One Identity Manager 9.2

Company Policies Administration Guide

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

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

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

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

Patents

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

Trademarks

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

Legend

> ⊗ **WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**

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

One Identity Manager Company Policies Administration Guide
Updated - 29 September 2023, 04:59

For the most recent documents and product information, see Online product documentation.

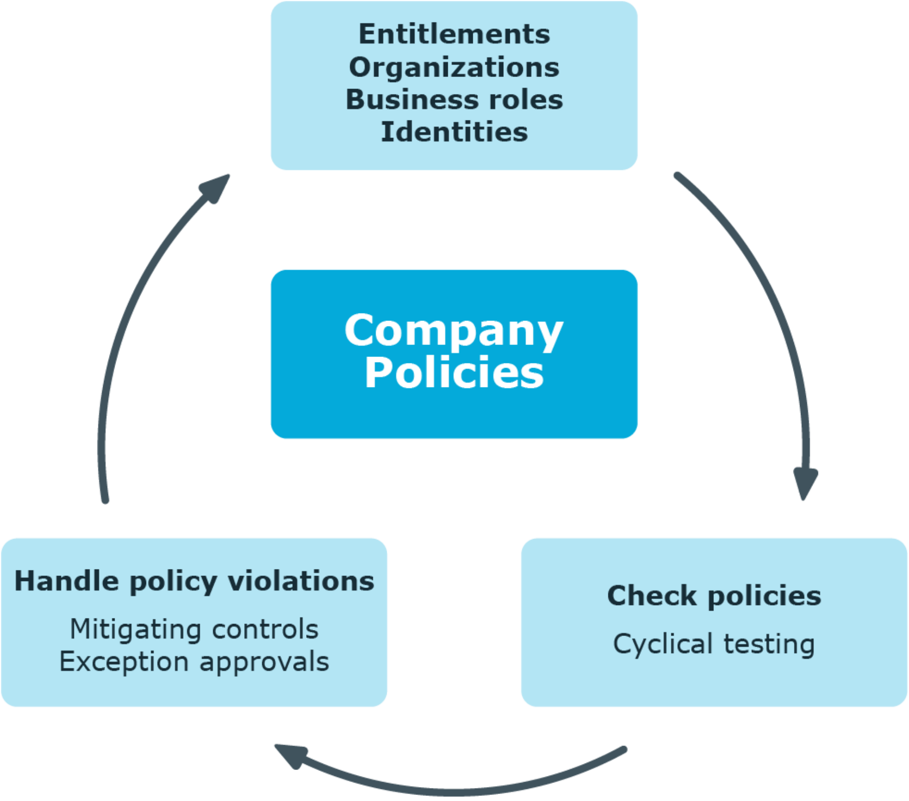
Contents

Company policies in One Identity Manager

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.

Figure 1: Company policies in 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.

Example of company policies are:

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

> NOTE: Prerequisite for the using company policies in One Identity Manager is the installation of the Company Policies Module. For more information about installing, see the *One Identity Manager Installation Guide*.

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 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 company policies

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

Table 1: 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.

Users	Tasks
	• 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.
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.

Users	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.
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.

2

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.

Detailed information about this topic

- Basisdaten für Unternehmensrichtlinien
- Using default company policies on page 25
- Creating and editing company policies on page 10
- Deleting company policies on page 26

Creating and editing 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. In the Manager, 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. In the Manager, select the **Company Policies > Policies** category.
    a. Select a 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. This opens the working copy, which you can then edit.

   - OR -

   In the Manager, 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 prompted.

General main data for company policies

Enter the following data for a company policy.

Table 2: 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. Use the **Enable policy** or **Disable policy** tasks to enable or disable a company policy. The working copy company policy is always disabled.

Property	Description
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 supervisors	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.
Attestation policy	Attestation policy to use for attesting objects that violate this company policy. NOTE: Ensure that the same objects are determined by this attestation policy as by the company policy. Check the assigned tables and conditions. This field is displayed only when the Attestation Module is installed. This functionality is used by default in the context of Behavior Driven Governance. For more information about this, see the *One Identity Manager Administration Guide for Behavior Driven Governance*.
Start attestation of new rule violations immediately	Specifies whether an attestation case is created immediately for each new policy violation. If this option is enabled, assign an attestation policy. This field is displayed only when the Attestation Module is installed. This functionality is used by default in the context of Behavior Driven Governance. For more information about this, see the *One Identity Manager Administration Guide for Behavior Driven Governance*.
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

Property	Description
	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 connection...	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 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

- Enabling and disabling company policies on page 21
- Policy groups on page 27
- Policy supervisors for company policies on page 34
- Exception approvers for policy violations on page 35
- Company policy attestors on page 33
- Displaying conditions of company policy working copies on page 17
- Configuring automatic attestation of policy violations on page 50

Related topics

- Notifications about policy violations without exception approval on page 47
- Requesting exception approval on page 47

Risk assessment for policy 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 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 ... 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. For more information about creating reports, see the *One Identity Manager Configuration Guide*.

