ONE IDENTITY™

One Identity Manager 8.0.3

Attestation Administration Guide

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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

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

One Identity Manager Attestation Administration Guide
Updated - March 2019
Version - 8.0.3

Contents

Attestation and Recertification

Table 1: General Configuration Parameter for Attestation

Configuration parameter	Meaning
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.

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

Attestation policies are defined in the One Identity Manager, which you use to carry out attestations. Attestation policies specify which objects are attested when, how often and by whom. Once an attestation is performed, the One Identity Manager creates attestation cases, which 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: The 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 107.

To use attestation functionality

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

One Identity Manager Users for Attestation

The following users are used for attestation.

Table 2: Users

User	Task
Administrators for attestation cases	Administrators are assigned to the application roles **Identity & Access Governance | Attestation | Administrators**. 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.
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, as required. • Enable or disable additional configuration parameters in the Designer, as required. • Create custom processes in the Designer, as required. • Create and configures schedules, as required. • Create and configure password policies, as required.
Attestors	• Check attestation objects in the Web Portal. • Confirm data correctness. • Initiate changes if data conflicts with internal rules.

User	Task
	Attestators in charge are determined through approval procedures.
Compliance & Security Officer	Compliance and security officers must be assigned to the application role **Identity & Access Governance | Compliance & Security Officer.** Users with this application role: • View all compliance relevant information and other analysis in the Web Portal. This includes attestation policies, company policies and policy violations, compliance rules and rule violations and risk index functions. • Edit attestation polices
Auditors	Auditors are assigned to the application role **Identity & Access Governance | Auditors**. Users with this application role: • See the Web Portal all the relevant data for an audit.
Chief approval team	The chief approver must be assigned to the application role **Identity & Access Governance| Attestation | Chief approval team**. 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 on page 11
Approval policies:	Approval Policies on page 42
Approval workflows:	Approval Workflows on page 45
Approval procedures:	Setting up Approval Procedures on page 68
Attestation procedures:	Attestation procedure on page 12
Schedules:	Schedules on page 17
Compliance frameworks:	Compliance Frameworks on page 21
Mail templates:	Creating Custom Mail Templates for Notifications on page 34
Chief approval team:	Chief approval team on page 22
Standard reasons:	Standard Reasons on page 23

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 category **Attestation | Basic configuration data | Attestation types**.
2. Select the attestation type in the result list. Select **Change master data** in the task view.

   – OR –

   Click + in the result list toolbar.
3. Edit the attestation type master data.
4. Save the changes.

Default Attestation Types

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

The 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

- Select the category **Attestation | Basic configuration data | Attestation types | Predefined**.

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

Additional Tasks for Attestation Types

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

The Attestation Type Overview

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

To obtain an overview of an attestation type

1. Select the category **Attestation | Basic configuration data | Attestation types**.
2. Select the attestation type in the result list.
3. Select **Attestation type overview** in the task view.

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. Select the category **Attestation | Basic configuration data | Attestation types**.
2. Select the attestation type in the result list.
3. Select **Assign attestation procedure** in the task view.
4. Double-click on an attestation procedure in **Add assignments** to assign it.

   – OR –

   Double-click on an attestation procedure in **Remove assignments** to remove the assignment.
5. 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. Select the category **Attestation | Basic configuration data | Attestation procedures**.
2. Select an attestation procedure in the result list. Select **Change master data** in the task view.

   – OR –

   Click + in the result list toolbar.
3. Edit the attestation procedure master data.
4. Save the changes.

General Master Data for an Attestation Procedure

Enter the following properties for an attestation procedure.

Table 3: General Master Data for 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	Spare text box 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 boxes **Property 1-4 (template)**.
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. Table containing a column `XObjectKey`. b. Table type is "Table", "View", "ReadOnly" or "Proxy". c. Usage type is "Reference 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.
Preprocessor condition	Specifies the preprocessor configuration parameters on which the attestation procedure depends. Attestation procedures, which are disabled through a preprocessor condition, are not displayed in the 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 $ notation. The template can access properties of base objects and objects accessible through foreign key relations.
Grouping column 1-3	Column headers for the columns **Grouping column 1-3 (template)**. The columns are multi-language. To enter a translation, click 🌐.

Property	Description
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 $ notation. The template can access properties of base objects and objects accessible through foreign key relations.
Property 1-4	Column headers for the columns **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 $ notation. The template can access properties of base objects and objects accessible through foreign key relations.
Related object 1-3 (template)	Template for formulating an object key for an object related to the attestation base object. Enter a value template in $ notation. The template can access properties of base objects and objects accessible through foreign key relations. Define the display value for this object in **Grouping column 1-3 (template)**.

Example

Attesting 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 Web Portal group's canonical name should be displayed with every group membership in the Active Directory. 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 master data form.

Table 4: 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 11
- Defining Reports for Attestation on page 15
- One Identity Manager Configuration Guide

Defining Reports for Attestation

Define attestation reports with the Report Editor. 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" to filter the report. This ensures that the report is displayed in the **Report** menu of the attestation procedure.
- Define a parameter "ObjectKeyBase" for the attestation object so that the exact information for the affected attestation object is reported for each attestation object. Use the parameters in the data source definition for the report in **Condition** text box.

  Example: `XObjectKey = @ObjectKeyBase`

Default reports

The One Identity Manager supplies some default reports for attestation. These are used in the default attestation procedures, amongst others. Default report are given the prefix "VI_".

> IMPORTANT: Changes to standard reports can lead to attestation errors. Do not change default reports.

Default Attestation Procedures

The 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 united namespace, can be attested. Using these default approval policies you can create attestation procedures easily in the Web Portal.

To display default attestation procedures

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

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

Related Topics

- User Attestation and Recertification on page 115
- Default Attestation and Withdrawal of Entitlements on page 107

Additional Tasks for Attestation Procedures

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

The Attestation Procedure Overview

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

To obtain an overview of an attestation procedure

1. Select the category **Attestation | Basic configuration data | Attestation procedures**.
2. Select the attestation procedure in the result list.
3. Select **Attestation procedure overview** in the task view.

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. Select the category **Attestation | Basic configuration data | Attestation procedures**.
2. Select the attestation procedure in the result list.
3. Select **Assign approval policies** in the task view.
4. Double-click on the approval policy in **Add assignments** to assign it.

   – OR –

   Double-click on the approval policy in **Remove assignments** to remove the assignment.
5. 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 72

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. Select the category **Attestation | Basic configuration data | Attestation procedures**.
2. Select the attestation procedure in the result list.
3. Select **Create copy** in the task view.
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 more detailed information, see the One Identity Manager Web Portal User Guide.
6. Edit the attestation procedure copy and save the changes.

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

Schedules

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

To edit schedules

1. Select the category **Attestation | Basic configuration data | Schedules**.

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

   – OR –

   Click 🗋 in the result list toolbar.
3. Edit the schedule’s master data.
4. Save the changes.

Enter the following properties for a schedule.

Table 5: Schedule Properties

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

Property	Meaning
run/Next planned run	interval type, rate of occurrence and the start time. NOTE: The One Identity Manager provides the start information in the time zone of the client where the program was started. Changes due to daylight saving are taken into account.

Default Schedules

The One Identity Manager supplies the following attestation schedules by default:

Table 6: Default Attestation Schedules

Calculation schedule	Description
Half-Yearly	Default schedules for any attestation.
Monthly	
Quarterly	
Weekly (Monday)	
Yearly	
Deactivated	Default schedule for user recertification. This schedule is disabled, by default. To run recertification, assign a custom schedule to the attestation policy and enable it.
Daily	Default schedules for any attestation. This schedule is assigned to the attestation policy "Certification of new users" by default.

Related Topics

- Preparing for Recertification on page 127
- Scheduled Attestation on page 124

Additional Tasks for Schedules

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

The Schedule Overview

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

To obtain an overview of a schedule

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

Assigning Attestation Policies

Use this task to assign attestation policies to the selected schedule, which will runs them. If you double click on one of the attestation policies you assign it to the current schedule.

To assign attestation policies to a schedule

1. Select the category **Attestation | Basic configuration data | Schedules**.
2. Select the schedule in the result list.
3. Select **Assign attestation polices** in the task view.
4. Double-click on the attestation policies you want to assign in **Add assignments**.
5. Save the changes.

To change an assignment

1. Select the category **Attestation | Basic configuration data | Schedules**.
2. Select the schedule in the result list.
3. Select **Assign attestation polices** in the task view.
4. Select **Show objects already assigned to other objects** in the assignment form context menu.

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

   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

To start a schedule immediately

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

   A message appears confirming that the schedule was started.

Compliance Frameworks

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

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

To edit compliance frameworks

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

   – OR –

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

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

Enter the following properties for compliance frameworks.

Table 7: Compliance Framework Properties

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

Additional Tasks for Compliance Frameworks

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

The Compliance Framework Overview

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

To obtain an overview of a compliance framework

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

Assigning Attestation Policies

Use this task to specify which attestation polices are encompassed by the selected compliance framework.

To assign attestation policies to a compliance framework

1. Select the category **Attestation | Basic configuration data | Compliance frameworks**.
2. Select the compliance framework from the result list.
3. Select **Assign attestation polices** in the task view.
4. Double-click on the attestation policies you want to assign in **Add assignments**.

   – OR –

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

Chief approval team

Sometimes, approval decisions cannot be made for attestation cases because the attestor is not available or does not have access to One Identity Manager tools. To complete the attestation case, however, 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, abort attestations in special cases or to authorize other attestors. For more information about application roles, see One Identity Manager Application Roles Administration Guide.

Table 8: Default Application Role for Chief Approval Team

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

To add members to the chief approval team

1. Select the category **Attestation | Basic configuration data | Chief approval team**.
2. Select **Assign employees** in the task view.
3. Assign employee authorized to approve attestations in **Add assignments**.

   - OR -

   Remove the assignments of employee to chief approval team in **Remove assignments**.
4. Save the changes.

Detailed information about this topic

- Attestation through Chief Approval Team on page 86

Standard Reasons

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

Standard reasons are display in the attestation history.

To edit standard reasons

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

– OR –

Click 🗋 in the result list toolbar.

3. Edit the master data for a standard reason.
4. Save the changes.

Enter the following properties for the standard reason.

Table 9: General Master Data for a Standard Reason

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

Predefined Standard Reasons

One Identity Manager provides predefined standard reasons. These standard reasons are entered into the attestation case by automatic approval through One Identity Manager.

To display predefined standard reasons

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

Attestation Policies

Attestation policies specify the concrete conditions for attestation. Use the master 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. Select the category **Attestation | Attestation policies**.
2. Select an attestation policy in the result list. Select **Change master data** in the task view.

   – OR –

   Click + in the result list toolbar.

3. Edit the master data for the attestation policy.
4. Save the changes.

General Master Data for Attestation Policies

Table 10: Configuration Parameters for Attestation Policies

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

Enter the following data for attestation policies.

Table 11: General Master Data for 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 into One Identity Manager is entered here by default. This can be changed.
Time required (days)	Number of day within which a decision must be made over the attestation. Enter "0" if you do not want to be specific. The One Identity Manager does not stipulate which action are carried out if processing times out. Define your own custom actions or evaluations to deal with this situation.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td>Description</td><td>Spare text box for additional explanation.</td></tr>
<tr><td>Risk index</td><td>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 property is only visible when the configuration parameter QER\CalculateRiskIndex is set.</td></tr>
<tr><td>Risk index (reduced)</td><td>Show the risk index taking mitigating controls into account. The risk index for an attestation policy is reduced by the <b>Significance reduction</b> value for all assigned mitigating controls.
This property is only visible when the configuration parameter QER\CalculateRiskIndex is set. The value is calculated by the One Identity Manager and cannot be edited.</td></tr>
<tr><td>Calculation schedule</td><td>Schedule for running attestation. Attestation cases are started automatically at the times specified by the schedule.</td></tr>
<tr><td>Disabled</td><td>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 under certain circumstances.
Under certain circumstances, closed attestation cases are deleted the moment the attestation polices is disabled.</td></tr>
<tr><td>Close obsolete tasks automatically</td><td>Specifies whether pending attestation cases are aborted if new ones are added.
If attestation is started and this option is set, first, all pending attestation cases for this attestation policy are canceled. Then, new attestation cases are created according to the condition.</td></tr>
<tr><td>Obsolete tasks limit</td><td>Specifies the maximum number of closed attestation cases that should remain in the database when closed attestation cases are deleted.
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>0:</td><td>No attestation cases are deleted.</td></tr>
<tr><td>> 0:</td><td>The given number of closed attestation cases to remain in the database.</td></tr>
</table></td></tr>
<tr><td>Reason for decision</td><td>Reason which is given if the option <b>Close obsolete tasks</b> is set and pending attestation cases are automatically closed.</td></tr>
<tr><td>Output format</td><td>Format in which the report is generated.</td></tr>
</table>

Property	Description
	This menu is only visible if the configuration parameter "QER\Attestation\AllowAllReportTypes" 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 a condition to determine the attestation objects from the database table specified in the attestation procedure.
Condition	Data query for finding attestation objects. This option is only available if the task **Show condition** has been run beforehand.
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, which were created in the Web Portal. You will see a corresponding message on the master 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 detailed information about editing attestation policies in the Web Portal, see the One Identity Manager Web Portal User Guide.

Detailed information about this topic

- Showing and Hiding Conditions on page 32
- Schedules on page 17
- Disabling Attestation Policies on page 34
- Mitigating Controls on page 130
- Setting up Multi-Factor Authentication for Attestation on page 75
- Creating a Copy on page 33

Related Topics

- Deleting Attestation Cases on page 92

Risk Assessment

Table 12: Configuration Parameter for Risk Assessment

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

You can use the One Identity Manager to evaluate the risk of 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 the 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.

