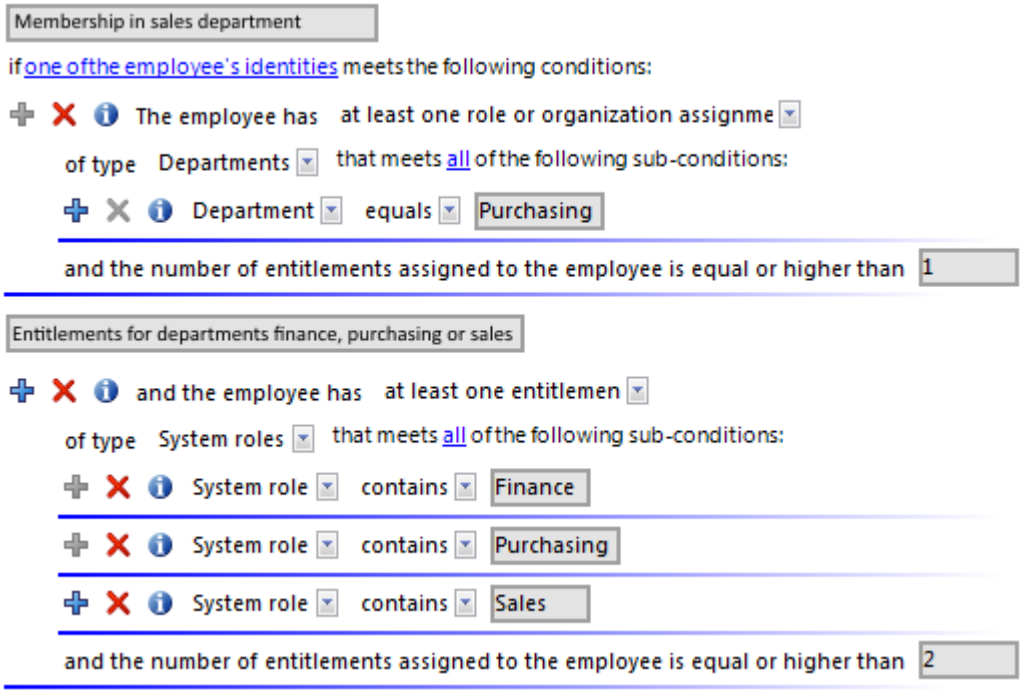
Related Topics

- One Identity Manager Identity Management Base Module Administration Guide
- A Simple Rule Example on page 49

Specifying Affected Entitlements

In order to take entitlements into account in the rule, you must define at least one rule block that determines the affected entitlements for employee groups. Each rule block can contain more than one partial condition. The partial conditions are linked through the options **all** or **at least one**.

Figure 4: Rule Block for Affected Entitlements



Use the following to options to limit the affected entitlements.

- at least one entitlement

  Define one entitlement per rule block.

Table 29: Specifying Affected Entitlements

Type	Partial condition	Description
<target system types> (System entitlements) (<groups>)	Properties	System entitlement property from the selected target system, for example, "Distinguished name" or "Container".
	Permissions controls	Permissions element defined for this target system.

Type	Partial condition	Description
		NOTE: Permissions elements are only created for custom target systems.
	Has extended property	Extended property assigned to the system entitlements.
	Has extended property in range	Extended property assigned to the system entitlements with a defined range of values. The rule verifies the correct value.
Resources Applications	Properties	Properties of resources/application, such as "application name" or "resource type".
	Memberships	Memberships of resources/applications in hierarchical roles and IT Shop structures.
Account definitions	Properties	Properties of account definitions, such as "resource type".
System roles	Properties	Properties of system roles, such as "display name".
	Memberships	Memberships of system roles in hierarchical roles and assignments to employee or workdesks.

Rules can be created for all the system entitlements displayed in the Unified Namespace. The rule conditions access the Unified Namespace database layers to do this. You can select target system types as entitlement **type**.

- At least one role or organization assignment

  Define one role class assignment per rule block (One Identity Manager application roles, departments, locations, cost centers, business roles).

Table 30: Specifying affected Role Memberships

Type	Partial condition	Description
Application roles Departments Locations Business roles Cost centers	Properties	Properties of the role, such as "full name" or "parent role".
	Assignment in other objects	Assignments of role to other objects, such as primary departments to different employees.
	Memberships	Memberships of company resource in roles, such as `DepartmentHasADSGroup`.

- at least one function

  Enter at least one SAP function to replace the rule.

  NOTE: This option can only be selected if the module SAP R/3 Compliance Add-on Module is installed.

- Number of entitlements

  You specify how many entitlements the employee must have to violate the rule.

  By default, a rule violation is identified, if one of the employee of the employee group affected, is assigned an object that fulfills the condition of the rule block. You can increase this number. The value "0" is not valid.

Related Topics

- A Simple Rule Example on page 49
- One Identity Manager Administration Guide for the SAP R/3 Compliance Add-on

A Simple Rule Example

The following examples show how rules can be created with the help of the Rule Editor and the effects of each option.

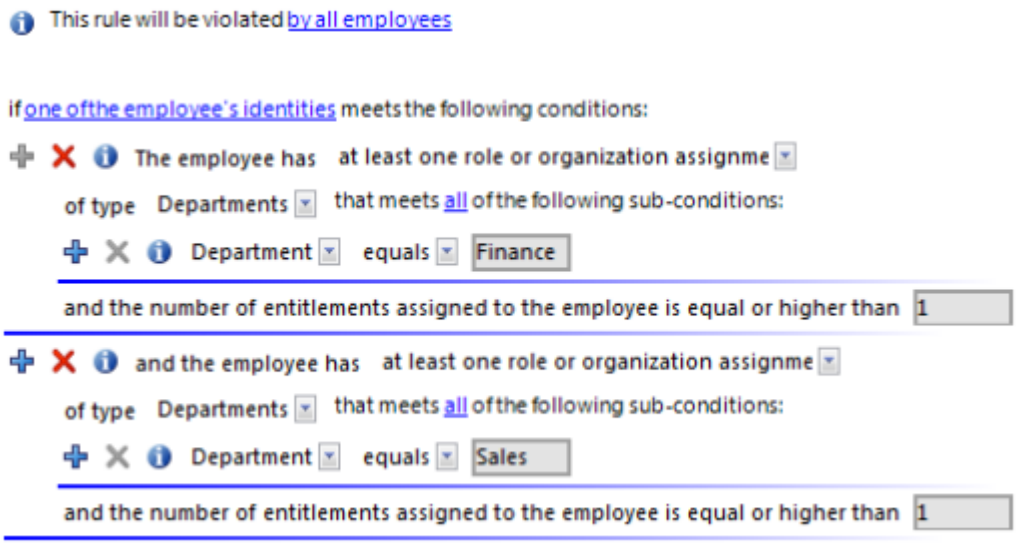
Example 1

Employees from department A may not belong to department B at the same time.

