One Identity Manager 9.2

Compliance Rules Administration Guide

Contents

Compliance rules and identity audit

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

Figure 1: Identity audit in One Identity Manager
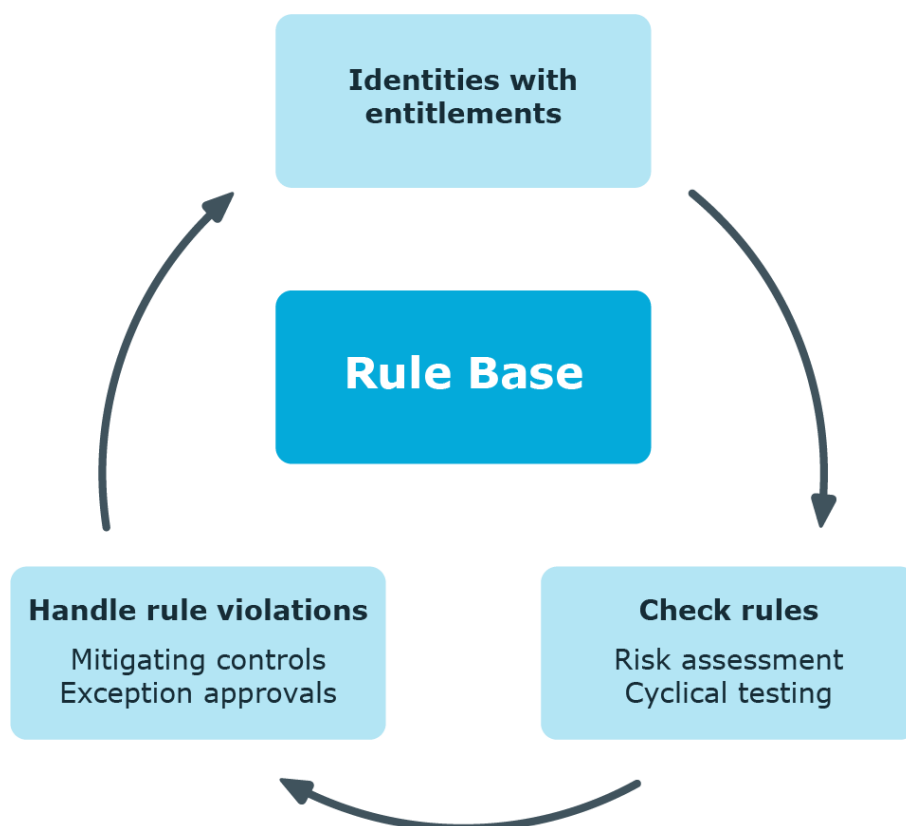
Simple rule examples are:

- An identity may not obtain two entitlements A and B at the same time.
- Only identities 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 One Identity Manager to:

- Define rules for any identity assignments
- Evaluate the risk of possible rule violations
- Specify mitigating controls
- Initiate regular or spontaneous rule checks
- Detailed testing of edit permissions for identities 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 made corrections to data in One Identity Manager and transfer them to the connected target systems. The integrated report function in One Identity Manager can be used to provide information for the appropriate tests.

To use the identity audit function

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

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

One Identity Manager users for identity audit

The following users are included in setting up and administration of the rule base and editing rule violations.

Table 1: Users

Users	Tasks
Administrators for Identity Audit	Administrators must be assigned to the **Identity & Access Governance	Identity Audit	Administrators** application role.
	Users with this application role:
	- Enter base data for setting up company policies.
	- Create compliance rules and assign rule supervisors to them.

Users	Tasks
	• 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 **Identity & Access Governance | Identity Audit | Rule supervisors** application role or a child application 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 Manager administrators	One Identity Manager administrator and administrative system users Administrative system users are not added to application roles.
	One Identity Manager administrators:
	• Create customized permissions groups for application roles for role-based login to administration tools in the Designer as required.
	• Create system users and permissions groups for non role-based login to administration tools in the Designer as required.
	• Enable or disable additional configuration parameters in the Designer as required.
	• Create custom processes in the Designer as required.
	• Create and configure schedules as required.
Exception approvers	Administrators must be assigned to the **Identity & Access**

Users	Tasks
	Governance | Identity Audit | Exception approvers application role or a child application 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 **Identity & Access Governance | Identity Audit | Attestors** application role.
	Users with this application role:
	• Attest compliance rules and exception approvals in the Web Portal for which they are responsible.
	• Can view main data for these compliance rules but not edit them.
	NOTE: This application role is available if the module Attestation Module is installed.
Compliance and security officer	Compliance and security officers must be assigned to the **Identity & Access Governance | Compliance & Security Officer** application role.
	Users with this application role:
	• View all compliance relevant information and other analysis in the Web Portal. This includes attestation policies, company policies and policy violations, compliance rules, and rule violations and risk index functions.
	• Edit attestation polices.
Auditors	Auditors are assigned to the **Identity & Access Governance | Auditors** application role.
	Users with this application role:
	• See the Web Portal all the relevant data for an audit.

Basic data for setting up rules

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

Rule groups:

Rule groups

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

To create or edit a rule group

1. In the Manager, select the **Identity Audit > Basic configuration data > Rule groups** category.

2. Select a rule group in the result list. Select the **Change main data** task.

   - OR -

   Click ➕ in the result list.

3. Edit the main data of the rule group.

4. Save the changes.

Enter the following data for a rule group

Table 2: Rule group properties

Property	Description
Group name	Name of the rule group.
Description	Text field for additional explanation.
Parent group	Rule group above this one in a hierarchy.
	To organize rule groups hierarchically, select the parent rule group in the menu.

Assigning compliance rules to rule groups

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

To assign compliance rules to a rule group

1. In the Manager, select the **Identity Audit > Basic configuration data > Rule groups** category.

2. Select the rule group in the result list.

3. Select the **Assign rules** task.

4. In the **Add assignments** pane, assign the compliance rules.

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

   ### *To remove an assignment*

   - Select the compliance rule and double-click ⊘.

5. Save the changes.

Displaying the rule group overview

You can display the most important information about a rule group on the overview form. In the **Rule violation overview** report, you can get an overview of all rule violations for a rule group.

To obtain an overview of a rule group

1. In the Manager, select the **Identity Audit > Basic configuration data > Rule groups** category.

2. Select the rule group in the result list.

3. Select the **Rule group overview** task.

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 create or edit compliance frameworks

1. In the Manager, select the **Identity Audit > Basic configuration data > Compliance frameworks** category.

2. Select a Compliance Framework in the result list and run the **Change main data** task.

   - OR -

   Click ➕ in the result list.

3. Edit the compliance framework main data.

4. Save the changes.

Enter the following properties for compliance frameworks.

Table 3: 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 for organizing compliance frameworks hierarchically.
Manager/supervisor	Application role whose members are allowed to edit all compliance rules assigned to this compliance framework
Description	Text field for additional explanation.

Assigning compliance rules to compliance frameworks

Use this task to assign compliance rules to the selected compliance framework.

To assign a compliance rule to compliance frameworks

1. In the Manager, select the **Identity Audit > Basic configuration data > Compliance frameworks** category.

2. Select the compliance framework from the result list.

3. Select the **Assign rules** task.

4. In the **Add assignments** pane, assign the compliance rules.

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

To remove an assignment

- Select the compliance rule and double-click ✓.

5. Save the changes.

Displaying the compliance frameworks overview

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

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

To obtain an overview of a compliance framework

1. In the Manager, select the **Identity Audit > Basic configuration data > Compliance frameworks** category.

2. Select the compliance framework from the result list.

3. Select the **Compliance framework overview** task.

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 create or edit schedules

1. In the Manager, select the **Identity Audit > Basic configuration data > Schedules** category.

   The result list shows all schedules configured for the `ComplianceRule` table.