Detailed information about this topic

- Mitigating Controls on page 130
- One Identity Manager Risk Assessment Administration Guide
- Report Editor in the One Identity Manager Configuration Guide

Default Attestation Policies

The 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 and system entitlements can be attested.

To display default attestation policies

- Select the category **Attestation | Attestation policies | Prefined**.

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
- Disabled
- Close obsolete tasks automatically
- Obsolete tasks limit
- Reason for decision

TIP: If you want to limit the number of attestation objects for default attestation polices, create a copy of the default attestation policy. You can edit the condition in the copy.

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 detailed information, see the One Identity Manager Web Portal User Guide.

Additional Tasks for Attestation Policies

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

The 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. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list.
3. Select **Attestation policy overview** in the task view.

Assigning Approvers

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. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list.
3. Select **Assign approvers** from the task list.
4. Double-click on an approver in **Add assignments** to assign it.

   – OR –

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

Detailed information about this topic

- Selecting Attestors on page 55

Assigning Compliance Frameworks

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. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list.
3. Select **Assign compliance frameworks** from the task list.
4. Double-click on a compliance framework in **Add assignments** to assign it.

   – OR –

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

Mitigating Controls

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

To edit mitigating controls

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

Detailed information about this topic

- Mitigating Controls on page 130
- Assigning Mitigating Controls on page 31
- Creating Mitigating Controls on page 31

Assigning Mitigating Controls

Specify which mitigating controls apply to the selected attestation policy.

To assign mitigating controls to an attestation policy

1. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list.
3. Select **Assign mitigating controls** from the task list.
4. Double-click on a mitigating control in **Add assignments** to assign it.

   – OR –

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

Creating Mitigating Controls

To create a mitigating control for attestation policies

1. Select the category **Attestation | Attestation policies**.
2. Select an attestation policy in the result list.
3. Select **Assign mitigating controls** from the task list.
4. Select **Create mitigating controls** from the task list.
5. Enter the master data for the mitigating control.
6. Save the changes.
7. Select **Assign attestation polices** in the task view.
8. Double-click on the attestation policies you want to assign in **Add assignments**.
9. Save the changes.

Detailed information about this topic

- Mitigating Controls on page 130

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 option **Close obsolete tasks automatically** is not taken into account in the list of attestation objects.

To start attestation for the selected objects

1. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list. Select **Change master data** in the task view.
3. Select **Run attestation cases for single objects...** in the task view.

   This opens a separate window.
4. Set **Attestation** for every object you want to include in the attestation.
5. Click **Run**.

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

Showing and 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 master data form.

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

1. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list. Select **Change master data** in the task view.
3. Select the task **Show condition** in the task view.

   This displays the **Condition** text box on the master 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. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list. Select **Change master data** in the task view.

3. Select **Hide condition** in the task view.

   The **Condition** text box is no longer displayed.

Creating a Copy

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

To copy an attestation policy

1. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list.
3. Select **Create copy** in the task view.
4. Confirm the security prompt with **Yes**.

   The attestation policy copy is displayed on the master 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. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list. Select **Change master data** in the task view.
3. Select **Show selected objects** in the task view.

   An additional tab **Result**, is show on the master data form. This displays a list of attestation objects found through the condition. The option **Close obsolete tasks automatically** is not taken into account in this case.

Deleting Attestation Policies

> IMPORTANT: Do not delete attestation policies, for audit reasons.
>
> Attestation policies can be removed from the One Identity Manager database under specific conditions. Ensure that the attestation policy is archived when deleted.
>
> For more detailed information about data archiving, see the One Identity Manager Configuration Guide.

Prerequisites

- The user is logged in to the Manager as the system user "viadmin".
- The attestation policy is disabled.

To delete an attestation policy

1. Select the category **Attestation | Attestation policies | Disabled policies**.
2. Select the attestation policy in the result list. Select **Change master data** in the task view.
3. Select **Delete attestation policy** in the task view.
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 34

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.

> TIP: Numerous default attestation policies are supplied with the 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. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list. Select **Change master data** in the task view.
3. Set **Disabled**.
4. Save the changes.

Creating Custom Mail Templates for Notifications

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

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

To edit mail templates

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

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

   – OR –

   Click ➕ in the result list toolbar.

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

To copy a mail template

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

To display a mail template preview

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

To delete a mail template

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

General Properties of a Mail Template

The following general properties are displayed for a mail template:

Table 13: Mail Template Properties

<table>
<tr><th>Property</th><th>Meaning</th></tr>
<tr><td>Mail template</td><td>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.</td></tr>
<tr><td>Base object</td><td>Mail template base object. A base object only needs to be entered if the mail definition properties of the base object are referenced.
Use the base object `AttestationCase` or `AttestationHelper` for notifications about attestation.</td></tr>
<tr><td>Report (parameter set)</td><td>Report, made available through the mail template.</td></tr>
<tr><td>Description</td><td>Mail template description. Translate the given text using the 🌐 button.</td></tr>
<tr><td>Target format</td><td>Format in which to generate email notification. Permitted values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>HTML</td><td>The email notification is formatted in HTML format. HTML format can contain formatting.</td></tr>
<tr><td>TXT</td><td>The email notification is formatted in text format. Text format cannot contain any formatting.</td></tr>
</table></td></tr>
<tr><td>Design type</td><td>Design in which to generate the email notification. Permitted values are:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>Mail template</td><td>The generated email notification contains mail text corresponding to the mail definition.</td></tr>
<tr><td>Report</td><td>The email notification is generated with the report contained under <b>Report (parameter set)</b> as mail body.</td></tr>
<tr><td>Mail template, report as attachment</td><td>The generated email notification contains mail text corresponding to the mail definition. The report entered in the <b>Report (parameter set)</b> field is attached to the mail as PDF file.</td></tr>
</table></td></tr>
<tr><td>Importance</td><td>Importance for the email notification. Permitted values are "low", "normal" and "high".</td></tr>
</table>

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

Creating and Editing an Email Definition

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

To create a new mail definition

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

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

To edit an existing mail definition

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

Using Base Object Properties

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

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

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

Table 15: Configuration Parameters for the Web Portal URL

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

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

Prerequisites for using this method

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

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

  with:

  `<Server> = Server name`

  `<App> = Web Portal installation directory path`

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

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

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

Default Functions for Creating Hyperlinks

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

Direct Function Input

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

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

Example:

```
$Script(VI_BuildAttestationLink_Approve)$
```

Default Functions for Requests

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

Table 16: Functions of the Script "VI_BuildAttestationLinks"

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.

Function	Usage
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 parameter.

Table 17: Configuration Parameters for Email Signatures

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

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

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 18: Events for Object `AttestationHelper`

Event	Triggered by
DecisionRequired	Create a new attestation case.
Remind	Sequence of reminder intervals.

Table 19: Events for Object "AttestationCase"

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 aborted.
Canceled	Obsolete attestation case aborted.

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

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 on page 42
- Approval Workflows on page 45
- Editing Approval Levels on page 49
- Default Approval Procedures on page 55

Approval Policies

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

To edit an approval policy

1. Select the category **Attestation | Basic configuration data | Approval policies**.
2. Select an approval policy from the result list. Select **Change master data** in the task view.

   – OR –

Click in the result list toolbar.

3. Edit the approval policy master data.
4. Save the changes.

General Master Data for Approval Policies

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

Table 20: General Master Data for 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	Once the approval process for attestation has been concluded, other employees can be notified by email. Select a mail template to use for email notifications for granting or denying approval for attestation or for canceling attestation.
Description	Spare text box for additional explanation.

Detailed information about this topic

- Setting Up Approval Workflows on page 48
- Notifications in Attestation on page 94

Default Approval Policies

The 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 role and system entitlements mapped in the united namespace can be attested. You can use default approval policies for creating attestation policies in the Web Portal.

To edit default approval policies

- Select the category **Attestation | Basic configuration data | Approval policies | Predefined**.

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

Related Topics

- User Attestation and Recertification on page 115
- Default Attestation and Withdrawal of Entitlements on page 107

Additional Tasks for Approval Policies

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

Editing Approval Workflows

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

To edit the assigned approval workflow

1. Select the category **Attestation | Basic configuration data | Approval policies**.
2. Select the approval policy in the result list.
3. Select the task **1. Edit approval workflow**.

   This opens the Workflow Editor.

Detailed information about this topic

- Working with the Workflow Editor on page 45

Validity Check

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. Select the category **Attestation | Basic configuration data | Approval policies**.
2. Select the approval policy in the result list.
3. Select **Validity check** in the task view.

Approval Workflows

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. Select the category **Attestation | Basic configuration data | Approval workflows**.
2. Select the approval workflow in the result list. Select **Change master data** in the task view.

   - OR -

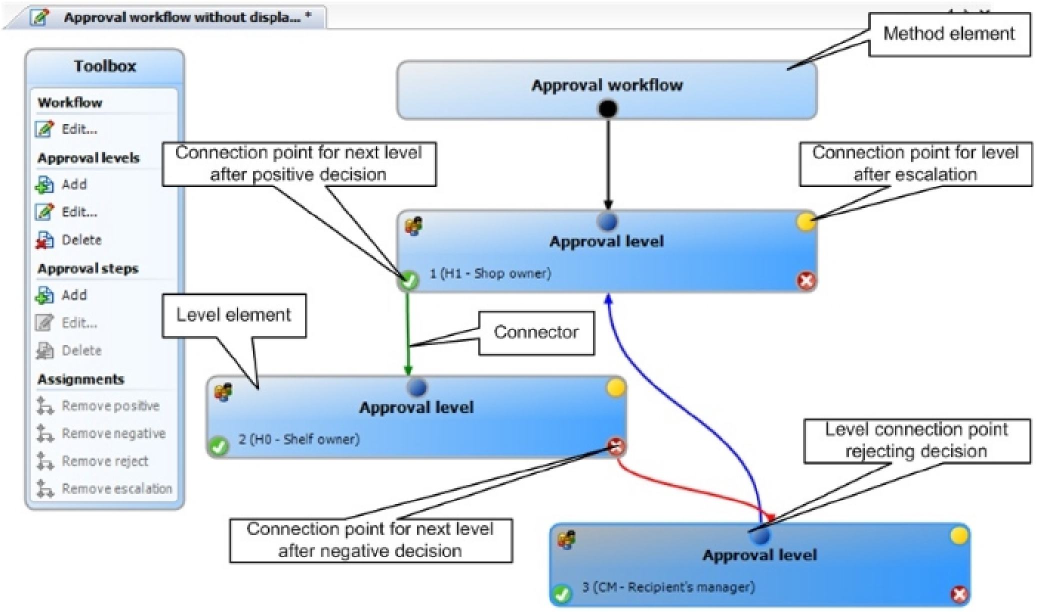
   Click + in the result list toolbar.

   This opens the Workflow Editor.
3. Edit the approval workflow master 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 methods are activated or deactivated depending on how they apply to the control element. You can move the layout position of the control elements in the workflow editor with the mouse.

Each of the elements has a properties window for editing the approval workflow, level or step data. Use **Toolbox | <Element> | Edit...** to open the properties window.

To delete a control, mark it and run **Toolbox | <Element> | Edit...**

Individual elements are linked to each other with a connector. Activate the connection points with the mouse. The mouse 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

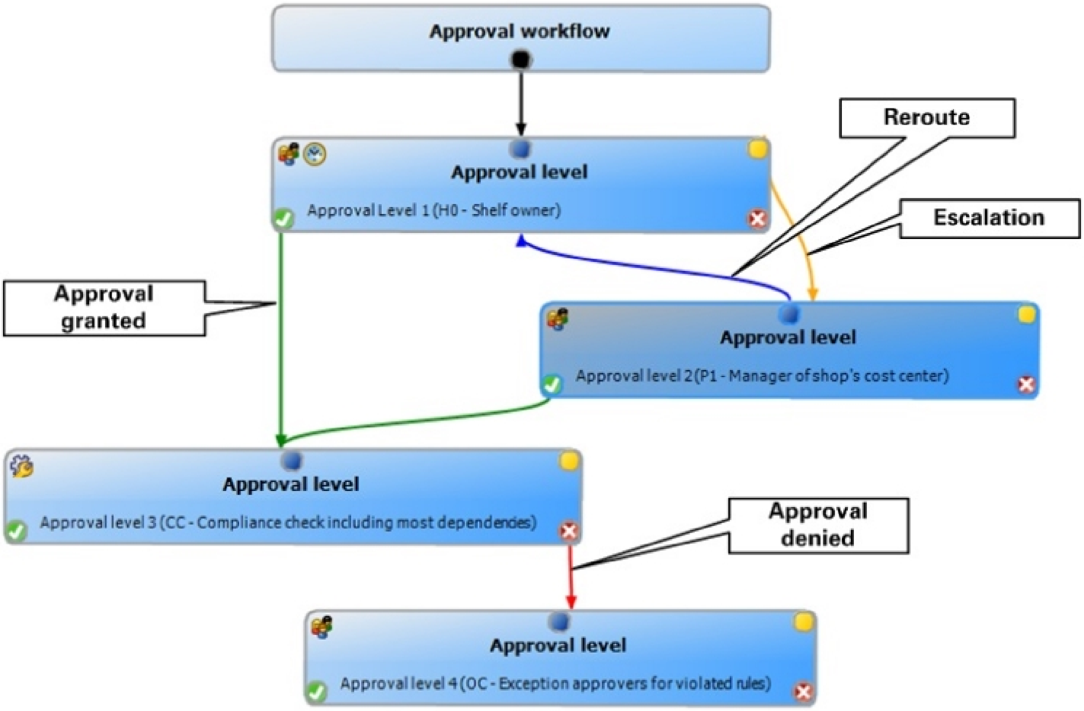

Approval workflow
Reroute
Approval level
Approval Level 1 (H0 - Shelf owner)
Escalation
Approval granted
Approval level
Approval level 2 (P1 - Manager of shop's cost center)
Approval level
Approval level 3 (CC - Compliance check including most dependencies)
Approval denied
Approval level
Approval level 4 (OC - Exception approvers for violated rules)

Table 21: Approval Workflow Connectors

Connector	Meaning
Approval	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 by-pass 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 **Toolbox | Assignments**. 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. All the approval steps in the attestation procedure for one approval level have to be executed before the next approval level can be called upon. 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 **Toolbox | Workflow | Edit...**.
3. Edit the workflow properties.
4. Click **OK**.

