One Identity Manager 8.2.1

Attestation Administration Guide

Contents

Attestation and recertification

Managers or others responsible for compliance can use the One Identity Manager attestation feature to certify correctness of permissions, requests, or exception approvals either scheduled or on demand. Recertification is the term generally used to describe regular certification of permissions. One Identity Manager uses the same workflows for recertification and attestation.

There are attestation policies defined in One Identity Manager for carrying out attestations. Attestation policies specify which objects are attested when, how often, and by whom. Once an attestation is performed, One Identity Manager creates attestation cases that contain all the necessary information about the attestation objects and the attestor responsible. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules.

Attestation cases record the entire attestation sequence. Each attestation step in the attestation case can be audit-proof reconstructed. Attestations are run regularly using scheduled tasks. You can also trigger single attestations manually.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

TIP: One Identity Manager provides various default attestation procedures for different data situations and default attestation procedures. If you use these default attestation procedures, you can configure how you deal with denied attestations.

For more information, see Default attestation and withdrawal of entitlements on page 140.

To use attestation functionality

- In the Designer, set the **QER | Attestation** 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 attestation

The following users are used for attestation.

Table 1: Users

User	Tasks
Administrators for attestation cases	Administrators are assigned to the **Identity & Access Governance | Attestation | Administrators** application role. Users with this application role: • Define attestation procedures and attestation policies. • Create approval policies and approval workflows. • Specify which approval procedure to use to find attestors. • Set up attestation case notifications. • Configure attestation schedules. • Enter mitigating controls. • Create and edit risk index functions. • Monitor attestation cases. • Manage application roles for attestation policy owners. • Maintain members of the chief approval team.
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.
Attestation policy owners	Owners of attestation policies must be assigned to a child application role of the **Identity & Access Governance | Attestation | Attestation policy owners** application role. Users with this application role:

User	Tasks
	• Are responsible for its content and handle the attestation policies assigned to it. • Assign the attestation procedure, approval policy, and calculation schedule. • Assign approvers, mitigating controls, and compliance frameworks. • Monitor attestation cases and attestation runs.
Attestors	• Check attestation objects in the Web Portal. • Confirm data correctness. • Initiate changes if data conflicts with internal rules. Attestators in charge are determined through approval procedures.
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.
Chief approval team	The chief approver must be assigned to the **Identity & Access Governance | Attestation | Chief approval team** application role. Users with this application role: • Approve using attestation cases. • Assign attestation cases to other attestors.

Attestation base data

The attestation framework and the objects to be attested are specified in the attestation policy. You require certain base data to define attestation policies.

Attestation types

Attestation types are used to group attestation procedures. These make it easier to assign a matching attestation procedure to the attestation policies.

To edit attestation types

1. Select the **Attestation > Basic configuration data > Attestation types** category.
2. Select an attestation type in the result list and run the **Change main data** task.

   – OR –

   Click ⊞ in the result list.
3. Edit the attestation type main data.
4. Save the changes.

Default attestation types

You cannot edit default attestation types and their attestation procedure assignments.

One Identity Manager supplies attestation types by default. These attestation types are assigned to default attestation procedures. They are necessary for setting up attestation policies in the Web Portal.

To display default attestation types

- In the Manager, select the **Attestation > Basic configuration data > Attestation types > Predefined** category.

For detailed information about using default attestation types, see the *One Identity Manager Web Designer Web Portal User Guide*.

Additional tasks for attestation types

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

Overview of the attestation type

You can see the most important information about an attestation type on the overview form.

To obtain an overview of an attestation type

1. In the Manager, select the **Attestation > Basic configuration data > Attestation types** category.
2. Select the attestation type in the result list.
3. Select the **Attestation type overview** task.

Assigning attestation procedures

Use this task to assign the selected attestation type to all the attestation procedures that should be included in the group.

To assign attestation procedures to attestation types

1. In the Manager, select the **Attestation > Basic configuration data > Attestation types** category.
2. Select the attestation type in the result list.
3. Select the **Assign attestation procedure** task.

   In the **Add assignments** pane, assign the attestation procedures.

   > TIP: In the **Remove assignments** pane, you can remove attestation procedure assignments.
   >
   > #### To remove an assignment
   >
   > - Select the attestation procedure and double-click ✅.
4. Save the changes.

Attestation procedure

Attestation procedures specify the attestation base object. They define which attestation object properties are to be attested. Attestation object data can be provided in list or report form.

To edit an attestation procedure

1. In the Manager, select the **Attestation > Basic configuration data > Attestation procedures** category.

2. Select an attestation procedure in the result list and run the **Change main data** task.

   - OR -

   Click ➕ in the result list.

3. Edit the attestation procedure main data.

4. Save the changes.

General main data of an attestation procedure

Enter the following properties for an attestation procedure.

Table 2: General main data of an attestation procedure

Property	Description
Attestation procedure	Any name for the attestation procedure.
Attestation type	Criteria for grouping attestation procedures. Attestation types make it easier to assign a matching attestation procedure to the attestation policies.
Description	Text field for additional explanation.
Report	Report for the attestor containing all the necessary information about the attestation objects.
	Predefined reports are supplied in a menu. If you do not want to assign a report, you can specify additional information about the attestation objects in the **Property 1-4 (template)** fields.
Table	Database table in which the attestation objects are to be found (= attestation base object). All tables, which fulfill the following conditions, are available:
	a. The table contains a XObjectKey column.
	b. The table type is **Table**, **View**, **ReadOnly**, or **Proxy**.

Property	Description
	c. The usage type is **User data**, **Materialized data**, or **Read only data**.
	d. It is not the basetree table. It is not an assignment table referencing basetree.
	e. Table belongs to the application data model.
	f. Table is not disabled.
	For more information about table types and usage types, see the *One Identity Manager Configuration Guide*.
Preprocessor condition	Specifies the preprocessor configuration parameters on which the attestation procedure depends. Attestation procedures that are disabled through a preprocessor condition are not displayed in One Identity Manager.
Grouping column 1-3 (template)	A value template for formatting the value used to group and filter pending attestation cases in the Web Portal.
	Enter a value template in dollar notation. This template can access the base object properties and the properties of all objects connected through foreign keys.
Grouping column 1-3	Column headers for **Grouping column 1-3 (template)**. The columns are multi-language. To enter a translation, click 🌐.
Property 1-4 (template)	Templates for formulating a value that supplies additional information about the attestation object. Use these fields to show additional information about the attestation object in the Web Portal.
	Enter a value template in dollar notation. This template can access the base object properties and the properties of all objects connected through foreign keys.
Property 1-4	Column headers for **Property 1-4 (template)**. The columns are multi-language. To enter a translation, click 🌐.
Risk index template	Template for formulating the value for the attestation case's risk index.
	Enter a value template in dollar notation. This template can access the base object properties and the properties of all objects connected through foreign keys.
Related object 1-3 (template)	Template for formulating an object key for an object related to the attestation base object. Required for displaying pending attestation cases in the Web Portal.
	Enter a value template in dollar notation. This template can access the base object properties and the properties of all objects connected through foreign keys.
	Define the display value for this object in **Grouping column 1-3 (template)**.

Example

You want to attest Active Directory group memberships. Group the attestation cases by user account display value, Active Directory group display value, and the display value of associated employees. The Active Directory group's canonical name should be displayed with every group membership in the Web Portal. The attestation case's risk index can be determined from the group membership's risk index. The object key for the object relation can be found from the Active Directory user account. The information required about the attestation objects will be summarized in a report. To do this, enter the following data on the main data form.

Table 3: Example of an attestation case definition

Property	Value
Table	Database table `ADSAccountInADSGroupTotal`
Report	<report name>
Grouping column 1	$UID_ADSAccount[d]$
Grouping column 2	$UID_ADSGroup[d]$
Grouping column 3	$FK(UID_ADSAccount).UID_Person[d]$
Property 1 (template)	$FK(UID_ADSGroup).CanonicalName$
Risk index template	$RiskIndexCalculated$
Object relation 1	$FK(UID_ADSAccount).XObjectKey$

Detailed information about this topic

- Attestation types on page 12
- Defining reports for attestation on page 16

Defining reports for attestation

Define attestation reports with the Report Editor. For more information about creating reports with the Report Editor, see the *One Identity Manager Configuration Guide*.

Note the following when you define a report for attestation:

- The base table for the report must be identical to the one for the attestation procedure.
- Enter **Attestation** as the report category. This ensures that the report is displayed in the **Report** menu of the attestation procedure.
- In order to create a report for each attestation object with the information relating exactly to the attestation object, define a `ObjectKeyBase` parameter for the attestation object in the report. Use the parameters in the data source definition for

the report in **Condition** field.

Example: XObjectKey = @ObjectKeyBase

Default reports

One Identity Manager supplies some default reports for attestation. These are used in the default attestation procedures, amongst others.

TIP: Default reports cannot be changed. If you want to customize a default report, create a copy and edit it according to your requirements. Then assign the copy to the attestation procedure.

Default attestation procedures

One Identity Manager provides a default approval procedure for default attestation of new users and recertification of all employees stored in the One Identity Manager database. Moreover, default approval procedures are supplied through which the different roles, user accounts, and system entitlements mapped in the Unified Namespace can be attested. Using these default approval policies you can create attestation procedures easily in the Web Portal.

To display default attestation procedures

- In the Manager, select the **Attestation > Basic configuration data > Attestation procedures > Predefined** category.

For detailed information about using default attestation procedures, see the *One Identity Manager Web Designer Web Portal User Guide*.

Related topics

- User attestation and recertification on page 150
- Default attestation and withdrawal of entitlements on page 140

Additional tasks for attestation procedures

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

Overview of the attestation procedure

You can see the most important information about an attestation procedure on the overview form.

To obtain an overview of an attestation procedure

1. In the Manager, select the **Attestation > Basic configuration data > Attestation procedures** category.

2. Select the attestation procedure in the result list.

3. Select the **Attestation procedure overview** task.

Assigning approval policies

Use this task to assign the selected attestation procedure to the approval policies that should be used in this attestation procedure. All approval policies permitted for the attestation base object are listed.

To assign approval policies to attestation procedures

1. In the Manager, select the **Attestation > Basic configuration data > Attestation procedures** category.

2. Select the attestation procedure in the result list.

3. Select **Assign approval policies** task.

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

    > TIP: In the **Remove assignments** pane, you can remove approval policy assignments.
    >
    > #### *To remove an assignment*
    >
    > - Select the approval policy and double-click ✅.

4. Save the changes.

Which approval policies are permitted depends on the approval procedures in use. Approval procedures dictate to which tables an approval procedure can be assigned.

Related topics

- Specifying permitted approval procedures for tables on page 92

Creating a copy

You can make copies of attestation procedures and those copies allow you to modify default attestation procedures.

To copy an attestation procedure

1. In the Manager, select the **Attestation > Basic configuration data > Attestation procedures** category.

2. Select the attestation procedure in the result list.

3. Select **Create copy** task.

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

5. Decide whether the condition types should be copied for the attestation wizard in the Web Portal as well.

    Condition types are required if attestation policies are created and edited with the attestation wizard in the Web Portal. For detailed information, see *One Identity Manager Web Designer Web Portal User Guide*.

6. Edit the attestation procedure copy and save the changes.

    The attestation procedure copy is displayed on the main data form with the name **<Name of original attestation procedure>(copy)**. You can rename and edit this attestation policy.

Attestation schedules

Use schedules to automate attestation. These specify when and how often attestation cases are created. One Identity Manager supplies several default schedules for attestation.

To edit schedules

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

    The result list shows all schedules configured for attestation policies (AttestationPolicy task).

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 4: Schedule properties

Property	Meaning
Name	Schedule ID. Translate the given text using the 🌐 button.
Description	Detailed description of the schedule. Translate the given text using the 🌐 button.
Table	Table whose data can be used by the schedule. Schedules for the attestation must reference the AttestationPolicy table.
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.

Property	Meaning
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.
	
	• **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.

Property	Meaning
	• **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.
	• 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	Rate of occurrence for running the schedule within the selected time

Property	Meaning
every	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 attestation schedules by default:

Table 5: Default attestation schedules

Schedule	Description
Half-Yearly	
Monthly	
Quarterly	Default schedules for any attestation.
Weekly (Monday)	
Yearly	
Deactivated	Default schedule for default attestation policies.
	The schedule is disabled by default and should not be enabled. To run attestation, assign another schedule to the attestation policies and enable that one.
Daily	Default schedules for any attestation.
	This schedule is assigned to the **New user certification** attestation policy by default.

Related topics

- Preparing for recertification on page 162
- Scheduled attestation on page 159

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. In the Manager, select the **Attestation > Basic configuration data > Schedules** category.

2. Select the schedule in the result list.

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

Assigning attestation policies

Use this task to assign attestation policies to the selected schedule, which will run them. The assignment form displays all the attestation policies that are assigned this selected schedule

To assign attestation policies to a schedule

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

2. Select the schedule in the result list.

3. Select the **Assign attestation polices** task.

4. In **Add assignments**, double-click the attestation policies that are to be assigned.

5. Save the changes.

To change an assignment

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

2. Select the schedule in the result list.

3. Select the **Assign attestation polices** task.

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

   This shows attestation policies that are already assigned to other schedules.

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

   The attestation policy is assigned to the currently selected schedule.

6. Save the changes.

NOTE: Assignments cannot be removed. Attestation policies must be assigned a schedule. It is compulsory.

Starting schedules immediately

NOTE: If a schedule is started, it starts attestation for all active attestation policies assigned with the schedule.

To start a schedule immediately

1. In the Manager, select the **Attestation > 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.

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. In the Manager, select the **Attestation > 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 attestation

Property	Description
	policies 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.

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. In the Manager, select the **Attestation > Basic configuration data > Compliance Frameworks** category.

2. Select the compliance framework from the result list.

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

Assigning attestation policies

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

To assign attestation policies to a compliance framework

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

2. Select the compliance framework from the result list.

3. Select the **Assign attestation polices** task.

   Assign the attestation policies in **Add assignments**.

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

   ### To remove an assignment

   - Select the approval policy and double-click ⊘.

4. Save the changes.

Chief approval team

Sometimes, approval decisions cannot be made for attestation cases because an attestor is not available or does not have access to One Identity Manager tools. To complete these attestations, you can define a chief approval team whose members are authorized to intervene in the approval process at any time.

There is a default application role in One Identity Manager for the chief approval team. Assign this application role to all employees who are authorized to approve, deny, cancel attestations in special cases, or to authorize other attestors. For detailed information about application roles, see the *One Identity Manager Authorization and Authentication Guide*.

Table 7: Default application role for chief approval team

User	Tasks
Chief approval team	The chief approver must be assigned to the **Identity & Access Governance | Attestation | Chief approval team** application role. Users with this application role: • Approve using attestation cases. • Assign attestation cases to other attestors.

To add members to the chief approval team

1. In the Manager, select the **Attestation > Basic configuration data > Chief approval team** category.

2. Select the **Assign employees** task.

   In the **Add assignments** pane, assign the employees who are authorized to approve all attestations.

   > TIP: In the **Remove assignments** pane, you can remove the assignment of employees.
   >
   > ### To remove an assignment
   >
   > • Select the employee and double-click ✅.

3. Save the changes.

Detailed information about this topic

• Attesting by chief approval team on page 108

Attestation policy owners

Default application roles for attestation policy owners are available in One Identity Manager. These owners have permission to edit attestation policies. For detailed

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

Table 8: Default application roles for attestation policy owners

User	Tasks
Attestation policy owners	Owners of attestation policies must be assigned to a child application role of the **Identity & Access Governance	Attestation	Attestation policy owners** application role. Users with this application role: • Are responsible for its content and handle the attestation policies assigned to it. • Assign the attestation procedure, approval policy, and calculation schedule. • Assign approvers, mitigating controls, and compliance frameworks. • Monitor attestation cases and attestation runs.
Direct owners	Direct owners are all employees assigned to an attestation policy as an **Owner** (UID_PersonOwner column). Members of this application role are determined through a dynamic role.
Owner role	This application role or child application role can be assigned to attestation policies as an **Owner (application role)** (UID_AERoleOwner column) This allows you to specify groups of employees as owners for attestation policies. Employees are added as members to application roles by direct assignment.

To add members to the owner role

1. In Manager, select the **Attestation > Basic configuration data > Attestation policy owners > Owner role** category.

2. Select the **Assign employees** task.

   In the **Add Assignments** pane, assign the employees who are allowed to edit an attestation policy.

   TIP: In the **Remove assignments** pane, you can remove the assignment of employees.

   To remove an assignment

   • Select the employee and double-click ⊘.

3. Save the changes.

If you want to restrict owner permissions to individual attestation policies, create child application roles.

To specify an owner role for an attestation policy

1. Log in to the Manager as an attestation administrator (**Identity & Access Governance | Attestation | Administrators** application role).

2. Select the **Attestation > Attestation policies** category.

3. Select the attestation policy in the result list.

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

5. In the **Owner (application role)** menu, select the owner role.

   - OR -

   Click next to the menu to create a new application role.

   a. Enter the application role name and assign the **Identity & Access Governance | Attestation | Attestation policy owners | Owner role** parent application role.

   b. Click **OK** to add the new application role.

6. Save the changes.

7. Assign employees to this application role who are permitted to edit the attestation policy.

Related topics

- General main data of attestation policies on page 30

Standard reasons for attestation

 For attestations, 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 attestors can select a suitable text from these standard reasons in the Web Portal and store it with the attestation case.

Standard reasons are displayed in the attestation history.

To create or edit standard reasons

1. In the Manager, select the **Attestation > 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 9: General main data of a standard reason

Property	Description
Standard reason	Reason text as displayed in the Web Portal and in the attestation history.
Description	Text field for additional explanation.
Automatic Approval	Specifies whether the reason text is only used for automatic approvals by One Identity Manager. This standard reason cannot be selected by manual 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 attestation.
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 attestations on page 29

Predefined standard reasons for attestations

One Identity Manager provides predefined standard reasons. These are added to the attestation case 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 **Attestation > 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 attestation on page 28

Attestation policies

Attestation policies specify the concrete conditions for attestation. Use the main data form to enter the attestation procedure, approval policy and the schedule. You can use a WHERE clause to limit the attestation objects.

To edit attestation polices

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select an attestation policy in the result list and run the **Change main data** task.

   - OR -

   Click in the result list.
3. Edit the main data of the attestation policy.
4. Save the changes.

General main data of attestation policies

Enter the following data for attestation policies.

Table 10: General main data of attestation policies

Property	Description
Attestation policy	Name of the attestation policy.
Attestation procedure	Attestation procedure used for attesting. Attestation procedures are displayed in a menu grouped by attestation type.
Approval policies	Approval policy for determining the attestor for the attestation objects.
Owner	Creator of the attestation policy. The name of the user logged in to One Identity Manager is entered here by default. This can be changed.
Owner (application role)	Application role whose members may edit the attestation policy. To create a new application role, click . Enter the application role name and assign a parent application role.
Sample	Sample that can be used for attestations. A sample can only be assigned to exactly one attestation policy. To create a new sample, click . Enter the name of the sample and assign the table from which to take the data for the sample. You cannot assign samples to default attestation policies.

Property	Description
Time required (days)	Number of days within which a decision must be made over the attestation. Enter **0** if you do not want to specify a particular processing period.
	Weekends and holidays are included by default when calculating the due date of attestation cases. If weekends and holidays should be treated as working days, set the **QER	Attestation	UseWorkingHoursDefinition**, **QBM	WorkingHours	IgnoreHoliday**, and **QBM	WorkingHours	IgnoreWeekend** configuration parameters. For more information about calculating working hours, see the *One Identity Manager Configuration Guide*.
	One Identity Manager does not stipulate which actions are carried out if processing times out. Define your own custom actions or evaluations to deal with this situation.
Description	Text field for additional explanation.
Risk index	Specifies the risk for the company if attestation for this attestation policy is denied. Use the slider to enter a value between **0** and **1**.
	• **0**: No risk.
	• **1**: The denied attestation is a problem.
	This input field is only visible if the **QER	CalculateRiskIndex** configuration parameter is activated.
Risk index (reduced)	Show the risk index taking mitigating controls into account. The risk index for an attestation policy is reduced by the **Significance reduction** value for all assigned mitigating controls.
	This input field is only visible if the **QER	CalculateRiskIndex** configuration parameter is activated. The value is calculated by One Identity Manager and cannot be edited.
Calculation schedule	Schedule for running attestation. Attestation cases are started automatically at the times specified by the schedule.
Deactivated	Specifies whether the attestation policy is disabled or not.
	Attestation cases cannot be added to disabled attestation policies and, therefore, no attestation is done. Disabled attestation policies can be deleted.
	Completed attestation cases can be deleted once the attestation policy is disabled.
Display objects to be attested	Specifies whether the objects affected by the attestation policy are calculated and displayed on the overview form.
Close obsolete tasks automat-	Specifies whether pending attestation cases are canceled if new ones are added.

Property	Description
ically	If attestation is started and this option is set, new attestation cases are created according to the condition. All pending, obsolete attestation cases for newly determined attestation objects of this attestation policy are stopped. Attestation cases for attestation objects that are not recalculated, remain intact.
Obsolete tasks limit	Specifies the maximum number of closed attestation cases for each attestation object that should remain in the database when closed attestation cases are deleted. • **0**: No attestation cases are deleted. • **> 0**: The given number of closed attestation cases for each attestation object to remain in the database. The value can be edited only if the **Delete attestation cases** function is configured. For more information, see Deleting attestation cases on page 118.
Reason for decision	Reason that is given if the **Close obsolete tasks automatically** option is set and pending attestation cases are automatically closed.
Output format	Format in which the report is generated. This menu is only visible if the **QER | Attestation | AllowAllReportTypes** configuration parameter is set. If the configuration parameter is not set, the default PDF format is used because it is the only format that is version compatible.
Edit connection…	Starts the WHERE clause wizard. Use this wizard to create or edit a condition to determine the attestation objects from the database table specified in the attestation procedure.

Condition	Data query for finding attestation objects.
	
	This shows the input field for new attestation policies.
	
	NOTE: For sample attestation, the condition must also query the sample data. There is a template to help set up the condition. This condition can be changed if necessary.
	
	Example of attesting employees using a sample:
	
	<pre>EXISTS (SELECT 1 FROM
	    (
	    SELECT ObjectKeyItem FROM QERPickedItem
	        WHERE UID_QERPickCategory = '$UID_QERPickCategory$'
	    ) as X
	    WHERE X.ObjectKeyItem = Person.XObjectKey)</pre>
	Example of attesting user accounts using a sample of employees:

Property	Description

```
EXISTS (SELECT 1 FROM
    (
    SELECT UID_Person FROM Person WHERE EXISTS
        (
        SELECT 1 FROM
            (
            SELECT ObjectKeyItem FROM QERPickedItem
                WHERE UID_QERPickCategory = '$UID_QERPick-
Category$'
            ) as X
            WHERE X.ObjectKeyItem = Person.XObjectKey
    ) ) as X
    WHERE X.UID_Person = UNSAccount.UID_Person)
```

To show the condition for existing attestation policies, run the **Show condition** task.

Attestation with multi-factor authentication	Attestation of this attestation policy requires multi-factor authentication.

NOTE: You can only edit attestation policies in the Web Portal that were created in the Web Portal. You will see a corresponding message on the main data form as to whether the attestation policy as created in the Web Portal.

If you want to edit attestation policies like this, create a copy in the Manager.

For more information about editing attestation policies in the Web Portal, see the *One Identity Manager Web Designer Web Portal User Guide*.

Detailed information about this topic

- Showing or hiding conditions on page 38
- Attestation schedules on page 19
- Disabling attestation policies on page 40
- Mitigating controls on page 165
- Setting up multi-factor authentication for attestation on page 96
- Copy attestation policies on page 39
- Attestation policy owners on page 26
- Using samples with attestation policies on page 45

Related topics

- Deleting attestation policies on page 39
- General main data of samples on page 42

Specifying risk indexes for attestation guidelines

You can use One Identity Manager to evaluate the risk of attestation cases. To do this, enter a risk index for the attestation policy. The risk index specifies the risk involved for the company in connection with the data to be attested. The risk index is given as a number in the range 0 .. 1. By doing this you specify whether data to be attested is considered not to be a risk (risk index = 0) or whether every denied attestation poses a problem (risk index = 1).

The risk that attestations will be denied approval can be reduced by using the appropriate mitigating controls. Enter these controls as mitigating controls in One Identity Manager. You reduce the risk by the value entered as the significance reduction on the mitigating control. This value is used to calculate the reduced risk index for the attestation policy.

You can create several reports with the Report Editor to evaluate attestation cases depending on the risk index. For more information, see the *One Identity Manager Configuration Guide*.

Risk assessments can be carried out when the **QER | CalculateRiskIndex** configuration parameter is enabled. For more information, see the *One Identity Manager Risk Assessment Administration Guide*.

Detailed information about this topic

-

Default attestation policies

One Identity Manager provides default attestation policies for default attestation of new users and recertification of all employees stored in the One Identity Manager database. In addition to this, default attestation policies are provided through which various roles, memberships in roles, user accounts, and system entitlements mapped in the Unified Namespace can be attested.

To display default attestation policies

- In the Manager, select the **Attestation > Attestation policies > Predefined** category.

You can customize the following properties for default attestation policies:

- Approval policies (if several approval policies can be assigned)
- Owner
- Processing time
- Risk index

- Calculation schedule
- Deactivated
- Close obsolete tasks automatically
- Obsolete tasks limit
- Reason for decision
- Condition
- Approval by multi-factor authentication

NOTE: You can edit attestation policies, whose condition is stored as a definition (XML), in the Web Portal. The definition (XML) cannot be edited in the Manager. For more information, see the *One Identity Manager Web Designer Web Portal User Guide*.

Additional tasks for attestation policies

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

The attestation policy overview

You can see the most important information about an attestation policy on the overview form.

To obtain an overview of an attestation policy

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select the attestation policy in the result list.
3. Select **Attestation policy overview** task.

Assigning approvers to attestation policies

Use this task to assign employees that can be determined as approvers in an attestation case to the selected attestation policy.

To assign approvers to an attestation policy

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select the attestation policy in the result list.
3. Select the **Assign approver** task.

   In the **Add assignments** pane, assign the approvers.

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

To remove an assignment

- Select the approver and double-click ✅.

4. Save the changes.

Detailed information about this topic

-

Assigning compliance frameworks to attestation policies

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

To assign compliance frameworks to an attestation policy

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select the attestation policy in the result list.
3. Select the **Assign compliance frameworks** task.

   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 ✅.

4. Save the changes.

Mitigating controls

Mitigating controls describe controls that are implemented if an attestation rule was violated. The attestation can be approved after the next attestation run, once controls have been applied.

To edit mitigating controls

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

   NOTE: If you disable the configuration parameter at a later date, model components and scripts that are 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*.

Detailed information about this topic

-
-
-

Assigning mitigating controls

Specify which mitigating controls apply to the selected attestation policy.