2. Select a schedule in the result list. Select **Change main data**.

   – OR –

   Click 📄 in the result list.

3. Edit the schedule's main data.

4. Save the changes.

Enter the following properties for a schedule.

Table 4: 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. NOTE: Only active schedules are run. Active schedules are only run if the **QBM | Schedules** configuration parameter is set.
Time zones	Unique identifier for the time zone that is used for running the schedule. Choose between **Universal Time Code** or one of the time zones in the menu. 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. If this day conflicts with the defined interval type, the first run is on the next available day based on the start date.
Validity period	Period within which the schedule is run. • If the schedule will be run for an unlimited period, select the **Unlimited duration** option. • To set a validity period, select the **Limited duration** option and enter the day the schedule will be run for the last time in **End (date)**.

Occurs	Interval in which the task is run. Other settings may be required depending on the settings.
	
	• **Every minute**: The schedule is run once a minute. The starting point is calculated from the rate of occurrence and the interval type.
	
	• **Hourly**: The schedule is run at defined intervals of a multiple of hours such as every two hours.
	  • Under **Repeat every**, specify after how many hours the schedule is run again.
	  • The starting point is calculated from the rate of occurrence and the interval type.
	
	• **Daily**: The schedule is run at specified times in a defined interval of days such as every second day at 6am and 6pm.
	  • Under **Start time**, specify the times to run the schedule.
	  • Under **Repeat every**, specify after how many days the schedule is run again.

Property	Meaning

- **Weekly**: The schedule is run at a defined interval of weeks, on a specific day, at a specified time such as every second week on Monday at 6am and 6pm.
    - Under **Start time**, specify the times to run the schedule.
    - Under **Repeat every**, specify after how many weeks the schedule is run again.
    - Specify the set day of the week for running the schedule.
- **Weekly**: The schedule is run at a defined interval of months, on a specific day, at a specified time such as every second month on the 1st and the 15th at 6am and 6pm.
    - Under **Start time**, specify the times to run the schedule.
    - Under **Repeat every**, specify after how many months the schedule is run again.
    - Specify the days of the month (1st - 31st of the month).

    NOTE: If the **Monthly** interval type with the sub interval **29**, **30** or **31** does not exist in this month, the last day of the month is used.

    Example:

    A schedule that is run on the 31st day of each month is run on April 30th. In February, the schedule is run on the 28th (or 29th in leap year).
- **Yearly**: The schedule is run at a defined interval of years, on a specific day, at a specified time such as every year on the 1st, the 100th, and the 200th day at 6am and 6pm.
    - Under **Start time**, specify the times to run the schedule.
    - Under **Repeat every**, specify after how many years the schedule is run again.
    - Specify the days of the year (1st - 366th day of the year).

        NOTE: If you select the 366th day of the year, the schedule is only run in leap years.
- **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, **Sunday**: The schedule is run on a defined day of the week, in specified months, at specified times such as every second Saturday in January and June at 10am.
    - Under **Start time**, specify the times to run the schedule.
    - Under **Repeat every**, specify after how many days of the month the schedule is run again. The values **1** to **4**, **-1** (last day of the week), and **-2** (last day but one of the week) are permitted.

Property	Meaning
	• Specify in which month to run the schedule. The values **1** to **12** are permitted. If the value is empty, the schedule is run each month.
Start time	Fixed start time Enter the time in local format for the chosen time zone. If there is a list of start times, the schedule is started at each of the given times.
Repeat every	Rate of occurrence for running the schedule within the selected time interval.
Last planned run/Next planned run	Activation time calculated by the DBQueue Processor. Activation times are recalculated whilst the schedule is running. The time of the next run is calculated from the interval type, rate of occurrence, and the start time. NOTE: 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 for identity audit

One Identity Manager provides the following schedules for Identity Audit.

Table 5: Default schedules

Schedule	Description
Compliance rule check	Default schedule for checking rules. This schedule generates a processing task in the DBQueue Processor at regular intervals for each rule.
Fill compliance rule objects	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 cyclically generates processing tasks for updating the auxiliary tables.

Related topics

- Checking compliance rules on page 55
- Determining potential rule violations on page 65

Assigning compliance rules to schedules

Use this task to assign compliance rules to the selected schedule, which will check them. By default, the **Fill compliance rule objects** and **Compliance rule check** schedules are assigned but you can use the assignments form to assign the selected schedule to any rules.

To assign the schedule to rules

1. In the Manager, select the **Identity Audit > Basic configuration data > Schedules** category.

2. Select the schedule in the result list.

3. Select the **Assign rules (for filling)** task.

   - OR -

   Select the **Assign rules (for testing)** task.

4. In the **Add assignments** pane, double-click the rules you want to assign.

5. Save the changes.

To change an assignment

1. In the Manager, select the **Identity Audit > Basic configuration data > Schedules** category.

2. Select the schedule in the result list.

3. Select the **Assign rules (for filling)** task.

   - OR -

   Select the **Assign rules (for testing)** task.

4. Select the **Show objects already assigned to other objects** menu item in the assignment form's context menu.

   This shows rules that are already assigned in other schedules.

5. In the **Add assignments** pane, double-click on one of these rules.

   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 for identity audit on page 16
- Extended data for compliance rules on page 33

Starting schedules immediately

To start a schedule immediately

1. In the Manager, select the **Identity Audit > Basic configuration data > Schedules** category.

2. Select the schedule in the result list.

3. Select the **Start immediately** task.

   A message appears confirming that the schedule was started.

Displaying the schedule overview

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

To obtain an overview of a schedule

1. In the Manager, select the **Identity Audit > Basic configuration data > Schedules** category.

2. Select the schedule in the result list.

3. Select the **Schedule overview** task.

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.

Creating property groups for extended properties

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. In the Manager, select the **Identity Audit > Basic configuration data > Extended properties** category.

2. Click in the result list.

3. Enter a name and description for the property group.

4. Save the changes.

Creating and editing extended properties

To create an extended property

1. In the Manager, select the **Identity Audit > Basic configuration data > Extended properties > <property group>** category.

2. Click in the result list.

3. On the main data form, edit the main data of the extended property.

4. Save the changes.

To edit main data of a extended property

1. In the Manager, select the **Identity Audit > Basic configuration data > Extended properties > <property group>** category.

2. Select the extended property in the result list. Select the **Change main data** task.

3. Edit the extended property's main data.

4. Save the changes.

Main data for extended properties

Enter the following data for an extended property.

Table 6: Extended property main 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 main data form. Extended properties are grouped by this property group in navigation.
	If you have to assign an extended property to several property groups, you can assign additional property groups.
Lower scope	Lower scope limit for further subdivision.

Property	Description
limit	
Upper scope limit	Upper scope limit for further subdivision.
Description	Text field for additional explanation.
Spare field no. 01 ... Spare field no. 10	Additional company-specific information. Use the Designer to customize display names, formats, and templates for the input fields.

Related topics

Assigning extended properties to 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.

If you want to assign more properties to a property group, use the **Assign extended properties** task.

To assign extended properties to a property group

1. In the Manager, select the **Identity Audit > Basic configuration data > Extended properties** category.

2. Select a property group in the result list.

3. Select the **Assign extended properties** task.

4. In the **Add assignments** pane, assign extended properties.

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

   ### *To remove an assignment*

   - Select the extended property and double-click ⊘.

5. Save the changes.

Related topics

Assigning additional property groups to 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. If an extended property needs to be assigned to several property groups, then you can use the **Assign property groups** task to assign additional property groups.

To assign an extended property to a property group

1. In the Manager, select the **Identity Audit > Basic configuration data > Extended properties > <property group>** category.