To assess the risk of a policy violation enter values for grading company policies on the **Assessment criteria** tab.

Table 3: 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** ... No impact **1** ... 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, the values **low**, **average**, **high**, and **critical** are listed.
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** ... No risk **1**... Every rule violation is a problem. This field is only visible if the **QER | CalculateRiskIndex** configuration parameter is set.
Risk index (reduced)	Show the risk index taking mitigating controls into account. 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**. 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 company policy. Use the slider to enter a value between **0** and **1**. **0** ... No transparency **1** ... Full transparency
Max. number of rule violations	Number of policy violations allowed for this company policy.

Detailed information about this topic

- Mitigating controls for company policies on page 52

Related topics

- Creating working copies for company policies on page 22

Additional data for company policies

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

Table 4: 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. By default, the **Policy Check** schedule is assigned but you can assign your own schedule.

Related topics

- Calculating policy violations on page 43
- Schedules for checking policies on page 29

Comparing working copies and original company policies

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.

> 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.

To compare a company policy with the working copy

1. In the Manager, 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.

   The comparison values are then displayed on the **Policy comparison** tab.

Table 5: Results of a policy comparison

Policy violations	Lists all identities 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

- Creating and editing company policies on page 10

Additional tasks for working copies of company policies

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

Enabling working copies of company policies

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. In the Manager, 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.

Copying working copies of company 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. In the Manager, 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 **Yes** to edit the copy's main data later.

Related topics

- Copying company policies on page 22

Displaying conditions of company policy working copies

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. In the Manager, 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. In the Manager, 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.

Related topics

- Displaying company policy conditions on page 23

Displaying selected objects for working copies

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. In the Manager, 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.

Related topics

- Showing selected objects for company policies on page 23

Maintaining exception approvers for working copies

Use this task to maintain exception approvers for the selected company policy. 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 company policies assigned to this application role.

To authorize identities as exception approvers

1. In the Manager, 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, 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 company policies on page 11
- Exception approvers for policy violations on page 35
- Maintaining exception approvers for company policies on page 24

Maintaining policy supervisors for working copies

Use this task to maintain policy supervisors for the selected company policy. You can assign identities 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 identities as policy supervisors

1. In the Manager, 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, 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 company policies on page 11
- Policy supervisors for company policies on page 34
- Maintaining policy supervisors for company policies on page 24

Assigning compliance frameworks to company policies

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. In the Manager, 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, 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.

Assigning mitigating controls to working copies

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. In the Manager, 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 the mitigating controls.

> TIP: In the **Remove assignments** pane, you can remove mitigating control assignments.
>
> ***To remove an assignment***
>
> - Select the mitigating control and double-click ✓.

5. Save the changes.

Detailed information about this topic

- Mitigating controls for company policies on page 52

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

Related topics

- Displaying the company policies overview on page 25

Additional tasks for company policies

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

Enabling and disabling company 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. In the Manager, 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. In the Manager, select the **Company Policies > Policies** category.
2. Select the company policy in the result list.
3. Select the **Disable policy** task.

Creating working copies for company policies

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. In the Manager, 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.

Related topics

- Creating and editing company policies on page 10
- Enabling working copies of company policies on page 16

Copying company 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. In the Manager, 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 **Yes** to edit the copy's main data later.

Related topics

- Copying working copies of company policies on page 17

Displaying company policy 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. In the Manager, 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. In the Manager, 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.

Related topics

- Displaying conditions of company policy working copies on page 17

Showing selected objects for company policies

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. In the Manager, 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.

Related topics

- Displaying selected objects for working copies on page 18

Maintaining exception approvers for company policies

Use this task to maintain exception approvers for the selected company policy. 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 company policies assigned to this application role.

To authorize identities as exception approvers

1. In the Manager, 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, 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 company policies on page 11
- Exception approvers for policy violations on page 35
- Maintaining exception approvers for working copies on page 18

Maintaining policy supervisors for company policies

Use this task to maintain policy supervisors for the selected company policy. You can assign identities 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 identities as policy supervisors

1. In the Manager, 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, 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 company policies on page 11
- Policy supervisors for company policies on page 34
- Maintaining policy supervisors for working copies on page 19

Displaying the company policies overview

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

To obtain an overview of a company policy

1. In the Manager, select the **Company Policies > Policies** category.
2. Select the company policy in the result list.
3. Select the **Company policy overview** task.