Table 23: Approval Workflow Properties

Property	Meaning
Name	Approval workflow name.
System abort (days)	Number of days to elapse after which the approval workflow, and therefore the system automatically ends the entire attestation procedure.
Description	Spare text box for additional explanation.

Detailed information about this topic

- Aborting an Attestation Case on Timeout on page 84

Editing Approval Levels

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

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 **Toolbox | Approval levels | Add...**.

   This opens the properties dialog for the first approval step.
2. Enter the approval step properties.
3. Save the changes.

For more information, see Setting up an Approval Step on page 50.

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 **Toolbox | Approval levels | Add...**.
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 **Toolbox | Approval levels | Add...**.
3. Enter the approval step properties.
4. Save the changes.

To edit approval level properties

1. Select the approval step.
2. Select **Toolbox | Approval levels | Add...**.

3. Edit the approval step properties.
4. Save the changes.

Setting up an Approval Step

The following data is requires for an approval step. If you add a new approval step, you must fill out the compulsory fields.

Table 24: Setting up an Approval Step

Property	Meaning
Single step	Approval step name.
Approval Procedure	Procedure to use for determining attestors.
Mail templates	Mail template that is used for email notifications for granting or denying approval, escalation, abort, rejection or delegation of an attestation case as well as a reminder.
Condition	Condition for calculating approval with approval procedures CD, EX or WC.
Role	Hierarchical roles for determining the attestor with default approval procedures "OM" and "OR".
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 not enough attestors can be found, the approval step is presented to the fallback approvers. The approval step is considered approved the moment **one** fallback approver has approved the attestation case. Enter the value -1 if approval decisions should be made for all the employees found using the applied approval procedure, for example all members of a role (default approval procedure "OR"). This overrides the maximum number of attestors defined in the approval procedure. The number of approvers defined in an approval step is not taken into account in the approval procedures CD, EX or WC.
Description	Spare text box for additional explanation.
Fallback approver	Applications 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

<table>
<tr><th>Property</th><th>Meaning</th></tr>
<tr><td></td><td>and assign a parent application role. For more information, see the One Identity Manager Application Roles Administration Guide.
NOTE: The number of approvers is not applied to the fallback approvers. The approval step is considered approved the moment <b>one</b> fallback approver has approved the request.</td></tr>
<tr><td>Reminder interval (hours)</td><td>Number of working hours to elapse after which the attestor is notified by mail that there are still pending requests for attestation cases for attestation.
NOTE: Ensure that a state and/or county is entered into the employee`s master data for determining the correct working hours.</td></tr>
<tr><td>TimeOut (working hours)</td><td>Number of working hours to elapse after which the approval step is automatically granted or denied approval.
The approvers work time applies to the time calculation.
NOTE: Ensure that a state and/or county is entered into the employee`s master data for determining the correct working hours.</td></tr>
<tr><td>Timeout behavior</td><td>Action, which is executed if the timeout expires.
<b>Table 25: Possible Timeout Behavior</b>
<table>
<tr><th>Method</th><th>Description</th></tr>
<tr><td>Approval</td><td>The attestation case is granted approval in this approval step. The next approval step is called.</td></tr>
<tr><td>Deny</td><td>The attestation case is denied approval in this approval step. The next approval step is called.</td></tr>
<tr><td>Escalation</td><td>The attestation case is escalated. The escalation approval step is called.</td></tr>
<tr><td>Abort</td><td>The approval, and therefore the entire attestation procedure, is aborted.</td></tr>
</table></td></tr>
<tr><td>Additional approver possible</td><td>Specifies whether a current attestor is allowed to instruct another employee to be an attestor. This additional attestor is authorized to make approvals for the current attestation case in parallel. 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.</td></tr>
<tr><td>Approval</td><td>Specifies whether the current attestation attestor can delegate to another</td></tr>
</table>

Property	Meaning
can be delegated	employee. This employee is added to the current approval step as attestor. The employee 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 that is affected by the attestation case can also approve it. If this option is not set, specify whether the employee to be attested can attest themselves, in the configuration parameter "QER\Attestation\PersonToAttestNoDecide".
Do not show in approval history	Specifies whether the attestation history is visible or not. This behavior can be applied to approval steps with approval procedure "CD - calculated approval", for example, steps are only used for branching in the approval workflow. This makes it easier to follow the attestation history.

Detailed information about this topic

- Notifications in Attestation on page 94
- Reminding Attestors on page 95
- Escalating an Attestation Case on page 81
- Automatic Approval on Timeout on page 84
- Aborting an Attestation Case on Timeout on page 84
- Finding Attestors using a Specified Role on page 64
- Calculated approval on page 65
- Making External Approvals on page 66
- Deferring Attestation on page 67
- Prevent Attestation by Employee Awaiting Attestation on page 78

Related Topics

- Selecting Attestors on page 55
- Attestors cannot be Established on page 83
- Attestation through Chief Approval Team on page 86

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 26: Links to Approval Levels

Link	Description
Approval	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 by-pass 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 level 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. It is not possible to reroute approval steps with the approval methods "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 one, then the attestation case is considered approved if the approval decision was to grant approval. If the approval is not granted, the attestation case is finally denied. The attestation procedure is closed in both cases.

Additional Tasks for Approval Workflows

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

The Approval Workflow Overview

To obtain an overview of an approval workflow

1. Select the category **Attestation | Basic configuration data | Approval workflows**.
2. Select the approval workflow in the result list.
3. Select **Approval workflow overview** in the task view.

Copying Approval Workflows

For example, you can copy default approval workflows in order to customize them.

To copy an approval workflow

1. Select the category **Attestation | Basic configuration data | Approval workflows**.
2. Select an approval workflow in the result list. Select **Change master data** in the task view.
3. Select **Copy workflow...** in the task view.
4. Enter a name for the copy.
5. Click **OK** to start the copy actions.

   - OR -

   Click **Cancel** to cancel the copy action.

Deleting Approval Workflows

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 approval policy master data form and assigned another approval workflow.
2. Select the category **Attestation | Basic configuration data | Approval workflows**.
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 53
- General Master Data for Approval Policies on page 43

Default Approval Workflows

The 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 role and system entitlements mapped in the united namespace can be attested. You can use default approval policies for creating attestation policies in the Web Portal.

To edit default approval workflows

- Select the category **Attestation | Basic configuration data | Approval workflows | Predefined**.

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

Related Topics

- User Attestation and Recertification on page 115
- Default Attestation and Withdrawal of Entitlements on page 107

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 approval for 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 there are several people are determined as approvers by an approval procedure, the number given in the approval step specifies how many people must approve the step. The attestation case can only be passed onto attestors in next level when this has been done. If an approver cannot be found for an approval step, the attestation procedure is aborted.

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

The DBQueue Processor calculates which person has the authority to grant approval at which 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 category **Attestation | Basic configuration data | Approval procedures | Predefined**.

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

Table 27: Approval Procedures for Attestation

Abbreviation	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 application role **Identity Management | Organizations | Attestors**. • Attestors for business roles must be assigned to the application role **Identity Management | Business roles | Attestors**. • Attestors for requests must be assigned to the application role **Request & Fulfillment | IT Shop | Attestors**.
AD	Recipient's department attestor	Attestor of the department to which the attestation object is primarily assigned. • Attestors for departments must be assigned to the application role **Identity Management | Organizations | Attestors**.
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 application role **Identity Management | Organizations | Attestors**.
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 application role **Request & Fulfillment | IT Shop | Attestors**.
AO	Recipient's primary role attestor	Attestor of the business role to which the attestation object is primarily assigned. Attestors for business roles must be assigned to the application role **Identity Management | Business roles | Attestors**.
AP	Recipient's cost	Attestor of the cost center to which the attestation

Abbreviation	Procedure Name	Attestors
	center attestor	object is primarily assigned. - Attestors for cost centers must be assigned to the application role **Identity Management | Organizations | Attestors**.
AR	Attestation compliance rule attestor	Attestor for the compliance rule to be attested. - Attestors must be assigned to the application role **Identity & Access Governance | Identity Audit | Attestors**.
AS	Approver for attestation policy	All employees assigned to the attestation policy as approver.
AT	Attestation organization attestor	Attestor of the organization (department, cost center, location), business role or IT Shop to be attested. - Attestors for departments, cost centers and locations must be assigned to the application role **Identity Management | Organizations | Attestors**. - Attestors for business roles must be assigned to the application role **Identity Management | Business roles | Attestors**. - Attestors for requests must be assigned to the application role **Request & Fulfillment | IT Shop | Attestors**.
AY	Attestor for attestation company policy	Attestor of the company policy to be attested. - Attestors must be assigned to the application role **Identity & Access Governance | Company policies | Attestors**.
CD	Calculated approval	-
CM	Recipient's manager	Manager of the employee to be attested.
DM	Manager of recipient's department	Department manager/deputy if employees of secondary memberships are attested in departments.
ED	Department manager for permission	Employee’s department manager whose system entitlements are to be attested.

Abbreviation	Procedure Name	Attestors
	attestation	
EM	Employee manager for permission attestation	Employee’s manager whose system entitlements are to be attested.
EN	Target system manager of the permission for attestation	Target system manager of the system entitlements to be attested.
EO	Product owner of the permission for attestation	Product owner whose system entitlements or system roles are to be attested.
EX	Approvals to be made externally	-
LM	Location manager	Location manager/deputy if employees of secondary memberships are attested in locations.
MO	Role owner	Business role manager/deputy if employees of secondary memberships are attested in roles.
OA	Product owners	All members of the assigned application role if service items or system entitlements are attested.
OM	Specific role Manager	Manager of the role selected in the approval workflow.
OR	Members of a certain role	All employees that are assigned to a secondary business role.
PA	Additional owner of Active Directory group	All employees to be found through the additional owner of the requested Active Directory group.
PM	Manager of recipient's cost center	Cost center manager/deputy if secondary memberships in cost centers are attested.
RE	Manager of system roles to be attested	System role manager to be attested.
RM	Role manager for attesting	Manager of role to be attested if secondary memberships in roles are attested.

Abbreviation	Procedure Name	Attestors
	memberships	
RR	Role manager for attesting roles	Manager of role to be attested.
SO	Target system manager of the permission for attestation	Target system manager of system entitlement or user account to be attested.
WC	Waiting for further approval	-

Finding Attestors using the Attestation Policy

Use the approval procedure "AS" 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 more detailed information, see the One Identity Manager Web Portal User Guide.

Related Topics

- Assigning Approvers on page 29

Finding Attestors using the Role of an Employee to Attest

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

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

Attestation objects are employees (table: Person) or request recipients (table: PersonWantsOrg). 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 approval procedures "AO" and "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

- Default Approval Procedures on page 55

Finding Attestors using Attestation Objects

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

	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 approval procedure "AA" finds the attestor using the role (departments, IT

Shop structures, locations, business roles, cost centers, IT Shop templates). The approval procedure "AN" finds the attestor using the service item assigned to the system entitlement or target system group.

Furthermore, the following also applies to the approval procedures "AT" and "AA":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: When the attestation base object is a business role, IT Shop structure or IT Shop template or rather the assignment to a business role, IT Shop structure or IT Shop template and "bottom-up" inheritance is defined for the associated role classes.
>
> - 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 55

Finding Attestors from Attestation Object Managers

If you want to allow company resource assignments for your employees, roles or role memberships, system roles or system entitlements for employees, roles or IT Shop structures through their managers, use the approval procedures "CM", "DM", "LM", "MO", "RM", "RR" or "RE".

Approval procedure	**Attestation Base Objects**	**Available in Module**
CM	Employees (`Person`)	
DM	Employees (`Person`) Employees: department memberships (`PersonInDepartment`)	
LM	Employees (`Person`) Employees: location memberships (`PersonInLocality`)	
MO	Employees (`Person`) Employees: business role memberships (`PersonInOrg`)	Business Roles Module
PM	Employees (`Person`) Employees: cost center memberships (`PersonInProfitCenter`)	
RE	System roles (`ESet`)	System

Approval procedure	Attestation Base Objects	Available in Module
	Employees: system role assignments (PersonHasESet) Departments: system role assignments(DepartmentHasESet) Business roles: system role assignments (OrgHasESet) IT Shop structures: system role assignments (ITShopOrgHasESet) IT Shop templates: system role assignments (ITShopSrcOrgHasESet) Cost centers: system role assignments (ProfitCenterHasESet) Locations: system role assignments (LocalityHasESet)	Roles Module
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 case of the approval procedure "RE", the system role manager is determined as attestor, for the approval procedures "RM" and "RR" the role/IT Shop structure manager. The approval procedures "DM", "LM", "MO" and "PO" find the department manager and deputy manager in which the employee to attest is a member.

