One Identity Manager On Demand

Company Policies Administration Guide

Contents

Company policies

Table 1: General configuration parameters for company policies

Configuration parameter	Meaning
QER | Policy	Preprocessor relevant configuration parameter for controlling company policy validation. Changes to the parameter require recompiling the database. If the parameter is enabled, you can use the model components.

Companies have varying requirements that they need for regulating internal and external employee access to company resources. They also have to demonstrate that they adhere to legal requirements. Such requirements can be defined as policies.

One Identity Manager allows you to manage these company policies and thus to assess the risk involved. Assuming the appropriate data is stored in the One Identity Manager database, One Identity Manager determines all the company resources that violate these company policies. You can also define company policies for the purpose of providing reports that do not have any connection with One Identity Manager.

Adherence to company policies is checked regularly using scheduled tasks. You can incorporate company policies into the regular attestation of your company resources to decide on further handling of any violated ones. Risk assessment can be run for all company policies. Different reports and statistics provide you with an overview of violated policies.

Figure 1: Company policies in One Identity Manager
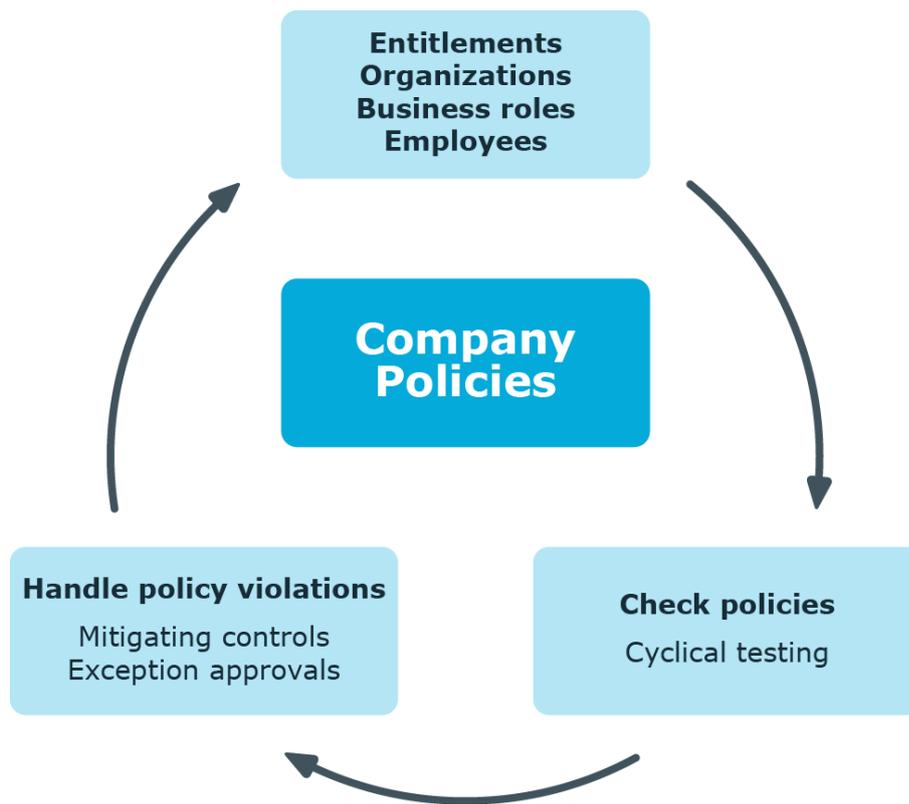
Example of company policies are:

- All cost centers are assigned a manager.
- All departments are assigned employees.
- All employees are attested.
- Deactivated employees do not have any enabled user accounts.

To be able to map company policies

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

If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

One Identity Manager users for company policies

The following users are used for setting up and administration of company policies.

Table 2: Users

Users	Tasks
Company policy administrators	Administrators must be assigned to the **Identity & Access Governance | Company policies | Administrators** application role. Users with this application role: • Enter base data for setting up company policies. • Set up policies and assign policy supervisors to them. • Can calculation policies and view policy violations if required. • Set up reports about policy violations. • Enter mitigating controls. • Create and edit risk index functions. • Administer application roles for policy supervisors, exception approvers and attestors. • Set up other application roles as required.
Policy supervisors	Policy supervisors must be assigned to the **Identity & Access Governance | Company policies | Policy supervisors** application role or another child application role. Users with this application role: • Are responsible for the contents of company policies. • Edit working copies of company policies. • Enable and disable company policies. • Can calculation policies and view policy violations if 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.