Define:

1. The option **by all employees** and **combination of all identities** in the rule block for the affected employee group.
2. Two rule blocks for the affected entitlements with the option **at least one role or organization**.

Figure 5: Rule Condition for Example 1



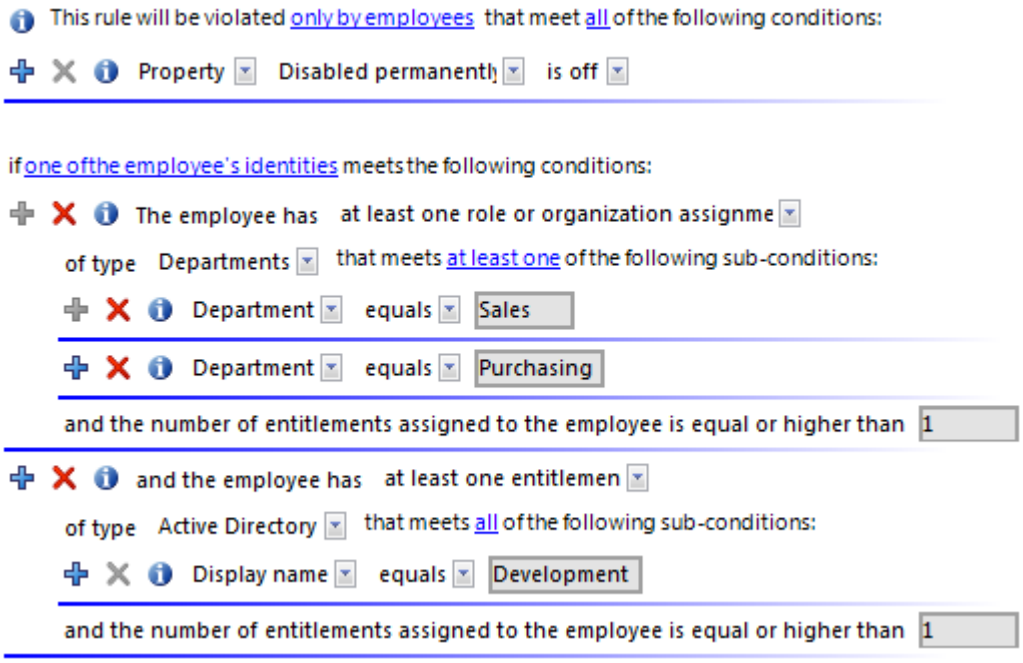
Example 2

Employees that belong to the department sales or the department purchasing, are not permitted to access the Active Directory group "Development". This rule is only checked for enabled employees.

Define:

1. The option **by all employees**, **all** and **a single identity** in the rule block for the affected employee group.
2. Two rule blocks for the affected entitlements with the options:
    a. **at least one role or organization assignment** and
    b. **at least one entitlement**

Figure 6: Rule Condition for Example 2



Example 3

All permitted entitlements are assigned to employees over system roles. One employee can have a maximum of two system roles. If an employee has more than one identity, the rule is also violated if the entitlements of all subidentities together result in a rule violation.

There are three system roles: Pool for finance, Pool for purchasing, Pool for sales

Jenny Basset has two subidentities. The main identity and both subidentities are respectively assigned to a system role.

Jenny Basset (HI): Pool for finance

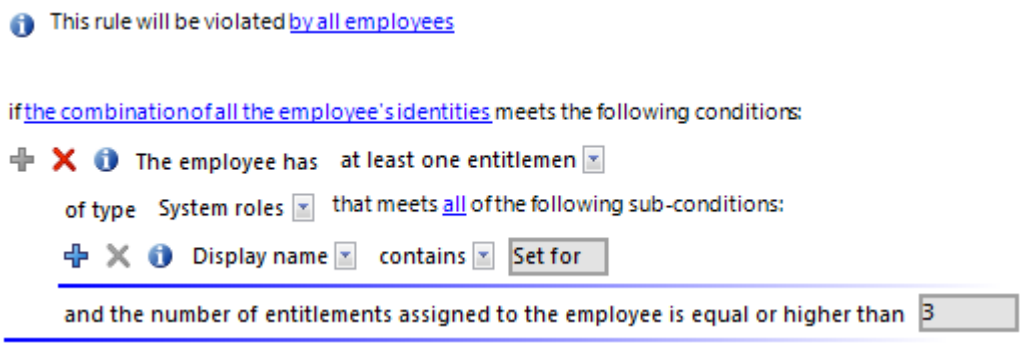
Jenny Basset (SI1): Pool for purchasing

Jenny Basset (SI2): Pool for sales

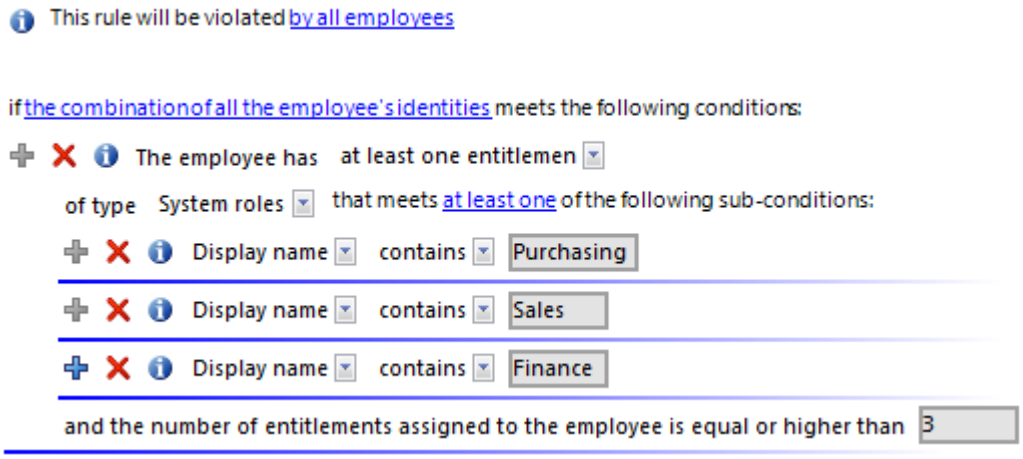
Define:

1. The option **by all employees** and **combination of all identities** in the rule block for the affected employee group.
2. One rule block for the affected entitlements with the option **at least one entitlement** of type **system roles** that fulfill **all** the following partial conditions
3. A partial condition: **display name contains** "Pool for"
4. The number of entitlements assigned to the employee is larger or equal to **3**.