Finding Attestors from those Responsible for the Attestation Object

If you want to attest system entitlements and the user account assigned to them, use the approval policies "ED", "EM", "EN", "EO" or "SO".

Attestation objects are system entitlements and the user accounts assigned to them as well as system roles which have system entitlements or system roles assigned to them. The approval procedures determine the following attestors:

	Attestation Base Objects	Attestors	Available in Module
ED	User accounts: system entitlement assignments (UNSAccountInUNSGroup)	Employee’s department manager (and deputy manager) to which 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 which 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 groups" (SAPUserInSAPGroup) 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
SO	User accounts: system entitlement assignments (UNSAccountInUNSGroup)	Target system manager for the target system to	Target System

Attestation Base Objects	Attestors	Available in Module
User accounts (`UNSAccount`) System entitlements: assignments to system entitlements (`UNSGroupInUNSGroup`)	which the system entitlement or user account belongs.	Base Module

Finding Attestors using a Specified Role

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

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

Finding Attestors from Product Owners

If service items or system entitlements need to be attested, product owners can be determined as attestors. Use the approval procedure "OA" to do this. Any number of service items and system entitlements which are assigned a service item can be attested.

Assign an application role to the service item in **Product owner**. This determines all employees as attestor who have the given application role.

Calculated approval

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

If you want to make attestation dependent on specific conditions, use the approval procedure "CD". This procedure does not determine an attestor. The 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 the One Identity Manager. If the condition does not return a result, the approval step is denied by the 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 approval procedure "CD"

1. Edit the approval step properties.

   For more information, see Editing Approval Levels on page 49.

2. Enter a valid WHERE clause for the database query in **Condition** or **Condition (Oracle)**. You can enter the SQL query directly or with a wizard. Refer to the condition using the variable '`@UID_AttestationCase`' (SQL) or '`v_uid_attestationcase`' (Oracle) in the definite case of an attestation instance.

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

Compliance should be tested when they meet the following conditions:

1. Compliance rule is enabled
2. A rule manager is assigned to the compliance rule

Find the objects that meet these conditions by using the approval procedure CD.

```
exists
      (SELECT 1 FROM (SELECT xobjectkey FROM ComplianceRule
      WHERE isnull(IsWorkingCopy, 0) = 0 AND EXISTS
            (SELECT 1 FROM (SELECT UID_AERole FROM AERole WHERE 1 = 1)
            as X WHERE X.UID_AERole = ComplianceRule.UID_OrgResponsible))
      as X WHERE X.xobjectkey = AttestationCase.ObjectKeyBase)
```

If the condition is met, the rule attestor should attest this compliance rule. To do this, extend the positive approval path with an approval step using approval procedure "AR".

If the condition is not met, the attestation should be denied by the One Identity Manager. In this case, no further approval steps are required.

Making External Approvals

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

Specify an event in the approval step that triggers an external approval. A process is started by the event 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. Define your own processes that:
    - Trigger an external approval
    - Analyze the results of the external approval
    - Subsequently grant or deny approval for the external approval step in One Identity Manager
2. Define an event, which 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 has to be changed. Use the process task `CallMethod` with the method `MakeDecision` 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 approved by external approval (`whereClause`). Parameter `param 1` specifies the attestor. Attestor is always the system user "sa". Parameter `param 2` is passed to the approval. If the attestation was granted approval the value must be "true". If the attestation was denied approval the value must be "false". Use parameter `Param3` to pass a reason text fro 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.

Use the Process Editor to define and edit processes.

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 process "P1" that saves a PDF report with data about the attestation object data and the attestation procedure on an external share
- An event "E1" that starts the process "P1".

  Enter the event "E1" in the approval step in the **Event** field and in the process "P1" as a trigger event for external approval.
- A process "P2" that checks the share for new text files, evaluates the content and calls the One Identity Manager task `CallMethod` with the method `MakeDecision`
- An event "E2" that starts the process "P2"
- A schedule that starts the events "E2" on a regular basis

For more detailed information about creating processes and schedules, see the One Identity Manager Configuration Guide.

Detailed information about this topic

- Setting up an Approval Step on page 50

Deferring Attestation

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

If you want to ensure that a specific data state exists in the One Identity Manager before attestation, then use the approval procedure "WC". 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. The function has to accept the attestation case UID as a parameter (`AttestationCase.UID_AttestationCase`). Use this UID to refer to each attestation object. It must define three return values as integers. One of the following actions is carried out depending on the function‛s return value:

Table 28: 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 value = 0	The condition is not yet fulfilled. Approval is rolled back and is retested the next time DBQueue Processor runs.

Return value	Action
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 approval procedure "CW". Enter the function call in **Condition**.

   Table 29: Syntax for the function call

SQL Server:	`dbo.<function name>`
Oracle Database:	`<database schema name>.<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 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. Select the category **Attestation | Basic configuration data | Approval procedures**.
2. Select an approval procedure in the result list. Select **Change master data** in the task view.

   – OR –

   Click ➕ in the result list toolbar.
3. Edit the approval procedure master data.
4. Save the changes.

To edit the condition

1. Select the category **Attestation | Basic configuration data | Approval procedures**.

2. Select an approval procedure from the result list.
3. Select **Change queries for approver selection** in the task view.

Detailed information about this topic

- General Master Data for an Approval Procedure on page 69
- Queries for Finding Attestors on page 69

General Master Data for an Approval Procedure

Enter the following master data for an approval procedure.

Table 30: General Master Data for 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 attestors. 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

- Setting up an Approval Step on page 50

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 to the group of attestors who have been determined through single queries.

To edit the condition

1. Select the category **Attestation | Basic configuration data | Approval procedures**.
2. Select an approval procedure from the result list.
3. Select **Change queries for approver selection** in the task view.

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 31: Query Properties

Approver selection	Query identifier, which determines the attestors.
Query	Database query for determining attestors. The database query must be formulated as a select statement. The column selected by the database query must return a `UID_Person`. The query returns one or more employees that are presented to the attestation case for approval. If the query does not return a result, the attestation case is aborted. NOTE: • A query contains exactly one select statement. To combine several select statements, create several queries. • You cannot enter a query to determine attestors if a DBQueue Processor task is assigned.

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 you access the attestation case waiting approval in the database query over the variable `@UID_AttestationCase` (SQL) or `v_uid_attestationcase` (Oracle) (example 2).

Example 1

The attestation case should be approved by a specified attestor.

Query:
```
select UID_Person from Person where InternalName='Rippington, Dr. Rudiger von'
```

Example 2

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

Query:
```
select pia.UID_Person from PersonInAERole pia

join ComplianceRule cr on pia.UID_AERole = cr.UID_OrgResponsible

join AttestationCase ac on ac.ObjectKeyBase = cr.XObjectKey

and ac.UID_AttestationCase = @UID_AttestationCase

where cr.IsWorkingCopy = '0'
```

TIP: To take delegations into account when attestors are being determined, identify the attestator from the table `HelperHeadOrg`. This table groups all hierarchical role managers, their deputy manager and employees delegated to the manager.

Additional Tasks for Approval Procedures

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

The Attestation Procedure Overview

To obtain an overview of an approval procedure

1. Select the category **Attestation | Basic configuration data | Approval procedures**.
2. Select an approval procedure from the result list.
3. Select **Approval procedure overview** in the task view.

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 which forms the attestation base object for an attestation procedure. You must specify which tables are permitted for use with custom approval procedures.

To specify the tables which permit this approval procedure

1. Select the category **Attestation | Basic configuration data | Approval procedures**.
2. Select an approval procedure from the result list.
3. Select the task **Assign tables**.
4. Double-click on the table to which the approval procedure can be assigned in **Add assignments**.

   – OR –

   Double-click on the tables no longer permitted to be assigned to the approval procedure in **Remove assignments**.
5. 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 16
- The Attestation Procedure Overview on page 71

Deleting Approval Procedures

To delete an approval procedure

1. Remove all assignments to approval steps.
   a. Check on the approval procedure overview form, 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. Select the category **Attestation | Basic configuration data | Custom defined | Approval procedures**.
3. Select an approval procedure from the result list.

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

Related Topics

- The Attestation Procedure Overview on page 71

Finding Attestors

Table 32: Configuration Parameters for Recalculating and Attestors

Configuration parameter	Description
QER\Attestation\ReducedApproverCalculation	This configuration parameter specifies, which approval steps are recalculated if the Attestor must be recalculated.

The DBQueue Processor calculates, which employee is authorized as approver in which approval level. Once a attestation is triggered, the attestors are determined for every approval step of the approval workflow to be processed. Changes to responsibilities may lead to an employee no longer being authorized as approver for an attestation that is not yet finally approved. In this case, 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 the One Identity Manager, for example, if a department manager, the attestation policy approver or the target system manager is changed.
- An employee obtains responsibilities in One Identity Manager and therefore is authorized as an approver, for example the manager of the employee to be attested.

Once an employee's responsibilities have change in the One Identity Manager, an attestor recalculation task is queued in the DBQueue. By default, all approval steps of the pending attestation cases are recalculated at the same time. 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 that has changed. To optimize this processing time, you can specify which approval steps the attestors are recalculated for.

To configure recalculation of attestors

- Set the configuration parameter "QER\Attestation\ReducedApproverCalculation" in the Designer and select one of the following options as a value.

Table 33: Options for Recalculating Attestors

Option	Description
No	All approval steps are recalculated. This behavior also applies if the configuration parameter is not set. Advantage: All valid attestors are displayed in the approval sequence. The rest of the approval sequence is transparent. Disadvantage: Recalculating attestors can take a long time.
CurrentLevel	Only attestors for the approval level currently being processed 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 attestors is probably faster. TIP: Use this option if performance problems within your system have occurred in connection with recalculating attestors. Disadvantage: In the approval sequence, the originally calculated attestors are displayed for the subsequent approval steps although they may no longer be authorized. The rest of the approval sequence is not correctly represented.
NoRecalc	Attestors are not recalculated. The previous attestors remain authorized to approve the current approval levels. 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 attestors is probably faster. TIP: Use this option if performance problems within your system have occurred in connection with recalculating attestors, although the "CurrentLevel" option is used. Disadvantage: In the approval sequence, the originally calculated attestors are displayed for the subsequent approval steps although they may no longer be authorized. The rest of the approval sequence is not correctly represented. Employees that are no longer authorized can approve the current approval level. In the best case, only attestors are found that do not have access to the 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.

Option	Description
	- OR - - Assign members to the chief approval team when you set up the attestation. These can always intervene in pending attestation cases.

Detailed information about this topic

- Setting up an Approval Step on page 50
- Chief approval team on page 22

Related Topics

- Modifying Approval Workflows on Pending Attestation Cases on page 91

Setting up Multi-Factor Authentication for Attestation

Table 34: Multi-factor Authentication Configuration Parameters

Configuration Parameter	Meaning
QER\Person\Defender	This configuration parameter specifies whether Starling Two-Factor Authentication is supported.
QER\Person\Defender\ApiEndpoint	This configuration parameter contains the URL of the Starling 2FA API end point used to register new users.
QER\Person\Defender\ApiKey	This configuration parameter contains your company's subscription key for accessing the Starling Two-Factor Authentication interface.

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.

To be able to use multi-factor authentication

1. Register your company in Starling Two-Factor Authentication.

   For more detailed information, see the Starling Two-Factor Authentication documentation.

2. Set the configuration parameter "QER\Person\Defender" in the Designer.

- Set the configuration parameter "QER\Person\Defender\ApiKey" and enter your company's subscription key as the value for accessing the Starling Two-Factor Authentication interface.

3. Enable assigning by event for the table `PersonHasQERResource`. For more information, see Editing Table Properties on page 76.
4. Enable the service item "New Starling 2FA token" in the Manager. For more information, see Preparing Starling 2FA Token Requests on page 77.
5. Enable the option **Approval by multi-factor authentication** in the Manager on the attestation policy to which to want to apply multi-factor authentication. For more information, see General Master Data for Attestation Policies on page 25.

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

If the user's telephone number has changed, cancel the current Starling 2FA token and request a new one. If the Starling 2FA token is no longer required, cancel it anyway.

Once the option "Approval by multi-factor authentication" 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.

> ℹ IMPORTANT: An attestation is not possible by email, if multi-factor authorization is configured for the attestation policy. Attestation emails for such requests produce an error message.

Related Topics

- Attestation by Mail on page 103

You can find detailed information about

- For requesting Starling 2FA tokens.
- Multi-factor authentication for attestation
- Canceling products

in the One Identity Manager Web Portal User Guide.

Editing Table Properties

> ℹ NOTE: If the option "Assign by event" is set, the process "HandleObjectComponent" is queued in the Job queue immediately after a resource is added to or removed from an employee.

To enable assigning by event for a table

1. Select the category **Designer Schema** in the One Identity Manager.
2. Select the table `PersonHasQERResource` and start the Schema Editor from the task **Show table definition**.
3. Select the view **Table properties | Table** and set the option **Assign by event**.
4. Save the changes.

For more information about editing table definitions, see the One Identity Manager Configuration Guide.

Preparing Starling 2FA Token Requests

One Identity Manager users must be registered with Starling Two-Factor Authentication in order to use multi-factor authentication. To register, a user must request the Starling 2FA Token in the Web Portal. Once the request has been granted approval, the user receives a link to the Starling Two-Factor Authentication app and a Starling 2FA user ID. The app generates one-time passwords, which are required for authentication. The Starling 2FA user ID is saved in the user's employee master data.