Users	Tasks
Exception approvers	Exception approvers must be assigned to the **Identity & Access Governance | Company policies | Exception approvers** application role or a child application role.
	Users with this application role:
	- Edit policy violations. - Can grant exception approval or revoke it.
Company policy attestors	Attestors must be assigned to the **Identity & Access Governance | Company policies | Attestors** application role.
	Users with this application role:
	- Attest company policies and exception approvals in the Web Portal for which they are responsible. - Can view the main data for these company policies 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 company policies

Various basic data is required to create company policies, run policy checks and handle policy violations.

Policy groups	Policy groups on page 9

Policy groups

Use policy groups to group together company policies by functionality. You can use policy to groups to structure company policies hierarchically.

To edit a policy group

1. Select the **Company Policies > Basic configuration data > Policy groups** category.

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

   - OR -

   Click ⊞ in the result list.

3. Edit the main data of the policy group.

4. Save the changes.

Enter the following data for a policy group

Table 3: General main data of a policy group

Property	Description
Group name	Name of the policy group.
Parent group	Policy group above this one in a hierarchy. Select a parent policy group area from the list for organizing your policy groups hierarchically.

In the **Policy violation overview** report, you can get an overview of all policy violations for a policy group.

Compliance frameworks

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

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

To edit compliance frameworks

1. Select the **Company Policies > 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 4: Compliance framework properties

Property	Description
Compliance framework	Name of the compliance framework.
Parent framework	Parent compliance framework in the framework hierarchy. Select an existing compliance framework in the menu for organizing compliance frameworks hierarchically.
Manager/supervisor	Application role whose members are allowed to edit all company rules assigned to this compliance framework
Description	Text field for additional explanation.

Additional tasks for compliance frameworks

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

You can obtain a summary of all a compliance framework's policy violations in the **Policy violation overview** report.

Compliance framework overview

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

To obtain an overview of a compliance framework

1. Select **Company Policies > Basic configuration data > Compliance frameworks**.

2. Select the compliance framework from the result list.

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

Assigning company policies

Use this task to assign company policies to the selected compliance framework.

To assign company policies to compliance frameworks

1. Select the **Company Policies > Basic configuration data > Compliance frameworks** category.

2. Select the compliance framework from the result list.

3. Select the **Assign company policies** task.

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

   - OR -

   In the **Remove assignments** pane, double-click the company policies whose assignment is to be deleted.

5. Save the changes.

Schedules for checking policies

Regular testing of company policies is managed through schedules. In the default installation of One Identity Manager, the "Policy check" schedule is assigned to every new company policy. This schedule generates a processing task at regular intervals for the DBQueue Processor for every company policy. You can configure your own schedule to check policies on a cycle which suits your requirements. Ensure that the schedules are assigned to the policies.

To edit schedules

1. Select the **Company Policies > Basic configuration data > Schedules** category.

   The result list shows all schedules configured for the QERPolicy table.

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

   – 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 5: Schedule properties

Property	Meaning
Name	Schedule ID. Translate the given text using the 🌐 button.
Description	Detailed description of the schedule. Translate the given text using the 🌐 button.
Enabled	Specifies whether the schedule is enabled. 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

ONE IDENTITY
by **Quest**

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.

- **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

Property	Meaning
	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.
	• 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

One Identity Manager supplies the following schedules for checking policies, by default.

Table 6: Default schedules

Schedule	Description
Default schedule policies	Default schedule for checking policies. To check policies, this schedule generates a processing task for the DBQueue Processor at regular intervals for each company policy.

Related topics

Additional tasks for schedules

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

Schedule overview

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

To obtain an overview of a schedule

1. Select the **Company Policies > Basic configuration data > Schedules** category.

2. Select the schedule in the result list.

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

Assigning company policies

Use this task to assign company policies to the selected schedule that will run them. By default, a company policy is assigned to the "default schedule policies" schedule. Using the assignment form you can assign the selected schedule to any of the company polices.

To assign a schedule to a company policy

1. Select the **Company Policies > Basic configuration data > Schedules** category.

2. Select the schedule in the result list.

3. Select **Assign company policies**.

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

5. Save the changes.

To change an assignment

1. Select the **Company Policies > Basic configuration data > Schedules** category.

2. Select the schedule in the result list.

3. Select the **Assign company policies** task.

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

   This shows company policies that are already assigned in other schedules.