Because Jenny Basset's main identity includes all three system roles due to her subidentities, the main identity violates this (and only this) rule.



Rule checking finds the same result if the rule is formulated as follows:



Rule Conditions in Advanced Mode

Table 31: Configuration Parameter for Entering More Rule Conditions

Configuration parameter	Meaning if Set
QER\ComplianceCheck\SimpleMode\NonSimpleAllowed	Rules can be created in advanced mode

There are two ways of defining rule conditions, the simple definition and advanced mode. The simple definition is used as default to create rule conditions with the Rule Editor. For more information, see Basics for Using the Rule Editor on page 44.

In advanced mode, employee's properties are defined in the rule condition that lead to a rule violation. The assignments are determined directly by the respective base tables, which contain the selected objects (for example, `PersonHasSAPGRoup` or `Person`).

To use advanced mode

1. Set the configuration parameter "QER\ComplianceCheck\SimpleMode\NonSimpleAllowed" in the Designer.

On the rule's master data form you will also fund the options **Rule for cyclical testing and risk analysis in IT Shop** and **Rule only for cyclical testing**.

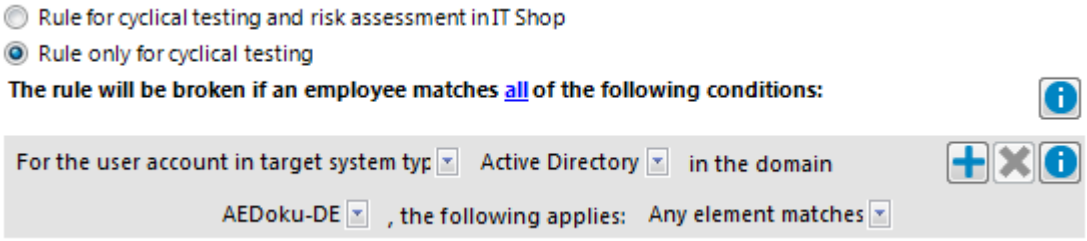
2. Set the option **Rule only for cyclical testing**.
3. Confirm the security prompt with **Yes**.

   The design of the rule condition is changed.

NOTE: You cannot return to the simple definition once a rule condition has been entered in advanced mode!

NOTE: Rules in advanced mode are not taken into account by rule checks within IT Shop request approval processes. No IT Shop properties can be defined for these rules. The **IT Shop properties** tab does not appear on the master data form for this rule.

Figure 7: Advanced Mode Condition



Rule conditions in advanced mode are based on the base object "Employees" (Table `Person`). The completed database query is put together internally:

```
Select Firstname, Lastname from Person where <Rule condition>order by 1,2
```

First you need to specify whether one or all of the following conditions have to be met in advanced mode. Specify the condition type in the first drop-down menu in the condition.

Table 32: Permitted Condition Types in Advanced Mode

Condition Type	Meaning
Property	Employee object properties. The drop-down menu with permitted properties is already restricted to the most important employee properties.
For the account with the target system type	Employee's user account. Valid user account properties depend on which target system is selected.
For entitlements with the target system type	Employee target system group. Valid group properties depend on which target system is selected.
SQL Query	Free choice of SQL query (WHERE clause). Click if you want to use the WHERE clause wizard.

You have the option to link several conditions together. Only "and" is supported here as link operation.

All other control elements you need for formulating a condition, are operators and properties. You can only select one entry from the drop-down menu. You can select more entries from extended drop-down menus, where the properties are displayed hierarchically and then added to the condition using an "or" operator. You may enter text directly into input fields. Pop-up menus and input fields are shown and hidden dynamically.

Rule Condition as SQL Query

Table 33: Configuration Parameter for Entering More Rule Conditions

Configuration parameter	Meaning if Set
QER\ComplianceCheck\PlainSQL	SQL text is only permitted for rules in advanced mode.

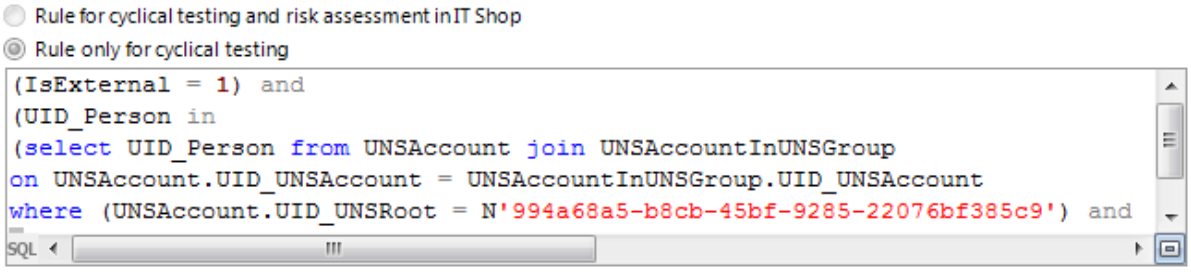
You can formulate rule conditions directly in advanced mode as an SQL query.

To formulate a rule condition directly as an SQL query

1. Set the configuration parameter "QER\ComplianceCheck\PlainSQL" in the Designer.
2. Select the option **Rule only for cyclical testing**.
3. Select **Enable SQL definition** for the working copy.