To assign mitigating controls to an attestation policy

1. In the Manager, select the **Attestation > Attestation policies** category.

2. Select the attestation policy in the result list.

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

    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 ✓.

4. Save the changes.

Creating mitigating controls

To create a mitigating control for attestation policies

1. In the Manager, select the **Attestation > Attestation policies** category.

2. Select an attestation policy in the result list.

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

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

5. Enter the main data of the mitigating control.

6. Save the changes.

7. Select the **Assign attestation polices** task.

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

9. Save the changes.

Detailed information about this topic

-

Running attestation for single objects

Use this task to start attestations independently from a schedule. If you run the task, a separate window is opened. Select the objects to be attested now from a list of all attestation objects. The selection is one-off.

The **Close obsolete tasks automatically** option is not taken into account for the selected attestation objects.

If a sample is assigned to the attestation policy, you can select individual objects from the sample data. The **Remove items after attestation run** option is not taken into account; the attestation data is not deleted after the attestation run.

To start attestation for the selected objects

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select the attestation policy in the result list. Select the **Change main data** task.
3. Select the **Run attestation cases for single objects...** task.

   This opens a separate window.
4. In the **Attestation** column, select every object for which attestation is to be run.
5. Click **Run**.

   Attestation cases are generated for the selected attestation objects. As soon as DBQueue Processor has processed the task, you will see the newly created attestation cases in the navigation view under the **Attestation runs > <attestation policy> > Attestation runs > <year> > <month> > <day> > Pending attestations** menu item.
6. Click **Close**.

Related topics

- General main data of attestation policies on page 30
- General main data of samples on page 42
- Starting attestation on page 111

Showing or hiding conditions

The condition for finding attestation objects can be viewed and edited in the Where Clause Wizard. The SQL query for this condition can be displayed on the main data form.

To show the condition for finding attestation objects on the main data form

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select the attestation policy in the result list and run the **Change main data** task.
3. Select the **Show condition** task.

This displays the **Condition** field on the main data form. The condition is written like a database query WHERE clause. You can edit it directly.

To hide the condition for finding attestation objects

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select the attestation policy in the result list and run the **Change main data** task.
3. Select the **Hide condition** task.

   The **Condition** field is no longer displayed on the main data form.

Copy attestation policies

You can make copies of attestation policies and use them to modify default attestation policies, for example.

To copy an attestation policy

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select the attestation policy in the result list.
3. Select the **Create copy** task.
4. Confirm the security prompt with **Yes**.

   The attestation policy copy is displayed on the main data form with the name **Copy of <Name of original attestation policy>**. You can edit this attestation policy.

Showing selected objects

To show a list of attestations found

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select the attestation policy in the result list and run the **Change main data** task.
3. Select **Show selected objects** task.

   An additional **Result** tab is shown on the main data form. This displays a list of attestation objects found through the condition.

Deleting attestation policies

IMPORTANT: Do not delete attestation policies, for audit reasons.

Attestation policies may still be removed from the One Identity Manager database under specific conditions. Ensure that the attestation policy is archived when deleted.

For more information about data archiving, see the *One Identity Manager Configuration Guide*.

ONE IDENTITY
by Quest

Prerequisite

- The attestation policy is disabled.

To delete an attestation policy

1. In the Manager, select the **Attestation > Attestation policies > Disabled policies** category.

2. Select the attestation policy in the result list and run the **Change main data** task.

3. Select **Delete attestation policy** task.

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

   The attestation policy is deleted. All associated attestation cases, approval workflows and the attestation history are deleted.

Related topics

- Disabling attestation policies on page 40

Disabling attestation policies

Attestations are run when the schedule assigned to an attestation policy is enabled. You can disabled attestation policies to prevent attestation cases being created for individual attestation policies.

IMPORTANT: All associated attestation cases are deleted. To be able to trace the changes later, configure how the data is logged. For more information, see Deleting attestation cases on page 118 and the *One Identity Manager Configuration Guide*.

TIP: Numerous default attestation policies are supplied with One Identity Manager. Check which of the default attestation policies are relevant for your data situation when you set up your database. Disable all unnecessary attestation policies.

To disable an attestation policy

1. In the Manager, select the **Attestation > Attestation policies** category.

2. Select the attestation policy in the result list and run the **Change main data** task.

3. Set **Disabled**.

4. Save the changes.

Related topics

- Suspending attestation on page 54

Reports about attestations

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 attestation policies.

Table 11: Reports about attestations

Report	Description
Overview attestation run results	This report shows the results of an attestation run for the selected attestation policy.
Overview attestation run results including attestation history	This report shows the results of an attestation run for the selected attestation policy including the attestation history.
Detailed status of an attestation run	This report shows the detailed status of an attestation run including the estimated completion date.
Detailed status of an attestation run including approval history	This report shows the detailed status of an attestation run including the estimated completion date and attestation history.

Sample attestation

Sample attestation provides a way to limit the set of attestation objects for an attestation. For example, this can be useful if attesting everyone in an audit would take too long. The sample data can either be generated automatically or compiled manually.

The One Identity Manager provides a standard sample that is used to attest memberships in system entitlements after organizational changes.

Detailed information about this topic

- Creating, editing, deleting samples on page 42
- Managing sample data on page 43
- Generating sample data automatically on page 44
- Using samples with attestation policies on page 45
- Displaying the sample overview on page 45
- Default sample for attesting memberships in system entitlements on page 46

Creating, editing, deleting samples

To be prepare sample attestations:

- Create samples.
- Define the sample data.
- Assign the samples to the attestation policies that will use them.

To create a sample

1. In the Manager, select the **Attestation > Samples** category.
2. Click ⊞ in the result list.
3. Edit the sample's main data.
4. Save the changes.

To edit a sample

1. In the Manager, select the **Attestation > Samples** category.
2. In the result list, select the sample and run the **Change main data** task.
3. Edit the sample's main data.
4. Save the changes.

To delete a sample

1. In the Manager, select the **Attestation > Samples** category.
2. In the result list, select the sample and click ⊠ .
3. Confirm the security prompt with **Yes**.

Detailed information about this topic

- General main data of samples on page 42
- Managing sample data on page 43
- Using samples with attestation policies on page 45

General main data of samples

Enter the following main data of a sample.

Table 12: General main data of a sample

Property	Description
Display name	Name of the sample.
Table	Table that contains the selected sample data.
Manually selected	Specifies whether the sample data is manually selected.
Remove items after attestation run	Specifies whether the sample data is deleted from the sample after each attestation run.
	After each attestation of this sample, the sample data must be regenerated.
	The option is not taken into account when attesting individually selected objects.

Related topics

Managing sample data

Sample data can either be generated automatically or compiled manually. To set sample data manually, assign sample items to the samples.

To assign sample items manually

1. In the Manager, select the **Attestation > Samples > Manually selected** category.

2. Select the sample in the results list.

3. Select the **Assign sample items** task.

   In the **Add assignments** pane, assign sample items.

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

   To remove an assignment

   - Select the sample item and double-click ✅.

4. Save the changes.

To display sample items for automatically selected samples

1. In the Manager, select the **Attestation > Samples > Automatically selected** category.

2. Select the sample in the results list.

3. Select the **Assign sample items** task.

Related topics

Generating sample data automatically

One Identity Manager distinguishes between manual sampling and automatic sampling. Automatic sampling can trigger the generation of sample data as follows:

- Event-based: All modified objects of an object class (table from which the sample data is selected) are calculated.

  Example: All user accounts whose risk index has increased since the previous attestation.

  For the default **Monthly organizational changes of employees** sample, the sample data are generated event-based.

Prerequisite

- In the sample, the **Manually selected** option is disabled.

To generate sample data for an event-based sample

- In the Designer, create a process that is generated when changes are made to the table given in the sample. Use the `Execute SQL` process task from the `SQLComponent` process component.

  - Determine the value of the `SQLStmt` parameter with the following query:

    ```
    Dim f As ISqlFormatter = Connection.SqlFormatter Value =
    f.StoredProcedure(New SQLFunction("QER", "''", "PPickedItemInsert"), _
    f.FormatValue("<UID_QERPickCategory>", ValType.String, True), _
    f.FormatValue($XObjectKey$, ValType.String, True) _ )
    ```

  - UID_QERPickCategory: Unique identifier of the sample whose sample data is to be generated.

For more information about defining processes, see the *One Identity Manager Configuration Guide*.

If the **Remove items after attestation run** option is set in the sample, the sample data will be deleted as soon as an attestation run is completed. This way ensures that the sample always contains only those objects that have been changed since the previous attestation.

Related topics

- Sample attestation on page 41
- General main data of samples on page 42
- Managing sample data on page 43

Using samples with attestation policies

To use sampling for attestation, assign a sample to the appropriate attestation policies. A sample can only be assigned to exactly one attestation policy.

To assign a sample to an attestation policy

1. In the Manager, select the **Attestation > Attestation policies** category.
2. Select an attestation policy in the result list and run the **Change main data** task.
3. In the **Sample** menu, select a sample.
    - To create a new sample, click ⊞. Enter the name of the sample and assign the table from which to take the data for the sample.
4. Save the changes.

Related topics

- General main data of attestation policies on page 30
- Managing sample data on page 43
- Sample attestation on page 41

Displaying the sample overview

You can see the most important information about a sample on the overview form. You can see the attestation policy that is used with sample.

To obtain an overview of a sample

1. In the Manager, select the **Attestation > Samples** category.
2. Select the sample in the results list.
3. Select the **Sample oerview** task .

Related topics

- Sample attestation on page 41
- Creating, editing, deleting samples on page 42

Default sample for attesting memberships in system entitlements

A default sample is provided for attesting memberships in system entitlements after organizational changes. This sample data is determined automatically. This identifies all individuals whose manager or primary department, cost center, or business role assignment has changed since the previous attestation. All memberships are attested whose user accounts are associated with these individuals.

To use attestation of memberships in system authorizations after organizational changes

1. In the Designer, set the **QER | Selections | PersonOrganizationalChanges** configuration parameter.
2. In the Manager, assign an enabled schedule to the **System entitlement memberships after organizational changes** attestation policy.

Once an attestation run is complete, the sample data is deleted. As soon as an individual's organizational data changes, they are included in the sample. This ensures that the sample always includes only those individuals whose organizational data has changed since the previous attestation.

TIP: Sample data is calculated by the `QER_Person_Add_to_PickCategory_Organizational_ Changes` process. You can customize the generating condition of this process.

Related topics

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.

Creating and editing attestation mail templates

To create and edit mail templates

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

   This shows all the mail templates that can be used for attestation cases 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.

Detailed information about this topic

- General properties of a mail template on page 47
- Creating and editing a mail definition on page 49

General properties of a mail template

The following general properties are displayed for a mail template:

Table 13: Mail template properties

Property	Meaning
Mail template	Name of the mail template. This name will be used to display the mail templates in the administration tools and in the Web Portal. Translate the given text using the 🌐 button.
Base object	Mail template base object. A base object only needs to be entered if the mail definition properties of the base object are referenced. Use the `AttestationCase` or `AttestationHelper` base object for notifications about attestation.
Report (parameter set)	Report, made available through the mail template.
Description	Mail template description. Translate the given text using the 🌐 button.

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

Creating and editing a mail 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 **Attestation > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for attestation cases 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 **Attestation > Basic configuration data > Mail templates** category.

   This shows all the mail templates that can be used for attestation cases 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*.

Example:

An attestor should receive email notification of new attestations.

Table 14: Email notification properties

Property	Value
Base object	AttestationHelper
Subject	New attestations
Mail body	Dear $FK(UID_PersonHead).Salutation[D]$ $FK(UID_ PersonHead).LastName$,
	There are new attestations pending for the attestation policy "$FK (UID_AttestationCase).UID_AttestationPolicy[D]$".
	Created: $FK(UID_AttestationCase).PolicyProcessed:Date$
	You can see this request in the "One Identity Manager Self Service Portal".
	Best regards

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 attestations.

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:

`$Script(VI_BuildAttestationLink_Approve)$`

Default functions for requests

The `VI_BuildAttestationLinks` script contains a collection of default functions for composing hyperlinks to directly grant or deny approval of requests from email notifications.

Table 15: Functions of the VI_BuildAttestationLinks script

Function	Usage
VI_BuildAttestationLink_Show	Opens the attestation page in the Web Portal.
VI_BuildAttestationLink_ Approve	Approves an attestation and opens the attestation page in the Web Portal.
VI_BuildAttestationLink_Deny	Denies an attestation and opens the attestation page in the Web Portal.
VI_BuildAttestationLink_ AnswerQuestion	Opens the page for answering a question in the Web Portal.
VI_BuildAttestationLink_ Pending	Opens the page with pending attestations 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 16: 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.

Copying mail templates for attestation

To copy a mail template

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

   This shows all the mail templates that can be used for attestation cases 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**.

Displaying attestation mail templates previews

To display a mail template preview

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

   This shows all the mail templates that can be used for attestation cases 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**.

Deleting mail templates for attestation

To delete a mail template

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

   This shows all the mail templates that can be used for attestation cases 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**.

Custom notification processes

Set up customized processes to send more email notifications within an attestation case. You can use following events for generating processes.

Table 17: Events for the `AttestationHelper` object

Event	Triggered by
DecisionRequired	New attestation case created
	Move to the next approval level
Remind	Reminder interval expired

Table 18: Events for the `AttestationCase` object

Event	Triggered by
Granted	Approval granted for an approval step.
Dismissed	Approval denied for an approval step.
OrderGranted	Approval granted for an entire approval procedure.
FinalDismissed	Approval denied for an entire approval procedure.
QueryToPerson	Making a query
AnswerFromPerson	Answering a query
RecallQuery	Recalling a query
Escalate	Attestation case escalated.
Aborted	Attestation case canceled.
Canceled	Obsolete attestation case canceled.

For detailed information about creating processes, see the *One Identity Manager Configuration Guide*.

Suspending attestation

To suspend attestation you have two options.

1. Disable the schedule assigned to the attestation policy.

   As long as the schedule is disabled, no new attestation cases will be generated. This applies to all attestation policies that have this schedule assigned to them.

   For more information, see Attestation schedules on page 19.

2. Disable the attestation policy

   Once an attestation policy is disabled, no new attestation cases are generated. In addition, all associated attestation cases are deleted. To avoid loosing the attestation history in the process, you can configure how data changes are logged.

   For more information, see Disabling attestation policies on page 40.

Related topics

- Deleting attestation cases on page 118

Approval processes for attestation cases

All attestation procedures are subject to a defined approval process. During this approval process, authorized employees grant or deny approval for attestation objects. You can configure this approval process in various ways, and therefore customize it to meet your company policies.

You define approval policies and approval workflows for approval processes. Specify the approval workflows to apply to the attestation cases in the approval policies. Use approval workflows to find out, which employees in which order, can grant or deny attestation. An approval workflow can contain several approval levels and several approval steps. A special approval procedure is used to determine the attestors in each approval step.

Detailed information about this topic

Approval policies for attestations

One Identity Manager uses approval policies to determine the attestor for each attestation case.

To edit an approval policy

1. In the Manager, select the **Attestation > Basic configuration data > Approval policies** category.

2. Select an approval policy in the result list and run the **Change main data** task.

   - OR -

   Click ![icon] in the result list.

3. Edit the approval policy main data.

4. Save the changes.

General main data of approval policies

Enter the following main data of an approval policy. If you add a new approval step, you must fill out the compulsory fields.

Table 19: General main data of approval policies

Property	Description
Approval policies	Approval step name.
Approval workflow	Workflow for finding attestors. Select any approval workflow from the menu or click ⊞ to set up a new approval workflow.
Mail templates	Mail template used to create email notifications for granting, denying, extending, unsubscribing, or canceling an attestation or for giving notice of its expiry.
Description	Text field for additional explanation.

Detailed information about this topic

- Setting up approval workflows on page 61
- Notifications in the attestation process on page 119

Default approval policies

One Identity Manager provides a default approval policy for default attestation of new users and recertification of all employees stored in the One Identity Manager database. Moreover, default approval policies are supplied through which different roles and system entitlements mapped in the Unified Namespace can be attested. You can use default approval policies for creating attestation policies in the Web Portal.

To edit default approval policies

- In the Manager, select the **Attestation > Basic configuration data > Approval policies > Predefined** category.

For detailed information about using default approval policies, see the *One Identity Manager Web Designer Web Portal User Guide*.

Related topics

- User attestation and recertification on page 150
- Default attestation and withdrawal of entitlements on page 140

Additional tasks for approval policies

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

Editing approval workflows

Here, you can edit the approval workflow assigned to the approval policy.

To edit the assigned approval workflow

1. Select **Attestation > Basic configuration data > Approval policies**.
2. Select the approval policy in the result list.
3. Select **1. Editing approval workflows**.

   This opens the Workflow Editor.

Detailed information about this topic

- Working with the workflow editor on page 58

Validity checking

Once you have edited an approval policy, you need to test it. This checks whether the approval steps can be used in the approval workflows in this combination. Non-valid approval steps are displayed in the error window.

To test an approval policy

1. In the Manager, select the **Attestation > Basic configuration data > Approval policies** category.
2. Select the approval policy in the result list.
3. Select the **Validity check** task.

Approval workflow for attestations

You need to allocate an approval workflow to the approval policies in order to find the attestors. In an approval workflow, you specify the approval procedures, the number of attestors and a condition for selecting the attestors.

Use the workflow editor to create and edit approval workflows.

To edit an approval workflow

1. In the Manager, select the **Attestation > Basic configuration data > Approval workflows** category.

2. Select the approval workflow in the result list and run the **Change main data** task.

   - OR -

   Click in the result list.

   This opens the Workflow Editor.

3. Edit the approval workflow main data.

4. Save the changes.

Working with the workflow editor

Use the workflow editor to create and edit approval workflows. The workflow editor allows approval levels to be linked together. Multi-step approval processes are clearly displayed in a graphical form.

Figure 1: Workflow editor
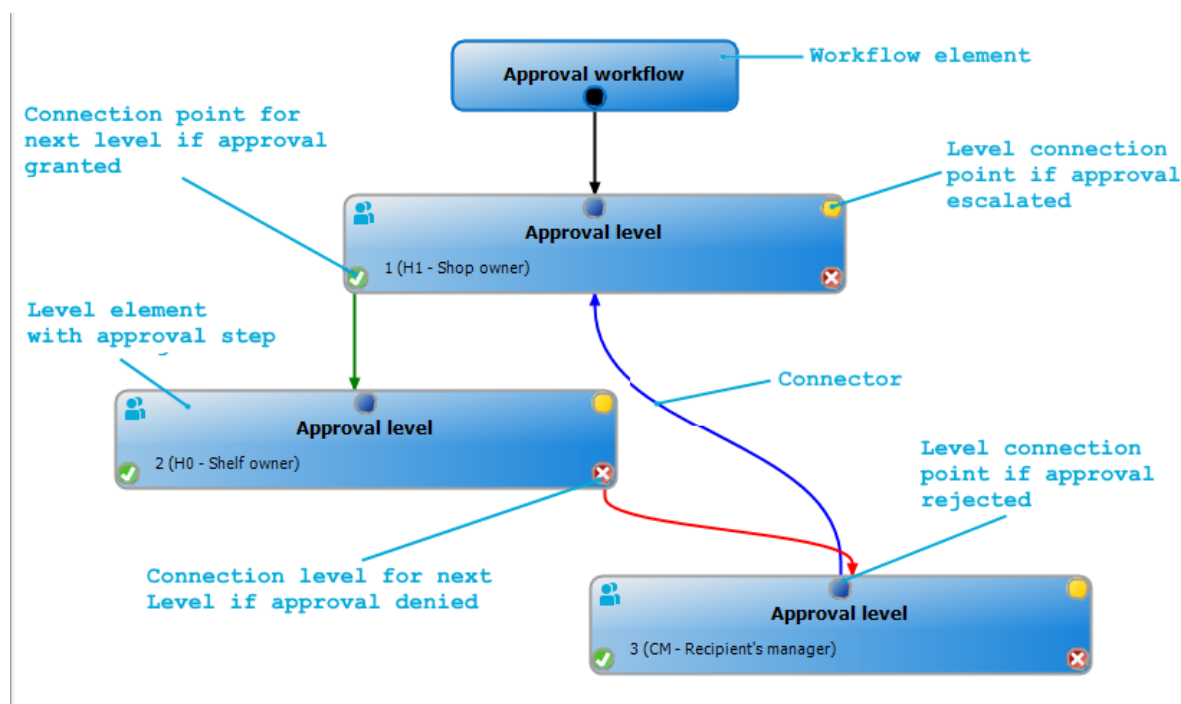
Approval levels and approval steps belonging to the approval workflow are edited in the workflow editor using special control elements. The workflow editor contains a toolbox. The toolbox items are activated or deactivated depending on how they apply to the control. You can move the layout position of the control elements in the workflow editor with the mouse or these can be moved automatically.

Table 20: Entries in the toolbox

Control	Item	Meaning
Workflow	Edit	Edit the properties of the approval workflow.
	Layout automatically	The workflow elements are aligned automatically. The workflow layout is recalculated.
Approval levels	Add	A new approval level is added to the workflow.
	Edit	Edit the properties of the approval workflow.
	Delete	Deletes the approval level.
Approval steps	Add	Add a new approval step to the approval level.
	Edit	Edit the properties of the approval step.
	Delete	Deletes the approval step.
Assignments	Remove positive	The **Approved** connector for the selected approval level is deleted.

Control	Item	Meaning
	Remove negative	The **Deny** connector for the selected approval level is deleted.
	Remove reroute	The **Reroute** connector for the selected approval level is deleted.
	Remove escal-ation	The **Escalate** connector for the selected approval level is deleted.

Each of the controls has a properties window for editing the data of the approval workflow, level, or step. To open the properties window, select the **Toolbox > < Control> > Edit** item.

To delete a control, select the element and then the **Toolbox > <Control> > Delete** item.

Individual elements are linked to each other with a connector. Activate the connection points with the mouse. The cursor changes into an arrow icon for this. Hold down the left mouse button and pull a connector from one connection point to the next.

Figure 2: Approval workflow connectors
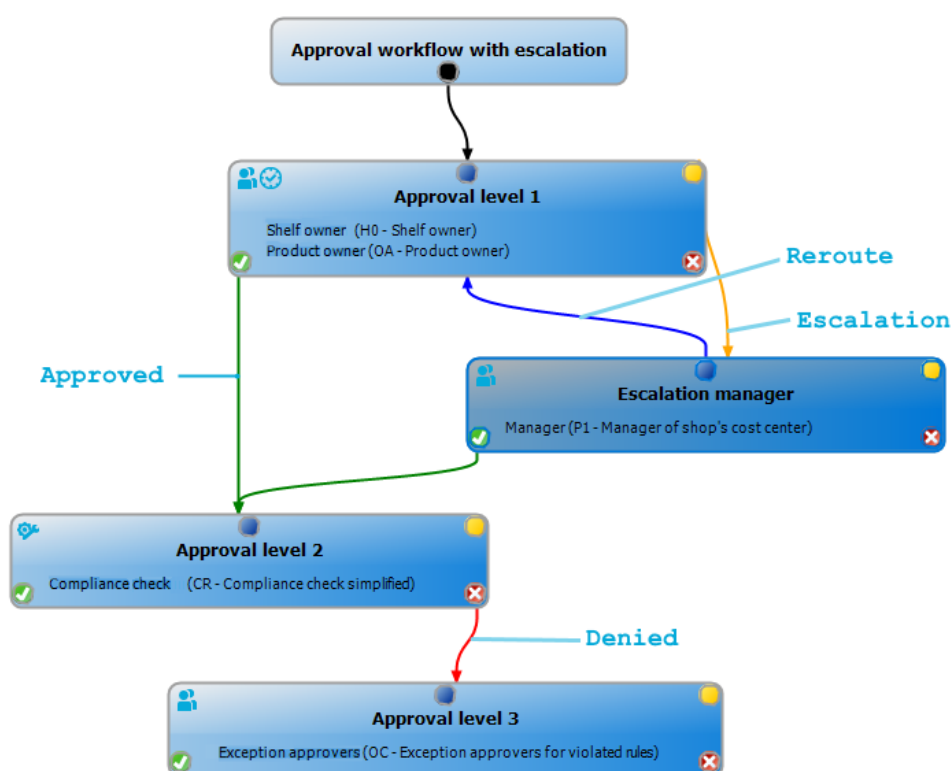
Table 21: Approval workflow connectors

Connector	Meaning
Approve	Link to next approval level if the current approval level was granted approval.
Deny	Link to next approval level if the current approval level was not granted approval.
Reroute	Link to other approval levels to bypass the current approval.
Escalation	Connection to another approval level when the current approval level is escalated after timing out.

By default, a connection between workflow elements and level elements is created immediately when a new element is added. If you want to change the level hierarchy, drag a new connector to another level element.

Alternatively, you can release connectors between level elements using the **Toolbox > Assignments** items. To do this, mark the level element where the connector starts. Then add a new connector.

Different icons are displayed on the level elements depending on the configuration of the approval steps.

Table 22: Icons on the level elements

Icon	Meaning
	The approval decision is made by the system.
	The approval decision is made manually.
	The approval step contains a reminder function.
	The approval step contains a timeout.

Changes to individual elements in the workflow do not take place until the entire approval workflow is saved. The layout position in the workflow editor is saved in addition to the approval policies.

Setting up approval workflows

An approval workflow consists of one or more approval levels. An approval level can contain one approval step or several parallel approval steps. Within the attestation process, all of the approval steps for one approval level must be run before the next approval level is called. Use connectors to set up the sequence of approval levels in the approval workflow.

When you add a new approval workflow, the first thing to be created is a new workflow element.

To edit approval level properties

1. Open the Workflow Editor.

2. Select the **Toolbox > Workflow > Edit** item.

3. Edit the workflow properties.

4. Click **OK**.

Table 23: Approval workflow properties

Property	Meaning
Name	Approval workflow name.
System halt (days)	Number of days to elapse after which the approval workflow, and therefore the system, automatically halts the entire attestation procedure.
Description	Text field for additional explanation.

Detailed information about this topic

- Halting an attestation case on timeout on page 107

Editing approval levels

An approval level provides a method of grouping individual approval steps. All the approval steps in one approval level are run in parallel. All the approval steps for different approval levels are run one after the other. You use the connectors to specify the order.

Specify the individual approval steps in the approval levels. At least one approval step is required per level. Enter the approval steps first before you add an approval level.

To add an approval level

1. Select the **Toolbox > Approval levels > Add** item.

   This opens the properties dialog for the first approval step.

2. Enter the approval step properties.

3. Save the changes.

You can edit the properties of an approval level as soon as you have added an approval level with at least one approval step.

To edit approval level properties

1. Select the approval level.

2. Select the **Toolbox > Approval levels > Edit** item.

3. Enter a display name for the approval level.

4. Save the changes.

NOTE: You can define more than one approval step for each approval level. In this case, the attestors of an approval level can make a decision about an attestation case in parallel rather than sequentially. The attestation case cannot be presented to the attestors at the next approval level until all approval steps in one approval level have been completed in the attestation procedure.