2. Select the extended property in the result list.

3. Select the **Assign property groups** task.

4. In the **Add assignments** pane, assign property groups.

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

   To remove an assignment

   - Select the property group and double-click ⊘.

5. Save the changes.

Related topics

- Main data for extended properties on page 19
- Assigning extended properties to property groups on page 20

Specifying scope limits for extended properties

You can subdivide extended properties by specifying scoped limits. You are not obliged to enter scoped limit. 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 limits:

- Basically, any string is permitted as a lower or upper scoped limit.
- 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.

Overview of extended properties

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. In the Manager, select the **Identity Audit > Basic configuration data > Extended properties > <property group>** category.

2. Select the extended property in the result list.

3. Select the **Extended property overview** task.

To obtain an overview of a property group

1. In the Manager, select the **Identity Audit > Basic configuration data > Extended properties** category.

2. Select a property group in the result list.

3. Select the **Property group overview** task.

Assigning objects to extended properties

You can assign extended properties to company resources, hierarchical roles, identities, and attestation cases.

To assign objects to an extended property

1. In the Manager, select the **Identity Audit > Basic configuration data > Extended properties > <property group>** category.

2. Select the extended property in the result list.

3. Select the **Assign objects** task.

4. In the **Table** menu, select the required object type.

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

5. In the **Add assignments** pane, assign objects.

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

   To remove an assignment
   - Select the object and double-click ⊘.

6. 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.

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

Example: Use of functional areas

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

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

To create or edit a functional area

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

   - OR -

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

Enter the following data for a functional area.

Table 7: Functional area properties

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

Compliance rules attestors

| NOTE: This function is only available if the Attestation Module is installed.

Identities 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 identities to this application role that are authorized to attest compliance rules. For more information about attestation, see the *One Identity Manager Attestation Administration Guide*.

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 the *One Identity Manager Authorization and Authentication Guide*.

Table 8: Default application roles for attestors

User	Tasks
Attestors for Identity Audit	Attestors must be assigned to the **Identity & Access Governance | Identity Audit | Attestors** application role.
	Users with this application role:
	• Attest compliance rules and exception approvals in the Web Portal for which they are responsible.
	• Can view main data for these compliance rules but not edit them.
	NOTE: This application role is available if the module Attestation Module is installed.

To add identities to default application roles for attestors

1. In the Manager, select the **Identity Audit > Basic configuration data > Attestors** category.

2. Select the **Assign identities** task.

3. In the **Add assignments** pane, add identities.

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

   To remove an assignment

   - Select the identity and double-click ⊘.

4. Save the changes.

Rule supervisors

You can assign compliance rules to identities 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 identities 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 Authorization and Authentication Guide*.

Table 9: Default application role for rule supervisors

User	Tasks
Rule supervisors	Rule supervisors must be assigned to the **Identity & Access Governance | Identity Audit | Rule supervisors** application role or a child application 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 add the identities to the default application as rule supervisors

1. In the Manager, select the **Identity Audit > Basic configuration data > Rule supervisors** category.

2. Select the **Assign identities** task.

3. In the **Add assignments** pane, add identities.

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

To remove an assignment

- Select the identity and double-click ✓.

4. Save the changes.

Exception approvers

Identities that 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 identities that 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 Authorization and Authentication Guide*.

Table 10: Default application role for exception approvers

User	Tasks
Exception approver	Administrators must be assigned to the **Identity & Access Governance | Identity Audit | Exception approvers** application role or a child application 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 add identities to default application roles for exception approvers

1. In the Manager, select the **Identity Audit > Basic configuration data > Exception approvers** category.

2. Select the **Assign identities** task.

3. In the **Add assignments** pane, add identities.

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

   To remove an assignment

   - Select the identity and double-click ✓.

4. Save the changes.

Related topics

- Granting exception approval on page 61

Standard reasons for rule violations

For exception approvals, you can specify reasons in the Web Portal that explain the individual approval decisions. You can freely formulate this text. You also have the option to predefine reasons. The exception approvers can select a suitable text from these standard reasons in the Web Portal and store it with the rule violation.

To create or edit standard reasons

1. In the Manager, select the **Identity Audit > Basic configuration data > Standard reasons** category.

2. Select a standard reason in the result list and run the **Change main data** task.

   - OR -

   Click ➕ in the result list.

3. Edit the main data of a standard reason.

4. Save the changes.

Enter the following properties for the standard reason.

Table 11: General main data of a standard reason

Property	Description
Standard reason	Reason text as displayed in the Web Portal.
Description	Text field for additional explanation.
Automatic Approval	Specifies whether the reason text is only used for automatic approvals by One Identity Manager for rule violations. This standard reason cannot be selected by exception approvals in the Web Portal.
	Do not set the 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 free text for the exception approval.
Usage type	Usage type of standard reason. Assign one or more usage types to allow filtering of the standard reasons in the Web Portal.

Related topics

- Predefined standard reasons for rule violations on page 28

Predefined standard reasons for rule violations

One Identity Manager provides predefined standard reasons. These are added to the policy violation by One Identity Manager during automatic approval. You can use the usage type to specify which standard reasons can be selected in the Web Portal.

To change the usage type

1. In the Manager, select the **Identity Audit > Basic configuration data > Standard reasons > Predefined** category.

2. Select the standard reason whose usage type you want to change.

3. Select the **Change main data** task.

4. In the **Usage type** menu, set all the actions where you want to display the standard reason in the Web Portal.

   Unset all the actions where you do not want to display the default reason.

5. Save the changes.

Related topics

- Standard reasons for rule violations on page 27

Setting up a rule base

You can define rules for maintaining and monitoring regulatory requirements in a rule base. A rule in 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 frameworks) 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 and editing compliance 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 **Identity & Access Governance | Identity Audit | Rule supervisors** application role can edit existing rules if they are entered as a rule supervisor in the general data.

To create a new rule

1. In the Manager, select the **Identity Audit > Rules** category.

2. Click ![icon] in the result list.

3. Enter the main data of the rule.

4. Save the changes.

   This adds a working copy.

5. Select the **Enable working copy** task. Confirm the security prompt with **OK**.

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

To edit an existing rule

1. In the Manager, select the **Identity Audit > Rules** category.

   a. Select the rule in the result list.

   b. Select the **Create working copy** task.

      The data from the existing working copy are overwritten by the data from the original rule after a prompt. This opens the working copy and you can edit it.

   - OR -

   In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.

   a. Select a working copy in the result list.

   b. Select the **Change main data** task.

2. Edit the working copy's main data.

3. Save the changes.

4. Select the **Enable working copy** task. Confirm the security prompt with **OK**.

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

General main data for compliance rules

Enter the following main data of a rule.

Table 12: 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 associ-

Property	Description
	ated rule violation is not changed.
Description	Text field 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 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 supervisors	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.
Mail template new violation	Mail template used to generate an email to inform rule supervisors or exception approvers about new rule violations.
Exception approval 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

Property	Description
	| 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 **QER | ComplianceCheck | SimpleMode | NonSimpleAllowed** configuration parameter is set.
Rule only for cyclical testing	Specifies whether the rule is only taken into account by cyclical testing.
	This option is only visible if the **QER | ComplianceCheck | SimpleMode | NonSimpleAllowed** configuration parameter 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 44
- Enabling and disabling compliance rules on page 42
- Rule groups on page 10
- Rule supervisors on page 25
- Exception approvers on page 26
- Exception approval over a limited period on page 62
- Compliance rules attestors on page 24
- Functional areas on page 23
- Creating rule conditions on page 44
- Rule conditions in advanced mode on page 52

Related topics

- Rule check analysis on page 57
- Granting exception approval on page 61
- Notifications about rule violations without exception approval on page 65
- Requesting exception approval on page 64

Risk assessment for rule violations

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

You can use 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. For more information about creating reports, see the *One Identity Manager Configuration Guide*.