NOTE: Rule conditions can only be formulated through an SQL query if the configuration parameter "QER\ComplianceCheck\SimpleMode" is not set and the configuration parameter "QER\ComplianceCheck\PlainSQL" is set.

Figure 8: Direct SQL Query Input



Deleting Rules

NOTE: All the information about a rule condition and rule violations is irrevocably deleted when the rule is deleted! The data cannot be retrieved at a later date.

Therefore, we advise you to write a report about the rule and its current violations before you delete it, if you want to retain the information (for example, audit security).

You can delete a rule if there are no rule violations attached to it.

To delete a rule

1. Select the category **Identity Audit | Rules**.
2. Select the rule to delete in the result list.
3. Select **disable rule** in the task view.

   Any existing rule violations are removed by the DBQueue Processor.
4. After the DBQueue Processor has recalculated rule violation for the rule, click in the toolbar.

   The rule, the associated rule violation object and the working copy are all deleted.

Rule check

To test a rule, processing tasks are created for the DBQueue Processor. The DBQueue Processor determines for each rule, which employees have violated the rule. Follow-up tasks assign the associated rule violation object to employees that have violated a rule. The specified rule approvers can test rule violations and if necessary grant exception approval.

Checking a Rule

You can start rule checking in different ways to find the current rule violations in the One Identity Manager database.

- Scheduled rule checking
- Automatic rule checking after modifications
- Ad hoc rule checking

Only operational rules are checked during rule checking. Disabled rule are not tested. If a rule is violated, the effected employees are assigned the corresponding object for rule violations. You can check all the rules again for these employees. For more information, see Rule Check Analysis on page 58.

In addition to locating existing rule violations, the One Identity Manager can also identify potential violations of IT Shop requests and business roles. For more information, see Determining Potential Rule Violations on page 67.

Scheduled rule checking

The schedule "default schedule compliance rule check" One Identity Manager is supplied with the default installation to run a complete check of all rules. This schedule generates

processing tasks at regular intervals for the DBQueue Processor.

Prerequisites

- The rule is enabled.
- The schedule stored with the rule is enabled.

Detailed information about this topic

- Schedules for Checking Rules on page 13
- Enabling and Disabling Rules on page 41

Checking Rule after Modifications

Table 34: Configuration Parameters for Rule Checking

Configuration parameter	Meaning if Set
QER\ComplianceCheck\CalculateImmediately	Processing tasks for recalculating rule violations are immediately started when relevant changes occur.

A processing task for rule checking is generated the moment an active rule is modified or deleted. All employees are checked to see if they fulfill the affected rule.

When specific changes are made to entitlements, you can immediately queue or schedule the calculation tasks to check the rules. Specify the desired behavior in the configuration parameter "QER\ComplianceCheck\CalculateImmediately". If the parameter is set, the processing task for recalculating rule violation for an employee are immediately queued. If the parameter is not set, the calculation task is started the next time the schedule is planned to run.

To trigger rule checks immediate after relevant changes have been made

- Set the configuration parameter "QER\ComplianceCheck\CalculateImmediately" in the Designer.

  The processing task for recalculating rule violations for an employee is immediately started when relevant changes occur.

NOTE: This configuration parameter only applies if data changes are relevant. These include:

- Changes to employee master data
- Changes to employee assignments (for example, table `PersonHasQERResource`)
- Changes to employees' role memberships
- Changes to membership in system entitlements (for example, table `ADSAccountInADSGroup`)
- Changes to SAP function matches (table `SAPUserInSAPFunction`)

Ad hoc rule checking

There are several tasks available for a rule, which immediately perform a rule check.

Table 35: Additional Tasks for Rules

Task	Description
Recalculate rule	All employees are checked to see if they comply to the current rule.
Recalculate for current user	All employees are checked to see if they comply to all rules.
Recalculate all	All employees are checked to see if they comply to all rules.

Speeding up Rule Checking

Scheduled rule checking can take a long time under certain circumstances. This might be the case, for example, if a lots of rules exist in which the employee group affected is not limited ("This rule is broken by all workers"). One Identity Manager supplies two consistency checks for optimizing performance of the calculation of affected employee groups. This reduces the amount of data in the auxiliary tables.

To optimize rule checking, start these consistency checks and repair the rules which are found.

To run a consistency check

1. Select the menu item **Database | Check data consistency...** in the Manager.
2. Click in the Consistency Editor's toolbar.
3. Click in the test option dialog box's toolbar.
4. Enable the tests "Content\Compliance\ComplianceRule change IsPersonStoreInverted to 1" and "Content\Compliance\ComplianceRule change IsPersonStoreInverted to 0".
5. Click **OK**.
6. Run the consistency check for the object "database".
7. Verify the analysis results.

   TIP: To obtain details of an error message
   a. Select the error message.
   b. Click in the toolbar.
8. To optimize the rule condition for an affected rule
   a. Select the error message.
   b. Click **Repair** for both the original and the working copy of the rule.

Detailed information about this topic

- One Identity Manager User Guide for One Identity Manager Tools User Interface and Default Functions

Related Topics

- Creating a Working Copy on page 41

Rule Check Analysis

Each rule references its own object for rule violations (table `NonCompliance`). Employees who violate rules are assigned to this objects (table `PersonInNonCompliance`). There are two forms available for rule checking that are supposed to answer the following questions:

- Which employees violate a specific rule?
- Which rules are violated by a specific employee?

Which employees violate a specific rule?

To display employees that violate a rule

1. Select the category **Identity Audit | Rule violations**.
2. Select a rule violation in the result list.
3. Select **Show rule violations** in the task view.

   This displays all employees assigned to the rule violation.

Table 36: Meaning of Rule Evaluation Icons

Icon	Meaning
	Employees pending a rule violation decision.
	Employees granted exception approval for their rule violation
	Employees not granted exception approval for their rule violation

Which rules are violated by a specific employee?

To view which rules the employee violates

1. Select the **Employees | Employees**.
2. Select an employee in the result list.

3. Select the report **Rule evaluation**.

   This not only shows the rule that the employee has violated with or without exception, but also those with no violations.

Table 37: Meaning of Icons in Employee Rule Analysis

Icon	Meaning
	The rule is not violated.
	The rule is violated. No exception approval has been granted for this rule exception.
	The rule is violated. No exception approval has been granted for this rule exception.