> NOTE: The user's default email address, mobile phone and country must be stored in their master data. This data is required for registering.

To facilitate requesting a Starling 2FA token

1. Select the category **IT Shop | Service catalog | Predefined**.
2. Select **New Starling 2FA token** in the result list.
3. Select **Change master data** in the task view.
4. Disable **Not available**.
5. Save the changes.

The Starling 2FA token request must be granted approval by the request recipient's manager.

Requesting a Security Code

Table 35: Configuration Parameter for Requesting Starling 2FA Security Codes

Configuration parameter	Meaning
QER\Person\Defender\DisableForceParameter	This configuration parameter specifies whether Starling 2FA is forced to send the OTP by SMS or phone call if one of these options is selected for multi-factor

Configuration parameter	Meaning
	authentication. If the configuration parameter is set, Starling 2FA can disallow the request and the user must request the OPT through Starling 2FA.

If the OTP is requested for a attestion, the user decides how the OTP is send. The following options are available:

- By Starling 2FA app
- By SMS
- By phone call

By default, Starling 2FA is forced to send the OTP by SMS or by phone call if the user has selected one of these options. However, for security reasons, the user should use the Starling 2FA app to generate the OTP. If the app is installed on the user's mobile phone, Starling 2FA can refuse the SMS or phone demand and the user must generate the OTP using the app.

To use this method

- Set the configuration parameter ""QER\Person\Defender\DisableForceParameter" in the Designer.

  Starling 2FA can refuse to transmit the OTP by SMS or phone call if the Starling 2FA app is installed on the phone. Then the OTP must be generated by the app.

If the configuration parameter is not set (default), Starling 2FA is forced to send the OTP by SMS or phone call.

Prevent Attestation by Employee Awaiting Attestation

Table 36: Configuration Parameter for Attestation by Employee Awaiting Attestation

Configuration parameter	Meaning
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_`

Configuration parameter	Meaning
	ObjectKey1, ObjectKey2 or ObjectKey3). If the parameter is not set, these employee are allowed to make approval decisions for this attestation case.

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 configuration parameter "QER\Attestation\PersonToAttestNoDecide".

> 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 option "Approval by affected employee" is set on an approval step, the configuration parameter has no effect.

To prevent employees from attesting themselves

- Set the configuration parameter "QER\Attestation\PersonToAttestNoDecide" in the Designer.

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 sub-identities of these main identities

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

Related Topics

Setting up an Approval Step on page 50

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. The 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 inquiry option does not, however, replace the granting or denying approval of an attestation case. There is no addition approval step required in the approval workflow to obtain the information.

Attestors can request information from anyone, in the form of a question. The attestation case is put on hold for the questioning period. Hold status is removed once the employee questioned has supplied the required information and the attestor has made an approval decision for the attestation case. The attestor can recall a pending inquiry at any time The request is taken off hold. The question and answer are logged in the approval sequence and made available to the attestors.

> NOTE: Hold status is revoked when the attestor who has asked a question is removed. The queried person must not answer. The attestation case is continued.

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

Detailed information about this topic

- Notifications with Questions on page 101
- One Identity Manager Web Portal User Guide

Appointing Other Attestors

Once an approval level in the approval workflow has been reached, attestors at this level can appoint another employee to deal with the approval. To do this, you have the options described below. The required behavior is configured in the approval workflow.

- Reroute approval

  The attestor appoints another approval level for attesting. To do this, create a connection to the approval level to which the approval can be rerouted.
- Appoint additional attestors

  .The attestor appoints another employee with the attestation. This adds another approval step to the current approval level. The new attestor must make an approval decision in addition to the known attestors.

  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 attestors can appoint another additional attestor.
- Delegate approval

  The attestor appoints another employee with attestation. This employee is added to the current approval step as attestor. The employee makes the approval decision instead of the attestor who made the delegation.

The current attestors can reject the approval and return the attestation case to the original attestor. The original attestors can accept the refusal and delegate a different employee, for example, if another attestor is not available.

Email notification can be sent to the original attestor and the others.

Detailed information about this topic

- Connecting Approval Levels on page 52
- Editing Approval Levels on page 49

Related Topics

- Delegating Attestation on page 100
- Approval Rejection on page 100
- Notifications from Additional Attestors on page 101

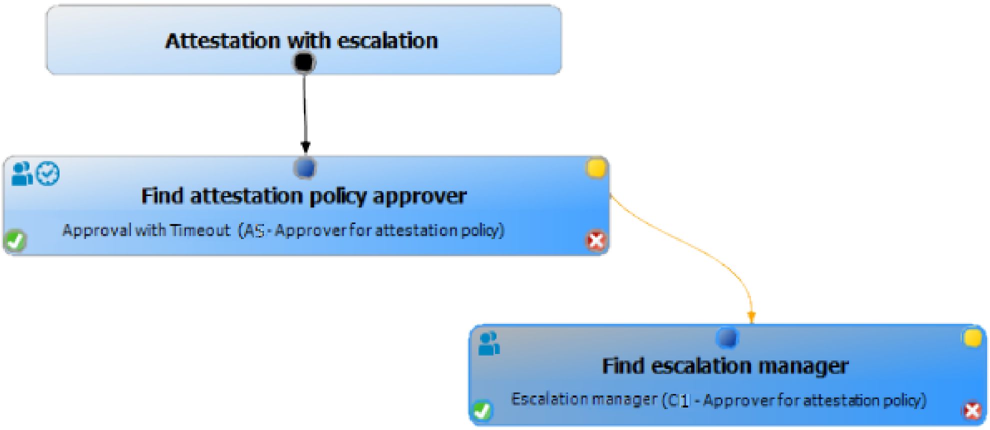
Escalating an Attestation Case

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


Attestation with escalation
Find attestation policy approver
Approval with Timeout (AS - Approver for attestation policy)
Find escalation manager
Escalation manager (O1 - Approver for attestation policy)

4. Configure the behavior for the approval step to be escalated when it times out.

Table 37: Approval Step Properties for Abort on Timeout

<table>
<tr><th>Eigenschaft</th><th>Bedeutung</th></tr>
<tr><td>Timeout (working hours)</td><td>Number of working hours to elapse after which the approval step is automatically granted or denied approval.
The approvers work time applies to the time calculation.
NOTE: Ensure that a state and/or county is entered into the employee`s master data for determining the correct working hours.</td></tr>
<tr><td>Timeout behavior</td><td>Action to be taken if the timeout expires.
<b>Table 38: Possible Methods for Escalation on Timeout</b>
<table>
<tr><th>Method</th><th>Description</th></tr>
<tr><td>Escalation</td><td>The attestation case is escalated. The escalation approval step is called.</td></tr>
</table></td></tr>
</table>

Emails can be sent to the new attestors and other employees on escalation.

Related Topics

- Demanding Attestation on page 95
- Attestation Case Escalation on page 99

Attestors cannot be Established

You can specify a fallback approver if attestation cases cannot be approved due to lack of attestor. An attestation case is always returned to the fallback approver for attestation if the approval step in a specified approval procedure, cannot determine an attestor.

To specify fallback approvers, define application roles and assign these to an approval step. Different attestation groups in the approval steps may 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 Application Roles Administration Guide.

To specify fallback approvers for an approval step

1. Select the category **Attestation | Basic configuration data | Approval workflows**.
2. Select a workflow in the result list. Select **Change master data** in the task view.
3. Mark the approval step in the workflow editor.
4. Select **Toolbox | Approval levels | Add...**.
5. Assign an application in **Fallback approver** or create a new application role.
6. Save the changes.

Attestation sequence with fallback approvers

1. An attestor cannot be established 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 made an approval decision, the attestation case is passed onto the attestation of the next approval level.

   > NOTE: Specify in the approval step, how many attestors must approve this approval step. This limit is **not** valid for the chief approval team. The approval step is considered approved the moment **one** fallback approver has approved the attestation.

3. The attestation case is aborted if no fallback approver can be established.

Fallback approvers can approve attestors for all manual approval steps. The fallback approvals are not permitted for approval steps with the approval procedures CD, EX and WC .

Related Topics

- Editing Approval Levels on page 49
- Selecting Attestors on page 55
- Attestation through Chief Approval Team on page 86

Automatic Approval on Timeout

Attestation instances can be automatically approved once a specified time period has been exceeded.

To configure automatic approval if the timeout expires

- Enter the following data for the approval step.

Table 39: Properties for Automatic Approval on Timeout

<table>
<tr><th>Property</th><th>Meaning</th></tr>
<tr><td>TimeOut (working hours)</td><td>Number of working hours to elapse after which the approval step is automatically granted or denied approval.
The approvers work time applies to the time calculation.
NOTE: Ensure that a state and/or county is entered into the employee`s master data for determining the correct working hours.</td></tr>
<tr><td>Timeout behavior</td><td>Action, which is executed if the timeout expires.
<b>Table 40: Possible Methods for Escalation on Timeout</b><table><tr><th>Method</th><th>Description</th></tr><tr><td>Approve</td><td>The attestation case is granted approval in this approval step. The next approval step is called.</td></tr><tr><td>Deny</td><td>The attestation case is denied approval in this approval step. The next approval step is called.</td></tr></table></td></tr>
</table>

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

Related Topics

- Granting or Denying an Attestation Case on page 98
- Editing Approval Levels on page 49

Aborting an Attestation Case on Timeout

Attestation instances can be automatically aborted once a specified time period has been exceeded. The abort takes place when either a single approval step or the entire approval process has exceeded the timeout.

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

- Enter the following data for the approval step.

Table 41: Approval Step Properties for Abort on Timeout

<table>
<tr><th>Property</th><th>Meaning</th></tr>
<tr><td>Timeout (working hours)Timeout behavior</td><td>Number of working hours to elapse after which the approval step is automatically granted or denied approval.
The approvers work time applies to the time calculation.
NOTE: Ensure that a state and/or county is entered into the employee`s master data for determining the correct working hours.</td></tr>
<tr><td>Action to be taken if the timeout expires.</td><td>Action, which is executed if the timeout expires.
<b>Table 42: Method for Abort on Timeout</b>
<table>
<tr><th>Method</th><th>Description</th></tr>
<tr><td>Abort</td><td>The approval, and therefore the entire attestation procedure, is aborted.</td></tr>
</table></td></tr>
</table>

To configure abort on timeout for the entire approval process

- Enter the following data for the approval workflow.

Table 43: Approval Step Properties for Abort on Timeout

Property	Meaning
System abort (days)	Number of days to elapse after which the approval workflow, and therefore the system automatically ends the entire attestation procedure.

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

Related Topics

- Aborting an Attestation Case on page 99
- Editing Approval Levels on page 49
- Setting Up Approval Workflows on page 48

Attestation through Chief Approval Team

Sometimes, approval decisions cannot be made for attestation cases because the attestor is not available or does not have access to One Identity Manager tools. To complete the attestation case, however, 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, abort attestations in special cases or to authorize 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.
> - Specify in the approval step, how many attestors must approve this approval step. This limit is not valid for the chief approval team. The approval step is considered approved once **one** member of the chief approval team has granted or denied approval for the attestation.

The chief approval team can approve attestations for all manual approval steps. The chief approvals are not permitted for approval steps with the approval procedures CD, EX and WC . If a member of the chief approval team is identified as a regular attestor for an approval step, he or she can only make an approval decision for this step as a regular attestor.

To add members to the chief approval team

1. Select the category **Attestation | Basic configuration data | Chief approval team**.
2. Select **Assign employees** in the task view.
3. Assign employee authorized to approve attestations in **Add assignments**.

   - OR -

   Remove the assignments of employee to chief approval team in **Remove assignments**.
4. Save the changes.

Related Topics

- Chief approval team on page 22

Attestation Sequence

Once attestation is automatically or manually started, the 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 menu item **Attestation runs | <attestation policy>**. 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 **Closed attestations**.

> NOTE: Attestation cases are edited in the Web Portal. For more detailed information, see the One Identity Manager 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: The 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 107.

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. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list. Select **Change master data** in the task view.
3. Enable the schedule entered in **Calculation schedule**.
    a. Select **Attestation | Basic configuration data | Schedules** in the navigation view.
    b. Select the schedule in the result list. Select **Change master data** in the task view.
    c. Set the option **Enabled**.
    d. Save the changes.

To start attestation for the selected objects

1. Select the category **Attestation | Attestation policies**.
2. Select the attestation policy in the result list. Select **Change master data** in the task view.
3. Select **Run attestation cases for single objects...** in the task view.

    This opens a separate window.
4. Set **Attestation** for every object you want to include in the attestation.
5. Click **Run**.

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

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

For more detailed information about configuring schedules, see the One Identity Manager Configuration Guide.

Detailed information about this topic

- General Master Data for Attestation Policies on page 25
- Schedules on page 17

Related Topics

- Running Attestation for Single Objects on page 32
- Finding Attestors on page 73

- Deleting Attestation Cases on page 92

Additional Tasks for Attestation Cases

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

The Attestation Case Overview

The overview form supplies you with the most important information about an attestation case. You can see here how long an attestation case is going to be processed depending on the processing time. The One Identity Manager does not stipulate which action 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. Select the category **Attestation | Attestation runs | <attestation policy> | Attestation runs | <year> | <month> | <day>** .
2. Select **Pending attestations** or **Completed attestations**.
3. Select an attestation case from the result list.
4. Select **Attestation case overview**.