To add more approval steps to an approval level

1. Select the approval level.
2. Select the **Toolbox > Approval steps > Add** item.
3. Enter the approval step properties.
4. Save the changes.

Related topics

- Properties of an approval step on page 63
- Editing approval steps on page 63

Editing approval steps

To edit approval level properties

1. Select the approval step.
2. Select the **Toolbox > Approval steps > Edit** item.
3. Edit the approval step properties.
4. Save the changes.

Detailed information about this topic

- Properties of an approval step on page 63

Properties of an approval step

On the **General** tab, enter the data described below. On the **Mail templates** tab, select the mail templates for generating mail notifications. If you add a new approval step, you must fill out the required fields.

Table 24: General properties of an approval step

Property	Meaning
Single step	Approval step name.
Approval	Procedure to use for determining the attestors.

Property	Meaning
procedure	
Role	Hierarchical role from which to determine the attestors.
	The role is used in the OM and OR default approval procedures. Additionally, you can use the role if you use a custom approval procedure in the approval step.
Fallback approver	Application role whose members are authorized to approve attestation cases if an attestor cannot be determined through the approval procedure. Assign an application from the menu.
	To create a new application role, click ⊞. Enter the application role name and assign a parent application role. For detailed information, see the *One Identity Manager Authorization and Authentication Guide*.
	NOTE: The number of approvers is not applied to the fallback approvers. The approval step is considered approved the moment as soon as one fallback approver has approved the request.
Condition	Condition for calculating the approval decision. The condition is used in the CD, EX, or WC default approval procedures. Additionally, you can use the role if you use a custom approval procedure in the approval step.
Number of approvers	Number of attestors required to approve an attestation case. Use this number to further restrict the maximum number of approvers of the implemented approval procedure.
	If there are several people allocated as approvers, then this number specifies how many people from this group have to approve an attestation case. A request can only be passed up to next level afterwards.
	If you want approval decisions to be made by all the employees found using the applicable approval procedure, for example all members of a role (default approval procedure OR), enter the value **-1**. This overrides the maximum number of attestors defined in the approval procedure.
	If not enough attestors can be found, the approval step is presented to the fallback approvers. The approval step is considered approved as soon as one fallback approver has approved the attestation case.
	If an approval decision is made by the chief approval team, it overrides the approval decision of just one regular attestor. This means, if three attestors must approve an approval step and the chief approval team one of the decision, two more are still required.
	The number of approvers defined in an approval step is not taken into account in the approval procedures CD, EX,or WC.
Description	Text field for additional explanation.
Approval reason	Reason entered in the attestation case if approval is automatically granted.

Property	Meaning
	This field is only shown for the approval procedures CD, EX, and WC.
Reject reason	Reason entered in the attestation case and the attestation history, if approval is automatically denied.
	This field is only shown for the approval procedures CD, EX, and WC.
Reminder after (minutes)	Number of minutes to elapse after which the attestor is notified by mail that there are still pending attestation cases for attestation. The input is converted into working hours and displayed additionally.
	The reminder interval is set to 30 minutes, by default. To change this interval, modify the **Checks reminder interval and timeout of attestation cases** schedule.
	NOTE: Ensure that a state, county, or both is entered into the employee's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating employees' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*.
	TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM	WorkingHours	IgnoreHoliday** or **QBM	WorkingHours	IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.
	If more than one attestor was found, each attestor will be notified. The same applies if an additional attestor has been assigned.
	If an attestor delegated the approval, the time point for reminding the delegation recipient is recalculated. The delegation recipient and all the other attestors are notified. The original attestor is not notified.
	If an attestor has made an inquiry, the time point for reminding the queried employee is recalculated. As long as the inquiry has not been answered, only this employee is notified.
Timeout (minutes)	Number of minutes to elapse after which the approval step is automatically granted or denied approval. The input is converted into working hours and displayed additionally.
	The timeout is check every 30 minutes, by default. To change this interval, modify the **Checks reminder interval and timeout of attestation cases** schedule.
	The working hours of the respective approver are taken into account when the time is calculated.
	NOTE: Ensure that a state, county, or both is entered into the employee's main data of determining the correct working hours. If this

Property	Meaning
	information is missing, a fallback is used to calculate the working hours. For more information about calculating employees' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*.

TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.

If more than one approver was found, then an approval decision for the approval step is not automatically made until the timeout for all approvers has been exceeded. The same applies if an additional approver has been assigned.

If an approver delegated approval, the time point for automatic approval is recalculated for the new approver. If this approval is rejected, the time point for automatic approval is recalculated for the original approver.

If an approver is queried, the approval decision must be made within the defined timeout anyway. The time point for automatic approval is not recalculated.

If additional approvers are determined by recalculating the current approvers, then the automatic approval deadline is not extended. The additional approvers must approve within the time frame that applies to the current approver. |
| Timeout behavior | Action that is run if the timeout expires.

- **Approved**: The attestation case is approved in this approval step. The next approval level is called.
- **Deny**: The attestation case is denied in this approval step. The approval level for denying is called.
- **Escalation**: The attestation case is escalated. The escalation approval level is called.
- **Cancel**: The approval step and, therefore, the entire attestation procedure, is canceled. |
| Additional approver possible | Specifies whether a current attestor is allowed to instruct another employee as an attestor. This additional attestor has parallel authorization to make approvals for the current attestation case. The attestation case is not passed on to the next approval level until both attestors have made a decision.

This option can only be set for approval levels with a single, manual approval step. |

Property	Meaning
Approval can be delegated	Specifies whether a current attestor can delegate the attestation to another person. This employee is added to the current approval step as the attestor. This employee then makes the approval decision instead of the attestor who made the delegation. This option can only be set for approval levels with a single, manual approval step.
Approval by affected employee	Specifies whether the employee who is affected by the approval decision can also approve it. If this option is set, employees to be attested can attest themselves. If this option is not set, use the **QER | Attestation | PersonToAttestNoDecide** configuration parameter to define whether the employees to be attested can attest themselves.
Do not show in approval history	Specifies whether or not the approval step should be displayed in the attestation history. For example, this behavior can be applied to approval steps with the **CD - calculated approval** procedure, which are used only for branching in the approval workflow. It It makes it easier to follow the attestation history.
Escalate if no approver found	Specifies whether the approval step is escalated if no attestor can be found and no fallback approver is assigned. In this case, the attestation case is neither canceled nor passed to the chief approval team. This option can only be enabled if an approval level is linked to escalation.

Detailed information about this topic

- Notifications in the attestation process on page 119
- Reminding attestors on page 121
- Escalating an attestation case on page 102
- Automatic approval on timeout on page 106
- Halting an attestation case on timeout on page 107
- Using a specified role to find attestors on page 82
- Calculated approval on page 85
- Approvals to be made externally on page 86
- Waiting for further approval on page 87
- Prevent attestation by employee awaiting attestation on page 97

Related topics

- Selecting attestors on page 70
- Attestors cannot be established on page 104
- Attesting by chief approval team on page 108

Connecting approval levels

When you set up an approval workflow with several approval levels, you have to connect each level with another. You may create the following links.

Table 25: Links to approval levels

Link	Description
Approve	Link to next approval level if the current approval level was granted approval.
Deny	Link to next approval level if the current approval level was not granted approval.
Reroute	Link to another approval level to bypass the current approval.
	Attestors can pass the approval decision through another approval level, for example, if approval is required by a manager in an individual case. To do this, create a connection to the approval levels to which the approval can be rerouted. This way, approvals can also be rerouted to a previous approval level, for example, if an approval decision is considered not to be well-founded. Starting from one approval level, more than one reroute can lead to different approval levels. The attestors select, in the Web Portal, which of these approval levels to reroute the approval to.
	It is not possible to reroute approval steps with the approval procedures EX, CD, SB, or WC.
Escalation	Link to another approval level when the current approval level is escalated after timing out.

If there are no further approval levels after the current approval level, the attestation case is considered approved if the approval decision was to grant approval. If approval is not granted, the attestation case is considered to be finally denied. The attestation procedure is closed in both cases.

Additional tasks for approval workflows

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

The approval workflow overview

To obtain an overview of an approval workflow

1. In the Manager, select the **Attestation > Basic configuration data > Approval workflows** category.

2. Select the approval workflow in the result list.

3. Select **Approval workflow overview**.

Copying approval workflows

You can copy default approval workflows in order to customize them.

To copy an approval workflow

1. In the Manager, select the **Attestation > Basic configuration data > Approval workflows** category.

2. Select an approval workflow in the result list and run the **Change main data** task.

3. Select the **Copy workflow** task.

4. Enter a name for the copy.

5. Click **OK** to start copying.

   - OR -

   Click **Cancel** to cancel copying.

6. To edit the copy immediately, click **Yes**.

   - OR -

   To edit the copy later, click **No**.

Deleting approval workflows

The approval workflow can only be deleted if it is not assigned to an approval policy.

To delete an approval workflow

1. Remove all assignments to approval policies.

   a. Check to which approval policies the approval workflow is assigned.

   b. Go to the main data form for the approval policy and assign a different approval workflow.

2. In the Manager, select the **Attestation > Basic configuration data > Approval workflows** category.

3. Select an approval workflow in the result list.

4. Click 🗙.

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

Detailed information about this topic

- The approval workflow overview on page 69
- General main data of approval policies on page 56

Default approval workflows

One Identity Manager provides a default approval workflow for default attestation of new users and recertification of all employees stored in the One Identity Manager database. Moreover, default approval workflows are supplied through which different roles and system entitlements mapped in the Unified Namespace can be attested. You can use default approval policies for creating attestation policies in the Web Portal.

To edit default approval workflows

- In the Manager, select the **Attestation > Basic configuration data > Approval workflows > Predefined** category.

For detailed information about using default approval workflows, see the *One Identity Manager Web Designer Web Portal User Guide*.

Related topics

- User attestation and recertification on page 150
- Default attestation and withdrawal of entitlements on page 140

Selecting attestors

One Identity Manager can make approvals automatically in an attestation procedure or through attestors. An attestor is an employee or a group of employees who can grant or deny an attestation case within an attestation procedure. It takes several approval procedures to grant or deny approval. You specify in the approval step which approval procedure should be used.

If several people are determined to be approvers by an approval procedure, the number given in the approval step specifies how many people must approve the step. A request can only be passed up to next level afterwards. The attestation procedure is canceled if an approver cannot be found for an approval step.

One Identity Manager provides approval procedures by default. You can also define your own approval procedures.

The DBQueue Processor calculates which employee is authorized as an approver and in which approval level. Take into account the special cases for each approval procedure when setting up the approval workflows to determine those authorized to grant approval.

Default approval procedures

To display default approval procedures

- Select the **Attestation > Basic configuration data > Approval procedures > Predefined** category.

The following approval procedures are defined to select the responsible attestors, by default.

Table 26: Approval procedures for attestation

Procedure Name	Attestors
AA - Attestor for the role to attest	Attestor of the organization (department, cost center, location), business role, or IT Shop if assignments of system entitlements or system roles to roles are attested. • Attestors for departments, cost centers and locations must be assigned to the **Identity Management | Organizations | Attestors** application role. • Attestors for business roles must be assigned to the **Identity Management | Business roles | Attestors** application role. • Attestors for requests must be assigned to the **Request & Fulfillment | IT Shop | Attestors** application role. For more information, see Using attestation objects to find attestors on page 77.
AD - Attestor of recipient's department	Attestor of the department to which the attestation object is primarily assigned. • Attestors for departments must be assigned to the **Identity Management | Organizations | Attestors** application role. For more information, see Using roles of employees to be attested to find attestors on page 76.
AL - Attestor for recipient's location	Attestor of the location to which the attestation object is primarily assigned. • Attestors for locations must be assigned to the **Identity Management | Organizations | Attestors** application role.

Procedure Name	Attestors
	For more information, see Using roles of employees to be attested to find attestors on page 76.
AM - Manager of account's person	Manager of the employee connected to the user account that is to be attested
	For more information, see Using persons responsible for attestation objects to find attestors on page 80.
AN - Attestor for the system entitlement to attest	Attestor of the system entitlement or system role if assignments of system entitlements or system roles to roles are attested. Attestors are determined through the assigned service item. • Attestors must be assigned to the **Request & Fulfillment | IT Shop | Attestors** application role. For more information, see Using attestation objects to find attestors on page 77.
AO - Attestor for recipient's primary role	Attestor of the business role to which the attestation object is primarily assigned. Attestors for business roles must be assigned to the **Identity Management | Business roles | Attestors** application role. For more information, see Using roles of employees to be attested to find attestors on page 76.
AP - Attestor for recipient's cost center	Attestor of the cost center to which the attestation object is primarily assigned. • Attestors for cost centers must be assigned to the **Identity Management | Organizations | Attestors** application role. For more information, see Using roles of employees to be attested to find attestors on page 76.
AR - Attestor for attestation compliance rule	Attestor for the compliance rule to be attested. • Attestors must be assigned to the **Identity & Access Governance | Identity Audit | Attestors** application role. For more information, see Using attestation objects to find attestors on page 77.
AS - Approver for attestation policy	All employees assigned to the attestation policy as approver. For more information, see Using attestation policies to find attestors on page 76.
AT - Attestor for the	Attestor of the organization (department, cost center, location),

Procedure Name	Attestors
organization to be attested	business role, or IT Shop to be attested. • Attestors for departments, cost centers and locations must be assigned to the **Identity Management | Organizations | Attestors** application role. • Attestors for business roles must be assigned to the **Identity Management | Business roles | Attestors** application role. • Attestors for requests must be assigned to the **Request & Fulfillment | IT Shop | Attestors** application role. For more information, see Using attestation objects to find attestors on page 77.
AY - Attestor for the company policy to be attested	Attestor of the company policy to be attested. • Attestors must be assigned to the **Identity & Access Governance | Company policies | Attestors** application role. For more information, see Using attestation objects to find attestors on page 77.
CD - Calculated approval	- For more information, see Calculated approval on page 85.
CM - Recipient's manager	Manager of the employee to be attested. For more information, see Using attestation object managers to find attestors on page 79.
CS - Employee themselves	Employee to be attested, attests themselves. For more information, see Determining attested employee as attestor on page 84.
DM - Manager of recipient's department	Department manager/deputy if employees of secondary memberships are attested in departments. For more information, see Using attestation object managers to find attestors on page 79.
AE - Employee assigned to account	Employee assigned to the user account to be attested. For more information, see Using employees assigned to user accounts to find attestors on page 84.
ED - Department manager for permission attestation	Employee's department manager whose system entitlements are to be attested. For more information, see Using persons responsible for attestation objects to find attestors on page 80.

Procedure Name	Attestors
EM - Employee manager for permission attestation	Employee's manager whose system entitlements are to be attested.
	For more information, see Using persons responsible for attestation objects to find attestors on page 80.
EN - Target system manager of the permission for attestation	Target system manager of the system entitlements to be attested.
	For more information, see Using persons responsible for attestation objects to find attestors on page 80.
EO - Product owner of the system entitlement to be attested	Product owner whose system entitlements or system roles are to be attested.
	For more information, see Using persons responsible for attestation objects to find attestors on page 80.
EX - Approvals to be made externally	-
	For more information, see Approvals to be made externally on page 86.
KA - Product owner and additional owner of the Active Directory Group	Product owner and additional owner of the Active Directory group, if Active Directory groups or group memberships are attested.
	For more information, see Using persons responsible for attestation objects to find attestors on page 80.
LM - Manager of recipient's location	Location manager/deputy if employees of secondary memberships are attested in locations.
	For more information, see Using attestation object managers to find attestors on page 79.
MD - Department manager of account's person	Manager of the main department of the employee who is connected to the user account to be attested
	For more information, see Using persons responsible for attestation objects to find attestors on page 80.
MO - Role owner	Business role manager/deputy if employees of secondary memberships are attested in roles.
	For more information, see Using attestation object managers to find attestors on page 79.
OA - product owner	All members of the assigned application role if service items, system entitlements or system roles are attested.
	For more information, see Using product owners to find attestors on page 83.
OM - Manager of a	Manager of the role selected in the approval workflow.

Procedure Name	Attestors
specific role	For more information, see Using a specified role to find attestors on page 82.
OP - Owner of a privileged object	All employees that can be determined as owners of the privileged request. For more information, see Using owners of a privileged object to find attestors on page 83.
OR - Members of a certain role	All employees that are assigned to a secondary business role. For more information, see Using a specified role to find attestors on page 82.
OT - Attestor of assigned service item	Attestor of the service item assigned to the object to be attested. • Attestors must be assigned to the **Request & Fulfillment | IT Shop | Attestors** application role. For more information, see Determining attestors using the attestation objects' service item on page 78.
PA - Secondary owner of Active Directory group	All employees to be found through the additional owner of the requested Active Directory group. For more information, see Using additional Active Directory group owners to find attestors on page 84.
PM - Manager of recipient's cost center	Cost center manager/deputy if secondary memberships in cost centers are attested. For more information, see Using attestation object managers to find attestors on page 79.
PO - Proposed owner	Proposed owner of the attestation object For more information, see Using owners of the attestation objects to find attestors on page 84.
RE - Manager of system roles to be attested	System role manager to be attested. For more information, see Using attestation object managers to find attestors on page 79.
RM - Role manager for attesting memberships	Manager of role to be attested if secondary memberships in roles are attested. For more information, see Using attestation object managers to find attestors on page 79.
RR - Role manager for attesting roles and role assignments	Manager of role to be attested. For more information, see Using attestation object managers to find attestors on page 79.

Procedure Name	Attestors
SO - Target system manager of the permission for attestation	Target system manager of system entitlement or user account to be attested. For more information, see Using persons responsible for attestation objects to find attestors on page 80.
WC - Waiting for further approval	- For more information, see Waiting for further approval on page 87.

Using attestation policies to find attestors

Use the AS approval procedure if you want to fix attestors for any object to an attestation policy. This approval procedure finds all employees that are assigned to the attestation procedure as approvers.

Use this procedure to allow any objects to be attested by any of the specified employees. These employees must be assigned to the attestation policy as approvers. The attestor can also be entered when you create attestation policies in the Web Portal. For detailed information, see *One Identity Manager Web Designer Web Portal User Guide*.

Related topics

- Assigning approvers to attestation policies on page 35

Using roles of employees to be attested to find attestors

Installed modules: Business Roles Module (for approval procedure AO).

If you want to attest company resource assignments to employees or their requests, use the AD, AL, AO, or AP approval procedures. The attestors found are members of the **Attestor** application role.

Attestation objects are employees (`Person` table) or request recipients (`PersonWantsOrg` table). These approval procedures determine the role (department, location, business role, cost center) for each attestation object to which the attestation object is primarily assigned. If the primarily assigned role is not directly assigned an attestor, the approval procedure finds the attestator's parents roles. If still no attestor can be determined, the attestation case is presented to the attestor of the associated role class for approval.

NOTE: When attestors are found using the AO approval procedure and when "bottom-up" inheritance is defined for business roles, note the following:

> - If there is no attestor given for the primary business role, attestors are taken from the child business role.

Related topics

-

Using attestation objects to find attestors

Use the AR, AY, or AT approval procedures if you want to attest the validity of compliance rules, rule violations, company policies, policy violations, or of departments, locations, cost centers, or business roles. The AT procedure is also suitable for attesting assignments to IT Shop structures (shops, shopping centers, or shelves). Use the AA or AN approval procedures to attest system entitlement or system role assignments to departments, locations, cost centers, business roles or IT Shop structures. The attestors found are members of the **Attestor** application role.

	Attestation base objects	Available in Module
AR	Rules (`ComplianceRule`) Rule violations (`PersonInNonCompliance`)	Compliance Rules Module
AY	Company policies (`QERPolicy`) Policy violations (`QERPolicyHasObject`)	Company Policies Module
AT	Departments (`Department`) IT Shop Structures (`ITShopOrg`) Locations (`Locality`) Business roles (`Org`) Cost centers (`ProfitCenter`) IT Shop Templates (`ITShopSrc`)	
AA, AN	System entitlement or target system group assignments to roles (`<BaseTree>HasUNSGroupB`, `<BaseTree>HasADSGroup`, `<BaseTree>HasEBSResp`, ...) System role assignments to roles (`<BaseTree>HasESet`)	Target System Base Module

These approval procedures determine the attestors to which the attestation object is assigned. The AA approval procedure finds the attestor using the role (departments, locations, business roles, cost centers) or IT Shop structures (IT Shop templates). The AN approval procedure finds the attestor using the service item assigned to the system entitlement or target system group.

Furthermore, the following also applies to the AT and AA approval procedures: If an attestor is not directly assigned to the attestation object, the approval procedure finds the

attestor of the parent roles/IT Shop structures. If still no attestor can be determined, the attestation case is presented to the attestor of the associated role class for approval.

NOTE: If the attestation base object is a business role or a business role assignment and bottom-up inheritance is defined for the associated role classes, the following applies:

- If there is no attestor assigned to the attestation object, the approval procedure finds attestors from the attestors of subordinate roles.

Related topics

- Default approval procedures on page 71

Determining attestors using the attestation objects' service item

The OT approval procedure is used to determine the attestors of the service item assigned to the attestation object. You can use this approval procedure for the following attestation base objects:

- Service items (`AccProduct`)
- System entitlements (`UNSGroup`)
- User accounts: system entitlement assignments (`UNSAccountInUNSGroup`)
- Account definitions (`TSBAccountDef`) and employee assignments (`PersonHasTSBAccountDef`)
- System roles (ESet) and employee assignments (`PersonHasESet`)
- Subscribable reports (`RPSReport`) and employee assignments (`PersonHasRPSReport`)
- Resources (`QERResource`) and employee assignments (`PersonHasQERResource`)
- Multi-requestable resources (`QERReuse`)
- Multi requestable/unsubscribable resources (`QERReuseUS`)
- Assignment resources (`QERAssign`)

The attestors found are members of the **Attestor** application role. If there is no attestor assigned to the service item, the attestors are taken from the associated service category.

Related topics

- Default approval procedures on page 71

Using attestation object managers to find attestors

If you want to have employees, user accounts, roles, system roles, role memberships, assignments of system roles, or entitlements for employees, roles, or IT Shop structures attested through their managers, use the CM, DM, LM, MO, RM, RR, or RE approval procedures.

Approval procedure	Attestation base objects	Available in Module
CM	Employees (Person)	
	Employees: memberships in application roles (PersonInAERole)	
	Employees: department memberships (PersonInDepartment)	
	Employees: location memberships (PersonInLocality)	
	Employees: cost center memberships (PersonInProfitCenter)	
	Employees: business role memberships (PersonInOrg)	
	Employees: system role assignments (PersonHasESet)	
DM	Employees (Person)	
	Employees: department memberships (PersonInDepartment)	
LM	Employees (Person)	
	Employees: location memberships (PersonInLocality)	
MO	Employees (Person)	Business Roles Module
	Employees: business role memberships (PersonInOrg)	
PM	Employees (Person)	
	Employees: cost center memberships (PersonInProfitCenter)	
RE	System roles (ESet)	System Roles Module
	Employees: system role assignments (PersonHasESet)	
	Departments: system role assignments (DepartmentHasESet)	
	Business roles: system role assignments (OrgHasESet)	
	IT Shop structures: system role assignments (ITShopOrgHasESet)	

Approval procedure	Attestation base objects	Available in Module
	IT Shop templates: system role assignments (`ITShopSrcOrgHasESet`)	
	Cost centers: system role assignments (`ProfitCenterHasESet`)	
	Locations: system role assignments (`LocalityHasESet`)	
RM	Employees: department memberships (`PersonInDepartment`)	
	Employees: IT Shop structure memberships (`PersonInITShopOrg`)	
	Employees: location memberships (`PersonInLocality`)	
	Employees: business role memberships (`PersonInOrg`)	
	Employees: cost center memberships (`PersonInProfitCenter`)	
RR	Departments (`Department`)	
	IT Shop Structures (`ITShopOrg`)	
	Locations (`Locality`)	
	Business roles (`Org`)	
	Cost centers (`ProfitCenter`)	
	IT Shop Templates (`ITShopSrc`)	
	All system entitlement or system role assignments to roles; for example **Roles and organizations: Active Directory group assignments** (`BaseTreeHasADSGroup`) or **Locations: EBS entitlement assignments** (`LocalityHasEBSResp`)	

These approval procedures find the manager associated with every attestation object. In the RE approval procedure, the system role manager is determined as attestor; in the RM and RR approval procedures, the role/IT Shop structure manager is determined. The approval procedures CM, DM, LM, MO, and PM find the department manager and deputy manager of the role in which the attesting employee is a member.

Using persons responsible for attestation objects to find attestors

If you want to attest system entitlements and the user accounts assigned to them, use the ED, EM, EN, EO, or SO approval policies. Use the approval procedures AM, MD, or SO to attest user accounts. Attestation objects are user accounts or system entitlements and the user accounts assigned to them as well as system roles that have system entitlements or system roles assigned to them.

You use the KA approval procedure to attest Active Directory groups and group memberships. This approval procedure is only available if the Active Roles Module is present.

The approval procedures determine the following attestors.

	Attestation base objects	Attestors	Available in Module
AM	User accounts (`UNSAccount`)	Employee's department manager to whom the user account is connected.	Target System Base Module
ED	User accounts: system entitlement assignments (`UNSAccountInUNSGroup`)	Employee's department manager (and deputy manager) to whom the user account is connected. The primary department assigned in this case.	Target System Base Module
EM	User accounts: system entitlement assignments (`UNSAccountInUNSGroup`)	Employee's department manager to whom the user account is connected.	Target System Base Module
EN	User accounts: system entitlement assignments (`UNSAccountInUNSGroup`) System entitlements (`UNSGroup`)	Target system manager of the target system area to which the system entitlement belongs.	Target System Base Module
EO	System roles: assignments (`ESetHasEntitlement`) All user account assignments to system entitlements; for example, **User accounts: system entitlement assignments** (`UNSAccountInUNSGroup`) or **SAP user accounts: assignments to roles** (`SAPUserInSAPRole`) All system entitlement or system role assignments to roles; for example, **Roles and organizations: Active Directory group assignments** (`BaseTreeHasADSGroup`) or **Locations: EBS entitlement assignments** (`LocalityHasEBSResp`)	Product owner of the service item to which the system entitlement or system role is assigned.	Target System Base Module or System Roles Module
MD	User accounts (`UNSAccount`)	Employee's department manager (and deputy	Target System Base

Attestation base objects	Attestors	Available in Module
	manager) to whom the user account is connected. The primary department assigned in this case.	Module
SO	User accounts: system entitlement assignments (`UNSAccountInUNSGroup`) User accounts (`UNSAccount`) System entitlements: assignments to system entitlements (`UNSGroupInUNSGroup`)	Target system manager for the target system to which the system entitlement or user account belongs.	Target System Base Module
KA	Active Directory groups (`ADSGroup`) Active Directory user Accounts: assignments Group (`ADSAccountInADSGroup`) User accounts: system entitlement assignments (`UNSAccountInUNSGroup`) System entitlements (`UNSGroup`)	Product owner and additional owner of the Active Directory Group If the groups were added automatically to the IT Shop, the account managers are identified as product owners. The additional owners of the Active Directory groups are determined only if the **TargetSystem | ADS | ARS_SSM** configuration parameter is enabled. For more information about these functions, see the *One Identity Manager Administration Guide for One Identity Active Roles Integration*.	Active Roles Module

Using a specified role to find attestors

If the attestors for any object are specified in a certain role, use the OR or OM approval procedure. You can allow any objects to be attested by employees from any role using these approval procedures. In the approval step, specify the role by means of which the attestors are to be determined. The approval procedures determine the following attestors.