Reports about Rule Violations

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. You can generate the following reports for all active rules, rule groups and compliance frameworks.

NOTE: Other sections may be available depending on the which modules are installed.

Table 38: Reports about Rule Violations

Report	Description
Overview of all assignments (for a rule)	This report shows all employees that violate the selected rule. The report shows which roles of a role class the employee belongs to. Employees that are not members of any role are not taken into account.
Rule violation overview (for a rule)	This report groups together all rule violations for the selected rule. All employees are listed that have objects that violation the rule. The result list is grouped by: • Employees pending a rule violation decision. • Employees without exception approval. • Employees with exception approval.
Show historical rule violations (for a rule)	This report groups together all historical rule violations for the selected rule. All employees are listed that violate the rule as well as the time period covering the rule violation.

Report	Description
Rule violation overview (for a rule group)	This report groups together all rule violations for the selected rule group. All rule violations are listed. The number of granted, denied and not yet processed rule violations are given in addition.
Rule violation overview (for a compliance framework)	This report groups together all rule violations for the selected compliance framework. All rule violations are listed. The number of granted, denied and not yet processed rule violations are given in addition.
Detailed list of rule violations (for a compliance framework)	This report groups together all rule violations for the selected compliance framework. All rule violations are listed. For each rule, the employee that violated the rule, the date and the reason for the approval decision are given.

Related Topics

- Overview of all Assignments on page 60

Overview of all Assignments

The report "Overview of all Assignments" is displayed for certain objects, for example, permissions, compliance rules or roles. The report finds all the roles, for example, departments, cost centers, locations, business roles and IT Shop structures in which there are employee who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Example

- If the report is created for a resource, all roles are determined in which there are employees with this resource.
- If the report is created for a group, all roles are determined in which there are employees with this group.
- If the report is created for a compliance rule, all roles are determined in which there are employees with this compliance rule.
- If the report is created for a department, all roles are determined in which employees of the selected department are also members.

- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the report **Overview of all assignments**.
- Use the **Used by button** in the report's toolbar to select the role class (department, location, business role or IT Shop structure) for which you determine if roles exist in which there are employees with the selected base object.

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. In the report's toolbar, click to open the legend.
- Double-click a control to show all child roles belonging to the selected role.
- By clicking the button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to to start a wizard that allows you to bookmark this list of employee for tracking. This creates a new business role to which the employees are assigned.

Figure 9: Toolbar for Report "Overview of all assignments"

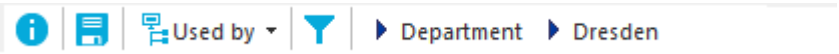


Table 39: Meaning of Icons in the Report Toolbar

Icon	Meaning
	Show the legend with the meaning of the report control elements
	Saves the current report view as a graphic.
	Selects the role class used to generate the report.
	Displays all roles or only the affected roles.

Granting Exception Approval

Table 40: Configuration Parameters for Exception Approvals

Configuration parameter	Meaning if Set
QER\ComplianceCheck\DisableSelfExceptionGranting	Excludes rule violators from becoming exception approvers. If this parameter is set, no one can approve their own rule violations.

Assignments, which violate rules, can be approved with hindsight. To do this, specially authorized employees can grant exception approval.

Prerequisites

- The option **Exception approval allowed** is set for the rule.
- The rule is assigned an application role for exception approvers.
- Employees are assigned to this application role.

NOTE: If the option **Exception approval allowed** is not set, unedited rule violations for this rule are automatically denied. Existing exception approvals are withdrawn.

You must also decide whether exception approvers are allowed to approve their own rule violations. By default, an employee who violates a rule is determined to be the exception approver for this rule if they are a member of the application role **Exception approvers** for the rule. This means they can approve their own rule violations.

To prevent an employee from granting themselves exception approval

- Set the configuration parameter "QER\ComplianceCheck\DisableSelfExceptionGranting".

  Employees that violate a rule, are not determined to be exception approvers for this rule violation. Neither the rule violator's main identity nor its subidentities can grant exception approval.

Detailed information about this topic

- Setting Up a Rule on page 28
- One Identity Manager Web Portal User Guide

Exception Approval over a Limited Period

Exception approvals can be set for a limited period of time. To do this, you can specify a validity period for exception approvals on each rule. When the validity period expires, the applicable exception approvals are canceled. A scheduled process plan checks whether an exception approval is still valid.

Once an exception approval has been granted, the expiry date is calculated from the current date and the validity period stored with the rule. You can only change the expiry date for future exception approvals. The expiry date for existing exception approvals does not change.

To set a time limit on exception approvals

1. Enter a validity period for a rule.
   a. Select the category **Identity Audit | Rules | Working copies of rules**.
   b. Select a working copy from the result list.

c. Select **Change master data** in the task view.

d. On the **General** tab, enter the number of days, in **Max. # days**, that the exception approval applies to this rule.

   If the value is "0", the exception approvals have no time limit.

e. Save the changes.

f. To transfer the changes to the current rule, select the task **Enable rule**.

2. Configure and set the schedule "Reset exception approval of compliance violations" in the Designer.

Related Topics

- One Identity Manager Configuration Guide

Granting Exception Approval in the Manager

You use the Web Portal to edit rule violations and grant exception approval, by default. You can, however, grant exception approval in the Manager. To do this, log in as non role-based to the Manager. This function is not available in the Manager for role-based login.

To grant exception approval for all employees violating a particular rule

1. Select the category **Identity Audit | Rule violations**.
2. Select the rule violation in the result list.
3. Select **Show rule violations** in the task view.
4. Select the employee for whom you want to grant exception approval by double-clicking.

   This opens the form **Edit rule violations**.
5. To obtain detailed information about the employee, click on the employee.
6. To obtain an overview of the rule violation, click on the rule violation.
7. Enter a reason
8. To approve the rule violation for this employee, click **Approve exception**.

   The data **Approver** and **Approval date** as well as the options **Exception is approved** and **Checked** are filled out on the form.
9. To deny exception approval for this employee, click **Deny exception**.

   The data **Approver** and **Approval date** as well as the option **Checked** are filled out on this form.
10. Save the changes.

To grant exception approval for all rules violated by a specific employee:

1. Select the **Employees | Employees**.
2. Select the employee in the result list.
3. Select the report **Rule evaluation**.
4. Double-click on the rule violation for which you want the employee to be grant exception approval.