Approval Sequence

You obtain the current status of the approval process for pending attestation cases. The approval sequence is show as soon as the DBQueue Processor has determined the attestor for the approval step. You can view the approval sequence, the result of each approval step and the attestor that has been found, in the approval workflow. If the approval procedure could not find an attestor, the attestation case is closed by the system.

To display the approval sequence of a pending attestation case

1. Select the category **Attestation | Attestation runs | <attestation policy> | Attestation runs | <year> | <month> | <day> | Pending attestations**.
2. Select the attestation case in the result list.
3. Select **Approval sequence**.

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

Table 44: 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. Select the category **Attestation | Attestation runs | <attestation policy> | Attestation runs | <year> | <month> | <day>** .
2. Select **Pending attestations** or **Completed attestations**.
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 45: 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 aborted. Case has been assigned to an extra attestor.

Color	Meaning
	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 aborted due to change of approver
Blue	Approver has rerouted approval Approval step has been automatically reset

Modifying Approval Workflows on Pending Attestation Cases

If the approval workflow for an unapproved attestation case changes, all previously effected approval workflows are reset. The attestation case goes through the approval process again.

Related Topics

- Finding Attestors on page 73

Close Attestation Cases for Deactivated Employees

Table 46: Configuration Parameter for Closing Pending Attestations

Configuration parameter	Effect
QER\Attestation\AutoCloseInactivePerson	If this configuration parameter is set, pending attestation cases for an employee are closed, when this employees is permanently deactivated.

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

- Set the configuration parameter "QER\Attestation\AutoCloseInactivePerson" in the Designer.

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 Master Data for Attestation Policies on page 25.

Deleting Attestation Cases

Table 47: Configuration Parameter for Logging Data Changes

Configuration parameter	Effect
Common\ProcessState\PropertyLog	When this configuration parameter is set, changes to individual values are logged and shown in the process view.

The table `AttestationCase` expands very quickly when attestation is performed regularly. To limit the number of attestation cases in the One Identity Manager, 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 detailed 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 detailed information about the archiving process, see the One Identity Manager Data Archiving Administration Guide.

Prerequisites

- The configuration parameter "Common\ProcessState\PropertyLog" is set.
- The attestation policy is enabled.

To delete attestation cases automatically

1. Set the option **Log changes when deleting** on at least three columns in the table `AttestationCase`.
    a. Start the Designer.
    b. Select the category **Database Schema | Tables | AttestationCase**.

   c. Select **Show table definition** in the task view.

      Opens the Schema Editor.

   d. Select a column in the Schema Editor.

   e. Select the **More** tab in the Schema Editor edit view.

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

   g. Repeat steps d) to F) for all columns to be recorded on deletion. These must be at least three.

   h. Click **Commit to database** in the toolbar and save the changes.

      These changes become effective the moment the DBQueue Processor has processed the tasks.

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

   a. Start the Designer**.**

   b. Select the category **Database Schema | Tables | AttestationHistory**.

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

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

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

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

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

   d. Enter a value larger than 0 in **Obsolete tasks limit**.

   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 this attestation policy.

Attestation cases are deleted once

- A new attestation is started for an attestation policy.

  – OR –

- An attestation policy is disabled.

The One Identity Manager tests how many closed attestation cases exists 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.

> NOTE: Closed attestation cases are are also deleted in the case of disabled attestation policies if the configuration parameter "Common\ProcessState\PropertyLog" is not set. In this case, the deleted attestation cases are not logged.

Related Topics

- General Master Data for Attestation Policies on page 25

Notifications in Attestation

Table 48: Configuration Parameter for Notifications

Configuration parameter	Meaning
QER\Attestation\DefaultSenderAddress	This configuration parameter contains the sender email address for automatically generated messages during attestation.

Different email notifications can be sent to attestors and other employees within an attestation case The notification procedure uses mail templates to create notifications. The mail text in a mail template is defined in several languages. This ensures that the language of the recipient is taken into account when the email is generated. Mail templates are supplied in the default installation with which you can configure the notification procedure.

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

To use notification in the request process

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

Related Topics

- Creating Custom Mail Templates for Notifications on page 34

Demanding Attestation

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

Prerequisite

- The configuration parameter "QER\Attestation\MailTemplateIdents\RequestApproverByCollection" is not set.

To set up the notification procedure

- Enter the following data for the approval step.

Table 49: Approval Step Properties for Notification

Property	Meaning
Mail template for demand	Select the template "Attestation - demand for approval (by mail)". TIP: If you allow approval by email, select the mail template "Attestation - demand for approval (by mail)".

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

Related Topics

- Scheduling Attestation Demands on page 96
- Attestation by Mail on page 103

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 work time applies to the time calculation.

Prerequisite

- The configuration parameter "QER\Attestation\MailTemplateIdents\RequestApproverByCollection" is not set.

To set up the notification procedure

- Enter the following data for the approval step.

Table 50: Approval Step Properties for Notification

Property	Meaning
Reminder interval (hours)	Number of working hours to elapse after which the attestor is notified by mail that there are still pending requests for attestation cases for attestation. NOTE: Ensure that a state and/or county is entered into the employee`s master data for determining the correct working hours.
Mail template reminder	Select the mail template "Attestation - remind approver". TIP: If you permit approval by email, select the mail template "Attestation - remind approver (by mail)".

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

Related Topics

- Scheduling Attestation Demands on page 96
- Attestation by Mail on page 103

Scheduling Attestation Demands

Table 51: Configuration Parameter for Scheduled Notifications

Configuration parameter	Meaning
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 demand" or "Mail template reminder" for single attestation cases can be entered to send an email for each request. If this configuration parameter is set, single mails are not sent.

Attestors can be regularly notified of attestation cases that are pending. Regular notifications replace single demands and attestation reminders, configured in the approval step.

To send notifications about pending attestations on a regular basis

1. Set the configuration parameter "QER\Attestation\MailTemplateIdents\RequestApproverByCollection" in the Designer.

   Notification with the mail template "Attestation - pending attestations for approver" is sent by default.

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

2. Configure and enable the schedule "Inform approver about pending attestations" in the Designer.

   For more detailed information, see the One Identity Manager Configuration Guide.

Reminding Attestors about an Attestation Object

Table 52: Configuration Parameter for Notifying Attestors about a Specific Attestation Object

Configuration Parameter	Meaning
QER\Attestation\MailTemplateIdents\RemindApproverByObject	This mail template is used for sending an email to an attestor who still has pending attestations for a specific attestation object.

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 send reminders to attestors of selected attestation objects.

To send notification about a specific attestation object

- Set the configuration parameter "QER\Attestation\MailTemplateIdents\RemindApproverByObject" in the Designer.

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

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

To send notifications user the Web Portal. For more detailed information, see the One Identity Manager Web Portal User Guide.

Granting or Denying an Attestation Case

When a 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. Enter the following data in the approval step when notification should immediately follow the approval decision of a single approval step:

Table 53: Approval Step Properties for Notification

Property	Meaning
Mail template on approval	Mail template for sending notification if an approval step is granted approval.
Mail template on denied	Mail template for sending notification if an approval step is denied approval.

- OR -

Enter the following data in the approval policy when notification should immediately follow completion of the approval procedure.

Table 54: Approval Policy Properties for Notification

Property	Meaning
Mail template on approval	Mail template for sending notification if an attestation case is granted approval.
Mail template on denied	Mail template for sending notification if an attestation case is denied approval.

Detailed information about this topic

- Creating Custom Mail Templates for Notifications on page 34
- Custom Notification Processes on page 40

Aborting an Attestation Case

Email notifications can be sent to other employees when an attestation case is aborted. 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 aborted.
2. Create company specific processes for notifications.
3. Enter the following data for the approval policy:

Table 55: Approval Policy Properties for Notification

Property	Meaning
Mail template on abort	Mail template for sending notification if an attestation case has aborted.

Detailed information about this topic

- Creating Custom Mail Templates for Notifications on page 34
- Custom Notification Processes on page 40

Attestation Case Escalation

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

To set up the notification procedure

- Enter the following data for the approval step.

Table 56: Properties of an Approval Step for Notification

Property	Meaning
Mail template Escalation	Select the mail template "Attestation - escalation".

Related Topics

- Escalating an Attestation Case on page 81

Delegating Attestation

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

- Enter the following data for the approval step.

Table 57: Approval Step Properties for Notification on Delegation

Property	Meaning
Mail template for delegation	Select the mail template "Attestation - delegated/additional approval". TIP: To allow approval by email, select the mail template "Attestation - delegated/additional approval (by mail)".

Related Topics

- Attestation by Mail on page 103

Approval Rejection

If an additional attestor or an employee refuses delegation of an attestor, the original attestor must be notified.

To set up the notification procedure

- Enter the following data for the approval step.

Table 58: Approval Step Properties for Notification on Rejection

Property	Meaning
Mail template for rejection	Select the mail template "Attestation - rejected approval". TIP: If you allow approval by email, select the mail template "Attestation - reject approval (by mail)".

Related Topics

- Attestation by Mail on page 103

Notifications with Questions

Table 59: Configuration Parameter for Notification of Approver Questions

Configuration Parameter	Meaning
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\AnswerToApprover	This mail template is used to send a notification with an answer to a question from an approver.

Employees can be notified when a question about an attestation is asked. The attestor can also be notified the moment the question is answered.

To notify an employee when an attestor asks a question

- Set the configuration parameter "QER\Attestation\MailTemplateIdents\QueryFromApprover" in the Designer.

  Notification with the mail template "Attestation - question" is sent by default.

To notify an attestor when an employee answers the question

- Set the configuration parameter "QER\Attestation\MailTemplateIdents\AnswerToApprover" in the Designer.

  Notification with the mail template "Attestation - answer" is sent by default.

TIP: Change the value of the configuration parameter in order to use custom mail templates for these mails.

Notifications from Additional Attestors

Table 60: Configuration Parameters for Notifying Attestors

Configuration Parameter	Meaning
QER\Attestation\MailTemplateIdents\InformAddingPerson	This mail template is used to notify attestors if the additional attestor has met an approval decision.
QER\Attestation\MailTemplateIdents\InformDelegatingPerson	This mail template is used to notify attestors if an approval decision has

Configuration Parameter	Meaning
	been made about their delegated step.

The original attestor can be notified when an additional attestor or 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 notification when the additional attestor approves or denies the attestation

- Set the configuration parameter "QER\Attestation\MailTemplateIdents\InformAddingPerson" in the Designer.

  By default, notification is sent using the template "Attestation - approval of added step".

To send notification when the employee who was delegated an approval approves or denies the request

- Set the configuration parameter "QER\Attestation\MailTemplateIdents\InformDelegatingPerson" in the Designer.

  By default, notification is sent using the template "Attestation - approval of delegated step".

ℹ TIP: Change the value of the configuration parameter in order to use custom mail templates for these mails.

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

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

Related Topics

- Creating Custom Mail Templates for Notifications on page 34

Attestation by Mail

Table 61: Configuration Parameters for Approval by Mail

Configuration Parameter	Meaning
QER\Attestation\MailApproval\Inbox	This Microsoft Exchange mailbox is used for "Approval by mail" processes.
QER\Attestation\MailApproval\Account	Name of user account for authentication of "Approval by mail" mailbox.
QER\Attestation\MailApproval\Domain	Domain of user account for authentication of "Approval by mail" mailbox.
QER\Attestation\MailApproval\Password	Password of user account for authentication of "Approval by mail" mailbox.
QER\Attestation\MailTemplateIdents\ITShopApproval	Mail template used for requests made through "Approval by mail".
QER\Attestation\MailApproval\DeleteMode	Specifies the way emails are deleted from the inbox.

You can set up attestation by mail to provide an option for attestors, who are temporarily unable to access One Identity Manager tools, to make attestation case decisions. In this way, attestors are notified by email when an attestation case is pending approval. Attestors 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 Microsoft Exchange mailbox. The One Identity Manager checks this mailbox regularly, evaluates the incoming emails and updates the status of the attestation case correspondingly.

IMPORTANT: An attestation is not possible by email, if multi-factor authorization is configured for the attestation policy. Attestation emails for such requests produce an error message.

Prerequisites

1. The Microsoft Exchange system is configured with
   - Microsoft Exchange Client Access Server version 2007, Service Pack 1 or later
   - Microsoft Exchange Web Service .NET API Version 1.2.1, 32 Bit

2. The user account used by One Identity Manager to register with Microsoft Exchange requires full access to the mailbox given in the configuration parameter "QER\Attestation\MailApprovalInbox".
3. The configuration parameter "QER\Attestation\MailTemplateIdents\RequestApproverByCollection" is not set.

To set up attestation by email

1. Set the configuration parameter "QER\Attestation\MailApprovalInbox" in the Designer and enter the mailbox to which to send the approval mails.
2. Set up mailbox access.
   a. By default, One Identity Manager uses the One Identity Manager Service user account to register with Microsoft Exchange and to access the mailbox.

      – OR –

   b. You enter a separate user account for registering on the Microsoft Exchange Server for mailbox access. Enabled the following configuration parameters to do this.

      Table 62: Configuration Parameters for Logging onto a Microsoft Exchange Server

Configuration Parameter	Meaning
QER\Attestation\MailApproval\Account	Name of the user account.
QER\Attestation\MailApproval\Domain	User account's domain.
QER\Attestation\MailApproval\Password	User account's password.

3. Set the configuration parameter "QER\Attestation\MailTemplateIdents\ITShopApproval" in the Designer.

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

   > TIP: Change the value of the configuration parameter in order to use custom mail templates for attestation mails. Customize the script `VI_MailApproval_ProcessMail` in this case, as well.