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 13: Assessment criteria for a rule

Property	Description
Severity code	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, the values **low**, **average**, **high**, and **critical** are listed.
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 14: Risk index dependent on effects** _(see table below)_ This value can be changed. Use the slider to enter a value between **0** and **1**.

Table 14: Risk index dependent on effects

Significance	Risk index
Low	0.0
Medium	0.33
High	0.66
Critical	1.0

Property	Description
	0 … No risk
	1 … Every rule violation is a problem.
	The template adjusts the risk index when the significance is changed.
	This field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set.
Risk index (reduced)	Show the risk index taking mitigating controls into account. 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**.
	This field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set. The value is calculated by One Identity Manager and cannot be edited.
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

- Mitigating controls for compliance rules on page 73

Related topics

- Creating rule conditions on page 44
- Creating working copies for compliance rules on page 42

Extended data for compliance rules

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

Table 15: Extended main data of a rule

Property	Description
Rule number	Additional name for the rule.
Implementation	Text field for additional explanation. You can use implementation

Property	Description
notes	notes to enter explanations about the content of the rule condition, for example.
Test schedule	Schedule for starting rule checks on a regular basis.
	By default, the **Compliance rule check** schedule is assigned but you can assign your own schedule.
Fill schedule	Schedule, which starts recalculation of the auxiliary tables for rule checking.
	By default, the **Fill compliance rule objects** schedule is assigned but 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 may be important for the next audit.

Related topics

- Checking compliance rules on page 55
- Determining potential rule violations on page 65

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 main data form.

Table 16: Results of a rule comparison

Rule violations	Lists all identities who, as a result of the change, would (not) violate the rule as follows
Newly added	Violate the rule for the first time
Identical	Still violate the rule
No longer included	Do not violate the rule anymore

TIP: In the Manager, all working copies with a different condition to that of the original rule are displayed in the **Identity audit > Rules > Working copies of rules > Modified working copies** category.

Detailed information about this topic

-

IT Shop properties for compliance rules

You can integrate checking requests for rule compliance into approval workflows in the 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 if the rule condition is created in the simplified version. For more information, see .

To enter IT Shop properties for a rule

1. In the Designer, set the **QER | ComplianceCheck | EnableITSettingsForRule** configuration parameter.
2. In the Manager, on the **General** tab of the rule's main data form, set the **Rule for cyclical testing and risk assessment in the IT Shop** option.
3. Select the **IT Shop properties** tab.
4. Edit the main data.
5. Save the changes.

Table 17: IT Shop properties

Property	Description
Rule violation identified	Specifies which rule violations are logged.

Table 18: Permitted values

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 **Explicit exception approval** option is set.

Property	Description
Explicit exception approval	Specifies whether exception approvals are presented again or whether existing exception approvals should be reused.

Table 19: Permitted values

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.
Not set	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 main data, you can run the following tasks.

Displaying the working copy overview

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

To obtain an overview of a working copy

1. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.
2. Select the rule in the result list.
3. Select the **Shelf overview** task.

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. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.

2. Select the working copy in the result list.

3. Select the **Assign compliance frameworks** task.

4. In the **Add assignments** pane, assign the compliance frameworks.

   TIP: In the **Remove assignments** pane, you can remove compliance framework assignments.

   ### To remove an assignment

   - Select the compliance framework and double-click ✅.

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

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

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

Detailed information about this topic

Assigning mitigating controls

Specify which mitigating controls apply to the selected role.

To assign mitigating controls to a rule

1. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.

2. Select the working copy in the result list.

3. Select the **Assign mitigating controls** task.

4. In the **Add assignments** pane, double-click the mitigating controls you want to assign.

   – OR –

   In the **Remove assignments** area, double-click mitigating controls to remove assignments.

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 information about this, 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. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.

2. Select a working copy in the result list.

3. Select the **Assign mitigating controls** task.

4. Select the **Create mitigating controls** task.

5. Enter the main data of the mitigating control.

6. Save the changes.

7. Select the **Assign rules** task.

8. In the **Add assignments** pane, double-click the rules you want to assign.

9. Save the changes.

Detailed information about this topic

- Mitigating controls for compliance rules on page 73

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. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.

2. Select the working copy in the result list.

3. Select the **Enable working copy** task.

4. Confirm the security prompt with **OK**.

TIP: In the Manager, all working copies with a different condition to that of the original rule are displayed in the **Identity audit > Rules > Working copies of rules > Modified working copies** category.

Recalculating

There are several tasks available for a working copy that immediately perform a rule check. For more information, see Checking compliance rules 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. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.

2. Select the working copy in the result list.

3. Select the **Change main data** task.

4. Select the **Copy rule** task.

5. Enter a name for the copy and click **OK**.

   This creates a working copy with the given name.

6. Click **Yes** to immediately edit the copy's main data.

   - OR -

   Click **Yes** to edit the copy's main data later.

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 **Rule comparison** tab of main data form.

To compare a rule with the working copy.

1. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.

2. Select the working copy in the result list.

3. Select the **Change main data** task.

4. Select the **Rule comparison** task.

Table 20: Results of a rule comparison

Rule violations	Lists all identities who, as a result of the change, would (not) violate the rule as follows
Newly added	Violate the rule for the first time
Identical	Still violate the rule
No longer included	Do not violate the rule anymore

To display the rule comparison as report

- In the Manager, select the **Show rule comparison** report.

Related topics

- Rule comparison on page 34

Maintaining exception approvers

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

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

To authorize identities as exception approvers

1. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.

2. Select the working copy in the result list.

3. Select the **Maintain exception approvers** task.

4. In the **Add assignments** pane, add identities.

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

To remove an assignment

- Select the identity and double-click ✅.

5. Save the changes.

Related topics

- General main data for compliance rules on page 29
- Exception approvers on page 26

Maintaining rule supervisors

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

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

To authorize identities as rule supervisors

1. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.
2. Select the working copy in the result list.
3. Select the **Maintain rule supervisors** task.
4. In the **Add assignments** pane, add identities.

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

   ### *To remove an assignment*

   - Select the identity and double-click ✅.

5. Save the changes.

Related topics

- General main data for compliance rules on page 29
- Rule supervisors on page 25

Enabling 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 53.

Additional tasks for compliance rules

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

Displaying the compliance rule overview

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

To obtain an overview of a rule

1. In the Manager, select the **Identity Audit > Rules** category.

2. Select the rule in the result list.

3. Select the **Shelf overview** task.

Creating working copies for compliance rules

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. In the Manager, select the **Identity Audit > Rules** category.

2. Select the rule in the result list.

3. Select the **Create working copy** task.

4. Confirm the security prompt with **Yes**.

TIP: In the Manager, all working copies with a different condition to that of the original rule are displayed in the **Identity audit > Rules > Working copies of rules > Modified working copies** category.

Enabling and disabling compliance 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. In the Manager, select the **Identity Audit > Rules** category.

2. Select the rule in the result list.

3. Select the **Enable rule** task.

To display a rule

1. In the Manager, select the **Identity Audit > Rules** category.

2. Select the rule in the result list.

3. Select the **Disable rule** task.

Recalculating

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

Copying compliance rules

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. In the Manager, select the **Identity Audit > Rules** category.

2. Select the rule in the result list.

3. Select the **Change main data** task.

4. Select the **Copy rule** task.

5. Enter a name for the copy and click **OK**.

    This creates a working copy with the given name.

6. Click **Yes** to immediately edit the copy's main data.

    - OR -

    Click **Yes** to edit the copy's main data later.