	Selectable Roles	Attestors
OM	Departments (Department)	Manager and deputy manager of the role specified in the approval step.
	Cost centers (ProfitCenter)	
	Locations (Locality)	
	Business roles (Org)	
OR	Departments (Department)	All secondary members of the role specified in the approval step.
	Cost centers (ProfitCenter)	
	Locations (Locality)	
	Business roles (Org)	
	Application roles (AERole)	

Using product owners to find attestors

Use the approval procedure OA to detemine whether product owners can be attestors. The following objects can be attested with this procedure:

- Service items
- System entitlements
- System entitlement assignments to user accounts or system entitlements
- System role assignments to employees

Prerequisites:

- A service item must be assigned to the system entitlements and system roles.
- An application role for product owners must be assigned to the service item.

All employees who are assigned this application role are determined as attestors.

Using owners of a privileged object to find attestors

Installed modules: Privileged Account Governance Module

Use the OP approval procedure if you want to allow privileged objects in a Privileged Account Management system, for example, PAM assets or PAM directory accounts, to be

attested by their owners. The owners attest the possible user accord to these privileged objects. The owners of the privileged objects must have the **Privileged Account Governance | Asset and account owners** application role or a child application role.

Using additional Active Directory group owners to find attestors

Installed modules: Active Roles Module

If the Active Directory group is attested, the attestor can be determined through additional owners of this Active Directory group. Use the PA approval procedure for this purpose. This finds all employees that are:

- A member in the assigned Active Directory group through their Active Directory user account
- Linked to the assigned Active Directory user account

NOTE: Only use the PA approval procedure if the **TargetSystem | ADS | ARS_SSM** configuration parameter is enabled. The column **Additional owners** is only available in this case.

Using owners of the attestation objects to find attestors

When you assign new owners to devices or system entitlements in the Web Portal, the new owner should agree with this assignment. An attestation with the PO approval procedure is carried out for this purpose.

Using employees assigned to user accounts to find attestors

If you want to allow user accounts to be attested by the employees assigned to them, use the EA approval procedure. This approval procedure can be used if the Target System Base Module is installed.

Determining attested employee as attestor

An employee can attest to the correctness of their own main data to confirm that it has been entered correctly, for example. Use the CS approval procedure to do this. Employees are the base object for attestation. The approval procedure is used by default to assign

managers to employees who do not have a manager assigned to them (**Attestation of initial manager assignment** attestation policy).

Calculated approval

NOTE: Only one approval step can be defined with the CD approval procedure per approval level.

If you want to make attestation dependent on specific conditions, use the CD approval procedure. This procedure does not determine an attestor. One Identity Manager makes the decision depending on the condition that is formulated in the approval step.

You can use the procedure for any attestation base objects. You create a condition in the approval step. If the condition returns a result, the approval step is approved through One Identity Manager. If the condition does not return a result, the approval step is denied by One Identity Manager. If there are no further approval steps, the approval procedure is either finally granted or denied.

To enter a condition for the CD approval procedure

1. Edit the approval step properties.

   For more information, see Editing approval levels on page 62.

2. In the **Condition** input field, enter a valid WHERE clause for database queries. You can enter the SQL query directly or with a wizard.

Example of a simple approval workflow with the CD approval procedure:

External employees should be attestation by their managers. If no manager is assigned, the members of a designated application role must attest the employees.

You can find all external employees, who have managers assigned to them by using the CD approval procedure and the following condition.

```
EXISTS

(SELECT 1 FROM

        (SELECT xobjectkey FROM Person WHERE (IsExternal = 1)

        AND (EXISTS

        (SELECT 1 FROM

                (SELECT UID_Person FROM Person WHERE 1 = 1) as X

        WHERE X.UID_Person = Person.UID_PersonHead) )) as X

WHERE X.xobjectkey = AttestationCase.ObjectKeyBase)
```

If the condition is fulfilled, the external employee's manager can attest the employee. To do this, add an approval step in the positive approval path with the CM approval procedure.

If the condition is not fulfilled, the employee is attested by the member of a designated application role. To do this, add an approval step in the negative approval path with the OR approval procedure and assign the application role.

Approvals to be made externally

Use external approvals (EX approval procedure) if an attestation needs to be approved as soon as a defined event from outside One Identity Manager takes place. You can also use this procedure to allow any number of objects to be attested by employees who do not have access to One Identity Manager.

Specify an event in the approval step that triggers an external approval. The event triggers a process that initiates the external approval for the attestation case and evaluates the result of the approval decision. The approval process waits for the external decision to be passed to One Identity Manager. Define the subsequent approval steps depending on the result of the external approval.

To use an approval procedure

1. In the Designer, define your own processes that:

    - Triggers an external approval.

    - Analyzes the results of the external approval.

    - Grants or denies approval in the subsequent external approval step in One Identity Manager.

2. Defines an event that starts the process for external approval. Enter the result in **Result** in the approval step.

If the external event occurs, the approval step status in One Identity Manager must be changed. Use the `CallMethod` process task with the `MakeDecision` method for this. Pass the following parameters to the process task:

MethodName: Value = "MakeDecision"

ObjectType: Value = "AttestationCase"

Param1: Value = "sa"

Param2: Value = <approval> ("true" = granted; "false" = denied)

Param3: Value = <reason for approval decision>

Param4: Value = <standard reason>

Param5: Value = <number approval steps> (PWODecisionStep.SubLevelNumber)

WhereClause: Value = "UID_AttestationCase ='"& $UID_AttestationCase$ &"'"

 Use these parameters to specify which attestation case is to be approved by external approval (`WhereClause`). `Param1` specifies the attestor. The attestor is always the **sa** system user. `Param2` passes down the approval decision. If the attestation was granted, a value of **True** must be returned. If the attestation was denied, a value of **False** must be returned. Use `Param3` to pass a reason text for the approval decision; use `Param4` to pass a predefined standard reason. If more than one external approval steps have been defined in an approval level, use `Param5` to pass the approval step count. This ensures the approval is aligned with the correct approval step.

Example

All compliance rules should be checked and attested by an external assessor. The attestation object data should be made available as a PDF on an external share. The assessor should save the result of the attestation in a text file on the external share. Use this approval procedure to make external approvals and define:

- A P1 process that saves a PDF report with data about the attestation object data and the attestation procedure on an external share

- An E1 event that starts the P1 process

  In the approval step, enter E1 in the **Event** field, and enter P1 in the process as the trigger for the external decision.

- A P2 process that checks the share for new text files, evaluates the content, and calls the One Identity Manager `CallMethod` process task the method `MakeDecision` method

- An E2 event that starts the P2 process

- A schedule that starts the E2 event on a regular basis

For detailed information about creating processes, see the *One Identity Manager Configuration Guide*. For detailed information about setting up schedules, see the *One Identity Manager Operational Guide*.

Detailed information about this topic

-

Waiting for further approval

NOTE: Only one approval step can be defined with the WC approval procedure per approval level.

If you want to ensure that a specific data state exists in One Identity Manager before an attestation case is finally approved, then use the WC approval procedure. Use a condition to specify which prerequisites have to be fulfilled so that attestation can take place. The condition is evaluated as a function call, which must accept the attestation case UID as a parameter (`AttestationCase.UID_AttestationCase`). You use this UID to reference the attestation object. The function must define three return values as integer values. One of the following actions is carried out depending on the function's return value.

Table 27: Return value for deferred approval

Return value	Action
Return value > 0	The condition is fulfilled. Deferred approval has completed successfully. The next approval step (in case of success) is carried out.
Return	The condition is not yet fulfilled. Approval is rolled back and is retested the

Return value	Action
value = 0	next time DBQueue Processor runs.
Return value < 0	The condition is not fulfilled. Deferred approval has failed. The next approval step (in case of failure) is carried out.

To use an approval procedure

1. Create a database function which tests the condition for the attestation.

2. Create an approval step with the WC approval procedure. Enter the function call in **Condition**.

   Syntax: dbo.<function name>

3. Specify an approval step in the case of success. Use the approval procedure with which One Identity Manager can determine the attestors.

4. Specify an approval step in the case of failure.

Setting up approval procedures

You can create your own approval procedures if the default approval procedures for finding the responsible attestors do not meet your requirements. The condition through which the attestors are determined is formulated as a database query. Several queries may be combined into one condition.

To set up an approval procedure

1. In the Manager, select the **Attestation > Basic configuration data > Approval procedures** category.

2. Select an approval procedure in the result list and run the **Change main data** task.

   - OR -

   Click in the result list.

3. Edit the approval procedure main data.

4. Save the changes.

To edit the condition

1. In the Manager, select the **Attestation > Basic configuration data > Approval procedures** category.

2. Select an approval procedure from the result list.

3. Select **Change queries for approver selection**.

Detailed information about this topic

- General main data of an approval procedure on page 89
- Queries for finding attestors on page 89

General main data of an approval procedure

Enter the following main data of an approval procedure.

Table 28: General main data of an approval procedure

Property	Description
Approval procedure	Descriptor for the approval procedure (maximum two characters).
Description	Approval procedure identifier.
DBQueue Processor task	Approvals can either be made automatically through a DBQueue Processor calculation task or by specified approvers. Assign a custom DBQueue Processor task if the approval procedure should make an automatic approval decision.
	You cannot assign a DBQueue Processor task if a query is entered for determining the attestors.
Max. number approvers	Maximum number of attestors to be determined by the approval procedure. Specify how many employees must really make approval decisions in the approval steps used by this approval procedure.
Sort order	Value for sorting approval procedures in the menu.
	Specify the value **10** to display this approval procedure at the top of the menu when you set up an approval step.

Related topics

- Properties of an approval step on page 63

Queries for finding attestors

The condition through which the attestors are determined is formulated as a database query. Several queries may be combined into one condition. This adds all employees determined by single queries to the group of attestors.

To edit the condition

1. In the Manager, select the **Attestation > Basic configuration data > Approval procedures** category.

2. Select an approval procedure from the result list.

3. Select **Change queries for approver selection**.

To create single queries

1. Click **Add**.

   This inserts a new row in the table.

2. Mark this row. Enter the query properties.

3. Add more queries if required.

4. Save the changes.

To edit a single query

1. Select the query you want to edit in the table. Edit the query's properties.

2. Save the changes.

To remove single queries

1. Select the query you want to remove in the table.

2. Click **Delete**.

3. Save the changes.

Table 29: Query properties

Property	Description
Approver selection	Query identifier that determines the attestors.
Query	Database query for determining the attestors.
	The database query must be formulated as a select statement. The column selected by the database query must return a UID_Person. Every query must return a value for UID_PWORulerOrigin. The query returns one or more employees to whom the attestation case is presented for approval. If the query fails to return a result, the attestation procedure is canceled.
	A query contains exactly one select statement. To combine several select statements, create several queries.
	If a DBQueue Processor task is assigned, you cannot enter a query to determine attestors.

You can, for example, determine predefined attestors with the query (example 1). The attestor can also be found dynamically depending on the attestation case to approve. To do

this, within the database query, using the `@UID_AttestationCase` variable to access the attestation case (example 2).

Example 1

The attestation cases should be approved by a specific attestor.

Query: select UID_Person, null as UID_PWORulerOrigin from Person where
         InternalName='Bloggs, Jan'

Example 2

All active compliance rules should be attested by the respective rule supervisor.

Query: select pia.UID_Person, null as UID_PWORulerOrigin from AttestationCase
         ac

         join ComplianceRule cr on cr.XObjectKey = ac.ObjectKeyBase and
         cr.IsWorkingCopy = '0'

         join PersonInBaseTree pia on pia.UID_Org = cr.UID_OrgResponsible
         and pia.XOrigin > 0

         where ac.UID_AttestationCase = @UID_AttestationCase

Taking delegation into account

To include delegation when determining attestors, use the query to also determine the employees to whom a responsibility has been delegated. If the managers of hierarchical roles are to make the attestation decision, determine the attestors from the `HelperHeadOrg` table. This table groups all hierarchical role managers, their deputy managers, and employees to whom a responsibility has been delegated. If the members of business or application roles are to make the approval decision, determine the approvers from the `PersonInBaseTree` table. This table groups all hierarchical role members and employees to whom a responsibility has been delegated.

Determine the `UID_PWORulerOrigin` in order to notify delegators when the recipient of the delegation has made a decision on an attestation case and thus allow the Web Portal to show if the attestor was originally delegated.

To determine the UID_PWORulerOrigin of the delegation

- Determine the `UID_PersonWantsOrg` of the delegation and copy this value as `UID_PWORulerOrigin` to the query. Use the `dbo.QER_FGIPWORulerOrigin` table function to do this.

    select dbo.QER_FGIPWORulerOrigin(XObjectKey) as UID_PWORulerOrigin

Modified query from example 2:

    select pia.UID_Person, dbo.QER_FGIPWORulerOrigin(pia.XObjectKey) as UID_
    PWORulerOrigin from AttestationCase ac

```
join ComplianceRule cr on cr.XObjectKey = ac.ObjectKeyBase and
cr.IsWorkingCopy = '0'

join PersonInBaseTree pia on pia.UID_Org = cr.UID_OrgResponsible and
pia.XOrigin > 0

where ac.UID_AttestationCase = @UID_AttestationCase
```

Additional tasks for approval procedures

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

Overview of the approval procedure

To obtain an overview of an approval procedure

1. In the Manager, select the **Attestation > Basic configuration data > Approval procedures** category.

2. Select an approval procedure from the result list.

3. Select the **Approval procedure overview** task.

Specifying permitted approval procedures for tables

You can only assign selected approval policies to attestation procedures. The approval policies permitted depend on the approval procedures applied in the approval policies and on the table that forms the attestation base object for an attestation procedure.

You specify which tables are permitted for use with custom approval procedures.

If you want to use custom tables with the default approval procedures AS, CD, EX, OM, OR, or WC then assign these table to the approval procedures.

To specify the tables that permit this approval procedure

1. In the Manager, select the **Attestation > Basic configuration data > Approval procedures** category.

2. Select an approval procedure from the result list.

3. Select the **Assign tables** task.

   In the **Add assignments** pane, assign the tables to which the approval procedure can be assigned.

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

To remove an assignment

- Select the table and double-click ⊘.

4. Save the changes.

You can see which tables allow an approval procedure on the approval procedure overview form.

Related topics

- Assigning approval policies on page 18
- Overview of the approval procedure on page 92

Copying an approval procedure

You can copy default approval procedures in order to customize them.

To copy an approval procedure

1. In the Manager, select the **Attestation > Basic configuration data > Approval procedures** category.

2. Select an approval procedure in the result list. Select the **Change main data** task.

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

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

5. Enter the short name for the copy.

   The short name for an approval procedure consists of a maximum of two characters.

6. Click **OK** to start copying.

   - OR -

   Click **Cancel** to cancel copying.

Deleting approval procedures

To delete an approval procedure

1. Remove all assignments to approval steps.

   a. On the approval procedure overview form, check which approval steps are assigned to the approval procedure.

   b. Switch to the approval workflow and assign another approval procedure to the approval step.

2. In the Manager, select the **Attestation > Basic configuration data > Approval procedures** category.

3. Select an approval procedure from the result list.

4. Click 🗑.

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

Related topics

-

Determining the responsible attestors

The DBQueue Processor calculates which employee is authorized as an approver and in which approval level. Once an attestation is triggered, the attestors are determined for every approval step of the workflow to be processed. Changes to responsibilities may lead to an employee no longer being authorized as an approver for an attestation that is not yet finally approved. In this case, the attestors must be recalculated. The following changes can trigger recalculation of pending attestations:

- Approval policy, workflow, step, or procedure changes.

- An authorized approver loses their responsibility in One Identity Manager, for example, if a change is made to the department manager, attestation policy approver, or target system manager.

- An employee obtains responsibilities in One Identity Manager and therefore is authorized as an approver, for example as the manager of the employee to be attested.

- An employee authorized as an approver is deactivated.

Once an employee's responsibilities have changed in One Identity Manager, a task for recalculating the attestors is queued in the DBQueue. All approval steps of the pending attestation cases are also recalculated by default. Approval steps that have already been approved remain approved, even if their attestor has changed. Recalculating attestors may take a long time depending on the configuration of the system environment and the amount of data to be processed. To optimize this processing time, you can specify the approval steps for which the attestors are to be recalculated.

To configure recalculation of the attestors

- In the Designer, set the **QER | Attestation | ReducedApproverCalculation** configuration parameter and select one of the following options as the value.

Table 30: Options for recalculating attestors

Option	Description
No	All approval steps are recalculated. This behavior also applies if the configuration parameter is not set.

Option	Description
	Advantage: All valid attestors are displayed in the approval process. The rest of the approval sequence is transparent.
	Disadvantage: Recalculating attestors may take a long time.
CurrentLevel	Only the attestors for the approval level that is currently to be edited are recalculated. Once an approval level has been approved, the attestors are determined for the next approval level.
	Advantage: The number of approval levels to calculate is lower. Calculating the attestors may be faster.
	TIP: Use this option if performance problems occur in your environment in connection with the recalculation of attestors.
	Disadvantage: The originally calculated attestors are still displayed in the approval sequence for each subsequent approval step, even though they may no longer have approval authorization. The rest of the approval sequence is not correctly represented.
NoRecalc	No recalculation of attestors. The previous attestors remain authorized to approve the current approval level. Once an approval level has been approved, the attestors are determined for the next approval level.
	Advantage: The number of approval levels to calculate is lower. Calculating the attestors may be faster.
	TIP: Use this option if performance problems occur in your environment in connection with the recalculation of attestors, even though the **CurrentLevel** option is used.
	Disadvantage: The originally calculated attestors are still displayed in the approval sequence for each subsequent approval step, even though they may no longer have approval authorization. The rest of the approval sequence is not correctly represented. Employees that are no longer authorized can approve the current approval level.
	In the worst-case scenario, the only attestors originally calculated here now have no access to One Identity Manager, for example, because they have left the company. The approval level cannot be approved.
	To see approval steps of this type through
	• Define a timeout and timeout behavior when you set up the approval workflows on the approval steps. - OR - • When setting up the attestation, assign members to the chief approval team. These members can access pending attestation cases at any time.

Detailed information about this topic

- Properties of an approval step on page 63
- Chief approval team on page 26

Related topics

- Modifying approval workflows for pending attestation cases on page 116

Setting up multi-factor authentication for attestation

You can set up additional authentication for particularly security critical attestations, which requires every attestor to enter a security code for attesting. Define which attestation policies require this authentication in your attestation policies.

Use One Identity Manager One Identity Starling Two-Factor Authentication for multi-factor authentication. The authentication information required is defined in the subparameters under the **QER | Person | Starling** or the **QER | Person | Defender** configuration parameter. For detailed information about setting up multi-factor authentication, see the *One Identity Manager Authorization and Authentication Guide*.

To be able to use multi-factor authentication

1. Set up multi-factor authentication as described in the *One Identity Manager Authorization and Authentication Guide*.

2. In the Manager, select the attestation policies for which the multi-factor authentication will be used.

3. Enable the **Approval by multi-factor authentication** option.

    Multi-factor authentication cannot be used for default attestation policies.

Once the **Approval by multi-factor authentication** option is set on an attestation policy, a security code is requested in each approval step of the approval process. This means that every employee who is determined to be an attestor for this attestation policy, must have a Starling 2FA token.

IMPORTANT: An attestation cannot be sent by email if multi-factor authentication is configured for the attestation policy. Attestation emails for such attestations produce an error message.

For detailed information about multi-factor authentication, see the *One Identity Manager Web Designer Web Portal User Guide*.

Related topics

- General main data of attestation policies on page 30
- Attestation by mail on page 129

Prevent attestation by employee awaiting attestation

The attestation object can also be determined as the attestor in an attestation case. which means the employees to be attested can attest themselves. To prevent this, set the **QER | Attestation | PersonToAttestNoDecide** configuration parameter.

NOTE:

- Changing the configuration parameter only affects new attestation cases. Attestors are not recalculated for existing attestation cases.

- The configuration parameter setting also applies for fallback approvers; it does not apply to the chief approval team.

- If the **Approval by affected employee** option is set on an approval step, this configuration parameter has no effect.

To prevent employees from attesting themselves

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

This configuration parameter affects all attestation cases in which employees included in the attestation object or in object relations, are attestors at the same time. The following employees are removed from the group of attestors.

- Employees included in `AttestationCase.ObjectKeyBase`

- Employees included in `AttestationCase.UID_ObjectKey1`, `ObjectKey2`, or `ObjectKey3`

- Employees' main identities

- All subidentities of these main identities

If the configuration parameter is not set or if **Approval by affected employee** is enabled for the approval step, these employees can attest themselves.

Related topics

Properties of an approval step on page 63

Attestation by peer group analysis

Using peer group analysis, approval for attestation cases can be granted or denied automatically. For example, a peer group might be all employees in the same department. Peer group analysis assumes that these employees require the same system entitlements. For example, if the majority of employees belonging to a department have a system entitlement, assignment to another employee in the department can be carried out automatically. This helps to accelerate approval processes.

Peer group analysis can be used during attestation of the following memberships:

- Assignment of system entitlements to user account (UNSAccountInUNSGroup table)

- Secondary memberships in business role (PersonInOrg table)

Peer groups contain all employees with the same manager or belonging to the same primary or secondary department as the employee linked to the attestation object (= employee to be attested). Configuration parameters specify which employee belong to the peer group. At least one of the following configuration parameters must be set.

- **QER | Attestation | PeerGroupAnalysis | IncludeManager**: Employees with the same manager as the employee being attested

- **QER | Attestation | PeerGroupAnalysis | IncludePrimaryDepartment**: Employees who belong to the same primary department as the employee being attested

- **QER | Attestation | PeerGroupAnalysis | IncludeSecondaryDepartment**: Employees whose secondary department corresponds to the primary or secondary department of the employee being attested

The number of employees in a peer group that must already own the membership to be attested is set by a threshold in the **QER | Attestation | PeerGroupAnalysis | ApprovalThreshold** configuration parameter. The threshold specifies the ratio of the total number of employees in the peer group to the number of employees in the peer group who already own this membership.

You can also specify that employees are not permitted to own cross-functional memberships, which means, if the membership and the employee being attested belong to different functional areas, the attestation case should be denied approval. To include this check in peer group analysis, set the **QER | Attestation | PeerGroupAnalysis | CheckCrossfunctionalAssignment** configuration parameter.

Whether a membership is cross-functional or not can only be tested if the following conditions are fulfilled.

- The employee being attested and the member of the peer group requested the membership in the IT Shop.

- The employee being attested is assigned a primary department and this department is assigned a function area.

- The service item that the membership is assigned to, is assigned a functional area.

Attestation cases are automatically approved for fully configured peer group analysis, if both:

- The membership being attested is not cross-functional
- The number of employees in the peer group who already own this membership equal or exceeds the given threshold

If this is not the case, attestation cases are automatically denied.

To use this functionality, One Identity Manager provides the `QER_PersonWantsOrg_Peer group analysis` process and the `PeergroupAnalysis` event. The process is run using an approval step with the EX approval procedure.

Configuring peer group analysis for attestations

To configure peer groups

1. In the Designer, set the **QER | ITShop | PeerGroupAnalysis** configuration parameter.

2. Set at least on of the following subparameters:

   - **QER | Attestation | PeerGroupAnalysis | IncludeManager**: Employees with the same manager as those with the employee linked to the attestation object

   - **QER | Attestation | PeerGroupAnalysis | IncludePrimaryDepartment**: Employees who belong to the same primary department as those with the employee linked to the attestation object

   - **QER | Attestation | PeerGroupAnalysis | IncludeSecondaryDepartment**: Employees whose secondary department corresponds to the primary or secondary department of the employee linked to the attestation object

   Thus, you specify which employees belong to the peer group. You can also set two or all of the configuration parameters.

3. To specify a threshold for the peer group, set the **QER | Attestation | PeerGroupAnalysis | ApprovalThreshold** configuration parameter and specify a value between **0** and **1**.

   The default value is **0.9**. That means, at least 90 percent of the peer group members must already have the membership to be attested in order for the attestation case to be approved.

4. (Optional) To check whether the membership to be attested is cross-functional, enable the **QER | Attestation | PeerGroupAnalysis | CheckCrossfunctionalAssignment** configuration parameter.

- Ensure that the following conditions are met:
  - The employee being attested and the member of the peer group requested the membership in the IT Shop.
  - The employee being attested is assigned a primary department and this department is assigned a function area.
  - The service item that the membership is assigned to, is assigned a functional area.

  Only functional areas that are primary assigned service items are taken into account.

  For more information about editing service items, see the *One Identity Manager IT Shop Administration Guide*. For more information about functional areas, see the *One Identity Manager Identity Management Base Module Administration Guide*.

5. In the Manager, create an approval workflow with at least one approval level. For the approval step, enter at least the following data:
   - Single step: **EXWithPeerGroupAnalysis**.
   - Approval procedure: **EX**
   - Event: **PeerGroupAnalysis**

   The event starts the `ATT_AttestationCase_Peer` group analysis process, which runs the `ATT_PeerGroupAnalysis_for_Attestation` script.

   The script runs automatic approval and sets the approval step type to **Grant** or **Deny**.

Detailed information about this topic

- Attestation by peer group analysis on page 98

Related topics

- Approvals to be made externally on page 86

Managing attestation cases

During attestation, you may find it necessary to assign someone else as default attestor responsible for the attestation because, for example, the actual attestor is absent. You may require additional information about an attestation object. One Identity Manager offers different possibilities to intervene in an open attestation case.

Getting more information

An attestor has the option to gather more information about an attestation case. This ability does not, however, replace the granting or denying approval of an attestation case. There is no additional approval step required in the approval workflow to obtain the information.

Attestors can request information from any employee. The attestation case is put on hold while the query is pending. Once the employee requested has supplied the required information and the attestors have made an decision on the approval step, hold status is revoked. Attestors can recall a pending query at any time. The request is taken off hold. The query and answer are logged in the approval sequence and made available to the attestors.

NOTE: Hold status is revoked if the attestor who asked a question is removed as an approver. The queried employee does not have to answer and the attestation process proceeds.

Email notification to the employees involved can be sent using unanswered inquiries.

For detailed information about queries, see the *One Identity Manager Web Designer Web Portal User Guide*

Detailed information about this topic

- Email notification: Notifications with questions on page 127

Appointing other attestors

 Once an approval level in the approval workflow has been reached, the attestors at this level can appoint another employee to handle the approval. To do this, you have the options described below:

- Rerouting approvals

  The attestor appoints another approval level to carry out attestations. To do this, set up a connection to the approval level in the approval workflow to which an approval decision can be rerouted.