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

   Table 63: Mail Template for Approval by Mail

Property	Main Template
Mail template for demand	Attestation - approval required (by mail)
Mail template reminder	Attestation - remind approver (by mail)
Mail template for delegation	Attestation -delegated/additional approval (by mail)

Property	Main Template
Mail template for rejection	Attestation - reject approval (by mail)

5. Enable the schedule "Processes attestation mail approvals" in the Designer.

   Based on this schedule, the One Identity Manager regularly checks the mailbox after each for new attestation mail. Based on this schedule, the regularly checks the mailbox 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

- Set the configuration parameter "QER\Attestation\MailApproval\DeleteMode in the Designer and select the following values.

Table 64: Cleaning up a Mailbox

Value	Method
`HardDelete`	Processed emails are deleted immediately
`MoveToDeletedItems`	Processed emails are moved to the "Deleted objects" folder in the mailbox.
`SoftDelete`	Processed emails are moved to the Active Directory trash but can be restored if necessary.

> NOTE: If you apply the method `MoveToDeletedItems` or `SoftDelete` you should empty the folder "Deleted objects" or the Active Directory trash at regular intervals.

Related Topics

- Modifying an Attestation Mail on page 106
- Creating Custom Mail Templates for Notifications on page 34
- Demanding Attestation on page 95
- Reminding Attestors on page 95
- Delegating Attestation on page 100
- Approval Rejection on page 100
- Setting up Multi-Factor Authentication for Attestation on page 75

Modifying an Attestation Mail

Table 65: Configuration Parameters for Approval by Mail

Configuration Parameter	Meaning
QER\Attestation\MailApproval\ExchangeURI	Specifies the Exchange Web Service URL. AutoDiscover mode is used to find the URL if it is not given.

The schedule "Processes attestation mail approvals" starts the process `VI_ITShop_Process Approval Inbox`. This process runs the script `VI_MailApproval_ProcessInBox`, which searches the mailbox for new attestation mails and updates the attestation cases in the One Identity Manager database. Then the contents of the attestation mail are processed.

> NOTE: The validity of the email certificate is checked with the script `VID_ValidateCertificate`. You can customize this script to suit your security requirements. Take into account that this script is also used for IT Shop request approvals by mail.
>
> 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 script `VI_MailApproval_ProcessInBox` finds the Exchange Web Service URL which 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 configuration parameter "QER\Attestation\MailApproval\ExchangeURI".

Attestation mails are processed with the script `VI_MailApproval_ProcessMail`. The script finds the matching approval, sets the option **Approved** and stores the reason for the approval decision with the attestation case. The attestor is found through the sender address. Then the attestation mail is removed from the mailbox depending on the selected clean up method.

> NOTE: If you use a custom mail template for an attestation mail, check the script and modify it as required. Take into account that this script is also used for attestations by mail.

Default Attestation and Withdrawal of Entitlements

Table 66: Configuration Parameter for Withdrawing Entitlements

Configuration parameter	Meaning
QER\Attestation\AutoRemovalScope	General configuration parameter for defining automatic withdrawal of memberships/assignments if attestation approval is not granted.

The One Identity Manager provide various default attestation procedures for different data situations and default attestation procedures.

Data Situations for Default Attestation

- System entitlements owned by an employee
- System entitlements assigned to system entitlements
- Business and application role memberships
- System roles assigned to en employee
- Employee master data for a new One Identity Manager user
- Employee master data for an existing One Identity Manager user

The attestation polices required for attesting employee master data are also supplied by default. You can also use the default supplied attestation policies without modifying them. For information about prerequisites and the attestation sequence for employee data, see User Attestation and Recertification.

You can set up attestation policies easily in 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 the One Identity Manager following the attestation.

To remove denied permissions automatically

- Set the configuration parameter "QER\Attestation\AutoRemovalScope" in the Designer.

> ℹ 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 approval procedure "EX" in the default approval workflows.

Attestation Sequence with Subsequence Removal of a Denied Entitlement

1. Attestation with one of the following attestation procedures is carried out.
    - Attestation of system entitlement memberships
    - Attestation of system entitlement assignments to system entitlements
    - Attestation of system role memberships
    - Attestation of application role memberships
    - Attestation of business role memberships
2. The attestator denies attestation. The approval step is not granted approval and approval is passed on the next approval level with the approval procedure "EX".
3. The approval step triggers the event `AUTOREMOVE`. This runs the process `VI_Attestation_AttestationCase_AutoRemoveMembership`.
4. The process runs the script `VI_AttestationCase_RemoveMembership`. 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

- System Entitlements Attestation on page 109
- System Role Attestation on page 111
- Application Role Attestation on page 112
- Business Role Attestation on page 113

System Entitlements Attestation

Installed Module: Target System Base Module

Table 67: Configuration Parameters for Removing System Entitlements

Configuration parameter	Meaning
QER\Attestation\AutoRemovalScope\GroupMembership	Determines default behavior for automatic removing of united namespace system entitlements if attestation approval is not granted.
QER\Attestation\AutoRemovalScope\UNSGroupInUNSGroup	Specifies the default behavior for removing assignments from system entitlements to system entitlement is attestation approval is not granted.

When you use the default attestation policy "System entitlement membership attestation" or have set up attestation policies with the default attestation procedure "System entitlement memberships", you can configure automatic removal of system entitlements through the configuration parameter "QER\Attestation\AutoRemovalScope\GroupMembership". After attestation approval has been denied, the One Identity Manager checks which type of assignment was used for the user account to become a member in the system entitlement.

Table 68: Effect of Configuration Parameters when Attestation Denied

Configuration parameter		
	Meaning	Advice
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 the employee obtained through this role.

Configuration parameter		
	Meaning	Advice
QER\Attestation\AutoRemovalScope\GroupMembership\RemoveRequestedRole		
	If membership in the system entitlement was inherited through a requested role, the role is canceled.	This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\GroupMembership\RemoveDelegatedRole		
	If membership in the system entitlement was inherited through role delegation, delegation of the role is ended.	This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\GroupMembership\RemoveRequested		
	If membership in the system entitlements was inherited through a the IT Shop, it is canceled.	
QER\Attestation\AutoRemovalScope\GroupMembership\RemoveSystemRole		
	System roles with system entitlements are withdrawn from the employee.	This removes all indirect assignments the employee obtained through this system role. NOTE: This configuration parameter is only available if the System Roles Module is installed.
QER\Attestation\AutoRemovalScope\GroupMembership\RemoveDirectRole		
	The system entitlement assignment to hierarchical roles is removed.	This removes the system entitlement assignment to all user accounts whose associated employees are members of these roles. IMPORTANT: Employees whose attestation has been approved can lose the system entitlement through this. Check the side-effects of this configuration parameter in your situation before you set it.

When you use the default attestation policy "System entitlement assignment membership attestation" or have set up attestation policies with the default attestation procedure "System entitlement assignment membership attestation", you can configure automatic removal of system entitlements through the configuration parameter "QER\Attestation\AutoRemovalScope\UNSGroupInUNSGroup".

Table 69: Effect of Configuration Parameters when Attestation Denied

Configuration parameter	Meaning
QER\Attestation\AutoRemovalScope\UNSGroupInUNSGroup\RemoveDirect	Assignment of the system entitlement to a system entitlement,is removed.

System Role Attestation

Installed Module: System Roles Module

Table 70: Configuration Parameters for Removing System Roles

Configuration parameter	Meaning
QER\Attestation\AutoRemovalScope\ESetAssignment	Determines default behavior for automatic removal of system role memberships if attestation approval is not granted.

When you use the default attestation policy "Attestation of system role membership" or have set up attestation policies with the default attestation procedure "Attestation of system role membership", you can configure automatic removal of system roles through the configuration parameter "QER\Attestation\AutoRemovalScope\ESetAssignment". After attestation approval has been denied, the One Identity Manager checks which type of assignment was used for the user account to become a member in the system role.

Table 71: Effect of Configuration Parameters when Attestation Denied

Configuration parameter		
	Meaning	Advice
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveDirect		
	Direct membership in the system role is removed.	This removes all indirect assignments the employee obtained through this 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 the employee obtained through this role.

Configuration parameter		
	Meaning	**Advice**
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveRequestedRole		
	If the system was inherited through a requested role, the role is canceled.	This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveDelegatedRole		
	If the system role was inherited through a delegated role, the role is ended.	This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveRequested		
	If the system role was requested through the IT Shop, it is removed.	This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveDirectRole		
	The system role assignment to hierarchical roles is removed.	This removes the system entitlement assignment to all user accounts whose associated employees are members of these roles. IMPORTANT: Employees whose attestation has been approved can lose the system role through this. Check the side-effects of this configuration parameter in your situation before you set it.

Application Role Attestation

Table 72: Configuration Parameters for Removing Application Roles

Configuration parameter	Meaning
QER\Attestation\AutoRemovalScope\AERoleMembership	Determines default behavior for automatic removal of application role memberships if attestation approval is not granted.

When you use the default attestation policy "Attestation of application role membership" or have set up attestation policies with the default attestation procedure "Attestation of application role membership", you can configure automatic removal of application roles through the configuration parameter "QER\Attestation\AutoRemovalScope\AERoleMembership". After attestation approval has been denied, the One Identity Manager checks which type of assignment was used for the user account to become a member in the application role.

Table 73: Effect of Configuration Parameters when Attestation Denied

Configuration Parameter	Meaning	Advice
QER\Attestation\AutoRemovalScope\AERoleMembership\RemoveDirectRole	The employee's secondary membership is removed from the application role.	This removes all indirect assignments the employee obtained through this application role. Membership in dynamic roles is not removed by this.
QER\Attestation\AutoRemovalScope\AERoleMembership\RemoveRequestedRole	If the employee requested the application role through the IT Shop, it is canceled.	This removes all indirect assignments the employee obtained through this application role.
QER\Attestation\AutoRemovalScope\AERoleMembership\RemoveDelegatedRole	If the application role was delegated to the employee, delegation is ended.	This removes all indirect assignments the employee obtained through this application role.

Business Role Attestation

Installed Module:	Business Roles Module

Table 74: Configuration Parameters for Removing Application Roles

Configuration parameter	Meaning
QER\Attestation\AutoRemovalScope\RoleMembership	Determines default behavior for automatic removal of business role memberships if attestation approval is not granted.

When you use the default attestation policy "Attestation of business role membership" have set up attestation policies with the default attestation procedure "Attestation of business role membership", you can configure automatic removal of business roles through the configuration parameter "QER\Attestation\AutoRemovalScope\RoleMembership". After attestation approval has been denied, the One Identity Manager checks which type of assignment was used for the user account to become a member in the business role.

Table 75: Effect of Configuration Parameters when Attestation Denied

Configuration parameter	
Meaning	**Advice**
QER\Attestation\AutoRemovalScope\RoleMembership\RemoveDirectRole	
The employee's secondary membership in the business role is removed.	This removes all indirect assignments the employee obtained 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, it is canceled.	This removes all indirect assignments the employee obtained through this business role.
QER\Attestation\AutoRemovalScope\RoleMembership\RemoveDelegatedRole	
If the business role was delegated to the employee, delegation is ended.	This removes all indirect assignments the employee obtained through this business role.

User Attestation and Recertification

Table 76: Configuration Parameters for Attesting New One Identity Manager Users

Configuration parameter	Meaning
QER\Attestation\UserApproval	Supports attestation procedures for regularly checking and confirming One Identity Manager users through their Manager.

Use the One Identity Manager attestation functionality to regularly check and authorize employees' master data, target system entitlement and assignments. Furthermore, the One Identity Manager provides default procedures for quickly attesting and certifying the master 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, should be provided with temporary access to the One Identity Manager. Regular recertification can be run through scheduled tasks.

In the context of an attestation, a manager can check and update the master data for the user to be certified, if necessary. Use the Web Portal for attestation.

To enable use of attestation and recertification functions for new users

1. Set the configuration parameter "QER\Attestation\UserApproval" in the Designer.
2. Assign at least one employee to the application role **Identity Management | Employees | Administrators**.

Related Topics

- One Identity Manager Application Roles Administration Guide
- One Identity Manager Web Portal User Guide
- One Identity Manager Configuration Guide

Users for Attestation and Recertification

The following user are involved in attestation and recertification of employees.

Table 77: User

User	Task
Employee administrators	Employee administrators must be assigned to the application role **Identity Management | Employees| Administrators**. Users with this application role: • Can edit master data for all employees • Can assign a manager. • Can assign company resources to employees. • Check and authorize employee master data. • Create and edit risk index functions. • Edit password policies for employee passwords
Managers	• Check employee master data of the user to be certified. • Update employee master data as required. • Assign another manager if required. • Attests the master data.
Administrators for attestation cases	Administrators must be assigned to the application role **Identity & Access Governance | Attestation | Administrators**. 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 master data,

Attesting New Users

Attestation of new users is divided into 3 use cases by the One Identity Manager:

1. Adding a new user by logging into the Web Portal
2. Adding New Employees in the Manager
3. Adding a new employee by importing employee master data

The result of attestation is the same in all three cases.

- Certified, enabled employees that can access all entitlements in the One Identity Manager assigned to them and the connected target systems.

  Company resources are inherited. Account definitions are assigned.

  - OR -

- Denied and permanently deactivated employees.

  Disable employees cannot log onto 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.

Adding New Users in Web Portal

New users can register on the Web Portal home page. These users can log into the One Identity Manager once the manager in charge of the employee’s master data has completed attestation.