Related topics

- Displaying the working copy overview on page 21

Using 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. In the Manager, select the **Company policies > Policies > Working copies of policies > Predefined** category.
2. Select the working copy in the result list.
3. Select **Enable working copy**.
4. Confirm the security prompt with **Yes**.
5. Enable the original policy. Confirm the prompt with **Yes**.

You can customize the following default company policy properties:

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

> 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.

Related topics

- Risk assessment for policy violations on page 13
- General main data for company policies on page 11
- Copying working copies of company policies 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. In the Manager, 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.

Policy groups

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

To create a policy group

1. In the Manager, select the **Company Policies > Basic configuration data > Policy groups** category.
2. Click in the result list.
3. Edit the main data of the policy group.
   - **Group name**: Name of the policy group.
   - **Parent group**: Parent policy group in a hierarchy. In the menu, select a parent policy group from the list for organizing your policy groups hierarchically.
4. Save the changes.

To edit a policy group

1. In the Manager, 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.
3. Edit the main data of the policy group.
4. Save the changes.

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 create or edit compliance frameworks

1. In the Manager, 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 6: 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.

Assigning compliance frameworks to company policies

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

To assign company policies to compliance frameworks

1. In the Manager, 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, 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 ✓.

5. Save the changes.

Displaying the compliance frameworks overview

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

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

To obtain an overview of a compliance framework

1. Select the **Company Policies > 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 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 create or edit schedules

1. In the Manager, 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 7: 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.

Assigning company policies to schedules

Use this task to assign company policies to the selected schedule that will run them. Using the assignment form you can assign the selected schedule to any of the company polices.

By default, company policies are assigned to the **Policy check** schedule.

> NOTE: Assignments cannot be removed. Assignment of a schedule is compulsory for company policies.

To assign a company policy to a schedule

1. In the Manager, 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, assign company policies.
5. Save the changes.

To change an assignment

1. In the Manager, 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.

Related topics

- Enabling working copies of company policies on page 16
- Additional data for company policies on page 15

Starting schedules immediately

To start a schedule immediately

1. In the Manager, 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.

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 **Company Policies > Basic configuration data > Schedules** category.
2. Select the schedule in the result list.
3. Select the **Schedule overview** task.

Company policy 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 company policies. To do this, assign the company policies to application roles for attestors. Assign identities to this application role who are authorized to attest company policies. 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
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 add identities to default application roles for attestors

1. In the Manager, select the **Company Policies > 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.

Policy supervisors for company policies

Identities that 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 more information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 9: 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: • 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 add identities to the default application for rule supervisors

1. In the Manager, select the **Company Policies > Basic configuration data > Policy 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.

Related topics

- Maintaining policy supervisors for working copies on page 19
- Maintaining policy supervisors for company policies on page 24

Exception approvers for policy violations

Identities that 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 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 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 add identities to default application roles for exception approvers

1. In the Manager, select the **Company Policies > 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 approvals on page 45
- Maintaining exception approvers for working copies on page 18
- Maintaining exception approvers for company policies on page 24

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 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 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 37

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 36

Mail templates for company policy notifications

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

Related topics

- Creating and editing mail definitions for company policies on page 38
- Base objects for company policy mail templates on page 39
- Editing company policy mail templates on page 39
- Use of hyperlinks in the Web Portal on page 41
- Default functions for creating hyperlinks on page 41

Creating and editing mail definitions for company policies

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 **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.

Base objects for company policy mail templates

> NOTE: Use the `QERPolicy` or the `QERPolicyHasObject` base objects in company policy mail templates.

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*.

Editing company policy mail templates

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**.

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 policy checks.

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**.

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:

```
$Script(VI_BuildQERPolicyLink_Show)$
```

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 12: Functions of the VI_BuildComplianceLinks script

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

Checking company policies

Processing tasks are created for the DBQueue Processor to check the validity of a company policy. For every company policy, the DBQueue Processor determines which objects violate the company policy. The specified company policy approvers can check policy violations and if necessary grant exception approval.

Detailed information about this topic

- Calculating policy violations on page 43
- Reports about policy violations on page 45
- Granting exception approvals on page 45
- Notifications about policy violations on page 46
- Displaying approval status of policy violations on page 48

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.

Related topics

- Scheduled policy checking on page 44
- Ad-hoc policy checking on page 44

Scheduled policy checking

You can use the **Policy check** schedule 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 29
- Enabling and disabling company policies on page 21

Ad-hoc policy checking

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

To review a selected company policy immediately

1. In the Manager, 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 **Recalculate policy** task.

To review all company policies immediately

1. In the Manager, 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 **Recalculate all** task.

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 13: Reports about policy violations

Report	Description
Policy violation overview (of a company policy)	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 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 (of 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 approvals

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.