- Appointing additional attestors

   The attestor appoints another employee to carry out the attestation. The other attestor must make an approval decision in addition to the known attestors. To do this, enable the **Additional approver possible** option in the approval step.

  The additional attestor can reject the approval and return the attestation case to the original attestor. The original attestor is informed about this by email. The original attestor can appoint another additional attestor.

- Delegate approval

The attestor appoints another employee with the attestation. This employee is added to the current approval step as the attestor. This employee then makes the approval decision instead of the attestor who made the delegation. To do this, enable the **Approval can be delegated** option in the approval step.

The current attestor can reject the approval and return the attestation case to the original attestor. The original attestor can withdraw the delegation and delegate a different employee, for example, if the other attestor is not available.

Email notifications can be sent to the original attestors and the others.

Detailed information about this topic

- Connecting approval levels on page 68
- Editing approval levels on page 62
- Properties of an approval step on page 63

Related topics

- Email notification: Delegating attestations on page 126
- Email notification: Rejecting approvals on page 127
- Email notification: Notifications from additional attestors on page 128
- Email notification: Scheduling attestation requests on page 122

Escalating an attestation case

Approval steps can be automatically escalated once the specified timeout is exceeded. The attestation case is presented again to another approval body. The attestation case can subsequently be processed again in the normal approval workflow.

To configure escalation of an approval step

1. Open the approval workflow in the Workflow Editor.
2. Add an additional approval level with one approval step for escalation.
3. Connect the approval step that is going to be escalated when the time period is exceeded with the new approval step. Use the connection point for escalation to do this.

Figure 3: Example of an approval workflow with escalation
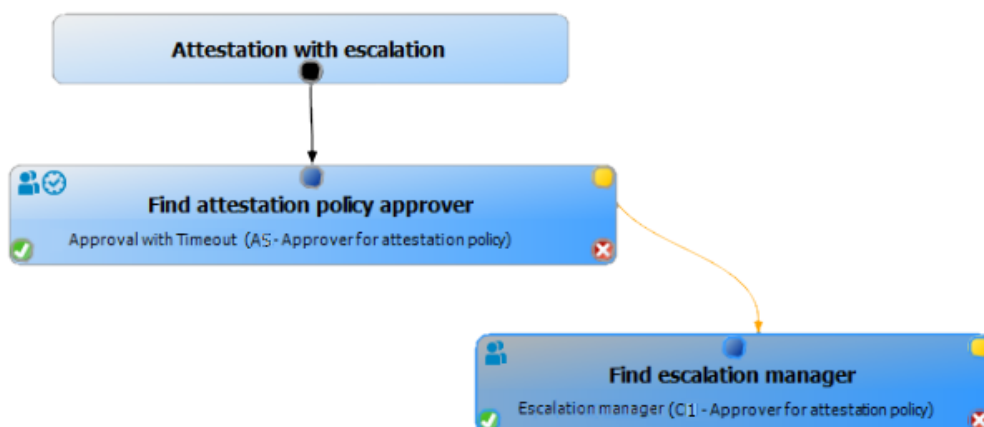
4. Configure the behavior for the approval step to be escalated when it times out.

Table 31: Properties for escalation on timeout

Property	Meaning
Timeout (minutes)	Number of minutes to elapse after which the approval step is automatically granted or denied approval. The input is converted into working hours and displayed additionally.
	The timeout is check every 30 minutes, by default. To change this interval, modify the **Checks reminder interval and timeout of attestation cases** schedule.
	The working hours of the respective approver are taken into account when the time is calculated.
	NOTE: Ensure that a state, county, or both is entered into the employee's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating employees' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*.
	TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM	WorkingHours	IgnoreHoliday** or **QBM	WorkingHours	IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.
	If more than one approver was found, then an approval decision for

Property	Meaning
	the approval step is not automatically made until the timeout for all approvers has been exceeded. The same applies if an additional approver has been assigned.
	If an approver delegated approval, the time point for automatic approval is recalculated for the new approver. If this approval is rejected, the time point for automatic approval is recalculated for the original approver.
	If an approver is queried, the approval decision must be made within the defined timeout anyway. The time point for automatic approval is not recalculated.
	If additional approvers are determined by recalculating the current approvers, then the automatic approval deadline is not extended. The additional approvers must approve within the time frame that applies to the current approver.
Timeout behavior	Action that is run if the timeout expires. • **Escalation**: The attestation case is escalated. The escalation approval level is called.

5. (Optional) If the approval step still needs to be escalated but no attestor be found and no fallback approver is assigned, set the **Escalate if no approver found** option.

   In this case, the attestation case is escalated instead of being canceled or passed to the chief approval team.

In the event of an escalation, email notifications can be sent to the new approvers and other employees.

Related topics

- Email notification: Requesting attestation on page 120
- Email notification: Escalation of attestation cases on page 126

Attestors cannot be established

You can specify a fallback approver if attestation cases cannot be approved because no attestors are available. An attestation case is then always assigned to the fallback approver for attestation if no attestor can be found in an approval step in the specified approval procedure.

To specify fallback approvers, define application roles and assign these to an approval step. Different attestation groups in the approval steps may also require different fallback approvers. Specify different application role for this, to which you can assign employees

who can be determined as fallback approvers in the approval process. For more information, see the *One Identity Manager Authorization and Authentication Guide*.

To specify fallback approvers for an approval step

- Enter the following data for the approval step.

Table 32: Approval step properties for fallback approvers

Property	Meaning
Fallback approver	Application role whose members are authorized to approve attestation cases if an attestor cannot be determined through the approval procedure. Assign an application from the menu.
	To create a new application role, click . Enter the application role name and assign a parent application role. For detailed information, see the *One Identity Manager Authorization and Authentication Guide*.
	NOTE: The number of approvers is not applied to the fallback approvers. The approval step is considered approved the moment as soon as one fallback approver has approved the request.

Attestation sequence with fallback approvers

1. No attestor can be found for an approval step in an approval process. The attestation is assigned to all members of the fallback approver application role.

2. Once a fallback approver has approved an attestation case, it is presented to the attestors at the next approval level.

   NOTE: You can specify in the approval step how many attestors are required for approval in this step. This limit is NOT valid for the chief approval team. The approval step is considered to be approved as soon as ONE fallback approver has approved the attestation.

3. The attestation case is canceled if no fallback approver can be found.

Fallback approvers can make approval decisions on attestation cases for all manual approval steps. Fallback approvals are not permitted for approval steps using the CD, EX, and WC approval procedures.

Related topics

- Editing approval levels on page 62
- Selecting attestors on page 70
- Attesting by chief approval team on page 108
- Escalating an attestation case on page 102

Automatic approval on timeout

Attestation cases can be automatically granted or denied approval once a specified time period has been exceeded.

To configure automatic approval if the timeout expires

- Enter the following data for the approval step.

  - **Timeout (minutes)**:

    Number of minutes to elapse after which the approval step is automatically granted or denied approval. The input is converted into working hours and displayed additionally.

    The timeout is check every 30 minutes, by default. To change this interval, modify the **Checks reminder interval and timeout of attestation cases** schedule.

    The working hours of the respective approver are taken into account when the time is calculated.

    > NOTE: Ensure that a state, county, or both is entered into the employee's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating employees' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*.

    > TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.

    If more than one approver was found, then an approval decision for the approval step is not automatically made until the timeout for all approvers has been exceeded. The same applies if an additional approver has been assigned.

    If an approver delegated approval, the time point for automatic approval is recalculated for the new approver. If this approval is rejected, the time point for automatic approval is recalculated for the original approver.

    If an approver is queried, the approval decision must be made within the defined timeout anyway. The time point for automatic approval is not recalculated.

    If additional approvers are determined by recalculating the current approvers, then the automatic approval deadline is not extended. The additional approvers must approve within the time frame that applies to the current approver.

  - **Timeout behavior**:

    Action, which is run if the timeout expires.

- **Approved**: The attestation case is approved in this approval step. The next approval level is called.
- **Deny**: The attestation case is denied in this approval step. The approval level for denying is called.

When the approval decision for an attestation case is made automatically, other people can be notified by email.

Related topics

- Email notification: Granting or denying attestation cases on page 123
- Editing approval levels on page 62

Halting an attestation case on timeout

Attestation cases can be automatically halted once a specified time period has been exceeded. The action halts when either a single approval step or the entire approval process has exceeded the timeout.

To configure halting after the timeout of a single approval step has been exceeded

- Enter the following data for the approval step.
  - **Timeout (minutes)**:

    Number of minutes to elapse after which the approval step is automatically granted or denied approval. The input is converted into working hours and displayed additionally.

    The timeout is check every 30 minutes, by default. To change this interval, modify the **Checks reminder interval and timeout of attestation cases** schedule.

    The working hours of the respective approver are taken into account when the time is calculated.

    NOTE: Ensure that a state, county, or both is entered into the employee's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating employees' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*.

    TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.

If more than one approver was found, then an approval decision for the approval step is not automatically made until the timeout for all approvers has been exceeded. The same applies if an additional approver has been assigned.

If an approver delegated approval, the time point for automatic approval is recalculated for the new approver. If this approval is rejected, the time point for automatic approval is recalculated for the original approver.

If an approver is queried, the approval decision must be made within the defined timeout anyway. The time point for automatic approval is not recalculated.

If additional approvers are determined by recalculating the current approvers, then the automatic approval deadline is not extended. The additional approvers must approve within the time frame that applies to the current approver.

- **Timeout behavior**:

  Action that runs if the timeout expires.

  - **Cancel**: The approval step and, therefore, the entire attestation procedure, is canceled.

To configure halting on timeout for the entire approval process

- Enter the following data for the approval workflow.

  - **System halt (days)**:

    Number of days to elapse after which the approval workflow, and therefore the system, automatically halts the entire attestation procedure.

When an attestation case is halted, other people can be notified by email.

Related topics

- Email notification: Canceling attestation cases on page 125
- Editing approval levels on page 62
- Setting up approval workflows on page 61

Attesting by chief approval team

Sometimes, approval decisions cannot be made for attestation cases because an attestor is not available or does not have access to One Identity Manager tools. To complete these attestations, you can define a chief approval team whose members are authorized to intervene in the approval process at any time.

The chief approval team is authorized to approve, deny, or cancel attestations in special cases or to appoint other attestors.

IMPORTANT:

- The four-eye principle can be broken like this because chief approval team members can make approval decisions for attestation cases at any time. Specify, on a custom basis, in which special cases the chief approval team may intervene in the approval process.

- The chief approval team is authorized to attest its own members. The configuration parameter setting **QER | Attestation | PersonToAttestNoDecide** does not apply to the chief approval team.

- In the approval step, you can specify how many attestors must make a decision on this approval step.

    - If an approval decision is made by the chief approval team, it overrides the approval decision of just one regular attestor. This means, if three attestors must approve an approval step and the chief approval team one of the decision, two more are still required.

    - The number of approvers if not taken into account when the attestation is assigned to fallback approvers. The chief approval team can also attest in this case. The approval decision is considered to be made as soon as one member of the chief approval team has made an approval decision about the attestation.

- If a regular attestor has added an additional attestor, the chief approval team can approve for both the regular and the additional attestors. If both approvals are pending, a chief approver first replaces the regular attestor's approval only. Only a second approval of the chief approval team can replace the approval of the additional attestor.

The chief approval team can approve attestations for all manual approval steps. The following applies:

- Chief approval team decisions are not permitted for approval steps using the CD, EX, and WC approval procedures.

- If a member of the chief approval team is also named as a regular attestor for an approval step, they can only make an approval decision for this step as a regular attestor.

- The chief approval team can also make an approval decision if a regular attestor has submitted a query and the attestation is in hold status.

To add members to the chief approval team

1. In the Manager, select the **Attestation > Basic configuration data > Chief approval team** category.

2. Select the **Assign employees** task.

    In the **Add assignments** pane, assign the employees who are authorized to approve all attestations.

    TIP: In the **Remove assignments** pane, you can remove the assignment of employees.

To remove an assignment

- Select the employee and double-click ⊘.

3. Save the changes.

Related topics

- Chief approval team on page 26
- Escalating an attestation case on page 102

Attestation sequence

Once attestation is automatically or manually started, One Identity Manager creates an attestation case for each attestation object. Attestation cases record the entire attestation sequence. Each attestation step in the attestation case can be audit-proof reconstructed.

You can view the attestation cases in the navigation view under the **Attestation runs > <attestation policy>** menu item. This is where you can monitor the status of the attestation cases. Attestation cases that were not yet subject to approval are grouped under **Pending attestations**. You can see the attestation cases that have been closed by attestors or One Identity Manager grouped under **Completed attestations**. The status of pending attestation cases is checked regularly by the DBQueue Processor. The **Attestation check** starts the check.

NOTE: Attestation cases are edited in the Web Portal. For detailed information, see *One Identity Manager Web Designer Web Portal User Guide*.

Attestation is complete when the attestation case has been granted or denied approval. You specify how to deal with granted or denied attestations on a company basis.

TIP: One Identity Manager provides various default attestation procedures for different data situations and default attestation procedures. If you use these default attestation procedures, you can configure how you deal with denied attestations.

For more information, see Default attestation and withdrawal of entitlements on .

Starting attestation

There are two ways for you to add attestation cases in the One Identity Manager. You can trigger attestation through a scheduled task or start selected objects individually.

Prerequisite

- The attestation policy for this attestation is set.

To start attestation using a scheduled task

1. In the Manager, select the **Attestation > Attestation policies** category.

2. Select the attestation policy in the result list and run the **Change main data** task.

3. Enable the schedule entered in the **Calculation schedule** field.

   a. In the navigation view, select the **Basic configuration data > Schedules** category.

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

   c. Set the **Enabled** option.

   d. Save the changes.

To start attestation for the selected objects

1. In the Manager, select the **Attestation > Attestation policies** category.

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

3. Select the **Run attestation cases for single objects...** task.

   This opens a separate window.

4. In the **Attestation** column, select every object for which attestation is to be run.

5. Click **Run**.

   Attestation cases are generated for the selected attestation objects. As soon as DBQueue Processor has processed the task, you will see the newly created attestation cases in the navigation view under the **Attestation runs > <attestation policy> > Attestation runs > <year> > <month> > <day> > Pending attestations** menu item.

6. Click **Close**.

NOTE: Under certain circumstances, old, closed attestation cases are deleted from the One Identity Manager database when new attestation cases are added.

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

TIP: If it takes longer than 48 hours to generate new attestation cases, the process is canceled. You can adjust the timeout for generating attestation cases to suit your requirements. To do this, in Designer, change the value of the **QER | Attestation | PrepareAttestationTimeout** configuration parameter.

Detailed information about this topic

Related topics

Additional tasks for attestation cases

Once you have started attestation for an attestation policy, you can monitor the attestation case in One Identity Manager. The task view contains different forms with which you can run the following tasks.

Attestation case overview

The overview form supplies you with the most important information about an attestation case. Here you can see the time by which an attestation case will be processed, depending on the processing time. One Identity Manager does not stipulate which actions are carried out if processing times out. Define your own custom actions or evaluations to deal with this situation.

To obtain an overview of an attestation case

1. In the Manager, select the **Attestation > Attestation runs > <attestation policy> > Attestation runs > <year> > <month> > <day>** category.
2. Select the **Pending attestations** or the **Completed attestations** filter.
3. Select an attestation case from the result list.
4. Select **Attestation case overview**.

Approval sequence

For pending attestation cases, see the current status of the approval process. The approval sequence is shown as soon as the DBQueue Processor has determined the attestors for the first approval step. In the approval workflow, you can view the approval sequence, the results of each approval step, and the attestors found. If the approval procedure could not find an attestor, the attestation case is canceled by the system.

To display the approval sequence of a pending attestation case

1. In the Manager, select the **Attestation > Attestation runs > <attestation policy> > Attestation Runs > <year> > <month> > <day> > Pending attestations** category.
2. Select an attestation case from the result list.
3. Select the **Approval sequence** task.

Each approval level of an approval workflow is represented by a special control. The attestors responsible for a particular approval step are shown in a tooltip. Pending attestation questions are also shown in tooltips. These elements are shown in color, the color code reflecting the current status of the approval level.

Table 33: Meaning of the colors in an approval sequence (in order of decreasing importance)

Color	Meaning
Blue	This approval level is currently being processed.
Green	This approval level has been granted approval.
Red	This approval level has been denied approval.
Yellow	This approval level has been deferred due to a question.
Gray	This approval level has not (yet) been reached.

Attestation history

The attestation history displays each step of an attestation case. Here you can follow all the approvals in the approval process in a chronological sequence. The attestation history is displayed for pending and closed attestations.

To display an attestation case in the attestation history

1. In the Manager, select the **Attestation > Attestation runs > <attestation policy> > Attestation runs > <year> > <month> > <day>** category.
2. Select the **Pending attestations** or the **Completed attestations** filter.
3. Select an attestation case from the result list.
4. Select the **Attestation history** report.

These elements are colored. The color code reflects the status of the approval steps.

Table 34: Meaning of colors in the attestation history

Color	Meaning
Yellow	Attestation case set up.
Green	Attestor has approved.
Red	Attestor has denied.
	Attestation has been escalated.
	Approver has recalled the approval decision
Gray	Attestation has been canceled.

Color	Meaning
	Case has been assigned to an extra attestor.
	Additional attestor has withdrawn approval decision.
	Approval has been delegated.
	New attestor has withdrawn the delegation.
Orange	Attestor has a question.
	The query has been answered.
	Query was canceled due to change of approver.
Blue	Approver has rerouted approval.
	The approval step was reset automatically.

Reports about attestation cases

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The **Attestation cases** report is available for attestors. The report shows all the attestor's pending and closed attestation cases. Attestors can use this report to make approval decisions in the Manager about attestation cases.

To display the Attestation cases report for an employee

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

2. Select the employee in the result list.

3. Select the **Attestation cases** report.

4. If a report has been defined for the attestation case, you can view it using the button in the **View report** column.

5. (Optional) To approve pending attestation cases

    a. Select the **Pending attestation cases** tab.

    b. Select an attestation case and enable the **Approve** or the **Deny** option in the list.

    c. Enter the **Reason for decision** or select a **Standard reason**.

    d. Click **Carry out approval**.

Modifying approval workflows for pending attestation cases

When approval workflows are changed, a decision must be made as to whether these changes should be applied to pending attestation cases. Configuration parameters are used to define the desired procedure.

Scenario: Another approval workflow was stored with the approval policy

The newly stored workflow is only used in new requests. If changes have been made to the approval workflow in an approval policy, any pending approval procedures are continued by default with the original workflow. The newly stored workflow is only used in new attestation cases. You can configure different behavior.

To specify how to handle pending attestation cases

- In the Designer, enable the **QER | Attestation | OnWorkflowAssign** configuration parameter and select one of the following values.

    - **CONTINUE**: Ongoing approval processes are continued with the originally applicable workflow. The newly stored workflow is only used in new attestation cases.

        This behavior also applies if the configuration parameter is not set.

    - **RESET**: In ongoing approval processes, all approval decisions already taken are reset. The approval processes are restarted with the newly stored workflow. The attestation cases are run through the approval process again.

    - **ABORT**: Ongoing approval processes are stopped. All pending attestation cases are closed. The next automatic or manual start of the attestation uses the new approval workflow.

A working copy of the originally applicable workflow is saved. The working copy is retained as long as it is used in ongoing approval processes. All unused working copies are regularly deleted using the **Maintenance approval workflows** schedule.

Scenario: A change was made to an approval workflow in use

If changes have been made to an approval workflow that is being used in pending attestation cases, any pending approval processes are continued by default with the original workflow. The changes to the approval workflow are only implemented for new attestation cases. You can configure different behavior.

To specify how to handle pending attestation cases

- In the Designer, enable the **QER | Attestation | OnWorkflowUpdate** configuration parameter and select one of the following values.

- **CONTINUE**: Ongoing approval processes are continued with the originally applicable approval workflow. The changes to the approval workflow are only implemented for new attestation cases.

  This behavior also applies if the configuration parameter is not set.

- **RESET**: In ongoing approval processes, all approval decisions already taken are reset. The approval processes are restarted with the changed approval workflow. The attestation cases are run through the approval process again.

- **ABORT**: Ongoing approval processes are stopped. All pending attestation cases are closed. The next automatic or manual start of the attestation uses the changed approval workflow.

A working copy of the approval workflow that contains the original version is saved. This working copy is retained as long as it is used in ongoing approval processes. All unused working copies are regularly deleted using the **Maintenance approval workflows** schedule.

Related topics

-

Closing attestation cases for deactivated employees

Pending attestation cases must still be processed even if they have permanently deactivated in the meantime. This is not required very often because the affected employee may have, for example, left the company. In this case, you can use the option to close an employee's pending attestation cases automatically, if the employee is permanently disabled.

To close attestation cases automatically

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

The configuration parameter only applies if the employee to be attested is deactivated after the attestation case was created.

The configuration parameter does not apply if the employee is temporarily deactivated.

TIP: Write a corresponding condition for finding the attestation object on the attestation policies to prevent attestation cases being created for deactivated employees. For more information, see General main data of attestation policies on page 30.

Deleting attestation cases

The `AttestationCase` table expands very quickly when attestation is performed regularly. To limit the number of attestation cases in the One Identity Manager database, you can delete obsolete, closed attestation cases from the database. The attestation case properties are logged and then the attestation cases are deleted. The same number of attestation cases remain in the database as are specified in the attestation policy. For more information about logging data changes tags, see the One Identity Manager Configuration Guide.

> NOTE: Ensure that the logged request procedures are archived for audit reasons. For more information about the archiving process, see the One Identity Manager Data Archiving Administration Guide.

Prerequisites

- The **Common | ProcessState | PropertyLog** configuration parameter is enabled.
- The attestation policy is enabled.

To delete attestation cases automatically

1. Set the `Log changes when deleting` option on at least three columns in the **AttestationCase** table.

    a. In the Designer, select the **Database schema > Tables > AttestationCase** category.

    b. Select the **Show table definition** task.

    This opens the Schema Editor.

    c. Select a column in the Schema Editor.

    d. In the edit view of the schema editor, select the **More** tab.

    e. Set the option **Log changes when deleting**.

    f. Repeat steps (c) to (e) for all columns that are to be recorded on deletion. There must be at least three.

    g. Click on **Commit to database** and save the changes.

    The changes take effect as soon as the DBQueue Processor has performed the calculation tasks.

2. Set the `Log changes when deleting` option on at least three columns in the **AttestationHistory** table.

    a. In the Designer, select the **Database schema > Tables > AttestationHistory** category.

    b. Repeat the steps 1(b) to 1(h) for the `AttestationHistory` table.

3. Enter the number of obsolete cases in the attestation policies.

a. In the Manager, select the **Attestation > Attestation policies** category.

b. Select the attestation policy in the result list whose attestation cases should be deleted.

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

d. In the **Obsolete tasks limit** field, enter a value greater than 0.

e. Save the changes.

TIP: If you want to prevent attestation cases being deleted for certain attestation policies, enter the value **0** for the obsolete task limit for these attestation policies.

Attestation cases are deleted as soon as a new attestation is started for an attestation policy.

One Identity Manager tests how many closed attestation cases exist in the database for each attestation object of this attestation policy. If the number is more than the number of obsolete attestation cases:

- The attestation case properties and their approval sequence are recorded.

  All columns are recorded, which are marked for logging on deletion.

- The attestation cases are deleted.

  The same number of attestation cases remain in the database as are specified in the obsolete tasks limit.

If the **Common | ProcessState | PropertyLog** configuration parameter is disabled later or not enough columns are marked with the **Record on delete** option, the value for **Number of obsolete processes** has no effect.

Notes for disabling attestation policies

- Disabling an attestation policy always deletes all attestation cases.

- The number of obsolete cases is not taken into account.

- The attestation case are also deleted if the **Common | ProcessState | PropertyLog** configuration parameter is disabled. In this case, the deleted attestation cases are not logged.

Related topics

- General main data of attestation policies on page 30
- Suspending attestation on page 54

Notifications in the attestation process

In an attestation process, various email notifications can be sent to attestors and other employees. 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 | Attestation | DefaultSenderAddress** configuration parameter and enter the sender address used to send the email notifications.

3. 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*.

4. 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*.

5. Configure the notification procedure.

Related topics

- Custom mail templates for notifications on page 46

Requesting attestation

When a new attestation case is made, the attestor is notified by mail. Requests for attestation can be configured separately for each approval step.

Prerequisite

- The **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** configuration parameter is not set.

To set up the notification procedure

- On the **Mail templates** tab of the approval step, enter the following data:

  Mail template request: Attestation - approval required

  TIP: To allow approval by email, select the **Attestation - approval required (by email)** mail template.

NOTE: You can schedule requests for attestation to send a general notification if there are attestations pending. This replaces single requests for attestation at each approval step.

Related topics

- Email notification:
-
-

Reminding attestors

If an attestor has not made a decision by the time the reminder timeout expires, notification can be sent by email as a reminder. The attestors working hours are taken into account when the time is calculated.

Prerequisite

- The **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** configuration parameter is not set.

To set up the notification procedure

- Enter the following data for the approval step.

  - **Reminder after (minutes)**:

    Number of minutes to elapse after which the attestor is notified by mail that there are still pending attestation cases for attestation. The input is converted into working hours and displayed additionally.

    The reminder interval is set to 30 minutes, by default. To change this interval, modify the **Checks reminder interval and timeout of attestation cases** schedule.

    NOTE: Ensure that a state, county, or both is entered into the employee's main data of determining the correct working hours. If this information is missing, a fallback is used to calculate the working hours. For more information about calculating employees' working hours, see the *One Identity Manager Identity Management Base Module Administration Guide*.

    TIP: Weekends and public holidays are taken into account when working hours are calculated. If you want weekends and public holidays to be dealt with in the same way as working days, set the **QBM | WorkingHours | IgnoreHoliday** or **QBM | WorkingHours | IgnoreWeekend** configuration parameter. For more information about this, see the *One Identity Manager Configuration Guide*.

    If more than one attestor was found, each attestor will be notified. The same applies if an additional attestor has been assigned.

    If an attestor delegated the approval, the time point for reminding the delegation recipient is recalculated. The delegation recipient and all the other attestors are notified. The original attestor is not notified.

If an attestor has made an inquiry, the time point for reminding the queried employee is recalculated. As long as the inquiry has not been answered, only this employee is notified.

- **Mail template reminder**: Select the **Attestation - remind approver** mail template.

  TIP: To allow approval by email, select the **Attestation - remind approver (by email)** mail template.

NOTE: You can schedule requests for attestation to send a general notification if there are attestations pending. This replaces single requests for attestation at each approval step.

Related topics

- Email notification: Notifications with questions on page 127
- Email notification: Scheduling attestation requests on page 122
- Attestation by mail on page 129
- Editing approval steps on page 63

Scheduling attestation requests

Attestors can be regularly notified of attestation cases that are pending. These regular notifications replace the individual prompts and attestation reminders that are configured in the approval step.