   This opens the form **Edit rule violations**.
5. To obtain detailed information about the employee, click on the employee.
6. To obtain an overview of the rule violation, click on the rule violation.
7. Enter a reason
8. To approve the rule violation for this employee, click **Approve exception**.

   The data **Approver** and **Approval date** as well as the options **Exception is approved** and **Checked** are filled out on the form.
9. To deny exception approval for this employee, click **Deny exception**.

   The data **Approver** and **Approval date** as well as the option **Checked** are filled out on this form.
10. Save the changes.

Related Topics

- Which rules are violated by a specific employee? on page 58
- Which employees violate a specific rule? on page 58

Notifications about Rule Violations

Table 41: Configuration Parameter for Notifications

Configuration parameter	Meaning
QER\ComplianceCheck\EmailNotification	This parameter is used for mail notifications. Information about notifying during compliance checking is defined under this parameter.
QER\ComplianceCheck\EmailNotification\DefaultSenderAddress	This configuration parameter contains the sender email address for automatically

Configuration parameter	Meaning
	generated messages during rule checking.

After rule checking, email notifications can be sent to exception approvers and rule supervisors through new rule violation. The notification procedure uses mail templates to create notifications. The mail text in a mail template is defined in several languages. This ensures that the language of the recipient is taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

Messages are not sent ti the chief approval team by default. Fallback approvers are only notified if not enough approvers could be found for an approval step.

To use notification in the request process

1. Ensure that the email notification system is configured in One Identity Manager. For more detailed information, see the One Identity Manager Configuration Guide.
2. Set the configuration parameter "QER\ComplianceCheck\EmailNotification" in the Designer.
3. Set the configuration parameter "QER\ComplianceCheck\EmailNotification\DefaultSenderAddress" in the Designer and enter the sender address with which the email notifications are sent.
4. Ensure that all employees have a default email address. Notifications are sent to this address. For more detailed information, see the One Identity Manager Identity Management Base Module Administration Guide.
5. Ensure that a language culture can be determined for all employees. Only then can they receive email notifications in their own language. For more detailed information, see the One Identity Manager Identity Management Base Module Administration Guide.
6. Configure the notification procedure.

Related Topics

- Creating Custom Mail Templates for Notifications on page 68

Demands for Exception Approval

Table 42: Configuration Parameters for Notifications about Rule Violations

Configuration parameter	Meaning if Set
QER\ComplianceCheck\EmailNotification\NewExceptionApproval	This configuration parameter contains the name of the mail

Configuration parameter	Meaning if Set
	template, which is sent if an approval exception for a new rule violation is required.

If new rule violations are discovered during a rule check, exception approvers are notified and prompted to make an approval decision.

Prerequisites

- The option **Exception approval allowed** is set for the rule.
- An **Exception approver** application role is assigned to the rule.
- Employees are assigned to this application role.

To send demands for exception approval

- Set the configuration parameter "QER\ComplianceCheck\EmailNotification\NewExceptionApproval" in the Designer.

  Notification with the mail template "Compliance - new exception approval required" is sent to all exception approvers, by default.

TIP: To use something other than the default mail template for these notifications, change the value of the configuration parameter.

Notifications about Rule Violations without Exception Approval

Table 43: Configuration Parameters for Notifications about Rule Violations

Configuration parameter	Meaning if Set
QER\ComplianceCheck\EmailNotification\NotPermittedViolation	This configuration parameter contains the name of the mail template which is sent if a new rogue rule violation occurs.

If new rule violations are discovered during a rule check, which cannot be issued with exception approval, rule supervisors are notified.

Prerequisites

- The option **Exception approval allowed** is not set for the rule.
- A **Rule supervisor** application role is assigned to the rule.
- Employees are assigned to this application role.

To inform a rule supervisor about rule violations

- Set the configuration parameter "QER\ComplianceCheck\EmailNotification\NotPermittedViolation" in the Designer.

  Notification with the mail template "Compliance - prohibited violation occurred" is sent by default.

TIP: To use something other than the default mail template for these notifications, change the value of the configuration parameter.

Determining Potential Rule Violations

In addition to locating existing rule violations, the One Identity Manager can also identify potential violations of IT Shop requests. To do this, you add an approval step with the approval procedure "CR - Compliance check simplified" in the approval process in the IT Shop.

To identify rule violations through IT Shop requests, auxiliary tables are evaluated for object assignments and the affected employees. These auxiliary tables are regularly updated by the DBQueue Processor. Changes to a rule are calculated immediately in the auxiliary tables.

The schedule "default schedule compliance rule fill" is included in the default One Identity Manager installation to add changes, such as, changes to entitlements or an extended property in the rule check. This schedule generates processing tasks, on a cyclical basis, for updating the auxiliary table. Create your own schedule to customize the auxiliary table calculation cycle meet your own requirements.

To customize the auxiliary table calculation cycle to meet your requirements

1. Select the category **Identity Audit | Basic configuration data | Schedules**.
2. Click in the result list toolbar.
3. Edit the schedule's master data.
4. Save the changes.
5. Select **Assign rules (for filling)** in the task view and assign all the rules to the schedule to which it applies.
6. Save the changes.

NOTE:

Rule checking does not completely check the requests. It is possible that under the following conditions, rule checking does not identify a rule violation.

- Customer permissions change after the auxiliary table have been calculated.
- A rule is not violated by the requested product but by an object inherited through the requested product. Inheritance is calculated after request approval and can therefore not be identified until after the auxiliary table is calculated again.
- The customer does not belong to the rule's employee group effected until the request is made.
- The rule condition was created in expert node or as an SQL query.

TIP: A complete check of assignments is achieved with cyclical testing of compliance rule using schedules. This finds all the rule violations that result from the request.

It is possible that under the following conditions, rule checking identifies a rule violation where there isn't one.

- Two products violate one rule when they are assigned at the same time. The product requests are, however, for a limited period. The validity periods does not overlap. Still a potential rule violation is identified.

TIP: These requests can be approved after checking by exception approver in so far as permitted by the definition of the violation rule.

For more detailed information about compliance checking IT Shop requests, see the One Identity Manager IT Shop Administration Guide.