Use the Web Portal to grant exception approvals. For more information, see the *One Identity Manager Web Designer Web Portal User Guide*.

You store exception approvals with policy violations. You can display 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.
- Identities are assigned to this application role.

> 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 11
- Displaying the company policies overview on page 25

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 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 | 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 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

- Editing company policy mail templates on page 39
- Requesting exception approval on page 47
- Notifications about policy violations without exception approval on page 47

Requesting 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.
- Identities 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 editing company policies on page 10
- General main data for company policies on page 11
- Editing company policy mail templates on page 39

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.
- Identities 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 editing company policies on page 10
- General main data for company policies on page 11
- Editing company policy mail templates on page 39

Displaying approval status of policy violations

Edit policy violations in the Web Portal. For more information, see the *One Identity Manager Web Designer Web Portal User Guide*.

In the Manager, you can get an overview of the approval status of each policy violation. 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. In the Manager, select the **Company Policies > Policies** category.
2. Select the company policy in the result list.
3. Select the **Company policy overview** task.
4. Select the form element for the policy violation and make the list entries visible. You have the following options:
   - **Policy violations: new**: Displays all policy violations pending approval.
   - **Policy violations: exception approved**: Displays all policy violations that have been granted approval.

    - **Policy violations: exception denied**: Displays all policy violations that have not been granted approval.

5. Click the policy violation you want to view.

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

Related topics

- Displaying the company policies overview on page 25

Automatic attestation of policy violations

NOTE: This functionality is only available if the Attestation Module in installed.

Automatic recertification of the affected entitlements can be provided for policy violations. As a result of recertification, entitlements that should not be used anymore can be automatically deactivated or removed. This functionality is used by default in the context of Behavior Driven Governance. However, you can also use this functionality for your own company policies and related authorization checks.

For more information about Behavior Driven Governance, see the *One Identity Manager Administration Guide for Behavior Driven Governance*.

Detailed information about this topic

- Configuring automatic attestation of policy violations on page 50
- Starting attestation of new rule violations on page 51

Configuring automatic attestation of policy violations

NOTE: This functionality is only available if the Attestation Module in installed.

Attestation of policy violations requires an attestation policy that matches the company policy. This attestation policy must determine the same objects as the company policy.

To set up automatic attesting of policy violations

1. Create an attestation policy for attesting objects that violate a company policy. Ensure that the same objects are determined by this attestation policy as by the company policy.

   For more information about creating and editing attestation policies, see the *One Identity Manager Attestation Administration Guide*.

2. Create a new company policy or edit an existing company policy. Enter the following data:

    - **Attestation policy**: From the menu, select the attestation policy to be used for attesting policy violations.

      Ensure that the same objects are determined by this attestation policy as by the company policy. Check the assigned tables and conditions.

    - **Start attestation of new rule violations immediately**: Specify whether an attestation case is created immediately for each new policy violation.

      If this option is disabled, attestation is only started by the schedule stored with the attestation policy.

Detailed information about this topic

- Creating and editing company policies on page 10
- General main data for company policies on page 11
- Automatic attestation of policy violations on page 50
- Starting attestation of new rule violations on page 51

Starting attestation of new rule violations

NOTE: This functionality is only available if the Attestation Module in installed.

There are several different ways to start attesting policy violations:

- Attest new policy violations immediately

  If **Start attestation of new rule violations immediately** is enabled on the company policy, an attestation case is created immediately for each new policy violation when policy checking is run. To do this, the `POL_QERPolicyHasObject_create_attestationcase` process is run for each `insert` into the `QERPolicyHasObject` table.

- Starting scheduled attestation of all rule violations

  Attestation is started by the schedule stored with the attestation policy.

Detailed information about this topic

- Automatic attestation of policy violations on page 50

5

Mitigating controls for company policies

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 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*.

Related topics

- Creating and editing mitigating controls for company policies on page 53
- Assigning company policies to mitigating controls on page 53
- Calculating mitigating controls for company policies on page 54
- Überblick über risikomindernde Maßnahmen anzeigen

Creating and editing mitigating controls for company policies

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 14: 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 company policies to mitigating controls

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 mitigating controls for company policies

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**.

Displaying mitigating 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.

Appendix A

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 15: 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 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 | 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 the risk index. Changes to the parameter require recompiling the database. If the parameter is enabled, values for the risk index can be

Configuration parameter	Meaning
	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*.

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