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

   The company policy 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. Company policies must be assigned a schedule. It is compulsory.

Related topics

Starting schedules immediately

To start a schedule immediately

1. Select the **Company Policies > 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.

Attestors

Installed modules: Attestation Module

Employees that can be used to attest attestation procedures can be assigned to company policies. To do this, assign an application role for attestors to a company policy on the main data form. Assign employees to this application role that are authorized to attest company policies.

A default application role for attestors is available in One Identity Manager. You may create other application roles as required. For detailed information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 7: Default application roles for attestors

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

To edit attestors

1. Select the **Company Policies > Basic configuration data > Attestors** category.

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

   - OR -

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

   - OR -

   Click in the result list.

3. Edit the application role's main data.

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

4. Save the changes.

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

6. In the **Add assignments** pane, assign employees.

   - OR -

   In the **Remove assignments** pane, remove employees.

7. Save the changes.

Policy supervisors

Employees who are responsible for the contents of company policies can be assigned to these company policies. To do this, assign an application role for policy supervisors to a company policy on the main data form.

A default application role for policy supervisors is available in One Identity Manager. You may create other application roles as required. For detailed information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 8: Default application role for rule supervisors

User	Tasks
Policy supervisors	Policy supervisors must be assigned to the **Identity & Access Governance | Company policies | Policy supervisors** application role or another child application role.
	Users with this application role:

User	Tasks
	• Are responsible for the contents of company policies.
	• Edit working copies of company policies.
	• Enable and disable company policies.
	• Can calculation policies and view policy violations if required.
	• Assign mitigating controls.

To edit a policy supervisor

1. Select the **Company Policies > Basic configuration data > Policy supervisors** category.

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

   - OR -

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

   - OR -

   Click 🗋 in the result list.

3. Edit the application role's main data.

Property	Value
Parent application role	Assign the **Identity & Access Governance	Company policies	Policy supervisors** application role or a child application role.

4. Save the changes.

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

6. In the **Add assignments** pane, assign employees.

   - OR -

   In the **Remove assignments** pane, remove employees.

7. Save the changes.

Exception approvers

Employees who can issue exception approvals for policy violations can be assigned to company policies. To do this, assign an application role for exception approvers to a company policy on the main data form.

A default application role for exception approvers is available in One Identity Manager. You may create other application roles as required. For detailed information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 9: Default application role for exception approvers

User	Tasks
Exception approvers	Exception approvers must be assigned to the **Identity & Access Governance | Company policies | Exception approvers** application role or a child application role.
	Users with this application role:
	• Edit policy violations.
	• Can grant exception approval or revoke it.

To edit exception approvers

1. Select the **Company Policies > Basic configuration data > Exception approvers** category.

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

   - OR -

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

   - OR -

   Click in the result list.

3. Edit the application role's main data.

Eigenschaft	Wert
Parent application role	Assign the **Identity & Access Governance | Company policies | Exception approvers** application role or a child application role.

4. Save the changes.

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

6. In the **Add assignments** pane, assign employees.

   - OR -

   In the **Remove assignments** pane, remove employees.

7. Save the changes.

Related topics

- Granting exception approval on page 38

Standard reasons for policy 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 policy violation.

To create or edit standard reasons

1. In the Manager, select the **Company Policies > 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 10: 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 policy 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 policy violations on page 20

Predefined standard reasons for policy 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 **Company Policies > 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 policy violations on page 19

Defining company policies

Company policies include more properties in One Identity Manager apart from just technical descriptions, for example, risk assessment of a policy violation and accountability. Classification of company policies by compliance framework and structuring in policy groups is also possible.

Creating and changing company policies

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

NOTE: One Identity Manager users with the **Identity & Access Governance | Identity Audit | Policy supervisors** application role can edit existing working copies that they are entered as being responsible for in the main data.

To create a new company policy

1. Select the **Company Policies > Policies** category.

2. Click ⬛ in the result list.

3. Enter the company policy's main data.

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 company policy. The working copy is retained and can be used to make changes later.

To edit an existing company policy

1. Select the **Company Policies > Policies** category.

    a. Select the company policy 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 company policy after a security prompt. The working copy is opened and can be edited.

    - OR -

    Select the **Company policies > Policies > Working copies of policies** 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 **Enable working copy**. Confirm the security prompt with **OK**.

    Changes to the working copy are transferred to the company policy. This can reenable a disabled company policy if required.

General main data for company policies

Enter the following data for a company policy.