To send regular notifications about pending attestations

1. Enable the **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** configuration parameter in the Designer.

   By default, a notification is sent with the **Attestation - pending requests for approver** mail template.

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

2. In the Designer, configure and enable the **Inform approver about pending attestations** schedule.

   For detailed information, see *One Identity Manager Operational Guide*.

Reminding attestors about attestation objects

The hierarchical role manager and those responsible for system entitlements or system roles can view all pending attestation cases for this object in the Web Portal. If necessary,

they can also send reminders to attestors of selected attestation objects.

To send notification about a specific attestation object

- In the Designer, set the **QER | Attestation | MailTemplateIdents | RemindApproverByObject** configuration parameter.

  By default, notification is sent using the **Attestation - remind approver of all open object attestations** template.

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

Use the Web Portal to send notifications. For detailed information, see *One Identity Manager Web Designer Web Portal User Guide*.

Granting or denying attestation cases

When an attestation case is granted approval or denied it, other employees receive notification. Notification may occur after approval or denial of a single approval step or once the entire approval process is complete. You can specify the recipient of the notification as required by the company.

Attestation cases can be automatically granted or denied approval once a specified time period has been exceeded. Notification is sent in the same way in this case.

To set up the notification procedure

1. Create custom mail templates for sending notification if attestation cases have been granted or denied approval.

2. Create company-specific processes for notifications.

3. If notification should be sent immediately after an approval decision is made for a single approval step, enter the following data on the **Mail templates** tab of the approval step.

   Table 35: Properties of the approval step for notification

Property	Meaning
Mail template approved	Mail template to be used for email notification when an approval step is approved.
Mail template denied	Mail template to be used for email notification when an approval step is denied.

   - OR -

   If notification should be sent after the entire approval procedure is complete, enter the following data in the approval policy.

Table 36: Properties of an approval policy for notifications

Property	Meaning
Mail template approved	Mail template to be used for email notifications when an attestation case is approved.
Mail template denied	Mail template to be used for email notifications when an attestation case is denied.

Detailed information about this topic

Notifying delegates

If required, a delegator can receive notifications if the deputy or recipient of the single delegation has made an approval decision in an attestation case. A notification is sent once an employee has been determined as an attestor due to delegation and has made an approval decision for the attestation case.

To send a notification when the employee who was delegated an approval approves or denies the attestation.

- In the Designer, set the **QER | ITShop | Delegation | MailTemplateIdents | InformDelegatorAboutDecisionAttestation** configuration parameter.

  By default, a notification is sent with the **Delegation - inform delegator about decided attestation** mail template.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Delegations are taken into account in the following default approval procedures.

Table 37: Delegation relevant default approval procedures

Delegation of	Approval procedure
Department responsibilities	DM, ED
Cost center responsibilities	PM
Location responsibilities	LM
Business role responsibilities	MO, OM, RM, RR

Delegation of	Approval procedure
Employee responsibilities	CM, EM
Memberships in business roles	OR
Memberships in application roles	AA, AD, AL, AN, AO, AP, AR, AS, AT, AY, EN, EO, OA, SO

> **Example**
>
> Jon Blogs is responsible for the R1 business role. He delegates his responsibility for the business role to Clara Harris. Clara Harris is herself responsible for R2 business role.
>
> A member of R1 business role is to be attested. Jon Bloggs is established as an attestor through the **OM - Manager of a specific role** approval process. The attestation case is assigned to Clara Harris for approval through delegation. Jon Blogs is notified as soon as Clara Harris has made her approval decision for the attestation case.
>
> A member of R2 business role is to be attested. Clara Harris is established as an attestor through the **OM - Manager of a specific role** approval process. No notification is sent because Clara Harris does not make the approval decision due to delegation.

For more information about delegating responsibilities, see the *One Identity Manager IT Shop Administration Guide*.

Related topics

- Default approval procedures on page 71
- Notifications from additional attestors on page 128

Canceling attestation cases

Email notifications can be sent to other employees when an attestation case is canceled. You can specify the recipient of the notification as required by the company.

To set up the notification procedure

1. Create custom mail templates for sending notification if attestation cases have been canceled.

2. Create company-specific processes for notifications.

3. Enter the following data for the approval policy:

Mail template stopped: Mail template to be used for email notifications when an attestation case is canceled.

Detailed information about this topic

Escalation of attestation cases

Email notifications can be sent to the attestation policy's owner when an attestation case is escalated.

To set up the notification procedure

1. On the **Mail templates** tab of the approval step, enter the following data:

   Mail template escalation: Attestation - Escalation

2. Assign an owner to the attestation policies.

Related topics

Delegating attestations

If, in an approval step, other attestors can be authorized to make the approval decision, the additional attestors can be prompted to approve by email. The same applies if the attestation can be delegated.

To set up the notification procedure

- On the **Mail templates** tab of the approval step, enter the following data:

   Mail template delegation: Attestation - Delegated/additional approval

   > TIP: To enable approval by email, select the **Attestation - delegated/additional approval (by email)** mail template.

Related topics

Rejecting approvals

The original attestor must be notified if an additional attestor or employee to whom an attestation has been delegated refuses the approval decision.

To set up the notification procedure

- On the **Mail templates** tab of the approval step, enter the following data:

  Mail template rejection: Attestation - Reject approval

  TIP: If you allow approval by email, select the mail template **Attestation - reject approval (by mail)**.

Related topics

Notifications with questions

Employees can be notified when a question about an attestation is asked. Similarly, the attestors can also be notified as soon as the question is answered.

To send a notification when an attestor asks a question

- In the Designer, enable the **QER | Attestation | MailTemplateIdents | QueryFromApprover** configuration parameter.

  A notification is sent by default with the **Attestation - question** mail template.

To send a notification to the attestor when the queried employee answers a question

- In the Designer, set the **QER | Attestation | MailTemplateIdents | AnswerToApprover** configuration parameter.

  A notification is sent by default with the **Attestation - answer** mail template.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Notifications from additional attestors

The original attestor can be notified when an additional attestor or an employee who has been delegated an attestation has granted or denied the attestation. This mail is send the moment the approval step has been decided.

To send a notification when the additional attestor approves or rejects the attestation

- In the Designer, set the **QER | Attestation | MailTemplateIdents | InformAddingPerson** configuration parameter.

  A notification is sent by default with the **attestation - approval of added step** mail template.

To send a notification when the employee who was delegated an approval approves or denies the attestation.

- In the Designer, set the **QER | Attestation | MailTemplateIdents | InformDelegatingPerson** configuration parameter.

  A notification is sent by default with the **attestation - approval of delegated step** mail template.

TIP: To use custom mail templates for emails of this type, change the value of the configuration parameter.

Link for verifying new external users

If a new user logs in to the Web Portal or new external employees need to be certified, they receive an email containing a link to the Password Reset Portal. Using the link, employees verify their contact email address, set a password and password questions.

To send notification with a verification link

- In the Designer, set the **QER | Attestation | MailTemplateIdents | NewExternalUserVerification** configuration parameter.

  By default, notification is sent using the **Attestation - new external user verification link** mail template.

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

Detailed information about this topic

Default mail templates

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 **Attestation > Basic configuration data > Mail templates > Predefined** category.

Related topics

- Custom mail templates for notifications on page 46

Attestation by mail

To provide attestors who are temporarily unable to access One Identity Manager tools with the option of making attestation case decisions, you can set up attestation by email. In this process, attestors are notified by email when an attestation case is pending their approval. Approvers can use the links in the email to make approval decisions without having to connect to the Web Portal. This generates an email that contains the approval decision and in which attestors can state the reasons for their approval decision. This email is sent to a central mailbox. One Identity Manager checks this mailbox regularly, evaluates the incoming emails and updates the status of the attestation cases correspondingly.

IMPORTANT: An attestation cannot be sent by email if multi-factor authentication is configured for the attestation policy. Attestation emails for such attestations produce an error message.

Prerequisites

- If you use a Microsoft Exchange mailbox, configure the Microsoft Exchange with:
    - Microsoft Exchange Client Access Server version 2007, Service Pack 1 or higher
    - Microsoft Exchange Web Service .NET API Version 1.2.1, 32-bit
- If you use an Exchange Online mailbox, register an application in your Azure Active Directory tenant in the Microsoft Azure Management Portal. For example, One Identity Manager <Approval by mail>.

    For detailed information about how to register an application, see https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-authenticate-an-ews-application-by-using-oauth#register-your-application.

- The One Identity Manager Service user account used to log into Microsoft Exchange or Exchange Online requires full access to the mailbox given in the **QER | Attestation | MailApproval | Inbox** configuration parameter.

- The **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** configuration parameter is not set.

To set up attestation by email

1. In the Designer, set the **QER | Attestation | MailApproval | Inbox** configuration parameter and enter the mailbox to which the approval mails are to be sent.

2. Set up mailbox access.

   - If you use a Microsoft Exchange mailbox:

     - By default, One Identity Manager uses the One Identity Manager Service user account to log in to the Microsoft Exchange Server and access the mailbox.

       - OR -

     - You enter a separate user account for logging in to theMicrosoft Exchange Server for mailbox access.

       - In the Designer, set the **QER | Attestation | MailApproval | Account** configuration parameter and enter the user account's name.

       - In the Designer, set the **QER | Attestation | MailApproval | Domain** configuration parameter and enter the user account's domain.

       - In the Designer, set the **QER | Attesatation | MailApproval | Password** configuration parameter and enter the user account's password.

   - If you use an Exchange Online mailbox:

     - In the Designer, set the **QER | Attestation | MailApproval | AppId** configuration parameter and enter the application ID that was generated when the application was registered in the Azure Active Directory tenant.

     - In the Designer, set the **QER | Attestation | MailApproval | Domain** configuration parameter and enter the domain for logging into Azure Active Directory.

     - In the Designer, set the **QER | Attestation | MailApproval | Password** configuration parameter and enter the client secret (application password) for the application.

3. In the Designer, set the **QER | Attestation | MailTemplateIdents | ITShopApproval** configuration parameter.

   The mail template used to create the attestation mail is stored with this configuration parameter. You can use the default mail template or add a custom mail template.

   TIP: To use a company-specific mail template for attestation mails, change the value of the configuration parameter.To use a company-specific mail template for

approval decision mails, change the value of the configuration parameter. In this case, also change the `VI_MailApproval_ProcessMail` script.

4. Assign the following mail templates to the approval steps.

Table 38: Mail templates for approval by mail

Property	Mail template
Mail template request	Attestation - approval required (by mail)
Mail template reminder	Attestation - remind approver (by mail)
Mail template delegation	Attestation - delegated/additional approval (by mail)
Mail template rejection	Attestation - reject approval (by mail)

5. In the Designer, configure and enable the **Processes attestation mail approvals** schedule.

   Based on this schedule, One Identity Manager regularly checks the mailbox for new attestation mails. The mailbox is checked every 15 minutes. You can change how frequently it checks, by altering the interval in the schedule as required.

To clean up a mail box

- In the Designer, set the **QER | Attestation | MailApproval | DeleteMode** configuration parameter and select one of the following values.

  - **HardDelete**: The processed email is immediately deleted.
  - **MoveToDeletedItems**: The processed email is moved to the **Deleted objects** mailbox folder.
  - **SoftDelete**: The processed email is moved to the Active Directory recycling bin and can be restored if necessary.

  NOTE: If you use the **MoveToDeletedItems** or **SoftDelete** cleanup method, you should empty the **Deleted objects** folder and the Active Directory recycling bin on a regular basis.

Related topics

- Processing attestation mails on page 132
- Custom mail templates for notifications on page 46
- Requesting attestation on page 120
- Reminding attestors on page 121
- Delegating attestations on page 126
- Rejecting approvals on page 127
- Setting up multi-factor authentication for attestation on page 96
- Adaptive cards attestation on page 132

Processing attestation mails

The **Processes attestation mail approvals** schedule starts the `VI_Attestation_Process Approval Inbox` process. This process runs the `VI_MailApproval_ProcessInBox` script, which searches the mailbox for new attestation mails and updates the attestation cases in the One Identity Manager database. The contents of the attestation mail are processed at the same time.

NOTE: The validity of the email certificate is checked with the `VID_ValidateCertificate` script. You can customize this script to suit your security requirements. Take into account that this script is also used for approval decisions for IT Shop requests by email.

If an self-signed root certification authority is used, the user account under which the One Identity Manager Service is running, must trust the root certificate.

TIP: The `VI_MailApproval_ProcessInBox` script finds the Exchange Web Service URL that uses AutoDiscover through the given mailbox as default. This assumes that the AutoDiscover service is running.

If this is not possible, enter the URL in the **QER | Attestation | MailApproval | ExchangeURI** configuration parameter.

Attestation mails are processed with the `VI_MailApproval_ProcessMail` script. The script finds the relevant approval decision, sets the **Approved** option if approval is granted, and stores the reason for the approval decision with the attestation cases. The attestor is found through the sender address. Then the attestation mail is removed from the mailbox depending on the selected cleanup method.

NOTE: If you use a custom mail template for the attestation mail, check the script and modify it as required. Take into account that this script is also used for approval decisions for IT Shop requests by email.

Adaptive cards attestation

To allow attestors who temporarily do not have access to the One Identity Manager tools to approve attestation cases, you can send adaptive cards. Adaptive cards contain all the information required for attesting the attestation case. These include:

- Current and next attestor
- Attestation history
- Link to the attestation case in the Web Portal
- Option to select a default reason or enter your own reason
- Message stating that the attested entitlement is automatically withdrawn if attestation is denied.
- Message stating whether the attestation object was already attested with the same attestation policy.

One Identity Starling Cloud Assistant uses a specified channel to post the adaptive cards to the attestor, waits for a response, and send this to One Identity Manager. Currently Slack and Microsoft Teams can be used to post adaptive cards. In Starling Cloud Assistant, channels are configured and can be allocated to each recipient separately.

Prerequisites

- The Starling Cloud Assistant service is enabled and the usable channels are configured.

  For more information, see the *One Identity Starling Cloud Assistant User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

  Access to the following endpoints must be ensured to reach a Starling organization in the respective data center.

  - United States of America:

    https://sts.cloud.oneidentity.com (to receive an authentication token)

    https://cloud-assistant-supervisor.cloud.oneidentity.com (to address the Starling Cloud Assistant API)

  - European Union:

    https://sts.cloud.oneidentity.eu (to receive an authentication token)

    https://cloud-assistant-supervisor.cloud.oneidentity.eu (to address the Starling Cloud Assistant API)

- One Identity Manager is connected to One Identity Starling.

  To connect One Identity Manager to One Identity Starling

  1. Start the Launchpad.
  2. Select **Connection to Starling Cloud** and click **Run**.

     This starts the Starling Cloud configuration wizard.
  3. Follow the Starling Cloud configuration wizard's instruction.

  For more information about One Identity Starling, see the *One Identity Starling User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

Related topics

- Using adaptive cards for attestations on page 134
- Default attestation and withdrawal of entitlements on page 140

Using adaptive cards for attestations

Attestators must be registered as recipients in Starling Cloud Assistant to be able to make approval decisions about attestation cases. Each recipient must be allocated to a channel that will be used to post the adaptive card. One Identity Manager provides adaptive cards for requesting attestation in German and English. These can be customized if necessary.

By default, an approval decision must be made within 5 minutes. If this deadline is exceeded, the Web Portal must be used to approve the attestation case. You can configure the deadline.

To use adaptive cards for attestations

1. In the Designer, set the **QER | Person | Starling | UseApprovalAnywhere** configuration parameter.

2. Ensure that a default email address is stored in One Identity Manager for each employee that will use adaptive cards. This address must correspond to the email address that the employee uses to log in to Microsoft Teams or Slack.

   For detailed information about the default email address, see the *One Identity Manager Identity Management Base Module Administration Guide*.

3. Ensure that a language can be identified for each employee that will use adaptive cards. This allows attestors to obtain adaptive cards in their own language.

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

4. In the Designer, disable the **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** configuration parameter.

5. On the **Mail template** tab, assign a **Mail template request** the approval steps.

6. Register all the employees, who are going to use adaptive cards for attesting, as recipients in Starling Cloud Assistant and assign them to the channel to use.

7. Install the Starling Cloud Assistant app that matches the channel.

   Every registered employee must install this app.

   For more information, see the *One Identity Starling Cloud Assistant User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

8. (Optional) Change the timeout for adaptive cards.

   - In the Designer, set the **QER | Person | Starling | UseApprovalAnywhere | SecondsToExpire** configuration parameter and adjust the value. Enter a timeout in seconds.

9. (Optional) Provide a country-specific template for adaptive cards or make adjust the adaptive cards settings.

   If a language cannot be identified or there is no suitable template for the language found, en-US is used as fallback.

Detailed information about this topic

-
-
-
-
-

Adding and deleting recipients and channels

Attestors can be registered in Starling Cloud Assistant as recipients through an IT Shop request and allocated to a channel. By default, the requests are approved immediately by self-service. Then the recipients are registered and the requested channel is assigned to them. Once the attestor has installed the Starling Cloud Assistant app, they can use adaptive cards to attest.

To add a recipient in Starling Cloud Assistant

- In the Web Portal, request the **New Starling Cloud Assistant recipient** product.

To allocate Microsoft Teams as a channel in Starling Cloud Assistant

1. In the Web Portal, request the **Teams channel for Starling Cloud Assistant recipient** product.

2. Install the Starling Cloud Assistant app for Microsoft Teams.

   For more information, see the *One Identity Starling Cloud Assistant User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

To allocate Slack as a channel in Starling Cloud Assistant

1. In the Web Portal, request the **Slack channel for Starling Cloud Assistant recipient** product.

2. Install the Starling Cloud Assistant app for Slack.

   For more information, see the *One Identity Starling Cloud Assistant User Guide* under https://support.oneidentity.com/starling-cloud-assistant/hosted/technical-documents.

To delete a recipient in Starling Cloud Assistant

- Cancel the **New Starling Cloud Assistant recipient** product.

To remove a channel

- Cancel the respective product.

For more information about requesting and unsubscribing products, see the *One Identity Manager Web Portal User Guide*.

Related topics

-
-

Creating, editing, and deleting adaptive cards for attestations

One Identity Manager provides adaptive cards for demanding attestation in German and English. These can be displayed in the Manager. You can create your own templates for adaptive cards, for example to make changes to the content or to provide adaptive cards in other languages. The recipient's language preferences are taken into account when an adaptive card is generated. If a language cannot be identified or there is no suitable template for the language found, en-US is used as fallback.

To use your own adaptive cards for attestations, configure the ATT_AttestationHelper approve anywhere process accordingly.

To display an adaptive card

1. In the Manager, select the **Attestation > Basic configuration data > Adaptive cards** category.
2. Select the adaptive card in the result list.
3. Select the **Change main data** task.
4. In the **Adaptive card templates** menu, select a template.

   This displays the adaptive card's definition in the **Template** field.

   - To display the entire JSON code, click ▣.

To create an adaptive card.

1. In the Manager, select the **Attestation > Basic configuration data > Adaptive cards** category.
2. Click ➕ in the result list.
3. Edit the adaptive card's main data.
4. Create a new template for adaptive cards.
5. Save the changes.
6. Create additional language-specific templates for this adaptive card as required and save the changes.

To use your customized adaptive card

1. In the Designer, edit the ATT_AttestationHelper approve anywhere process.
    a. Select the **Send Adaptive Card to Starling Cloud Assistant** process step.
    b. Edit the value of the **ParameterValue2** parameter and replace the name and UID with the values of your customized adaptive card.
2. Save the changes.

To delete an adaptive card.

1. In the Manager, select the **Attestation > Basic configuration data > Adaptive cards** category.
2. Select the adaptive card in the result list.
3. Click 📄 in the result list.

    This deletes the adaptive card and all the templates belonging to it.

Related topics

- Creating, editing, and deleting adaptive cards templates for attestations on page 137
- Using adaptive cards for attestations on page 134
- Adding and deleting recipients and channels on page 135
- Deploying and evaluating adaptive cards for attestations on page 138

Creating, editing, and deleting adaptive cards templates for attestations

To use your own adaptive cards or to provide adaptive cards in other languages, create your own adaptive card's templates.

To create an adaptive card template

1. In the Manager, select the **Attestation > Basic configuration data > Adaptive cards** category.
2. Select the adaptive card in the result list.
3. Edit the adaptive card's main data.
4. Next to the **Adaptive card templates** menu, click 📄.
5. In the **Language** menu, select a language for the adaptive card.

    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*.

6. In the **Template** field, enter a definition for the adaptive card.

   - To display the entire JSON code, click 🖻.

   You can use the Adaptive Card Designer from Microsoft or the Visual Studio Code Plugin to help.

7. Save the changes.

8. In the Designer, check the `ATT_CloudAssistant_ApprovalAnywhere` script and modify it to suit your requirements.

To edit an adaptive card template

1. In the Manager, select the **Attestation > Basic configuration data > Adaptive cards** category.

2. In the result list, select the adaptive card whose template you want to edit.

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

4. In the **Adaptive card templates** menu, select a template.

5. In the **Template** field, edit the adaptive card definition.

   - To edit the entire JSON code, click 🖻.

6. Save the changes.

To delete an adaptive card template

1. In the Manager, select the **Attestation > Basic configuration data > Adaptive cards** category.

2. In the result list, select the adaptive card whose template you want to delete.

3. Edit the adaptive card's main data.

4. In the **Adaptive card templates** menu, select the template.

5. Click 🗑 next to the menu.

6. Save the changes.

Related topics

Deploying and evaluating adaptive cards for attestations

If an attestor is found in an approval step and this approval step has a mail template allocated to it, the `ATT_AttestationHelper approve anywhere` process is run. The process is generated if the following conditions are fulfilled:

- The attestor is registered as the recipient in Starling Cloud Assistant.

- A default email address is stored for the attestor.

- The **QER | Person | Starling | UseApprovalAnywhere** configuration parameter is set.

- An expiry date is entered in the **QER | Person | Starling | UseApprovalAnywhere | SecondsToExpire** configuration parameter.

- The **QER | Attestation | MailTemplateIdents | RequestApproverByCollection** configuration parameter is not set.

The process calls the `ATT_CloudAssistant_CreateMessage_AttestationHelper` script passing to it the name and UID of the adaptive card to send. The script creates the adaptive card from the JSON template for adaptive cards and the data in the attestation case and then sends it to the attestor. The `QER_CloudAssistant_CheckMessage_AttestationHelper` script checks if the attestor has sent a response, evaluates the response and updates the attestation case according to the approval decision.

HINWEIS: If you want to use your own adaptive cards template, check the `ATT_CloudAssistant_CreateMessage_AttestationHelper`, `ATT_CloudAssistant_CreateData_AttestationHelper`, and `ATT_CloudAssistant_CheckMessage_AttestationHelper` scripts and adjust them if necessary to reflect content changes in the template. For more information about overriding scripts, see the *One Identity Manager Configuration Guide*.

Related topics

- Creating, editing, and deleting adaptive cards templates for attestations   on page 137

- Creating, editing, and deleting adaptive cards for attestations on page 136

- Using adaptive cards for attestations on page 134

Default attestation and withdrawal of entitlements

One Identity Manager provide various default attestation procedures for different data situations and default attestation procedures.

Data situations for default attestations:

- System entitlements owned by an employee
- System entitlements assigned to system entitlements
- System entitlements assigned to hierarchical roles
- System roles assigned to an employee
- Company resources assigned to system roles
- System roles assigned to hierarchical roles
- Business and application role memberships
- Employee main data of a new One Identity Manager user
- Employee main data of an existing One Identity Manager user

The attestation polices required for attesting employee main data are also supplied by default. You can also use the default supplied attestation policies without modifying them. The prerequisites and the attestation sequence for employee data are described in User attestation and recertification.

You can set up attestation policies easily in the Web Portal using default attestation procedures for other data situations. You can also use the default attestation policies supplied without customizing them. Furthermore, you can configure how to deal with denied attestations that are based on these default attestation procedures. If your specific data situation allows, denied entitlements can be removed by One Identity Manager following the attestation.

To remove denied permissions automatically

1. In the Designer, set the **QER | Attestation | AutoRemovalScope** configuration parameter and the configuration subparameters.

2. If the entitlements were obtained through IT Shop, specify whether these requests should be unsubscribed or canceled. To do this, set the **QER | Attestation |**

AutoRemovalScope | PWOMethodName configuration parameter and select a value.

- **Abort**: Requests are canceled. In this case, they do not go through a cancellation workflow. The requested entitlements are withdrawn without additional checks.

- **Unsubscribe**: Requests are unsubscribed. They go through the cancellation workflow defined in the approval policies. Withdrawal of the entitlement can thus be subjected to an additional check.

  If the cancellation is denied, the entitlement is not withdrawn even though the attestation has been denied.

  If the configuration parameter is not set, the requests are canceled.

IMPORTANT: If role memberships or system roles are removed from an employee they lose the unapproved entitlement. They also lose all other company resources inherited through this role. These may be other system entitlements or account definitions. If necessary, system entitlements are removed and company resources are deleted from the employee.

Check whether your data situation allows automatic withdrawal of entitlements before you enable configuration parameters under **QER | Attestation | AutoRemovalScope**.

Automatic removal of entitlements is triggered by an additional approval step with the EX approval procedure in the default approval workflows.

Attestation sequence with subsequence withdrawal of denied entitlements:

1. Attestation is carried out using a default attestation procedure.

2. The attestor denies attestation. The approval step is not granted approval and approval is passed on the next approval level with the EX approval procedure.

3. The approval step triggers the `AUTOREMOVE` event. This runs the `VI_Attestation_ AttestationCase_AutoRemoveMembership` process.

4. The process runs the `VI_AttestationCase_RemoveMembership` script. This removes the affected entitlement depending on which configuration parameters are set.

5. The script sets the approval step status to **Denied**. This means the entire attestation case is finally denied.

6. Tasks to recalculate inheritance are entered in the DBQueue.

Detailed information about this topic

Attesting system entitlements

Installed modules: Target System Base Module

When you use the **System entitlement memberships attestation** default attestation
policy or have set up attestation policies with the **System entitlement memberships
attestation** default attestation procedure, you can configure automatic removal of system
entitlements through the **QER | Attestation | AutoRemovalScope |
GroupMembership** configuration parameter. After attestation approval has been denied,
One Identity Manager checks which type of assignment was used for the user account to
become a member in the system entitlement.

Table 39: Effect of configuration parameters when attestation denied

Configuration parameter	Effect when set
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveDirect	Direct membership of the user account in the system entitlement, is removed.
QER | Attestation | AutoRemovalScope | GroupMembership | RemovePrimaryRole	If membership in the system entitlement was inherited through a primary role, the role is withdrawn from the employee. This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveRequestedRole	If membership of the system entitlement was inherited through a requested role, the role request is canceled or unsubscribed. This removes all indirect assignments obtained by the employee through this role. Set the desired behavior in the **QER | Attestation | AutoRemovalScope | PWOMethodName** configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveDelegatedRole	If membership in the system entitlement was inherited through a delegated role, delegation of this role is canceled or unsubscribed. This removes all indirect assignments obtained by the employee through this role. Set the desired behavior in the **QER | Attestation | AutoRemovalScope | PWOMethodName** configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.