Maintaining exception approvers

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

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

To authorize identities as exception approvers

1. In the Manager, select the **Identity Audit > Rules** category.

2. Select the rule in the result list.

3. Select the **Maintain exception approvers** task.

4. In the **Add assignments** pane, add identities.

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

   To remove an assignment
   - Select the identity and double-click ⊘.

5. Save the changes.

Related topics

- General main data for compliance rules on page 29
- Exception approvers on page 26

Maintaining rule supervisors

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

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

To authorize identities as rule supervisors

1. In the Manager, select the **Identity Audit > Rules** category.
2. Select the rule in the result list.
3. Select the **Maintain rule supervisors** task.
4. In the **Add assignments** pane, add identities.

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

   To remove an assignment
   - Select the identity and double-click ⊘.

5. Save the changes.

Related topics

- General main data for compliance rules on page 29
- Rule supervisors on page 25

Creating rule conditions

In the rule condition, you combine all the entitlements that lead to a rule violation. In the rule condition, the identities and the entitlements affected are separately restricted. The affected identities are used to determine which identities and sub-identities the rule

condition is applied to. The affected entitlements are used to define the properties that result in the affected identities violating a rule. The entitlements are determined through the object relations of the affected persons (`PersonHasObject` table).

> TIP: If the **QER | ComplianceCheck | SimpleMode | NonSimpleAllowed** configuration parameter is set, rule conditions can be created in advanced mode as well as in the simplified definition.
>
> ***To use the simplified definition***
>
> - In the rule's general main data, enable the **Rule for cyclical testing and risk assessment in IT Shop** option.
>
> For more information, see Rule conditions in advanced mode on page 52.

Basics for using 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 **QER | ComplianceCheck | SimpleMode | ShowDescriptions** configuration parameter 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
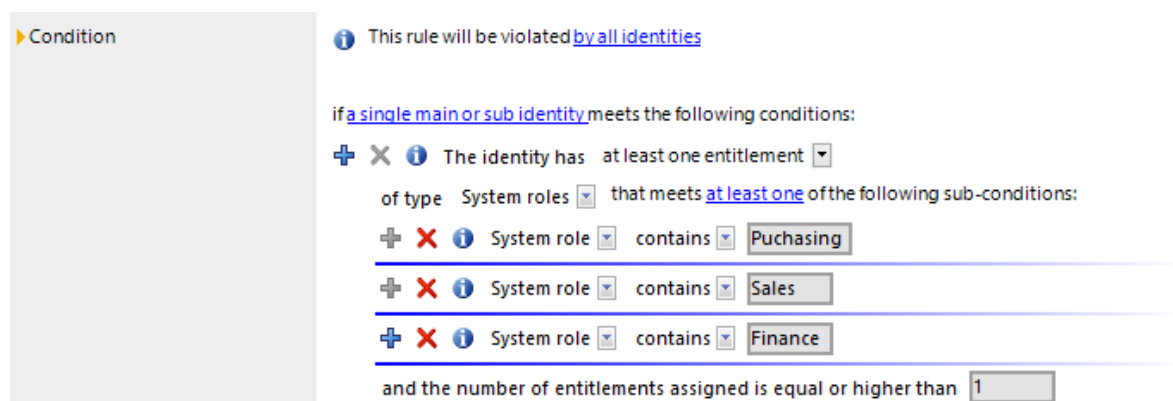
The Rule Editor control elements supply operators and properties that you need for formulating partial conditions. You can only select one entry from the drop-down menu. You can select more entries from extended drop-down menus, where the properties are displayed hierarchically and then added to the 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 person, with properties and assignments, can be matched to all the rule blocks.

There are two types of rule blocks:

- Affected identities

  Each rule must obtain exactly one rule block that determines the identities that the rule should be applied to. By default, all identities with all subidentities are taken into account. You can, however, restrict the identities further.

- 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 identities affected are defined here. You can check the following entitlements in the rule block: roles, target system groups, system entitlements, system roles, software, 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 21: 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 Rule Editor in the ⓘ.
2. Click 🔍 in the preview window to display the list of affected objects.

Specifying affected identities

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

Figure 3: Rule block for the identities affected
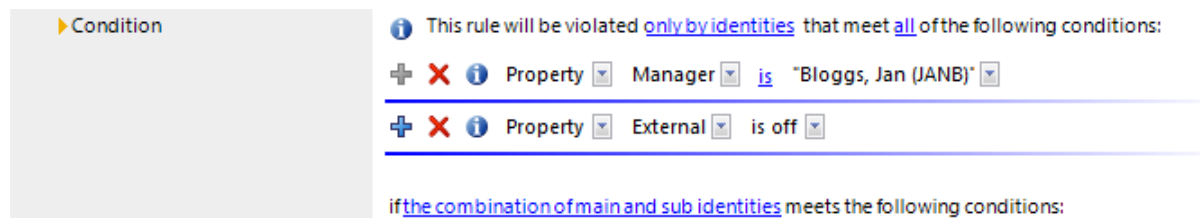
Use the following to options to limit the affected identity groups.

- **By all identities**

  All identities are taken into account.

- **only by identities** that fulfill **all|at least one** of the following conditions:

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

  You can specify a condition type in the first menu of the partial condition which restricts the affected identities.

  - **Property**: Identity properties. The permitted properties menu is already limited to the most important identity properties.

  - **For the user account with target system type**: Properties of the user accounts to which the identities are connected, having the selected target system type.

  - **SQL Clause**: Freely defined SQL condition (WHERE clause). For more information about the WHERE clause wizard, see the *One Identity Manager User Guide for One Identity Manager Tools User Interface*.

Specify whether the main or subidentities are taken individually or collectively into account by the rule check.

- **A single main or subidentity**

  If an identity has subidentities, they are considered individually and independently of another by the rule check. The rule is violated if the main identity or a subidentity satisfies the rule condition.

  The rule is not violated if the main identity satisfies the rule condition only because of its subidentities.

- **The combination of main and subidentities**

  If an identity has subidentities and the main identity belongs to the affected identities, they are considered collectively in the rule check. The rule is violated if:

  - the main identity or a subidentity fulfills the rule condition

    - OR -

  - the main identity fulfills the rule condition only due to its sub-identities.

  If the subidentity alone belongs to the affected identities, the rule is only violated if the subidentity fulfills the rule condition itself. If the main identity or another subidentity fulfills the rule condition, the rule for the determined subidentity is not violated.

For more information about main and subidentities, see the *One Identity Manager Identity Management Base Module Administration Guide*.

Related topics

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 identities. 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.

  Select the type of entitlement, such as a target system type or the **Resource** type, and define the partial condition.

  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.

- At least one role or organization assignment

  For each rule block, define the membership in a hierarchical role (application role, department, location, cost center, business role).

  Select the type of role, such as **Departments**, and define the partial condition.

- At least one function

  Enter at least one SAP function to replace the rule.

This option can only be selected if the SAP R/3 Compliance Add-on Module module is installed. For more information, see the *One Identity Manager Administration Guide for the SAP R/3 Compliance Add-on*.

- Number of entitlements

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

  By default, a rule violation is identified, if one affected identity is assigned at least one object that fulfills the condition of the rule block. You can increase this number. The value **0** is not valid.

Define the partial conditions as follows:

- **Properties**: Properties of the objects, such as **Distinguished name** or **Resource type**.
- **Assignments in other objects**: Assignments of objects to other objects, for example, the assignment of a department as primary department of various identities.
- **Memberships**: Memberships of entitlements in hierarchical roles and IT Shop structures. Assignments to identities or workdesks if the **System roles** permissions type has been selected.