Table 11: General main data of company policies

Property	Description
Policy	Name of the company policy.
Description	Text field for additional explanation.
Main version number	Current state of the company policy as a version number. The version number is incremented in One Identity Manager's default installation each time you make a change to the condition.
Working copy	Specifies whether this is a working copy of the company policy.
Deactivated	Specifies whether the company policy is disabled or not. Only company policies that are enabled are included in policy checking.

Property	Description
	Use the **Enable policy** or **Disable policy** tasks to enable or disable a company policy. The working copy company policy is always disabled.
Policy group	Policy group to which the company policy belongs, based on its content. Select a policy group from the menu. To create a new policy group, click . Enter a name and description for the policy group.
Policy super-visors	Application role whose members are responsible for the company policy, 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 policy is violated. Assignments that cause the policy to be violated can be approved and issued anyway with this.
Exception approvers	Application role, whose members are entitled to grant exception approval for violations to this company policy. 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 policy violations.
Exception approvers info	Information, which the exception approver may require for making a decision. This advice should describe the risks and side effects of an exception.
Attestors	Applications role whose members are authorized to approve attestation cases for company policies and policy violations. To create a new application role, click . Enter the application role name and assign a parent application role.
Without condition	Specifies whether the company policy a direct relationship to the One Identity Manager data model or not. If this option is set, the **Edit condition...** button is disabled. If the option is not set, a condition must be entered that finds all the objects that violate the policy.
Base table	Base table referenced by the company policy. Based on this table, the system determines which objects violate the company policy.
Edit connec-tion...	Starts the WHERE clause wizard. Use the WHERE clause wizard to set up a condition that finds all the objects in the base table that violate the company policy. Use the **Expert view** button to enter the condition in SQL

Property	Description
	syntax straight away.
Condition	Data query that finds all the objects that violate the company policy. This option is only available if the **Show condition** task has been run beforehand.

Detailed information about this topic

Related topics

Risk assessment

Table 12: Configuration parameter for risk assessment

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

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

You can use the Report Editor to assess policy violations depending on the risk index by creating various reports.

To assess the risk of a policy violation enter values for grading company policies 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 company policy. Use the slider to enter a value between 0 and 1. 0 means no impact 1 means that every policy violation is a problem.
Significance	Provides a verbal description of the impact on the company of violations to this company policy. In the default installation value list is displayed with the entries {NONE, 'low', 'average', 'high', 'critical'}.
Risk index	Specifies the risk for the company of violations to this company policy. Use the slider to enter a value between 0 and 1. 0 means no risk 1 means every rule violation is a problem. The field is only visible if the "QER | CalculateRiskIndex" configuration parameter is set.
Risk index (reduced)	Show the risk index taking mitigating controls into account. The risk index for a company policy is reduced by the significance reduction value for all assigned mitigating controls. The risk index (reduced) is calculated for the original company policy. To copy the value to a working copy, run the task **Create working copy**. The 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 company policy. Use the slider to enter a value between 0 and 1. 0 means no transparency 1 means full transparency
Max. number of rule violations	Number of policy violations allowed for this company policy.

Detailed information about this topic

- Mitigating controls on page 48
- One Identity Manager Risk Assessment Administration Guide
- Report Editor in the One Identity Manager Configuration Guide

Related topics

- Creating a working copy on page 32

Additional data on company policies

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

Table 14: General main data of company policies

Property	Description
Policy number	Additional identifier for the company policy.
Implementation notes	Text field for additional explanation. You can use implementation notes to enter explanations about the content of the policy condition, for example.
Status	Status of the company policy with respect to its audit status.
Schedule	Schedule for starting policy checks on a regular basis. The "Default schedule policies" schedule is assigned by default. You can assign your own schedule.

Related topics

- Calculating policy violations on page 36

Policy comparison

You can compare the results of a working copy with the original policy. The comparison values are then displayed on the **Policy comparison** tab.

Table 15: Results of a policy comparison

Policy violations	Lists all employees who, as a result of the change, would (not) violate the company policy as follows
Newly added	would violate the policy for the first time
Identical	would still violate the policy
No longer included	would no longer violate the policy

TIP: All working copies with a different condition to that of the original company policy are displayed in the **Company policies > Policies > Working copies of policies > Modified working copies** category.

Detailed information about this topic

Default company policies

One Identity Manager provides various default company polices as working copies. In order to include these company polices in the policy check, enable the working copies.