Related Topics

- Schedules for Checking Rules on page 13
- Assign Rules on page 16

Creating Custom Mail Templates for Notifications

A mail template consists of general master data such as target format, important or mail notification confidentiality and one or more mail definitions. Mail text is defined in several languages in the mail template. This ensures that the language of the recipient is taken into account when the email is generated.

There is a One Identity Manager in the Mail Template Editor to simplify writing notifications. You can use the Mail Template Editor to create and edit mail text in WYSIWYG mode.

To edit mail templates

1. Select the category **Identity Audit | Basic configuration data | Mail templates**.

   This shows all the mail templates that can be used for Identity Audit in the result list.
2. Select the mail template in the result list. Select **Change master data** in the task view.

   – OR –

   Click in the result list toolbar.

   This opens the mail template editor.
3. Edit the mail template.
4. Save the changes.

To copy a mail template

1. Select the category **Identity Audit | Basic configuration data | Mail templates**.
2. Select the mail template you want to copy from the result list. Select **Change master data** in the task view.
3. Select **Copy mail template...** in the task view.
4. Enter the name of the new mail template in **Name of copy**.
5. Click **OK**.

To display a mail template preview

1. Select the category **Identity Audit | Basic configuration data | Mail templates**.
2. Select the template in the result list. Select **Change master data** in the task view.
3. Select **Preview...** in the task view.
4. Select the base object.
5. Click **OK**.

To delete a mail template

1. Select the category **Identity Audit | Basic configuration data | Mail templates**.
2. Select the template in the result list.
3. Click in the result list toolbar.
4. Confirm the security prompt with **Yes**.

General Properties of a Mail Template

The following general properties are displayed for a mail template:

Table 44: Mail Template Properties

Property	Meaning
Mail template	Name of the mail template. This name will be used to display the mail templates in the administration tools and in the Web Portal. Translate the given text using the button.
Base object	Mail template base object. A base object only needs to be entered if the mail definition properties of the base object are referenced. Use the base object `ComplianceRule` or `PersonInNonCompliance` for notifications about rule violations.
Report (parameter set)	Report, made available through the mail template.
Description	Mail template description. Translate the given text using the button.
Target format	Format in which to generate email notification. Permitted values are: **Value** — **Description** HTML — The email notification is formatted in HTML format. HTML format can contain formatting. TXT — The email notification is formatted in text format. Text format cannot contain any formatting.
Design type	Design in which to generate the email notification. Permitted values are: **Value** — **Description** Mail template — The generated email notification contains mail text corresponding to the mail definition. Report — The email notification is generated with the report contained under **Report (parameter set)** as mail body. Mail template, report as attachment — The generated email notification contains mail text corresponding to the mail definition. The report entered in the **Report (parameter set)** field is attached to the mail as PDF file.
Importance	Importance for the email notification. Permitted values are "low", "normal" and "high".
Confidentiality	Confidentiality for the email notification. Permitted values are "normal", "personal", "private" and "confidential".
Can unsubscribe	Specifies whether the recipient can unsubscribe email notification. If this option is set, the emails can be unsubscribed through the Web Portal.

Property	Meaning
Disabled	Specifies whether this mail template is disabled.
Mail definitions	Unique name for the mail definition.
Language culture	Language which applies to the mail template.
Subject	Subject of the email message
Mail body	Content of the email message.

Creating and Editing an Email Definition

Mail texts can be defined in these different languages in a mail template. This ensures that the language of the recipient is taken into account when the email is generated.

To create a new mail definition

1. Open the mail template in Mail Template Editor.
2. Click the button next to the **Mail definition** list.
3. Select the language culture you want the mail definition to apply to from the **Language culture** menu.

   All active language cultures are shown in the list.To use other languages, enable the corresponding countries in the Designer. For more information, see theOne Identity Manager Configuration Guide.
4. Enter the subject in the **Subject** field.
5. Edit the mail text in the **Mail definition** view with the help of the Mail Text Editor.
6. Save the changes.

To edit an existing mail definition

1. Open the mail template in Mail Template Editor.
2. Select the language in the **Mail definition** list.
3. Edit the mail subject line and the body text.
4. Save the changes.

Using Base Object Properties

You can use all the properties of the object entered under **Base object** in the subject line and in the mail body. You can also use the object properties that are referenced by foreign key relation.

To access properties use dollar notation. For more information, see the One Identity Manager Configuration Guide.

Use of Hyperlinks in the Web Portal

Table 45: Configuration Parameters for the Web Portal URL

Configuration parameter	Active Meaning
QER\WebPortal\BaseURL	Web Portal URL This address is used in mail templates to add hyperlinks to the Web Portal.

You can insert hyperlinks to the Web Portal in the mail body. If the recipient clicks on the hyperlink in the email, the Web Portal is opened on that web page and further actions can be carried out. In the default version, this method is implemented in Identity Audit.

Prerequisites for using this method

- The configuration parameter "QER\WebPortal\BaseURL" is set and contains the Web Portal URL.

  `http://<Server>/<App>`

  with:

  `<Server> = Server name`

  `<App> = Web Portal installation directory path`

To add a hyperlink to the Web Portal into the mail text

1. Click in the mail body at the point where you want to add the hyperlink.
2. Open the context menu and select **Hyper Link...**.
3. Enter the hyperlink in **Display text**.
4. Set the option **File or website**.
5. Enter the address of the page to be opened in the Web Portal in **Address**.

   Use the default functions.
6. To accept the input, click **OK**.

Default Functions for Creating Hyperlinks

Several default functions are available to help you create hyperlinks. You can use these functions to directly insert a hyperlink in a mail body or into processes.

Direct Function Input

A function is referenced in the **Address** field when a hyperlink is inserted:

```
$Script(<Function>)$
```

Example:

```
$Script(VI_BuildComplianceLink_Show)$
```

Default Functions for Identity Audit

The script `VI_BuildComplianceLinks` contains a collection of default functions for composing hyperlinks for exception approval of rule violations.

Table 46: Functions of the Script, "VI_BuildComplianceLinks"

Function	Usage
VI_BuildComplianceLink_Show	Opens the exception approval page in the Web Portal.

Customizing Email Signatures

Configure the email signature for mail templates using the following configuration parameter.