  Assignments of company resources to the roles, such as `DepartmentHasADSGroup`.
- **Permissions controls**: Permissions controls defined for the selected target system.

  | NOTE: permissions controls are only created for custom target systems.
- **Has extended property** Extended properties assigned to the objects.
- **Has extended property in group**: Extended properties from the selected extended property group that are assigned to the objects.
- **Has extended property in range**: Extended properties assigned to the objects and for which a range of values is defined. The rule verifies the correct value.
- **SQL Clause**: Freely defined SQL condition (WHERE clause). For more information about the WHERE clause wizard, see the *One Identity Manager User Guide for One Identity Manager Tools User Interface*.

Related topics

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

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

Define:

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

Figure 5: Rule condition for example 1

Example 2

Identities from the department A or department B are not permitted to access the Active Directory group xyz. This rule is only checked for identities who are activated.

Define:

1. The **by all identities**, **all**, and **a single main or sub identity** options in the rule block for the affected identities.
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

This rule will be violated only by identities that meet all of the following conditions:

➕ ✖ ⓘ Property ▾ Disabled permanently ▾ is off ▾

if a single main or sub identity meets the following conditions:

➕ ✖ ⓘ The identity has at least one role or organization assignment ▾

of type Departments ▾ that meets at least one of the following sub-conditions:

➕ ✖ ⓘ Department ▾ equals ▾ Sales

➕ ✖ ⓘ Department ▾ equals ▾ Purchasing

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

➕ ✖ ⓘ and the identity has at least one entitlement ▾

of type Active Directory ▾ that meets all of the following sub-conditions:

➕ ✖ ⓘ Display name ▾ equals ▾ Development

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

Example 3

All permitted entitlements are assigned to persons through system roles. One identity can have a maximum of two system roles. If an identity has subidentities, the rule is also violated if the entitlements of main and sub identities result together in a rule violation.

There are three system roles: Package for department A, Package for department B, Package for department C

One identity has two subidentities. The main identity (HI) and the two subidentities (SI1 and SI2) are each assigned a system role.

HI: Package for department A

SI1: Package for department B

SI2: Package for department C

Define:

1. The **by all identities** and **the combination of main and sub identities** in the rule block for the affected identities
2. One rule block for the affected entitlements with the option **at least one entitlement** of type **System roles** that fulfills **at least one** of the following partial conditions
3. Three partial conditions: **System role is equal Package for department [A|B|C]**
4. The number of entitlements assigned is larger or equal to **3**.

Because the main identity has all three system roles due to its subidentities, the main identity violates this (and only this) rule.

Rule conditions 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 45.

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

To use advanced mode

1. In the Designer, set the **QER | ComplianceCheck | SimpleMode | NonSimpleAllowed** configuration parameter.

   On the main data form for a rule, the options **Rule for cyclical testing and risk assessment in IT Shop** and **Rule only for cyclical testing** are displayed.

2. Set **Rule only for cyclical testing**.

3. Confirm the security prompt with **Yes**.

   The filter designer is displayed.

NOTE:

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

- Rules in advanced mode are not taken into account by rule checks in the 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 main data form for this rule.

Figure 7: Advanced mode condition

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

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

> NOTE: If you select the **For the account with the target system type** or **For the entitlement with target system type** condition type in the filter designer, only columns that are mapped in Unified Namespace and for which the **Display in the filter designer** column property is enabled can be selected.

For more information about using the filter designer, see the *One Identity Manager User Guide for One Identity Manager Tools User Interface*.

Table 22: Permitted condition types

Condition Type	Meaning
Property	Properties of identities. The permitted properties menu is already limited to the most important identity properties.
For the account with the target system type	Identity's user account. Valid user account properties depend on which target system is selected.
For entitlements with the target system type	Identity target system group. Valid group properties depend on which target system is selected.
SQL Query	Free choice of SQL query (WHERE clause). To use the WHERE clause wizard, click ✨.

Rule condition as SQL query

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

To formulate a rule condition directly as an SQL query

1. In the Designer, set the **QER | ComplianceCheck | PlainSQL** configuration parameter.
2. Select **Rule only for cyclical testing**.
3. Select the **Enable SQL definition** task for the working copy.

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

Figure 8: Direct SQL query input
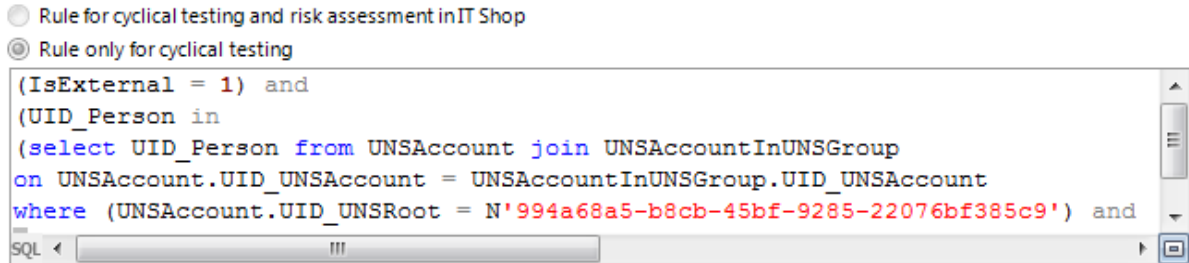
Deleting compliance rules

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. In the Manager, select the **Identity Audit > Rules** category.

2. Select the rule to delete in the result list.

3. Select the **Disable rule** task.

   Existing rule violations are removed by the DBQueue Processor.

4. 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. For each rule, the DBQueue Processor determines which identities have violated that rule. Follow-up tasks assign the associated rule violation object to identities that have violated a rule. The specified rule approvers can test rule violations and if necessary grant exception approval.

By default, permissions that an identity receives because they can use an administrative user account with shared identity are included in the rule check.

To exclude administrative user accounts with shared identity from rule checking

- In the Designer, disable the **QER | ComplianceCheck | IncludeTSBPersonUsesAccount** configuration parameter.

  Object relations from the `TSBPersonUsesAccount` table are ignored when calculating entries for the `PersonHasObject` table.

Checking compliance rules

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 identities are assigned the corresponding object for rule violations. You can check all the rules again for these identities. For more information, see Rule check analysis on page 57.

In addition to locating existing rule violations, 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 65.

Scheduled rule checking

The **Compliance rule check** schedule, is supplied with the One Identity Manager 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

Rule checking rule modifications

A processing task for rule checking is generated the moment an active rule is modified or deleted. All identities 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 **QER | ComplianceCheck | CalculateImmediately** configuration parameter. If the parameter is set, the processing task for recalculating rule violation for an identity 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

- In the Designer, set the **QER | ComplianceCheck | CalculateImmediately** configuration parameter.

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

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

- Changes to identity main data
- Changes to identity assignments (for example, the `PersonHasQERResource` table)
- Changes to identities' role memberships
- Changes to membership in system entitlements (for example, the `ADSAccountInADSGroup` table)
- Changes to SAP function matches (the `SAPUserInSAPFunction` table)

Ad-hoc rule checking

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

Table 23: Additional tasks for rules

Task	Description
Recalculate rule	All identities are checked to see if they comply to the current rule.
Recalculate for current user	All identities are checked to see if they comply to all rules.
Recalculate all	All identities 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. For example, this may happen if a lot of rules exist in which the identities affected are not limited ("This rule is broken by all identities"). One Identity Manager supplies two consistency checks for optimizing the performance of calculating affected identities. 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. In the Manager, select the **Database > Check data consistency** menu item.

2. Click ✪ in the Consistency Editor's toolbar.

3. Click ⚠ in the "Test options" dialog's toolbar.

4. Set the **Content > Compliance > ComplianceRule change IsPersonStoreInverted to 1** and **Content > Compliance > ComplianceRule change IsPersonStoreInverted to 0** checks.

5. Click **OK**.

6. Run the consistency check for the **Database** object.

7. Verify the analysis results.

   > TIP: For details about an error message
   >
   > 1. Select the error message.
   > 2. Click ❌ in the toolbar.