To use a default company policy

1. Select the **Company policies > Policies > Working copies of policies > Predefined** category.
2. Select the company policy in the result list.
3. Select the **Enable working copy** task.
4. Confirm the security prompt with **OK**.

You can customize the following default company policy properties:

- Manager/supervisor
- Exception approval allowed
- Exception approvers
- Exception approvers info
- Attestors

TIP: If you want to edit more properties, create a copy of a default company policy. You can changes more properties in the working copy.

Additional tasks for working copies

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

Overview of the working copy

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

To obtain an overview of a working copy

1. Select the **Company policies > Policies > Working copies of policies** category.
2. Select the company policy in the result list.
3. Select the **Company policy overview** task.

Assigning compliance frameworks

Use this task to specify which compliance frameworks are relevant for the selected company policy. Compliance frameworks are used to classify company policies according to regulatory requirements.

To assign compliance frameworks to a company policy

1. Select the **Company policies > Policies > Working copies of policies** category.

2. Select the working copy in the result list.

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

4. In the **Add assignments** pane, double-click on a compliance framework to assign it.

   – OR –

   In the **Remove assignments** pane, double-click on the compliance framework for which you want to delete the assignment.

5. Save the changes.

Assigning mitigating controls

Mitigating controls describe controls that are implemented if a company policy was violated. The next policy check should not find any rule violations once the controls have been applied. Specify which mitigating controls apply to the selected company policy.

To assign mitigating controls to a company policy

1. Select the **Company policies > Policies > Working copies of policies** category.

2. Select the working copy in the result list.

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

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

   – OR –

   In the **Remove assignments** pane, Remove mitigating control assignments.

5. Save the changes.

Detailed information about this topic

- Mitigating controls on page 48

Maintaining exception approvers

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

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

To authorize employees as exception approvers

1. Select the **Company policies > Policies > Working copies of policies** category.

2. Select the working copy in the result list.

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

4. In the **Add assignments** pane, double-click on the employees you want to assign be assigned to the application role.

   – OR –

   In the **Remove assignments** pane, double-click on the compliance rules that you want to remove.

5. Save the changes.

Related topics

- General main data for company policies on page 22
- Exception approvers on page 18

Maintaining policy supervisors

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

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

To authorize employees as policy supervisors

1. Select the **Company policies > Policies > Working copies of policies** category.

2. Select the working copy in the result list.

3. Select the **Maintain supervisors** task.

4. In the **Add assignments** pane, double-click on the employees you want to assign be assigned to the application role.

   – OR –

   In the **Remove assignments** pane, double-click on the compliance rules that you want to remove.

5. Save the changes.

Related topics

Enabling working copies

When you enable the working copy, the changes are transferred to the original company policy. A company policy is added to a new working copy. Only original company policies are included in policy checking.

To enable a working copy

1. Select the **Company policies > Policies > Working copies of policies** 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: All working copies with a different condition to that of the original company policy are displayed in the **Company policies > Policies > Working copies of policies > Modified working copies** category.

Showing conditions

By default, the database query for finding objects that violate company policies, is not displayed on the main data form.

To show the database query on the main data form

1. Select the **Company policies > Policies > Working copies of policies** category.

2. Select the working copy in the result list.

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

4. Select the **Show condition** task.

To hide the database query on the main data form

1. Select the **Company policies > Policies > Working copies of policies** category.

2. Select the working copy in the result list.

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

4. Select the **Hide condition** task.

Copying policies

Company policies can be copied, for example, to reuse complex policy conditions. Working copies as well as active company policies can be used as copy templates.

To copy a working copy

1. Select the **Company policies > Policies > Working copies of policies** category.

2. Select the working copy in the result list.

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

4. Select the **Copy policy...** 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 **No** category.to edit the copy's main data later.

Comparing a company policy working copy with the original

You can compare the results of a working copy with the original company policy. Company policies can only be compared when an original of the working copy exists.

To compare a company policy with the working copy

1. Select the **Company policies > Policies > Working copies of policies** category.

2. Select the working copy in the result list.

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

4. Select the **Compare policy** task.

Table 16: Results of a policy comparison

Policy violations	Lists all employees who, as a result of the change, would (not) violate the company policy as follows
Newly added	would violate the policy for the first time
Identical	would still violate the policy
No longer included	would no longer violate the policy

To display the policy comparison as report

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

Related topics

Showing selected objects

Use this task to show the list of objects found using the condition on the main data form.