Table 47: Configuration Parameters for Email Signatures

Configuration Parameter	Description
Common\MailNotification\Signature	Data for the signature in email automatically generated from mail templates.
Common\MailNotification\Signature\Caption	Signature under the salutation.
Common\MailNotification\Signature\Company	Company name.
Common\MailNotification\Signature\Link	Link to company website.

The script `VI_GetRichMailSignature` combines the components of an email signature according to the configuration parameters for use in mail templates.

2

Mitigating Controls

Table 48: Configuration Parameter for Risk Assessment

Configuration parameter	Active Meaning
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 set, a value for the risk index can be entered and calculated.

Effective permissions of employees, roles or user accounts are checked in the context of Identity Audit on the basis of regulatory requirements. Violation of regulatory requirements can harbor different risks for companies. To evaluate these risks, you can apply risk indexes to compliance rules, and company policies. These risk indexes provide information about the risk involved for the company in violating the respective rule, function. 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 a compliance rule was violated. The next rule check should not find any rule violations once the controls have been applied.

An example of a mitigating control is the assignment of system entitlements only through authorized requests in the IT Shop. If system entitlements are issued to the employee through the IT Shop, a rule check can be integrated into the request's approval procedure. System entitlements that would lead to a rule violation are therefore assigned not at all or only after gaining exception approval. The risk that rules are violated is thus reduced.

To edit mitigating controls

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

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

General Master Data for a Mitigating Control

To edit mitigating controls

1. Select the category **Risk index functions | Mitigating controls**.
2. Select a mitigating control in the result list. Select **Change master data** in the task view.

   - OR -

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

Enter the following master data for mitigating controls.

Table 49: 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 apply different tasks to it. The task view contains different forms with which you can run the following tasks.

The 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 the category **Risk index functions | Mitigating controls**.
2. Select the mitigating control in the result list.
3. Select the task **Mitigating control overview**.

Assigning Rules

Use this task to specify for which compliance rules a mitigating control is valid. You can only assign original rules on the assignment form.

To assign compliance rules to mitigating controls

1. Select the category **Risk index functions | Mitigating controls**.
2. Select the mitigating control in the result list.
3. Select the task **Assign rules**.
4. Double-click on the rules you want to assign in **Add Assignments**

   - OR -

   Double-click on the rules you want to remove in **Remove Assignment**.
5. Save the changes.

Calculating Mitigation

Table 50: Configuration Parameters for Calculating Risk Indexes of Rule Violations

Configuration Parameter	Active Meaning
QER\CalculateRiskIndex\MitigatingControlsPerViolation	This configuration parameter controls calculation of risk indexes for rule violations. If the parameter is set, exception approvers can assign mitigating controls to rule violations. The risk index calculation only takes these mitigating controls into account. If the parameter is disabled, risk index calculation take mitigating control assigned to compliance rules into account.

The significance reduction of a mitigating control supplies the value by which to reduce a compliance rule's risk index if 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.

Calculating mitigation for rule violations depends on the configuration parameter "QER\CalculateRiskIndex\MitigatingControlsPerViolation".

Table 51: Effect of the Configuration Parameter "QER\CalculateRiskIndex\MitigatingControlsPerViolation" on Calculating Mitigation

Configuration parameter	Effect
Disabled	The compliance rule's reduced risk index is calculated. This takes mitigating controls into account that are assigned to a compliance rule.
Enabled	The compliance rule's risk index is not reduced. The reduced risk index corresponds, therefore, to the compliance rule's risk index. The reduced risk index of employees with rule violations is calculated. This takes mitigating controls into account that were assigned to a rule violation during exception approval.

```
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.

A

Configuration Parameters for Identity Audit

The following configuration parameters are additionally available in One Identity Manager after the module has been installed. Some general configuration parameters are relevant for Identity Audit. The following table contains a summary of all applicable configuration parameters for Identity Audit.

Table 52: Overview of Configuration Parameters

Configuration parameter	Meaning
QER\ComplianceCheck	Preprocessor relevant configuration parameter to control component parts for Identity Audit. Changes to the parameter require recompiling the database. If the parameter is set the components can be used.
QER\ComplianceCheck\CalculateImmediately	Processing tasks for recalculating rule violations are immediately started when relevant changes occur.
QER\ComplianceCheck\DisableSelfExceptionGranting	Excludes rule violators from becoming exception approvers. If this parameter is set, no one can approve their own rule violations.

Configuration parameter	Meaning
QER\ComplianceCheck\EmailNotification	This parameter is used for mail notifications. Information about notifying during compliance checking is defined under this parameter.
QER\ComplianceCheck\EmailNotification\DefaultSenderAddress	This configuration parameter contains the sender email address for automatically generated messages during rule checking.
QER\ComplianceCheck\EmailNotification\NewExceptionApproval	This configuration parameter contains the name of the mail template which is sent if an approval exception for a new rule violation is required.
QER\ComplianceCheck\EmailNotification\NotPermittedViolation	This configuration parameter contains the name of the mail template which is sent if a new rogue rule violation occurs.
QER\ComplianceCheck\EnableITSettingsForRule	IT Shop properties for the compliance rule are visible and can be edited.
QER\ComplianceCheck\PlainSQL	SQL text is only permitted for rules in advanced mode.
QER\ComplianceCheck\SimpleMode	Preprocessor relevant configuration parameter for controlling the definition of rule conditions for compliance rules. Changes to the parameter require

Configuration parameter	Meaning
	recompiling the database. If this parameter is set, you can set up rule conditions with a simplified definition.
QER\ComplianceCheck\SimpleMode\NonSimpleAllowed	Rules can be created in advanced mode
QER\ComplianceCheck\SimpleMode\ShowDescriptions	Displays additional input fields for describing the compliance rules in the Rule Editor.
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 set, a value for the risk index can be entered and calculated.
QER\CalculateRiskIndex\MitigatingControlsPerViolation	This configuration parameter controls calculation of risk indexes for rule violations. If the parameter is set, exception approvers can assign mitigating controls to rule violations. The risk index calculation only takes these mitigating controls into account. If the parameter is disabled, risk index

Configuration parameter	Meaning
	calculation take mitigating control assigned to compliance rules into account.

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 or other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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

N

O

P

R

S

T

W