8. To optimize the rule condition for an affected rule

   a. Select the error message.

   b. Click on **Repair** both for the original rule and the working copy.

For more information about consistency checking, see the *One Identity Manager Operational Guide*.

Related topics

- Creating working copies for compliance rules on page 42

Rule check analysis

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

Which identities violate a specific rule?

To display identities that violate a rule

1. In the Manager, select the **Identity Audit > Rule violations** category.
2. Select a rule violation in the result list.
3. Select the **Show rule violations** task.

   This displays all identities assigned to the rule violation.

Table 24: Meaning of rule evaluation icons

Icon	Meaning
🔵	Identities pending a rule violation decision.
🟢	Identities granted exception approval for their rule violation.
🔴	Identities not granted exception approval for their rule violation.

Which rules are violated by a specific identity?

To view which rules the identity violates

1. In the Manager, select the **Identities > Identities** category.
2. Select an identity in the result list.
3. Select the **Rule evaluation** report.

   This not only shows the rule that the identity has violated with or without exception, but also those the identity does not violate.

Table 25: Meaning of icons in identity 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 26: Reports about rule violations

Report	Description
Overview of all assignments (of a rule)	This report shows all identities that violate the selected rule. The report shows which roles of a role class the identity belongs to. Identities that are not members of any role are not taken into account.
Rule violations overview (of a rule)	This report groups together all rule violations for the selected rule. All identities are listed that have objects that violation the rule. The result list is grouped by: • Identities pending a rule violation decision. • Identities without exception approval. • Identities with exception approval.
Show historical rule violations (of a rule)	This report groups together all historical rule violations for the selected rule. All identities are listed that violate the rule as well as the time period covering the rule violation.
Rule violations overview (of 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 violations overview (of 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 (of a compliance framework)	This report groups together all rule violations for the selected compliance framework. All rule violations are listed. For each rule, the identity 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 **Overview of all assignments** report is displayed for some objects, such as authorizations, 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 identities 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 identities with this resource.
> - If the report is created for a group or another system entitlement, all roles are determined in which there are identities with this group or system entitlement.
> - If the report is created for a compliance rule, all roles are determined in which there are identities who violate this compliance rule.
> - If the report is created for a department, all roles are determined in which identities of the selected department are also members.
> - If the report is created for a business role, all roles are determined in which identities 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 **Overview of all assignments** report.

- Click the ⊹ **Used by** button in the report toolbar to select the role class for which you want to determine whether roles exist that contain identities 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 identities with the selected base object. The meaning of the report control elements is explained in a separate legend. To access the legend, click the ⓘ icon in the report's toolbar.

- 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 identities 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 identities for tracking. This creates a new business role to which the identities are assigned.

Figure 9: Toolbar of the Overview of all assignments report.
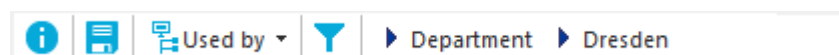
Table 27: Meaning of icons in the report toolbar

Icon	Meaning
ℹ	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

Assignments that violate rules can be approved in hindsight. To do this, specially authorized identities can grant exception approval.

Prerequisites

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

NOTE: If the **Exception approval allowed** option 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 identity that violates a rule is determined to be the exception approver for this rule if they are a member of the **Exception approvers** application role for the rule. This means they can approve their own rule violations.

To prevent an identity from granting themselves exception approval

- In the Designer, disable the **QER | ComplianceCheck | DisableSelfExceptionGranting** configuration parameter.

  Identities 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

- General main data for compliance rules on page 29
- *One Identity Manager Web Designer 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. In the Manager, select the **Identity Audit > Rules > Working copies of rules** category.

    b. Select a working copy from the result list.

    c. Select the **Change main data** task.

    d. On the **General** tab, in the **Validity period (max. # days)** field, enter the number of days for which exception approvals may apply for this rule.

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

    e. Save the changes.

    f. To transfer the change to the active rule, select the **Enable working copy** task.

2. In the Designer, configure and enable the **Reset exception approval of compliance rule violations** schedule.

For more information about setting up schedules, see the *One Identity Manager Operational Guide*.

Granting exception approvals 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 to identities violating a particular rule

1. In the Manager, select the **Identity Audit > Rule violations** category.

2. Select the rule violation in the result list.

3. Select the **Show rule violations** task.

4. Double-click to select the identity you want to grant exception approval to.

   This opens the **Edit rule violations** form.

5. To obtain detailed information about the identity, select the identity.

6. To obtain an overview of the rule violation, select the rule violation.

7. Enter a reason

8. To approve the rule violation for this identity, select **Approve exception**.

   The **Approver** and **Approval date** fields and set the **Exception is approved** and **Checked** options are preselected.

9. To deny exception approval for this identity, select **Deny exception**.

   The **Approver** and **Approval date** fields and the **Checked** option are preselected.

10. Save the changes.

To grant exception approval for rules violated by a specific identity

1. In the Manager, select the **Identities > Identities** category.

2. Select the identity in the result list.

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

4. Double-click to select the rule violation for the identity to grant exception approval to.

   This opens the **Edit rule violations** form.

5. To obtain detailed information about the identity, select the identity.

6. To obtain an overview of the rule violation, select the rule violation.

7. Enter a reason

8. To approve the rule violation for this identity, select **Approve exception**.

   The **Approver** and **Approval date** fields and set the **Exception is approved** and **Checked** options are preselected.

9. To deny exception approval for this identity, select **Deny exception**.

   The **Approver** and **Approval date** fields and the **Checked** option are preselected.

10. Save the changes.

Related topics

- Which rules are violated by a specific identity? on page 58
- Which identities violate a specific rule? on page 58

Notifications about rule violations

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

To use email notifications

1. Ensure that the email notification system is configured in One Identity Manager. For more information, see the *One Identity Manager Installation Guide*.

2. In the Designer, set the **QER | ComplianceCheck | EmailNotification** configuration parameter.

3. In the Designer, set the **QER | ComplianceCheck | EmailNotification | DefaultSenderAddress** configuration parameter and enter the sender address used to send the email notifications.

4. Ensure that all identities have a default email address. Notifications are sent to this address. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

5. Ensure that a language can be determined for all identities. Only then can they receive email notifications in their own language. For more information, see the *One Identity Manager Identity Management Base Module Administration Guide*.

6. Configure the notification procedure.

Related topics

Requesting exception approval

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

Prerequisites

- Exception approvals for rule violations are permitted.
- An **Exception approver** application role is assigned to the rule.
- Identities are assigned to this application role.

To send requests for exception approval

- Enter the following data for the compliance rule.
    - **Exception approval allowed**: Enabled
    - **Mail template new violation**: Compliance - new exception approval required

TIP: To use a mail template other than the standard for these notifications, create a mail template with the `ComplianceRule` base object.

Related topics

-
-
-

Notifications about rule violations without exception approval

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

Prerequisites

- Exception approvals for rule violations are not permitted.
- A **Rule supervisor** application role is assigned to the rule.
- Identities are assigned to this application role.

To inform a rule supervisor about rule violations

- Enter the following data for the compliance rule.
  - **Exception approval allowed**: Not enabled
  - **Mail Template New Violation**: Compliance - prohibited violation occurred

    TIP: To use a mail template other than the standard for these notifications, create a mail template with the `ComplianceRule` base object.

Related topics

-
-
-

Determining potential rule violations

In addition to locating existing rule violations, One Identity Manager can also identify potential violations of IT Shop requests. To do this, you add an approval step with the **CR - Compliance check simplified** approval procedure 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 identities. These auxiliary tables are regularly updated by the DBQueue Processor. Changes to a rule are calculated immediately in the auxiliary tables.