To show a list of the objects found

1. Select the **Company policies > Policies > Working copies of policies** category.

2. Select the company policy in the result list.

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

4. Select the **Show selected objects** task.

   This shows the **Result** tab on the main data form, which displays a list of objects found through the database query.

Additional tasks for company policies

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

Overview of company policies

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

To obtain an overview of a company policy

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

3. Select the **Company policy overview** task.

Creating a working copy

To modify an existing company policy, you need to make a working copy of it. The working copy can be created from the enabled company policy. The data from the existing working copy are overwritten by the data from the enabled company policy after a security prompt.

To create a working copy

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

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

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

TIP: All working copies with a different condition to that of the original company policy are displayed in the **Company policies > Policies > Working copies of policies > Modified working copies** category.

Enabling and disabling policies

Enable the company policy so that policy violation can be found. To exclude company policies from policy testing, you can disable them. The DBQueue Processor then removes all information about policy violation for this company policy from the database. The working copy company policy is always disabled.

To enable company policies

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

3. Select the **Enable policy** task.

To disable company policies

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

3. Select the **Disable policy** task.

Showing conditions

The database query for finding objects which violate company policies, is not displayed on the main data form by default.

To show the database query on the main data form

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

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

4. Select the **Show condition** task.

To hide the database query on the main data form

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

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

4. Select the **Hide condition** task.

Copying policies

Company policies can be copied, for example, to reuse complex policy conditions. Working copies as well as active company policies can be used as copy templates.

To copy company policies

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

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

4. Select the **Copy policy...** 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 **No** category.to edit the copy's main data later.

Showing selected objects

Use this task to show the list of objects found using the condition on the main data form.

To show a list of the objects found

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

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

4. Select the **Show selected objects** task.

   This shows the **Result** tab on the main data form, which displays a list of objects found through the database query.

Recalculating

There are several tasks available for immediately checking a company policy. For more information, see Checking company policies on page 36.

Maintaining exception approvers

Use this task to maintain exception approvers for the selected company policy. You can assign employees to the application role for exception approvers on the main data form

and remove them from it.

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

To authorize employees as exception approvers

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

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

4. In the **Add assignments** pane, double-click on the employees you want to assign be assigned to the application role.

   – OR –

   In the **Remove assignments** pane, double-click on the compliance rules that you want to remove.

5. Save the changes.

Related topics

- General main data for company policies on page 22
- Exception approvers on page 18

Maintaining policy supervisors

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

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

To authorize employees as policy supervisors

1. Select the **Company Policies > Policies** category.

2. Select the company policy in the result list.

3. Select the **Maintain supervisors** task.

4. In the **Add assignments** pane, double-click on the employees you want to assign be assigned to the application role.

   – OR –

   In the **Remove assignments** pane, double-click on the compliance rules that you want to remove.

5. Save the changes.

Related topics

- General main data for company policies on page 22
- Policy supervisors on page 17

Deleting company policies

> IMPORTANT: All information about a company policy and policy violations is irrevocably deleted when the company policy is deleted! The data cannot be retrieved at a later date.
>
> One Identity therefore recommends that you create a report about the company policy and its current violations before deleting it, if you want to retain the information (for audit reasons, for example).

You can delete a company policy, if no policy violations exist for it.

To delete a company policy

1. Select the **Company Policies > Policies** category.
2. Select the company policy to delete in the result list.
3. Select the **Disable policy** task.

    Existing policy violations are removed by the DBQueue Processor.

4. After the DBQueue Processor has recalculated policy violations for the company policy, click 🗙 in the toolbar to delete the company policy.

    The company policy and the working copy are deleted.

Checking company policies

Processing tasks are created for the DBQueue Processor to check the validity of a company policy. The DBQueue Processor determines which employees satisfy the company policy and which employees violate the policy in the case of each company policy. The specified company policy approvers can check policy violations and if necessary grant exception approval.

Calculating policy violations

You can start policy checking in different ways to determine current policy violations in the One Identity Manager database:

- Scheduled policy checking
- Ad-hoc policy checking

Furthermore, company policy testing is triggered by different events:

- A company is enabled.
- A working copy is enabled.
- A company policy is enabled.

During policy checking, all objects are found that fulfill the condition defined in the company policy. Only enabled company policies are taken into account.

Scheduled policy checking

You can use the default schedule policies from One Identity Manager's default installation to test all company policies in full. This schedule generates processing tasks at regular intervals for the DBQueue Processor.

Prerequisites

- The company policy is enabled.
- The schedule stored with the company policies is enabled.