Configuration parameter	Effect when set
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveRequested	If membership of the system entitlement was requested through the IT Shop, the request is canceled or unsubscribed.
	Set the desired behavior in the **QER | Attestation | AutoRemovalScope | PWOMethodName** configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveSystemRole	System roles incorporating the system entitlements are withdrawn from the employee.
	This removes all indirect assignments obtained by the employee through this system role.
	This configuration parameter is only available if the System Roles Module is installed.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveDirectRole	If membership in the system entitlement was inherited through a secondary role (organization or business role), the employee's membership is removed from this role.
	This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveDynamicRole	If membership in the system entitlement was inherited through a dynamic role, the employee is excluded from the dynamic role.
	This removes all indirect assignments obtained by the employee through this role.

When you use the **Attestation of assignments to system entitlements** default attestation policy or have set up attestation policies with the **Attestation of assignments to system entitlements** default attestation procedure, you can configure automatic removal of system entitlements through the **QER | Attestation | AutoRemovalScope | UNSGroupInUNSGroup** configuration parameter.

Table 40: Effect of configuration parameters when attestation denied

Configuration parameter	Effect when set
QER | Attestation | AutoRemovalScope | UNSGroupInUNSGroup | RemoveDirect	Assignment of the system entitlement to a system entitlement is removed.

You can configure automatic withdrawal of system entitlement assignments to hierarchical roles, if you use the following default attestation policies or procedures:

- Attestation of system entitlement assignments to department
- Attestation of system entitlement assignments to cost centers

- Attestation of system entitlement assignments to locations
- Attestation of system entitlement assignments to business roles

Enabled the following configuration parameters to do this.

Table 41: Effect of configuration parameters when attestation denied

Configuration parameter	Effect when set
QER | Attestation | AutoRe-movalScope | Depart-mentHasUNSGroup | RemoveDirect	The assignment of the system entitlement to a department is removed. Therefore the system entitlement is removed from all employees that inherit assignments from this department.
QER | Attestation | AutoRe-movalScope | ProfitCen-terHasUNSGroup | RemoveDirect	The assignment of the system entitlement to a cost center is removed. Therefore the system entitlement is removed from all employees that inherit assignments from this cost center.
QER | Attestation | AutoRe-movalScope | LocalityHasUNSGroup | RemoveDirect	The assignment of the system entitlement to a location is removed. Therefore the system entitlement is removed from all employees that inherit assignments from this location.
QER | Attestation | AutoRe-movalScope | OrgHasUNSGroup | RemoveDirect	The assignment of a system entitlement to a business role is removed. Therefore the system entitlement is removed from all employees that inherit assignments from this business role.

System role attestation

Installed modules: System Roles Module

If you use the **System role membership attestation** default attestation policy or have set up attestation policies with the **System entitlement memberships attestation** default attestation procedure, you can configure automatic removal of system roles through the **QER | Attestation | AutoRemovalScope | ESetAssignment** configuration parameter. After attestation approval has been denied, One Identity Manager checks which type of assignment was used for the user account to become a member in the system role.

Table 42: Effect of configuration parameters when attestation denied

Configuration parameter	Effect when set
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveDirect	Direct membership in the system role is removed. This removes all indirect assignments obtained by the employee through this system role.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemovePrimaryRole	If the system role was inherited through a primary role, the role is withdrawn. This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveRequestedRole	If the system role was inherited through a requested role, the role request is canceled or unsubscribed. This removes all indirect assignments obtained by the employee through this role. Set the desired behavior in the **QER | Attestation | AutoRemovalScope | PWOMethodName** configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveDelegatedRole	If the system role was inherited through a delegated role, the delegation of this role is canceled or unsubscribed. This removes all indirect assignments obtained by the employee through this role. Set the desired behavior in the **QER | Attestation | AutoRemovalScope | PWOMethodName** configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveRequested	If the system role was requested through the IT Shop, the request is canceled or unsubscribed. This removes all indirect assignments obtained by the employee through this system role. Set the desired behavior in the **QER | Attestation | AutoRemovalScope | PWOMethodName** configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveDirectRole	If the system role was inherited through a secondary role (organization or business role), the employee's membership is removed from this role. This removes all indirect assignments obtained by the employee through this role.

Configuration parameter	Effect when set
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveDynamicRole	If the system role was inherited through a dynamic role, the employee is excluded from the dynamic role.
	This removes all indirect assignments obtained by the employee through this role.

If you use the **System role entitlement assignment attestation** default attestation policy or have set up attestation policies with the **System role entitlement assignment attestation** default attestation procedure, you can configure automatic removal of the assignments through the **QER | Attestation | AutoRemovalScope | ESetHasEntitlement** configuration parameter.

Table 43: Effect of configuration parameters when attestation denied

Configuration parameter	Effect when set
QER | Attestation | AutoRemovalScope | ESetHasEntitlement | RemoveDirect	Assignment of the company resource to a system role is removed.

You can configure automatic withdrawal of system role assignments to hierarchical roles, if you use the following default attestation policies or procedures:

- Department system role assignment attestation
- Cost center system role assignment attestation
- Location system role assignment attestation
- Business role system role assignment attestation

Enabled the following configuration parameters to do this.

Table 44: Effect of configuration parameters when attestation denied

Configuration parameter	Effect when set
QER | Attestation | AutoRemovalScope | DepartmentHasESet | RemoveDirect	The assignment of the system role to a department is removed.
	Therefore the system role is removed from all employees that inherit assignments from this department.
QER | Attestation | AutoRemovalScope | ProfitCenterHasESet | RemoveDirect	The assignment of the system role to a cost center is removed.
	Therefore the system role is removed from all employees that inherit assignments from this cost center.
QER | Attestation | AutoRe-	The assignment of the system role to a location is

Configuration parameter	Effect when set
movalScope | LocalityHasESet | RemoveDirect	removed. Therefore the system role is removed from all employees that inherit assignments from this location.
QER | Attestation | AutoRemovalScope | OrgHasESet | RemoveDirect	The assignment of the system role to a business role is removed. Therefore the system role is removed from all employees that inherit assignments from this business role.

Application role attestation

When you use the **Application role membership attestation** default attestation policy or have set up attestation policies with the **Application role membership attestation** default attestation procedure, you can configure automatic removal of application roles through the **QER | Attestation | AutoRemovalScope | AERoleMembership** configuration parameter. After attestation approval has been denied, One Identity Manager checks which type of assignment was used for the user account to become a member in the application role.

Table 45: Effect of configuration parameters when attestation denied

Configuration parameter	Effect when set
QER | Attestation | AutoRemovalScope | AERoleMembership | RemoveDirectRole	The employee's secondary membership is removed from the application role. This removes all indirect assignments obtained by the employee through this application role. Membership in dynamic roles is not removed in this process.
QER | Attestation | AutoRemovalScope | AERoleMembership | RemoveRequestedRole	If the employee requested the application role through the IT Shop, the request is canceled or unsubscribed. This removes all indirect assignments obtained by the employee through this application role. Set the desired behavior in the **QER | Attestation | AutoRemovalScope | PWOMethodName** configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.
QER | Attestation | AutoRemovalScope |	If the application role was delegated to the employee, delegation is canceled or unsubscribed.

Configuration parameter	Effect when set
AERoleMembership | RemoveDelegatedRole	This removes all indirect assignments obtained by the employee through this application role.
	Set the desired behavior in the **QER | Attestation | AutoRemovalScope | PWOMethodName** configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.
QER | Attestation | AutoRemovalScope | AERoleMembership | RemoveDynamicRole	The employee is excluded from the application role's dynamic role.
	This removes all indirect assignments obtained by the employee through this application role. This does not remove memberships in the application role that were created in another way.

Business role attestation

Installed modules: Business Roles Module

When you use the **Business role membership attestation** default attestation policy and have set up attestation policies with the **Business role membership attestation** default attestation procedure, you can configure automatic removal of business roles through the **QER | Attestation | AutoRemovalScope | RoleMembership** configuration parameter. After attestation approval has been denied, One Identity Manager checks which type of assignment was used for the user account to become a member in the business role.

Table 46: Effect of configuration parameters when attestation denied

Configuration parameter	Effect when set
QER | Attestation | AutoRemovalScope | RoleMembership | RemoveDirectRole	The employee's secondary membership in the business role is removed.
	This removes all indirect assignments obtained by the employee through this business role. Membership in dynamic roles is not removed by this.
QER | Attestation | AutoRemovalScope | RoleMembership | RemoveRequestedRole	If the employee requested the business role through the IT Shop, the request is canceled or unsubscribed.
	This removes all indirect assignments obtained by the employee through this business role.
	Set the desired behavior in the **QER | Attestation | AutoRe-**

Configuration parameter	Effect when set
	movalScope | PWOMethodName configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.
QER | Attestation | AutoRemovalScope | RoleMembership | RemoveDelegatedRole	If the business role was delegated to the employee, delegation is canceled or unsubscribed.
	This removes all indirect assignments obtained by the employee through this business role.
	Set the desired behavior in the **QER | Attestation | AutoRemovalScope | PWOMethodName** configuration parameter. For more information, see Default attestation and withdrawal of entitlements on page 140.
QER | Attestation | AutoRemovalScope | RoleMembership | RemoveDynamicRole	The employee is excluded from the business role's dynamic role.
	This removes all indirect assignments obtained by the employee through this business role. This does not remove memberships in the business role that were created in another way.

User attestation and recertification

Use the One Identity Manager attestation functionality to regularly check and authorize employees' main data and target system entitlements and assignments. In addition, One Identity Manager provides default procedures for managers to quickly attest and certify the main data of newly added One Identity Manager users in the One Identity Manager database. This functionality can be used, for example, if external employees, such as contract workers, are provided with temporary access to the One Identity Manager. The sequence is different for internal and external employees.

Regular recertification can be run through scheduled tasks.

In the context of an attestation, a manager can check and update the main data of the user to be certified, if necessary. Use the Web Portal for attestation.

Detailed information about this topic

One Identity Manager users for attesting and recertifying users

The following users are used for attesting and recertifying employees.

Table 47: Users

Users	Tasks
Employee administrators	Employee administrators must be assigned to the **Identity Management | Employees| Administrators** application role.
	Users with this application role:
	- Can edit main data for all employees

Users	Tasks
	• Assign managers to employees.
	• Can assign company resources to employees.
	• Check and authorize employee main data.
	• Create and edit risk index functions.
	• Edit password policies for employee passwords
	• Delete employee's security keys (WebAuthn)
	• Can see everyone's requests, attestations, and delegations and edit delegations in the Web Portal.
Manager	• Check employee main data of the internal user to be certified.
	• Update employee main data as required.
	• Assign another manager if required.
	• Attests the main data.
Attestors for external users	Attestors for external users must be assigned to the **Identity & Access Governance | Attestation | Attestors for external users** application role. Users with this application role: • Attests new, external employees.
Administrators for attestation cases	Administrators must be assigned to the **Identity & Access Governance | Attestation | Administrators** application role. Users with this application role: • Modify the attestation policies if necessary. • Create more schedules if required.
Web Portal users	• Log on to the Web Portal and enter their main data,
Self-registered employees	External employees, who have self-registered in the Web Portal, are assigned to the **Base roles | Self-registered employees** application role through a dynamic role. Users with this application role: • Specify their password and password questions for logging in to One Identity Manager tools.

Configuring user attestation and recertification

To use the attestation and recertification function for new internal users

1. In the Designer, set the **QER | Attestation | UserApproval** configuration parameter.

2. Assign at least one employee to the **Identity Management | Employees | Administrators** application role.

   All employees with this application role can assign a manager to the employee being attested during the attestation process.

To use the attestation and recertification function for new external users

1. In the Designer, set the following configuration parameters:

   - **QER | Attestation | ApproveNewExternalUsers**: Select the value **1**.

   - **QER | WebPortal | PasswordResetURL**: Enter the URL for the Password Reset Portal.

   - **QER | Attestation | MailTemplateIdents | NewExternalUserVerification**: Mail template sending verification links.

   - **QER | Attestation | NewExternalUserTimeoutInHours**: For new external users, specify the duration of the verification link in hours.

     The default is 4 hours. If logging in to the Password Reset Portal fails because the timeout has expired, the user can ask for a new verification link to be sent. To change the duration of the verification link, change the value in the configuration parameter.

   - **QER | Attestation | NewExternalUserFinalTimeoutInHours**: Specify the duration in hours, within which self-registration must be successfully completed.

     If the user does not complete registration with 24 hours, the attestation case quits. To register anyway, the user must log in again to the Web Portal from the beginning. To change the checkout duration of registration, change the value of the configuration parameter.

2. Assign at least one employee to the **Identity & Access Governance | Attestation | Attestor for external users** application role.

Detailed information about this topic

- Self-registration of new users in the Web Portal on page 153
- Adding new employees using a manager or employee administrator on page 155
- Importing new employee main data on page 158

Attesting new users

Attestation of new users is divided into three use cases by One Identity Manager:

1. Registration of new external users logging in to the Web Portal.

2. Adding new employees in the Manager or using a manager in the Web Portal.

3. Adding a new employee by importing employee main data.

The result of attestation is the same in all three cases.

- Certified, activated employees who can access all entitlements assigned to them in One Identity Manager and the connected target systems.

  Company resources are inherited. Account definitions are assigned to internal employees.

  - OR -

- Denied and permanently deactivated employees.

  Disable employees cannot log in to One Identity Manager tools. Company resources are not inherited. Account definitions are not automatically assigned. User accounts associated with the employee are also locked or deleted. You can customize the behavior to meet your requirements.

Self-registration of new users in the Web Portal

Users who are not yet registered have the option to register themselves to use the Web Portal. These users can log in to the Web Portal once a manager has attested the user's main data and the set the user's password. This adds an external employee to the One Identity Manager database.

Attestation sequence:

1. The user logs in to the Web Portal for the first time and enters the required properties.

   A new employee object is added to the One Identity Manager database with properties:

Table 48: Properties of a newly added employee

Property	Value
Certification status	New
External	Set
Contact email address	Email address to send the verification link to.
Permanently deactivated	Set
No inheritance	Set

2. Attestation is started automatically.

   Attestation policy used: **New user certification**

   NOTE: The attestation only starts automatically if the **QER | Attestation | UserApproval** configuration parameter is set. Otherwise the new user remains permanently deactivated until a manager changes the employee main data manually.

3. Attestors are found.

   Effective approval policy: **Certification of users**

4. If the **QER | Attestation | ApproveNewExternalUsers** configuration parameter is set and the value is **1**, attestation of members of the **Identity & Access Governance | Attestation | Attestors for external users** is submitted.

   a. If an attestor for external users denies the attestation, the attestation case is closed. The employee object's properties are updated in the database.

   Table 49: Properties of an external employee with denied attestation

Property	Value	Explanation
Certification status	Denied	
External	Set	
Permanently deactivated	Set	The user cannot log in to the Web Portal.
No inheritance	Set	Company resources are not inherited.

   b. If an attestor for external users approves attestation, an email with a verification link is sent to the new user.

   NOTE: If the **QER | Attestation | ApproveNewExternalUsers** configuration parameter is not set or the value is **0**, an email with a verification link is sent immediately to the new user.

5. Once the user has followed the link and a password and a password question have been set, the attestation case is approved. The employee object's properties are

updated in the database.

Table 50: Properties of an external employee with approved attestation

Property	Value	Explanation
Certification status	Certified	
External	Set	
Permanently deactivated	Not set	The user can log in to the Web Portal.
No inheritance	Not set	Company resources are inherited.

The default is 4 hours. If logging in to the Password Reset Portal fails because the timeout has expired, the user can ask for a new verification link to be sent.

If the user does not complete registration with 24 hours, the attestation case quits. To register anyway, the user must log in again to the Web Portal from the beginning.

Related topics

Adding new employees using a manager or employee administrator

You can also attest new users if new employees are added in the Manager or if a manager in the Web Portal adds a new employees. Specify the required behavior with the configuration parameter **QER | Attestation | UserApproval | InitialApprovalState**. This configuration parameter has the default value **0**. This gives each new employee the certification status **Certified**. Automatic attestation is not carried out.

To automatically attest new users

- In the Designer, enable the **QER | Attestation | UserApproval | InitialApprovalState** configuration parameter and set the value to **1**.

    All employees added to the database from this point on are given the certification status **New**. This means automatic attestation of these employees is carried out.

The sequence is different for internal and external employees.

Attestation sequence:

1. Enter the new user's main data and assign a manager to them.

For detailed information about adding employees, see the *One Identity Manager Identity Management Base Module Administration Guide* and the *One Identity Manager Web Designer Web Portal User Guide*.

The certification status corresponds to the value of the **QER | Attestation | UserApproval | InitialApprovalState** configuration parameter. If the configuration parameter has the value **1**, certification status is set to **New**.

The employee is activated by default. They can therefore log in to One Identity Manager immediately. To ensure that the employee cannot log in to One Identity Manager until their main data has been attested, deactivate the employee.

- To do this, run the **Deactivate person permanently** task.

2. Once the employee main data has been saved, attestation starts.

   Attestation policy used: **New user certification**

3. Attestors are found.

   Effective approval policy: **Certification of users**

4. If the **External** option is set for the employee:

   Attestation takes place as described in the Self-registration of new users in the Web Portal section, steps 4 to 5.

5. If the **External** option is set for the employee:

   a. One Identity Manager checks whether you have assigned a manager to the employee.

      - If you have assigned a manager to the employee, the case is immediately passed on to them for approval.

      - If you have not assigned a manager to the employee, the case is assigned to the employee administrators for approval.

   b. An employee administrator checks your main data and also assigns a manager to you.

      - The employee administrator assigns a manager and approves attestation. The attestation case is assigned to the manager for approval.

      - If the employee administrator does not assign a manager and approves attestation, the attestation case is closed. Your employee properties are updated in the database.

      Table 51: Properties of an employee with approved attestation

Property	Value	Explanation
Certification status	Certified	
External	Not set	
Disabled permanently	Not set	
No inheritance	Not set	Company resources are inherited.

- If an employee administrator denies attestation approval, the attestation case is closed. Your employee properties are updated in the database.

Table 52: Properties of an employee with rejected attestation

Property	Value	Explanation
Ceritifcation status	Rejected	
External	Not set	
Permanently disabled	Set	
No inheritance	Set	Company resources are not inherited. User accounts are not created automatically.

c. The manager can deny attestation approval if he is not the manager in charge of the employee.

- The manager can assign another person as manager. The attestation case is immediately assigned to this manager.
- If the manager does not know who your manager is, approval is returned to the employee administrators. These can
    - Assign another manager
    - Not assign another manager and grant attestation approval
    - Deny attestation approval

d. If the manager approves attestation, the attestation case is closed. Your employee properties are updated in the database.

Table 53: Properties of an employee with approved attestation

Property	Value	Explanation
Certification status	Certified	
External	Not set	
Disabled permanently	Not set	
No inheritance	Not set	Company resources are inherited.

NOTE: Only employee administrators can ultimately deny attestation approval. If a manager denies attestation, the case is returned to the employee administrators for approval in any case.

Related topics

Importing new employee main data

You can request attestation of new employees if the main data is imported from other systems into the One Identity Manager database. To ensure that new employees are automatically attested, you must set the employee's certification status to **New** (`Person.ApprovalState = '1'`). There are two possible ways to do this:

1. The **QER | Attestation | UserApproval | InitialApprovalState** configuration parameter is evaluated for certification status. If the configuration parameter has the value **1**, certification status is set to **New**.

   Prerequisite: The import does not alter the `Person.ApprovalState` property.

   > NOTE: The **QER | Attestation | UserApproval | InitialApprovalState** configuration parameter has the value **0** by default. This gives each new employee the certification status **Certified**. Automatic attestation is not carried out.
   >
   > If you want to attest new employees immediately, change the value of the configuration parameter to **1**.

2. The import sets the `Person.ApprovalState` property explicitly.

   - The import sets `ApprovalState='1'` (**New**).

     The employee is automatically sent to the manager for attestation.

   - The import sets `ApprovalState='0'` (**Certified**).

     Imported employee main data has already been authorized. It should not be attested again.

   - The import sets `ApprovalState='3'` (**Denied**).

     The employee is deactivated permanently and is not attested.

Attestation of new users is triggered when:

- The **QER | Attestation | UserApproval** configuration parameter is set
- New employee main data was imported into the One Identity Manager database
- The certification status for new employees is set to **New**
- No **Import data source** is stored with the employee.

If the **External** option is not set for an employee, attestation takes place as described in the Adding new employees using a manager or employee administrator section, step 5.

If the **External** option is set for the employee, attestation takes place as described in the Self-registration of new users in the Web Portal section, steps 4 to 5.

The **New user certification** attestation policy is run.

Related topics

- Configuring user attestation and recertification on page 152

Scheduled attestation

Users are also attested when the certification status for an employee is set to **New** at a later date (manually or through import). The **Daily** schedule is assigned to the **New user certification** attestation policy for this purpose. Attestation of new users is started when the time set in the schedule is reached. This process determines all employees with the certification status **New** and for whom no attestation cases are pending.

You can assign a custom schedule to the attestation policy if required.

Detailed information about this topic

Limiting attestation objects for certification

IMPORTANT: In order to customize the default **New user certification** attestation policy, you must make changes to One Identity Manager objects. Always use a custom copy of the respective object to make changes.

It may be necessary to limit attestation of new users to a certain group of employees, for example, if only employees in a specific departments should be attested. To do this, you can extend the condition attached to the attestation policy. Create a custom attestation policy for this.

The following objects must be changed so that attestation of new users can be carried out with this attestation policy. Always create a copy of the respective object to do this.

- **New user certification** attestation policy
- VI_Attestation_Person_new_AttestationCase_for_Certification process
- VI_Attestation_AttestationCase_Person_Approval_Granted process
- VI_Attestation_AttestationCase_Person_Approval_Dismissed process

IMPORTANT: In order for attestation to run correctly in the Web Portal, the default **Certification of users** attestation procedure and the default **Certification of users** approval policy must be assigned to the attestation policy.

The default attestation procedure, the default approval policy, and the default **Certification of users** approval workflow must not be changed.

To customize default attestation of new users

1. Copy the **Certification of users** attestation policy and customize it.

   Table 54: Attestation policy properties

Property	Value
Attestation procedure	Certification of users.
Approval policies	Certification of users.
Editing conditions	Copy the default condition without modification so that the correct attestation object is selected.
	To limit the number of attestation objects, you can add additional partial conditions to the database query.

2. In the Designer, create a copy of the `VI_Attestation_Person_new_AttestationCase_for_Certification` process from the `Person` base object and customize the copy.

   Table 55: Process properties with changes

Process step	Parameter	Change
Create attestation instance	WhereClause	Replace the UID of the **New user certification** attestation policy with the UID of the new attestation policy.

3. In the Designer, copy the `VI_Attestation_AttestationCase_Person_Approval_Granted` process of the `AttestationCase` base object and customize the copy.

   Table 56: Process properties with changes

Process property	Change
Pre-script for generating	Replace the UID of the **New user certification** attestation policy with the UID of the new attestation policy.
Generating condition	

4. In the Designer, copy the `VI_Attestation_AttestationCase_Person_Approval_Dismissed` process of the `AttestationCase` base object and customize the copy.

Table 57: Process properties with changes

Process property	Change
Pre-script for generating	Replace the UID of the **New user certification** attestation policy with the UID of the new attestation policy.
Generating condition	

For detailed information about editing processes, see the *One Identity Manager Configuration Guide*.

Detailed information about this topic

- General main data of attestation policies on page 30
- Copy attestation policies on page 39

Recertifying existing users

IMPORTANT: Access to connected target systems may possibly be denied to One Identity Manager users as a result of recertification. You can configure this behavior to meet your company's requirements. Read the following section thoroughly before you use the recertification function.

One Identity Manager provides an attestation policy for performing cyclical attestation of existing users allowing companies to regularly test and authorize employee main data stored in the One Identity Manager database. Cyclical attestation is triggered through a scheduled task. This resets the certification status for all employees stored in the database. One Identity Manager uses the same procedure for this as for attesting new users. The case is referred to as recertification.

Result of recertification

- Certified, activated employees who can access all entitlements assigned to them in One Identity Manager and the connected target systems.

  Company resources are inherited. Account definitions are assigned to internal employees.

  - OR -

- Denied and permanently deactivated employees.

  Disable employees cannot log in to One Identity Manager tools. Company resources are not inherited. Account definitions are not automatically assigned. User accounts associated with the employee are also locked or deleted. You can customize the behavior to meet your requirements.

Preparing for recertification

To set up regular user attestation

1. In the Designer, set the required configuration parameters.

2. Create a schedule and assign it to the **User recertification** attestation policy. By doing this, you replace the schedule assigned by default.

   - Enable the schedule.

Detailed information about this topic

- Configuring user attestation and recertification on page 152

Related topics

- General main data of attestation policies on page 30
- Attestation schedules on page 19

The recertification sequence

One Identity Manager uses the same method for recertification as for certification of new users. User recertification is triggered when all the following are true:

- The **QER | Attestation | UserApproval** configuration parameter is set.
- No **Import data source** is stored with the employee or the **Import data source** is not **E-Business Suite**.
- The processing time in the schedule stored for the **User recertification** attestation policy has been reached.

Internal employees are attested by their manager. If an employee is not assigned a manager, the employee administrator assigns an initial manager for them. Only employee administrators can ultimately deny recertification. If a manager denies recertification, the case is always returned to the employee administrators to decide approval.

External employees are attested by members of the **Identity & Access Governance | Attestation | Attestors for external users** application role.

If the **External** option is not set for an employee, attestation takes place as described in the Adding new employees using a manager or employee administrator section, step 5.

If the **External** option is set for the employee, attestation takes place as described in the Self-registration of new users in the Web Portal section, steps 4 to 5.

The attestors are determined using the **Certification of users** approval policy.

Limiting attestation objects for recertification

IMPORTANT: In order to customize the **User recertification** default attestation policy, you must make changes to One Identity Manager objects. Always use a custom copy of the relevant object to make these changes.

All employees saved in the database are recertified using the **User recertification** attestation policy supplied in One Identity Manager. It may be necessary to limit recertification of new users to a certain group of employees, for example, if only employees in a specific departments should be attested. To do this, you can extend the condition attached to the attestation policy. Create a custom attestation policy for this.

The following objects must be changed so that recertification of users can be carried out with this attestation policy. Always create a copy of the respective object to do this.

- **User recertification** attestation policy
- VI_Attestation_AttestationCase_Person_Approval_Granted process
- VI_Attestation_AttestationCase_Person_Approval_Dismissed process

IMPORTANT: In order for recertification to run correctly in the Web Portal, the default **Certification of users** attestation procedure and the default **Certification of users** approval policy must be assigned to the attestation policy.

The default attestation procedure, the default approval policy, and the default **Certification of users** approval workflow must not be changed.