The **default schedule compliance rule fill** schedule is included in the One Identity Manager default 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. In the Manager, select the **Identity Audit > Basic configuration data > Schedules** category.

2. Click ⊞ in the result list.

3. Edit the schedule's main data.

4. Save the changes.

5. Select the **Assign rules (for filling)** task 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.

- If memberships are requested in business role or organization, a rule is violated by an object that is inherited through the business role or organization. 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 identities affected by a rule 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 one does not exist:

- 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 as permitted by the definition of the violation rule.

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

Related topics

-
-

Mail templates for notifying about identity auditing

One Identity Manager supplies mail templates by default. These mail templates are available in English and German. If you require the mail body in other languages, you can add mail definitions for these languages to the default mail template.

To edit a default mail template

- In the Manager, select the **Identity Audit > Basic configuration data > Mail templates > Predefined** category.

Related topics

-
-
-
-
-

Creating and editing mail definitions for Identity Audit

For more information about creating and editing mail template, see the *One Identity Manager Operational Guide*.

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. In the Manager, select the **Identity Audit > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for Identity Audit in the result list.

2. Select a mail template in the result list and run the **Change main data** task.

3. In the result list, select the language for the mail definition in the **Language** menu.

   All active languages are shown. To use another language, in the Designer, enable the corresponding countries. For more information, see the *One Identity Manager Configuration Guide*.

4. Enter the subject in **Subject**.

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. In the Manager, select the **Identity Audit > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for Identity Audit in the result list.

1. Select a mail template in the result list and run the **Change main data** task.

2. In the **Mail definition** menu, select the language for the mail definition.

   NOTE: If the **Common | MailNotification | DefaultCulture** configuration parameter is set, the mail definition is loaded in the default language for email notifications when the template is opened.

3. Edit the mail subject line and the body text.

4. Save the changes.

Related topics

- Base objects for mail templates using Identity Audit on page 68
- Use of hyperlinks in the Web Portal on page 69
- Default functions for creating hyperlinks on page 70

Base objects for mail templates using Identity Audit

NOTE: Use the `ComplianceRule` or `PersonInNonCompliance` base objects in the mail templates for notifications about rule violations.

In the subject line and body text of a mail definition, you can use all properties of the object entered under **Base object**. 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*.

Related topics

Use of hyperlinks in the Web Portal

You can add hyperlinks to the Web Portal in the mail text of a mail definition. If the recipient clicks on the hyperlink in the email, the Web Portal opens 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 **QER | WebPortal | BaseURL** configuration parameter is enabled and contains the URL to the API Server. You edit the configuration parameter in the Designer.

  `http://<server name>/<application>`

  with:

  `<server name> = name of server`

  `<application> = path to the API Server installation directory`

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

1. Click the position in the mail text of the mail definition where you want to insert a hyperlink.

2. Open the **Hyperlink** context menu and enter the following information.

   - **Display text**: Enter a caption for the hyperlink.
   - **Link to**: Select the **File or website** option.
   - **Address**: Enter the address of the page in the Web Portal that you want to open.

     NOTE: One Identity Manager provides a number of default functions that you can use to create hyperlinks in the Web Portal.

3. To accept the input, click **OK**.

Related topics

Default functions for creating hyperlinks

Several default functions are available to help you create hyperlinks. You can use the functions directly when you add a hyperlink in the mail body of a mail definition or in processes

Direct function input

You can reference a function when you add a hyperlink in the **Address** field of the **Hyperlink** context menu.

Syntax:

`$Script(<Function>)$`

> **Example:**
>
> `$Script(VI_BuildComplianceLink_Show)$`

Default functions for identity audit

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

Table 28: Functions of the VI_BuildComplianceLinks script

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

Related topics

- Use of hyperlinks in the Web Portal on page 69

Editing mail templates for identity auditing

For more information about creating and editing mail template, see the *One Identity Manager Operational Guide*.

A mail template consists of general main data such as target format, importance, 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.

To create and edit mail templates

1. In the Manager, select the **Identity Audit > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for Identity Audit in the result list.

2. Select a mail template in the result list and run the **Change main data** task.

   - OR -

   Click ➕ in the result list.

   This opens the mail template editor.

3. Edit the mail template.

4. Save the changes.

To copy a mail template

1. In the Manager, select the **Identity Audit > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for Identity Audit in the result list.

2. Select the mail template that you want to copy in the result list and run the **Change main data** task.

3. Select the **Copy mail template** task.

4. Enter the name of the new mail template in the **Name of copy** field.

5. Click **OK**.

To display a mail template preview

1. In the Manager, select the **Identity Audit > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for Identity Audit in the result list.

2. Select a mail template in the result list and run the **Change main data** task.

3. Select the **Preview** task.

4. Select the base object.

5. Click **OK**.

To delete a mail template

1. In the Manager, select the **Identity Audit > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for Identity Audit in the result list.

2. Select the template in the result list.

3. Click ✖ in the result list.

4. Confirm the security prompt with **Yes**.

Related topics

- Creating and editing mail definitions for Identity Audit on page 67

Mitigating controls for compliance rules

Effective permissions of identities, 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. These risk indexes provide information about the risk involved for the company if a particular rule is violated. Once the risks have been identified and evaluated, mitigating controls can be implemented.

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

Mitigating controls describe controls that are implemented if 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 identities through the IT Shop, a rule check can be integrated into the request's approval process. 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

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

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

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

Creating and editing mitigating controls for compliance rules

To create or edit mitigating controls

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

   - OR -

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

Enter the following main data of mitigating controls.

Table 29: General main data of a mitigating control

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

Assigning compliance rules to mitigating controls

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. In the Manager, select the **Risk index functions > Mitigating controls** category.
2. Select the mitigating control in the result list.
3. Select the **Assign rules** task.
4. In the **Add assignments** pane, assign the compliance rules.

> **TIP:** In the **Remove assignments** pane, you can remove assigned compliance rules.
>
> ***To remove an assignment***
>
> - Select the compliance rule and double-click ✓.

5. Save the changes.

Displaying the mitigation controls overview

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

To obtain an overview of a mitigating control

1. In the Manager, select the **Risk index functions > Mitigating controls** category.

2. Select the mitigating control in the result list.

3. Select the **Mitigating control overview** task.

Calculating mitigating controls fro compliance rules

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

Calculating mitigation for rule violations depends on the **QER | CalculateRiskIndex | MitigatingControlsPerViolation** configuration parameter.

Table 30: Effect of configuration parameters on calculating mitigation

Configuration parameters	Effect
Deactivated	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

Configuration parameters	Effect
	corresponds, therefore, to the compliance rule's risk index.
	This calculates the reduced risk index of identities with rule violations and takes into account mitigating controls that were assigned to a rule violation during an 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**.

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 31: 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 enabled, you can use the model components.
	If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
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.
QER	ComplianceCheck	EmailNotification	This parameter is used for mail notifications.
	Information about notifying during compliance checking is defined under this parameter.
QER	ComplianceCheck	EmailNotification		Sender's default email address for sending automatically generated notifications about rule checking.

Configuration parameter	Meaning
DefaultSenderAddress	Replace the default address with a valid email address.
QER | ComplianceCheck | EnableITSettingsForRule	IT Shop properties for the compliance rule are visible and can be edited.
QER | ComplianceCheck | IncludeTSBPersonUsesAccount	This configuration parameter specifies whether permissions for using shared identities are included in rule checking.
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 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 enabled, values for the risk index can be entered and calculated. If you disable the configuration parameter at a later date, model components and scripts that are no longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
QER | 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.

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

Contacting us

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

Technical support resources

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

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

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

Index

SQL 52-53

standard reason 27

    usage type 28

T

transparency index 32

W

working copy 29

    assign mitigating control 37

    compare to rule 39

    copy 39

    create 42

    enable 38

    overview form 36