Detailed information about this topic

- Schedules for checking policies on page 11
- Enabling and disabling policies on page 33

Ad-hoc policy checking

Various tasks for immediate policy checking are available for an enabled company policy.

Table 17: Additional tasks for company policies

Task	Description
Recalculate policy	This immediately checks the company policy.
Recalculate all	All company policies are immediately checked.

Reports about policy 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 enabled company policies and compliance frameworks.

Table 18: Reports about policy violations

Report	Description
Policy violation	This report groups together all policy violations for the selected policy. All the objects that violate the company policy are listed. The result list is

Report	Description
overview (of a company policy)	grouped by: - Policy violations that still need to be decided - Policy violations without exception approval - Policy violation with exception approval
Policy violation overview (of a policy group)	This report groups together all policy violations for the selected policy group. All the objects that violate the company policy are listed. The number of granted, denied, and not yet processed policy violations are given in addition.
Policy violation overview (for a compliance framework)	This report groups together all policy violations for the selected compliance framework. All the objects that violate the company policy are listed. The number of granted, denied, and not yet processed policy violations are given in addition.

Granting exception approval

There can be individual cases where it is not possible to adhere to company policy. Policy violations can only be accepted occasionally, but only if you take the required measures to ensure that these violations are regularly checked. For this purpose, you may grant exception approval for certain policy violations.

You store exception approvals with policy violations. You can see an overview of all unprocessed (new) company policies and policies that have been granted or denied on the overview form for a company policy.

Prerequisites

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

Use the Web Portal to grant exception approvals.

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

Detailed information about this topic

- General main data for company policies on page 22
- One Identity Manager Web Designer Web Portal User Guide

Notifications about policy violations

After policy checking, email notifications can be sent through new policy violations to exception approvers and policy supervisors. 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 notification in the request process

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 | Policy | EmailNotification** configuration parameter.

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

4. Ensure that all employees 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 employees. 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

- Creating custom mail templates for notifications on page 41

Request for exception approval

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

Prerequisites

- Exception approvals for policy violations are permitted.
- The company policy is assigned to an **Exception approvers** application role.
- Employees are assigned to this application role.

To send demands for exception approval

- Enter the following data for the company policy:

  Exception approval allowed: Enabled

  Mail template new violation: Policies - new exception approval required

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

Related topics

- Creating and changing company policies on page 21
- General main data for company policies on page 22
- Creating custom mail templates for notifications on page 41

Notifications about policy violations without exception approval

Policy supervisors are notified if new policy violations are discovered during a policy check and these cannot be granted exception approval.

Prerequisites

- Exception approvals for policy violations are not permitted.
- An application role for **Policy superviors** is assigned to the company policy.
- Employees are assigned to this application role.

To inform a policy supervisor about policy violations

- Enter the following data for the company policy:

  Exception approval allowed: Not enabled

  Mail Template New Violation: Policies - rogue violation occurred

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

Related topics

- Creating and changing company policies on page 21
- General main data for company policies on page 22
- Creating custom mail templates for notifications on page 41

Approval status of a policy violation

Edit policy violations in the Web Portal. You can also get an overview of the approval status of each policy violation in the Manager. To do this, open the overview form of the enabled company policy whose policy violations you want to look at. You will see new, granted, and denied policy violations here.

To display details of a policy violation

1. Select the form element for the policy violation and make the list entries visible.

2. Click the policy violation you want to view.

   This opens the policy violation main data form, This shows you an overview of the object that caused the violation, the approval status and the exception approver responsible.

Related topics

- Overview of company policies on page 32

Creating custom mail templates for notifications

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 **Company Policies > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for policy checks 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 **Company Policies > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for policy checks 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 **Company Policies > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for policy checks 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 **Company Policies > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for policy checks 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**.

General properties of a mail template

The following general properties are displayed for a mail template.

Table 19: Mail template properties

Property	Meaning
Mail template	Name of the mail template. This name will be used to display the mail templates in the administration tools and in the Web Portal. Translate the given text using the 🌐 button.