To customize default recertification of users

1. Copy the **User recertification** attestation policy and customize it.

   Table 58: Attestation policy properties

Property	Value
Attestation procedure	Certification of users.
Approval policies	Certification of users.
Editing conditions	Copy the default condition without modification so that the correct attestation object is selected.
	To limit the number of attestation objects, you can add additional partial conditions to the database query.

2. In the Designer, copy the VI_Attestation_AttestationCase_Person_Approval_ Granted process of the AttestationCase base object and customize the copy.

Table 59: Process properties with changes

Process property	Change
Pre-script for generating	Replace the UID of the **User recertification** attestation policy with the UID of the new attestation policy.
Generating condition	

3. In the Designer, copy the `VI_Attestation_AttestationCase_Person_Approval_` `Dismissed` process of the `AttestationCase` base object and customize the copy.

Table 60: Process properties with changes

Process property	Change
Pre-script for generating	Replace the UID of the **User recertification** attestation policy with the UID of the new attestation policy.
Generating condition	

For detailed information about editing processes, see the *One Identity Manager Configuration Guide*.

Detailed information about this topic

- General main data of attestation policies on page 30
- Copy attestation policies on page 39

Mitigating controls

Violation of regulatory requirements can harbor different risks for companies. To evaluate these risks, you can apply risk indexes to attestation 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 an attestation rule was violated. The attestation can be approved after the next attestation run, once 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*.

General main data of mitigating controls

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 61: 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 attestation policies

Use this task to specify for which attestation policies the mitigating control is valid.

To assign attestation 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 attestation polices** task.

   Assign the attestation policies in **Add assignments**.

   > TIP: In **Remove assignments**, you can remove the assignment of attestation policies.
   >
   > ### *To remove an assignment*
   >
   > - Select the approval 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 an attestation 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**.

Setting up attestation in a separate database

Scheduled attestations are often processes that generate a high load. It is possible to outsource such processes to a separate database and thus relieve the central database. To synchronize both databases, set up system synchronization using the One Identity Manager connector. You can optimize use of One Identity Manager functionality by synchronizing with a central database, containing all the data, on a regular basis.

All data required for attestation are transferred from the central database to a work database. The attestation is set up and carried out in the work database. The results of the attestation are transferred to the central database. Subsequent processes, such as the withdrawing entitlements after attestation is denied or risk index calculations, are carried out in the central database.

Detailed information about this topic

Requirements for the central database

The prerequisites and guidance for connecting a One Identity Manager database apply, as described in the *One Identity Manager User Guide for the One Identity Manager Connector*.

Prerequisites

- The central database has at least version 8.2.
- The System Synchronization Service Module (ISM) is installed in the central database.

- Disable the **ISM | PrimaryDB | AppServer** configuration parameter. The central database connection parameters are configured in the work database.

- Even if the work and central database have the same product version, it is recommended you connect the central database through an application server and enable the required plugins. This is the only way to use the function that automatically revokes entitlements if attestation is denied.

The Attestation Module can be present in the central database, but it does not have to be. Regardless of this, attestation configuration, such as attestation policies or approval workflows, and the attestation cases themselves, are not synchronized with the central database. Only the attestations results are transferred to enable the evaluation and further processing of the results in the central database.

Related topics

Setting up work databases

Ensure that the minimum system requirements for installing the work database are met. For more information, see the *One Identity Manager Installation Guide*.

To set up the work database

1. Install a work database with at least version 8.2.

   - Install the same modules as in the central database, including the System Synchronization Service Module.

   - In addition, install the Attestation Module (ATT).

2. Set up a Job server to handle SQL processes for the work database.

3. To be able to use the Web Portal for attestations

   a. Install an application server

   b. Install an API Server.

   For more information, see the *One Identity Manager Installation Guide*.

4. In the work database, set the following configuration parameters and specify the credentials to connect to the central database's application server.

   Use the same settings that are used when setting up synchronization between the central and working databases.

- **ISM | PrimaryDB | AppServer | AuthenticationString**:

  Authentication data for establishing a connection using the REST API of the central database's application server.

  Syntax: `Module=<authentication module>;<property1>=<value1>;<property2>=<value2>,…`

  All authentication modules provided by the application server being addressed are allowed. For more information about authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

  Recommended values are:
  - `Module=DialogUser;User=<user name>;Password=<password>`
  - `Module=DialogUserAccountBased`
  - `Module=Token`

    For authentication using an OAuth 2.0 access token, additionally specify **ClientId**, `ClientSecret`, and `TokenEndpoint` in the `ConnectionString` configuration parameter. For more information about OAuth 2.0/OpenID Connect authentication, see the *One Identity Manager Authorization and Authentication Guide*.

- **ISM | PrimaryDB | AppServer | ConnectionString**:

  Connection parameters for establishing a connection using the REST API of the central database's application server.

  Syntax: `Url=<application server URL>`

  If **Module=Token** is set in the `AuthenticationString` configuration parameter, the following parameter are required in addition:
  - `ClientId`: Client ID for authentication at the token endpoint.
  - `ClientSecret`: Secret value for authentication at the token endpoint.
  - `TokenEndpoint`: URL of the token endpoint.

  Syntax: `url=<application server URL>[;ClientId=<client ID>;ClientSecret=<secret>;TokenEndpoint=<token endpoint>]`

Related topics

Setting up synchronization between central and work databases

Synchronization between the work and central databases is handled by the One Identity Manager connector. You can set up synchronization through individual configuration, configuring it completely manually. To ensure that all data required for attestation are transferred to the work database and the attestation results are returned, set up the system synchronization. The One Identity Manager supports you with the scripts provided.

System synchronization allows you to map selected application data from the central database to the work database. The synchronization configuration is generated completely automatically based on selected criteria. The synchronization project is set up on the work database.

To set up the system synchronization, proceed as described in the *One Identity Manager User Guide for the One Identity Manager Connector*.

To set up the system synchronization

1. Provide One Identity Manager users with the necessary permissions to set up synchronization.

2. Install and configure a synchronization server and declare the server as a Job server in One Identity Manager.

3. Determine which application data to attest.

   a. In Designer, mark the tables and columns required for this purpose. You can use the scripts provided for this purpose.

      NOTE: The scripts select all tables and columns that contain application data to attest. If only a limited section of this application data requires attesting, you can also mark the required tables and columns manually.

   b. Check the automatically selected tables and columns. You can modify this selection to suit your requirements.

4. Generate a synchronization project with the Synchronization Editor.

   When selecting the database system, use the same settings that are specified in the configuration parameters under **ISM | PrimaryDB | AppServer**.

5. Start the initial synchronization.

To automatically mark the tables and columns

Run the following scripts on the given database using a suitable program for SQL queries. The scripts are located on the installation media in the `ATT\dvd\AddOn\SDK\SystemSyncPreConfig` directory.

1. On the work database, run the `AttestationInAnotherOneIMDB_Part1_ GeneralConfig.sql` script.

   The script makes some general settings.

2. On the central database, run the `AttestationInAnotherOneIMDB_Part1_` `GeneralConfig.sql` script.

3. On the work database, run the `AttestationInAnotherOneIMDB_Part2_` `TableConfig.sql` script.

   The script selects all the necessary tables and sets the values required in the table properties.

4. On the work database, run the `AttestationInAnotherOneIMDB_Part3_` `ColumnConfig.sql` script.

   The script selects all required columns and sets the mapping direction.

5. Check the selected tables and columns as well as the set properties and adjust if necessary.

NOTE:

- If you change the tables or columns to be synchronized after the synchronization project has been generated, the synchronization project will be updated automatically.

- Only the connection credentials for the connected systems may be changed manually in a generated synchronization project.

Related topics

- Setting up attestation in a separate database on page 168
- Requirements for the central database on page 168
- Setting up work databases on page 169
- Setting up and running attestations in the work database on page 172

Setting up and running attestations in the work database

After you have initially loaded all the data into the work database, set up the attestation and then start it. For more information, see Attestation and recertification on page 9.

The status of completed attestation cases is stored in the attestation overview (`ISMObjectAttLast` table) and immediately provisioned to the central database. This is where subsequent processes are carried out, such as the withdrawal of entitlements after attestation is denied or risk index calculations.

NOTE: When attestations are carried out in a work database, the risk indexes of the attested objects in the central database are calculated based on the attestation overview (`ISMObjectAttLast` table). Separate calculation functions are provided for this purpose.

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

Related topics

Configuration parameters for attestation

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

Table 62: Overview of configuration parameters

Configuration parameter	Description
QER | Attestation	Preprocessor relevant configuration parameter for controlling the model parts for attestation. Changes to the parameter require recompiling the database.
	If the parameter is enabled you can use the attestation function.
	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 | Attestation | AllowAllReportTypes	This configuration parameter specifies whether all report formats are permitted for attestation policies. By default, only PDF is allowed because it is the only audit secure format.
QER | Attestation | ApproveNewExternalUsers	This configuration parameter specifies whether new external users must be attested before the are enabled.
QER | Attestation | AutoCloseInactivePerson	If this configuration parameter is set, pending attestation cases for an employee are closed, when this employees is permanently deactivated.

Configuration parameter	Description
QER | Attestation | AutoRemovalScope	General configuration parameter for defining automatic withdrawal of memberships/assignments if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | AERoleMembership	Determines default behavior for automatic removal of application role memberships if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | AERoleMembership | RemoveDelegatedRole	If this configuration parameter is set, it ends the application role delegation if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | AERoleMembership | RemoveDirectRole	If this configuration parameter is set, the employee's membership of the application role is removed if attestation approval is not granted. This removes all indirect assignments obtained by the employee through this application role!
QER | Attestation | AutoRemovalScope | AERoleMembership | RemoveRequestedRole	If this configuration parameter is set, the request for membership of the application role is canceled if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | AERoleMembership | RemoveDynamicRole	If this configuration parameter is set, the employee is excluded from the application role's dynamic role if attestation approval is not granted. This removes all indirect assignments obtained by the employee through this application role!
QER | Attestation | AutoRemovalScope | DepartmentHasESet	Determines default behavior for automatic removal of system role assignments to departments if attestation approval has been denied.
QER | Attestation | AutoRemovalScope | DepartmentHasESet | RemoveDirect	If this configuration parameter is set, system role to department assignments are removed if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | DepartmentHasUNSGroup	Determines default behavior for automatic removal of system entitlement assignments to departments if attestation approval has been denied.
QER | Attestation | AutoRemovalScope | DepartmentHasUNSGroup | RemoveDirect	If this configuration parameter is set, system entitlement to department assignments are removed if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | ESetAssignment	Determines default behavior for automatic removal of system role memberships if attestation approval is not granted.

Configuration parameter	Description
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveDelegatedRole	If this configuration parameter is set, it ends the role delegation through which the employee obtained the system role if attestation approval is not granted.
	This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveDirect	If this configuration parameter is set, the direct user account membership in the system role will be removed if attestation approval is not granted.
	This removes all indirect assignments obtained by the employee through the system role.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveDirectRole	If this configuration parameter is set, the secondary membership of the employee in the role (organization or business role) through which the employee obtained the system role is removed if attestation approval is not granted.
	This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveDynamicRole	If this configuration parameter is set, the employee is excluded from the dynamic role through which the employee obtained the system role if attestation approval is not granted.
	This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemovePrimaryRole	If this configuration parameter is set, the primary role assignment through which the employee obtained the system role is removed from the employee if attestation approval is not granted.
	This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveRequested	If this configuration parameter is set, the requested system role is canceled if attestation approval is not granted.
	This removes all indirect assignments obtained by the employee through the system role.
QER | Attestation | AutoRemovalScope | ESetAssignment | RemoveRequestedRole	If this configuration parameter is set, the request for the role through which the employee obtained the system role is canceled if attestation approval is not granted.

Configuration parameter	Description
	This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | ESetHasEntitlement	Determines default behavior for automatic removal of system role assignments after attestation approval has been denied.
QER | Attestation | AutoRemovalScope | ESetHasEntitlement | RemoveDirect	If this configuration parameter is set, company resource assignments to system roles are removed if attestation approval is denied.
QER | Attestation | AutoRemovalScope | GroupMembership	Determines default behavior for automatic removal of united namespace system entitlements if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveDelegatedRole	If this configuration parameter is set, it ends the role delegation through which the employee obtained the system entitlement if attestation approval is not granted. This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveDirect	If this configuration parameter is set, the direct user account membership in the system entitlement will be removed if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveDirectRole	If this configuration parameter is set, secondary membership of the employee in the role (organization or business role) through which the employee obtained the system entitlement is removed if attestation approval is not granted. This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveDynamicRole	If this configuration parameter is set, the employee is excluded from the dynamic role through which the employee obtained the system entitlement if attestation approval is not granted. This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | GroupMembership | RemovePrimaryRole	If this configuration parameter is set, the primary role assignment through which the employee obtained the system entitlement is removed from the employee if attestation approval is not granted. This removes all indirect assignments obtained by

Configuration parameter	Description
	the employee through this role.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveRequested	If this configuration parameter is set, the requested system entitlement is canceled if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveRequestedRole	If this configuration parameter is set, the request for the role through which the employee obtained the system entitlement is canceled if attestation approval is not granted.
	This removes all indirect assignments obtained by the employee through this role.
QER | Attestation | AutoRemovalScope | GroupMembership | RemoveSystemRole	If this configuration parameter is set, the system role assignment through which the employee obtained the system entitlement is removed from the employee if attestation approval is not granted.
	This removes all indirect assignments obtained by the employee through this system role.
	NOTE: This configuration parameter is only available if the System Roles Module is installed.
QER | Attestation | AutoRemovalScope | LocalityHasESet	Determines default behavior for automatic removal of system role assignments to locations if attestation approval has been denied.
QER | Attestation | AutoRemovalScope | LocalityHasESet | RemoveDirect	If this configuration parameter is set, system role to location assignments are removed if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | LocalityHasUNSGroup	Determines default behavior for automatic removal of system entitlement assignments to locations if attestation approval has been denied.
QER | Attestation | AutoRemovalScope | LocalityHasUNSGroup | RemoveDirect	If this configuration parameter is set, system entitlement to location assignments are removed if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | OrgHasESet	Determines default behavior for automatic removal of system role assignments to business roles if attestation approval has been denied.
QER | Attestation | AutoRemovalScope | OrgHasESet | RemoveDirect	If this configuration parameter is set, system role to business role assignments are removed if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | OrgHasUNSGroup	Determines default behavior for automatic removal of system entitlement assignments to business

Configuration parameter	Description
	roles if attestation approval has been denied.
QER | Attestation | AutoRe-movalScope | OrgHasUNSGroup | RemoveDirect	If this configuration parameter is set, system entitlement to business role assignments are removed if attestation approval is not granted.
QER | Attestation | AutoRe-movalScope | ProfitCenterHasESet	Determines default behavior for automatic removal of system role assignments to system roles if attestation approval has been denied.
QER | Attestation | AutoRe-movalScope | ProfitCenterHasESet | RemoveDirect	If this configuration parameter is set, system role to cost center assignments are removed if attestation approval is not granted.
QER | Attestation | AutoRe-movalScope | ProfitCen-terHasUNSGroup	Determines default behavior for automatic removal of system entitlement assignments to system roles if attestation approval has been denied.
QER | Attestation | AutoRe-movalScope | ProfitCen-terHasUNSGroup | RemoveDirect	If this configuration parameter is set, system entitlement to cost center assignments are removed if attestation approval is not granted.
QER | Attestation | AutoRe-movalScope | PWOMethodName	Method to be run on requests if the requested assignment is to be deleted if attestation approval is not granted. The requests can be unsubscribed (**Unsubscribe**) or canceled (**Abort**). If the configuration parameter is not set, the requests are canceled by default.
QER | Attestation | AutoRemovalScope | RoleMembership	Determines default behavior for automatic removal of business role memberships if attestation approval is not granted.
QER | Attestation | AutoRemovalScope | RoleMembership | RemoveDelegatedRole	If this configuration parameter is set, it ends the business role delegation if attestation approval is not granted. This removes all indirect assignments the employee obtained through this business role.
QER | Attestation | AutoRemovalScope | RoleMembership | RemoveDirectRole	If this configuration parameter is set, the employee secondary membership in the business role will be removed if attestation approval is not granted. This removes all indirect assignments the employee obtained through this business role.
QER | Attestation | AutoRemovalScope | RoleMembership | RemoveDynamicRole	If this configuration parameter is set, the employee is excluded from the business role's dynamic role if attestation approval is not granted.

Configuration parameter	Description
	This removes all indirect assignments the employee obtained through this business role.
QER | Attestation | AutoRemovalScope | RoleMembership | RemoveRequestedRole	If this configuration parameter is set, the request for membership of the business role is canceled if attestation approval is not granted. This removes all indirect assignments the employee obtained through this business role.
QER | Attestation | AutoRemovalScope | UNSGroupInUNSGroup	Specifies the default behavior for removing assignments from system entitlements to system entitlement is attestation approval is not granted.
QER | Attestation | AutoRemovalScope | UNSGroupInUNSGroup | RemoveDirect	If this configuration parameter is set, the system entitlement assignment to a system entitlement is removed if attestation approval is not granted.

QER | Attestation | DefaultSenderAddress	Sender's default email address for sending automatically generated notifications about attestation cases. Replace the default address with a valid email address.
	
	Syntax:
	
	`sender@example.com`
	
	Example:
	
	`NoReply@company.com`
	
	You can enter the sender's display name in addition to the email address. In this case, ensure that the email address is enclosed in chevrons (**<>**).
	
	Example:
	
	`One Identity <NoReply@company.com>`

QER | Attestation | MailApproval | Account	Name of the user account for authenticating the mailbox used for approval by mail.
QER | Attestation | MailApproval | AppID	Exchange Online application ID for authentication with OAuth 2.0. If the value is not set, the **Basic** or the **NTML** authentication method is used.
QER | Attestation | MailApproval | DeleteMode	Specifies the way emails are deleted from the inbox.
QER | Attestation | MailApproval | Domain	Domain of the user account for authenticating the mailbox used for approval by mail.
QER | Attestation | MailApproval |	URL of the Microsoft Exchange web service for

Configuration parameter	Description
ExchangeURI	accessing the mailbox. If this is not given, `AutoDiscover` mode is used to detect the URL.
QER | Attestation | MailApproval | Inbox	Microsoft Exchange mailbox to which approvals by mail are sent.
QER | Attestation | MailApproval | Password	Password of the user account for authenticating the mailbox used for approval by mail.
QER | Attestation | MailTemplateIdents | AnswerToApprover	This mail template is used to send a notification with an answer to a question from an approver.
QER | Attestation | MailTemplateIdents | AttestationApproval	Mail template used for attestation by mail.
QER | Attestation | MailTemplateIdents | InformAddingPerson	This mail template is used to notify approvers that an approval decision has been made for the step they added.
QER | Attestation | MailTemplateIdents | InformDelegatingPerson	This mail template is used to notify approvers that an approval decision has been made for the step they delegated.
QER | Attestation | MailTemplateIdents | NewExternalUserVerification	Mail template for sending a message with a verification link to a new external user.
QER | Attestation | MailTemplateIdents | QueryFromApprover	This mail template is used to send a notification with a question from an approver to an employee.
QER | Attestation | MailTemplateIdents | RequestApproverByCollection	This mail template is used for generating an email when there are pending attestation for an approver. If this configuration parameter is not set, a **Mail template request** or **Mail template reminder** can be entered for single approval steps. This template is then sent for each individual attestation case. If this configuration parameter is set, single mails are not sent.
QER | Attestation | NewExternalUserFinalTimeoutInHours	Number of hours given for new external users to register (default: 24 hrs).
QER | Attestation | NewExternalUserTimeoutInHours	Number of hours that the passcode and verification link for new external users are valid (default: 4 hrs).
QER | Attestation | OnWorkflowAssign	This configuration parameter specifies how pending attestation cases are handled when a new approval

Configuration parameter	Description
	workflow is assigned to the approval policy.
QER | Attestation | OnWorkflowUpdate	This configuration parameter specifies how pending attestations are handled when the approval workflow is changed.
QER | Attestation | PeerGroupAnalysis	This configuration parameter allows automatic approval of attestation cases by peer group analysis.
QER | Attestation | PeerGroupAnalysis | ApprovalThreshold	This configuration parameter defines a threshold for peer group analysis between 0 and 1. The default value is 0.9.
QER | Attestation | PeerGroupAnalysis | Check-CrossfunctionalAssignment	This configuration parameter specifies whether functional areas should be take into account in peer group analysis. If the parameter is set, the attestation case is only approved if the employee linked to the attestation case and the attestation object belong to the same functional area.
QER | Attestation | PeerGroupAnalysis | IncludeManager	This configuration parameter specifies whether employees can be added to the peer group who have the same manager as the employee linked to the attestation case.
QER | Attestation | PeerGroupAnalysis | IncludePrimaryDepartment	This configuration parameter specifies whether employees can be added to the peer group who are primary members of the primary department of the employee linked to the attestation object.
QER | Attestation | PeerGroupAnalysis | IncludeSecondaryDepartment	This configuration parameter specifies whether employees can be added to the peer group who are secondary members of the secondary department of the employee linked to the attestation object.
QER | Attestation | PersonToAttestNoDecide	This configuration parameter specifies whether employees to be attested are allowed to approve this attestation case. If the parameter is set, an attestation case cannot be approved by employees, which are contained in the attestation object (`AttestationCase.ObjectKeyBase`) or in the objects identifiers 1-3 (`AttestationCase.UID_ObjectKey1`, `ObjectKey2` or `ObjectKey3`). If the parameter is not set, these employee are allowed to make approval decisions for this attestation case.
QER | Attestation | PrepareAttestationTimeout	Number in hours given to generate new attestation cases (default: 48). If exceeded, the process is

Configuration parameter	Description
	canceled.
QER	Attestation	ReducedApproverCalculation	This configuration parameter specifies, which approval steps are recalculated if modifications require attestors to be redetermined.
QER	Attestation	UserApproval	Supports attestation procedures for regularly checking and confirming One Identity Manager users through their Manager.
QER	Attestation	UserApproval	InitialApprovalState	Certification status for new employees. If an employee is added with the certification status 1 = new, data attestation by the employee's manager is started.
QER	Attestation	UseWork-ingHoursDefinition	Specifies whether working days should be taken into account when calculating the due date of attestation processes according to the definition in the **QBM	WorkingHours** configuration parameter.
QER	CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database.
	If the parameter is enabled, values for the risk index can be entered and calculated.
	If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant config-uration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
QER	Employee	Defender	This configuration parameter specifies whether Starling Two-Factor Authentication is supported.
QER	Employee	Defender	ApiEndpoint	This configuration parameter contains the URL of the Starling 2FA API end point used to register new users.
QER	Employee	Defender	ApiKey	This configuration parameter contains your company's subscription key for accessing the Starling Two-Factor Authentication interface.
QER	Person	Defender	DisableForceParameter	This configuration parameter specifies whether Starling 2FA is forced to send the OTP by SMS or

Configuration parameter	Description
	phone call if one of these options is selected for multi-factor authentication. If the configuration parameter is set, Starling 2FA can disallow the request and the user must request the OPT through Starling 2FA.
QER | WebPortal | BaseURL	Web Portal URL This address is used in mail templates to add hyperlinks to the Web Portal.
QER | WebPortal | PasswordResetURL	URL for the Password Reset Portal. This address is used to navigate.
Common | MailNotification | DefaultCulture	This configuration parameter contains the default language for email notifications if no language can be determined for the recipient.
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.
Common | MailNotification | SMTPAccount	User account name for authentication on an SMTP server.
Common | MailNotification | SMTPDomain	User account domain for authentication on the SMTP server.
Common | MailNotification | SMTPPassword	User account password for authentication on the SMTP server.
Common | MailNotification | SMTPPort	Port for SMTP services on the SMTP server (default: 25).
Common | MailNotification | SMTPRelay	SMTP server for sending notifications.
Common | MailNotification | SMTPUseDefaultCredentials	If this configuration parameter is set, the One Identity Manager Service credentials are used for authentication on the SMTP server. If this configuration parameter is not set, the login data stored in the configuration parameters **Common |**

Configuration parameter	Description
	MailNotification | SMTPDomain and **Common | MailNotification | SMTPAccount** or **Common | MailNotification | SMTPPassword** is used.
Common | ProcessState | PropertyLog	When this configuration parameter is set, changes to individual values are logged and shown in the process view. Changes to the parameter require recompiling 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*.
QBM | WorkingHours | IgnoreHoliday	The configuration parameter specifies whether holidays are taken into account when calculating working hours. If the configuration parameter is set, holidays are not taken into account.
QBM | WorkingHours | IgnoreWeekend	The configuration parameter specifies whether weekends are included in the calculation of working hours. If the configuration parameter is set, holidays are not taken into account.
ISM	General configuration parameter for the system synchronization service module.
ISM | PrimaryDB	Information about the central database located within the corporate infrastructure.
ISM | PrimaryDB | AppServer	Connection parameter for the central database's application server.
ISM | PrimaryDB | AppServer | AuthenticationString	Authentication data for establishing a connection using the REST API of the central database's application server.
	Syntax: `Module=<authentication module>;<property1>=<value1>;<property2>=<value2>,…`
	All authentication modules provided by the application server being addressed are allowed. For more information about authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.
ISM | PrimaryDB | AppServer |	Connection parameters for establishing a

Configuration parameter	Description
ConnectionString	connection using the REST API of the central database's application server.
	Syntax: `url=<application server URL> [;ClientId=<client ID>;ClientSecret=<secret>;TokenEndpoint=<token endpoint>]`

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

A

adaptive card 132, 134

  apply 136

  attestation template 137

  attestors 135

  channel 135

  create 136, 138

  delete 136

  edit 136

  evaluate 138

  process ATT_AttestationHelper approve anywhere 136

  script 138

  template 136

application role

  attestation policy owner 26

  chief approval team 26, 94

approval 68

approval by mail 129

approval level 62

  connect 68

approval policies 30, 55

  default 56

  user certification 153, 155

  verify 57

approval procedure 71

  Active Directory group product owner and additional owner 80

  add 88

  approvals made externally 86

  approver for attestation policy 76

  attestation compliance rule

    attestor 77

  attestation organization attestor 77

  attestor assigned service item 78

  attestor for attestation company policy 77

  calculated approval 85

  condition 89

  copy 93

  custom 88

  delete 93

  department manager 80

  department manager of account's person 80

  employee manager 80

  employee themselves 84

  escalation 102

  manager of account's person 80

  manager of system roles to be attested 79

  members of a certain role 82

  overview form 92

  owner of a privileged object 83

  permitted for tables 92

  product owners 80

  proposed owner 84

  query 89

  recipient's location attestor 76

  recipient's manager 79

  recipient's cost center attestor 76

  recipient's department attestor 76

  recipient's primary role attestor 76

  role manager 79

T

timeout 68

U

user certification

approval policies 56

approval workflow 70

calculation schedule 22

W

Web Portal installation 169

work database 169

Workflow Editor

open 58