Property	Meaning
Base object	Mail template base object. A base object only needs to be entered if the mail definition properties of the base object are referenced. Use the `QERPolicy` or `QERPolicyHasObject` base object for notifications about policy violations.
Report (parameter set)	Report, made available through the mail template.
Description	Mail template description. Translate the given text using the 🌐 button.
Target format	Format in which to generate email notification. Permitted values are: • **HTML**: The email notification is formatted in HTML. Text formats, for example, different fonts, colored fonts, or other text formatting, can be included in HTML format. • **TXT**: The email notification is formatted as text. Text format does not support bold, italics, or colored font, or other text formatting. Images displayed directly in the message are not supported.
Design type	Design in which to generate the email notification. Permitted values are: • **Mail template**: The generated email notification contains the mail body in accordance with the mail definition. • **Report**: The generated email notification contains the report specified under **Report (parameter set)** as its mail body. • **Mail template, report in attachment**: The generated email notification contains the mail body in accordance with the mail definition. The report specified under **Report (parameter set)** is attached to the notification as a PDF file.
Importance	Importance for the email notification. Permitted values are **Low**, **Normal**, and **High**.
Confidentiality	Confidentiality for the email notification. Permitted values are **Normal**, **Personal**, **Private**, and **Confidential**.
Can unsubscribe	Specifies whether the recipient can unsubscribe email notification. If this option is set, the emails can be unsubscribed through the Web Portal.
Deactivated	Specifies whether this mail template is disabled.
Mail definition	Selects the mail definition in a specific language. 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.
Language	Language that applies to the mail template. The recipient's language preferences are taken into account when an email notification is

Property	Meaning
	generated.
Subject	Subject of the email message.
Mail body	Content of the email message.

Creating and editing an email definition

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

To create a new mail definition

1. In the Manager, select the **Company Policies > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for policy checks 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 **Company Policies > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for policy checks 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.

Using base object properties

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*.

Use of hyperlinks in the Web Portal

Table 20: Configuration parameters for the Web Portal URL

Configuration parameter	Effect when set
QER | WebPortal | BaseURL	Web Portal URL This address is used in mail templates to add hyperlinks to 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 policy checks.

Prerequisites for using this method

- The **QER | WebPortal | BaseURL** configuration parameter is enabled and contains the URL path to the Web Portal. You edit the configuration parameter in the Designer.

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

  with:

  `<server name> = name of server`

  `<application> = path to the Web Portal 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**.

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.

$Script(<Function>)$

Example:

$Script(VI_BuildQERPolicyLink_Show)$

Default function for policy checking

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

Table 21: Functions of the VI_BuildComplianceLinks script

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

Customizing email signatures

Configure the email signature for mail templates using the following configuration parameters. Edit the configuration parameters in the Designer.

Table 22: Configuration parameters for email signatures

Configuration parameter	Description
Common | MailNotification | Signature	Data for the signature in email automatically generated from mail templates.
Common | MailNotification | Signature | Caption	Signature under the salutation.
Common | MailNotification | Signature | Company	Company name.
Common | MailNotification | Signature | Link	Link to the company's website.
Common | MailNotification | Signature | LinkDisplay	Display text for the link to the company's website.

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

Mitigating controls

Violation of regulatory requirements can harbor different risks for companies. To evaluate these risks, you can apply risk indexes to company policies. These risk indexes provide information about the risk involved for the company if this particular policy 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 company policy was violated. The next policy check should not find any rule violations once the controls have been applied.

To edit mitigating controls

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

If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

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

Entering main data

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 23: 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.

Additional tasks for mitigating controls

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

Mitigating controls overview

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

To obtain an overview of a mitigating control

1. 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.

Assigning company policies

Use this task to specify for which company policies the mitigating control is valid. You can only assign company policy working copies on the assignment form.

To assign company policies 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 company policies** task.

   In the **Add assignments** pane, assign company policies.

   > TIP: In the **Remove assignments** pane, you can remove company policies.

   > *To remove an assignment*
   > - Select the company policy and double-click ⊘.

4. Save the changes.

Calculating mitigation

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

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

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

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

General configuration parameter for company policies

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

Table 24: Overview of configuration parameters

Configuration parameter	Meaning
QER | Policy	Preprocessor relevant configuration parameter for controlling company policy validation. Changes to the parameter require recompiling the database.
	If the parameter is enabled, you can use the model components.
	If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
QER | Policy | EmailNotification	This parameter is used for mail notifications.
	Information about notifications during company policy checks is stored under the parameter.
QER | Policy | EmailNotification | DefaultSenderAddress	Sender's default email address for sending automatically generated notifications when company policies are checked. Replace the default address with a valid email address.
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.

Configuration parameter	Meaning
	If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

About us

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

Contacting us

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

Technical support resources

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

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

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

Index

ONE IDENTITY
by Quest