Attestation Sequence

1. The new user enters his or her own master data in the Web Portal.

   A new employee object is added to the One Identity Manager database with the properties:

   Table 78: Properties of New Employee

Property	Value
Certification status	New
Permanently disabled	Enabled
No inheritance	Enabled

2. Attestation is started automatically.

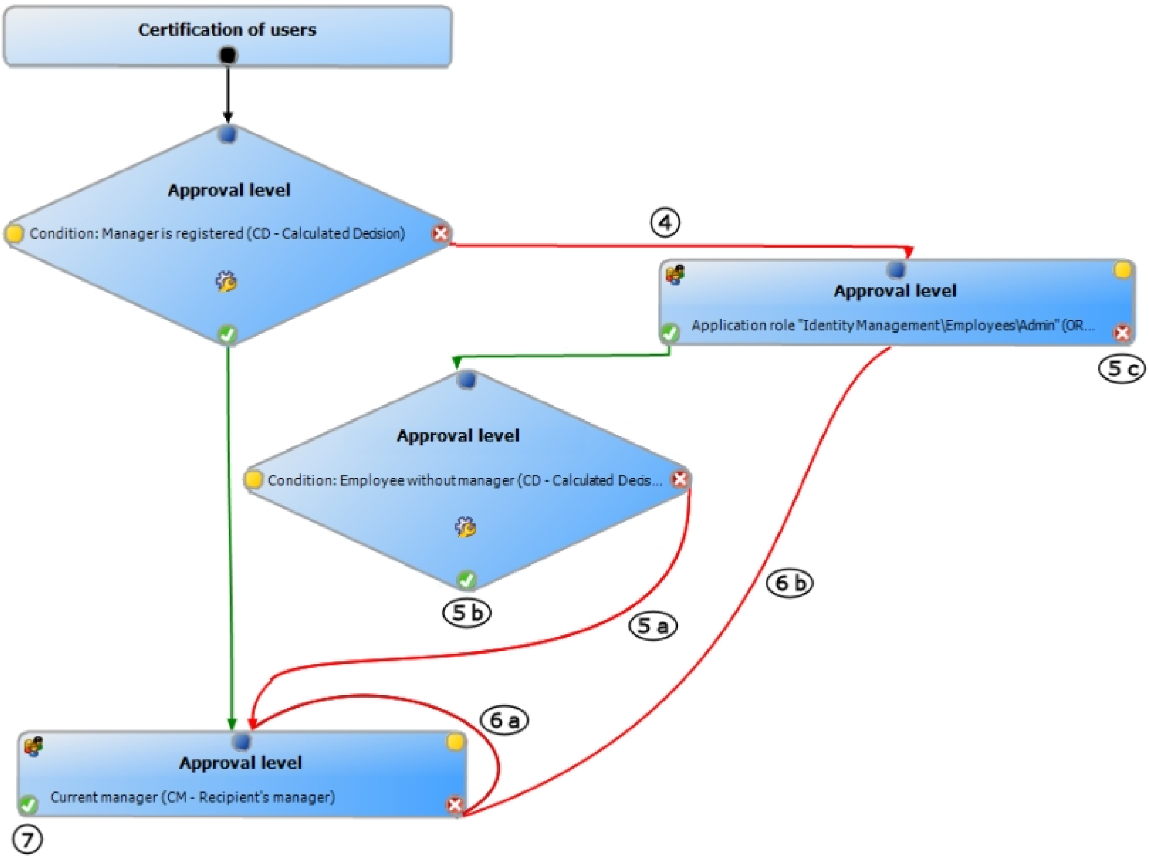
Attestation policy used:	"Certification of new users"

   NOTE: Attestation is only started automatically if the configuration parameter "QER\Attestation\UserApproval" is set. Otherwise the new user remains disabled permanently until the manager in charge of the employee’s master data changes it manually.

3. Attestors are found.

Effective approval policy:	"Certification of users"

Figure 4: Approval Workflow "Certification of Users" Adding in Web Portal


Certification of users
Approval level
Condition: Manager is registered (CD - Calculated Decision)
4
Approval level
Application role "Identity Management\Employees\Admin" (OR...
5 c
Approval level
Condition: Employee without manager (CD - Calculated Decis...
5 b
5 a
6 b
6 a
Approval level
Current manager (CM - Recipient's manager)
7

4. When a new user is added to the Web Portal, there is no manager assigned to them. Therefore, the process is passed on to One Identity Manager users with the application role **Identity Management | Employees | Administrators** (called "employee administrators" in the following) for approval.
5. An employee administrator checks your master data and also assigns a manager to you.
    a. The employee administrator assigns a manager and approves attestation. The attestation case is assigned to the manager for approval.
    b. 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 79: Properties of an Employee with Approved Attestation

Property	Value	Explanation
Certification status	Certified	
Permanently disabled	Disabled	The user can log on to the Web Portal.
No inheritance	Disabled	Company resource are inherited.

c. If an employee administrator denies attestation approval, the attestation case is closed. Your employee properties are updated in the database.

Table 80: Properties of an Employee with Denied Attestation

Property	Value	Explanation
Certification status	Denied	
Permanently disabled	Enabled	The user can **not** log in to the Web Portal.
No inheritance	Enabled	Company resources are not inherited. User accounts are not created automatically.

6. The manager can deny attestation approval if they are not the manager in charge of the employee.
   a. The manager can assign another person as manager. The attestation case is immediately assigned to this manager.
   b. If the manager does not know who is your manager, approval is returned to the employee administrators. These can either:
      - Assign another manager (5 a)
      - Not assign a new manager and approve attestation (5 b)
      - Deny attestation approval (5 c).
7. If the manager approves attestation, the attestation case is closed. Your employee properties are updated in the database.

Table 81: Properties of an Employee with Approved Attestation

Property	Value	Explanation
Certification status	Certified	
Permanently disabled	Disabled	The user can log on to the Web Portal.
No inheritance	Disabled	Company resource 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.

Employee administrators and managers use the Web Portal for attestation.

Related Topics

- One Identity Manager Web Portal User Guide

Adding New Employees in the One Identity Manager

Table 82: Configuration Parameters for Attesting New One Identity Manager Users

Configuration parameter	Meaning
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.

You can also attest new users if employees are added with the Manager. You specify which behavior you require 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.

This allows new users to be attested through the assigned manager.

- Set the configuration parameter "QER\Attestation\UserApproval\InitialApprovalState" to "1" in the Designer.

  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.

Attestation Sequence

1. Enter the master data of the new users in the category **Employees | Employees** and assign a manager.

   The certification status corresponds to the value of the configuration parameter "QER\Attestation\UserApproval\InitialApprovalState". If the configuration parameter has the value "1", certification status is set to "New".

   The employee is enabled by default and can log in immediately to One Identity Manager.

   - If new users are allowed to log in to One Identity Manager for the first time, if their master data has been attested, run the task **Disable employee permanently**.

2. Once the employee master data has been saved, attestation starts.

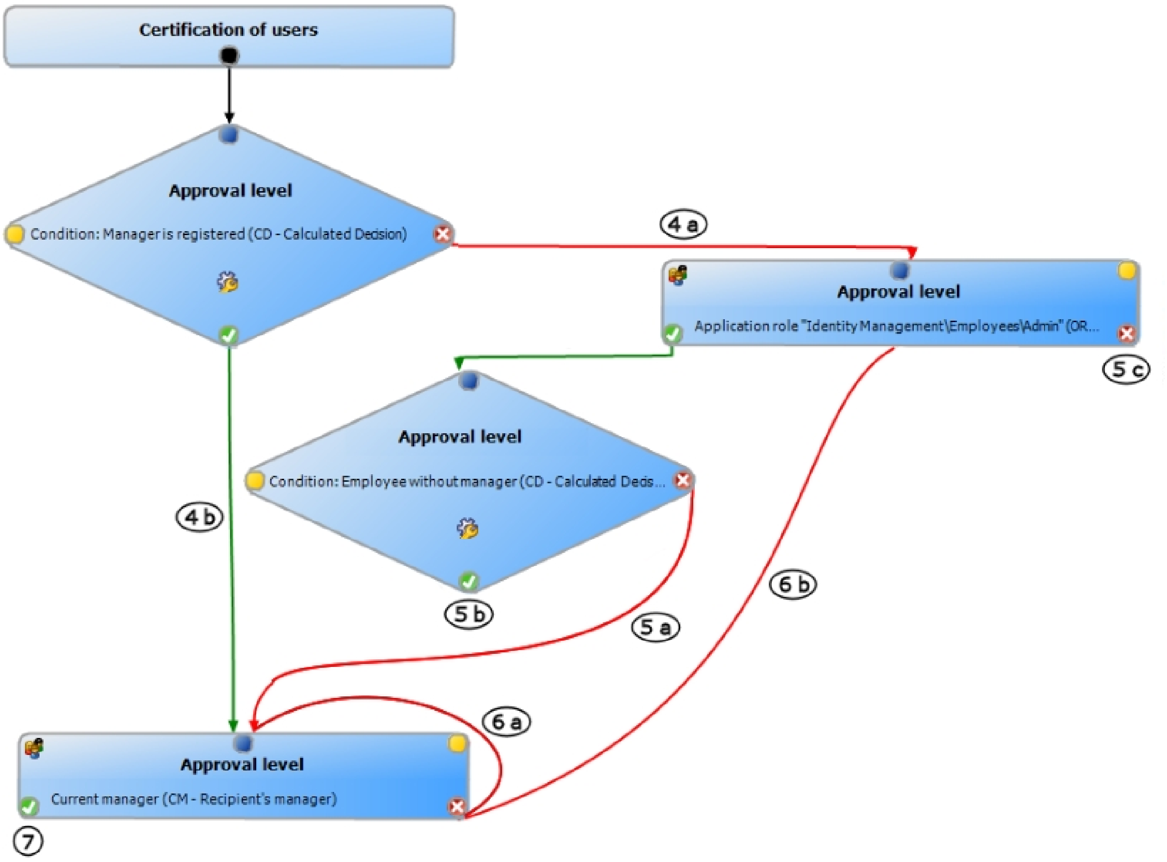
   Attestation policy used: "Certification of new users"

3. Attestors are found.

   Effective approval policy: "Certification of users"

The attestation takes place as described below. Employee administrators and managers use the Web Portal for attestation.

Figure 5: Approval Workflow "Certification of Users" Adding in Manager


Certification of users
Approval level
Condition: Manager is registered (CD - Calculated Decision)
4 a
Approval level
Application role "Identity Management\Employees\Admin" (OR...
5 c
Approval level
Condition: Employee without manager (CD - Calculated Decis...
4 b
6 b
5 b
5 a
6 a
Approval level
Current manager (CM - Recipient's manager)
7

4. One Identity Manager checks whether you have assigned a manager to the employee.
   a. If you have assigned a manager to the employee, the case is immediately passed on to them for approval.
   b. If there is no manager assigned to the employee the case is allocated to the employee administrators for approval.
5. An employee administrator checks your master data and also assigns a manager to you.
   a. The employee administrator assigns a manager and approves attestation. The attestation case is assigned to the manager for approval.
   b. 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 83: Properties of an Employee with Approved Attestation

Property	Value	Explanation
Certification status	Certified	
Permanently disabled	Disabled	
No inheritance	Disabled	Company resources are inherited.

c. If an employee administrator denies attestation approval, the attestation case is closed. Your employee properties are updated in the database.

Table 84: Properties of an Employee with Denied Attestation

Property	Value	Explanation
Certification status	Denied	
Permanently disabled	Enabled	
No inheritance	Enabled	Company resources are not inherited. User accounts are not created automatically.

6. The manager can deny attestation approval if they are not the manager in charge of the employee.
    a. The manager can assign another person as manager. The attestation case is immediately assigned to this manager.
    b. If the manager does not know who is your manager, approval is returned to the employee administrators. These can either:
        - Assign another manager (5 a)
        - Not assign a new manager and approve attestation (5 b)
        - Deny attestation approval (5 c).
7. If the manager approves attestation, the attestation case is closed. Your employee properties are updated in the database.

Table 85: Properties of an Employee with Approved Attestation

Property	Value	Explanation
Certification status	Certified	
Permanently disabled	Disabled	
No inheritance	Disabled	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

- One Identity Manager Web Portal User Guide

Importing New Employee Master Data

Table 86: Configuration Parameters for Attesting New One Identity Manager Users

Configuration parameter	Meaning
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.

You can request attestation of new employees if the master data is imported from other system in the One Identity Manager database. To ensure that new employees are automatically attested, the employee's certification status must be set to "new" (`Person.ApprovalState` = '1'). There are two possible ways to do this:

1. The configuration parameter "QER\Attestation\UserApproval\InitialApprovalState" is evaluated to find the certification status. If the configuration parameter has the value "1", certification status is set to "New".

   Prerequisite: The import does not alter the property `Person.ApprovalState`.

   NOTE: The configuration parameter "QER\Attestation\UserApproval\InitialApprovalState" is set to "0" by default. This gives each new employee the certification status "certified". Automatic attestation is not carried out.

   If you want employees to be attested immediately, change the value of the configuration parameter to "1".

2. The import sets the property `Person.ApprovalState` explicitly.

   - Import sets `ApprovalState` = '1' ("new").

     Employees are automatically attested by their manager.

   - Import sets `ApprovalState` = '0' ("certified").

     Imported employee master data has already been authorized. It should not be attested again.

- Import sets `ApprovalState` = '3' ("denied").

  Employees are disabled permanently and not attested.

Attestation of new users is triggered when:

- The configuration parameter "QER\Attestation\UserApproval" is set
- New employee master data is imported into the One Identity Manager database
- Certification status for new employees is set to "new"
- No **data source import** is stored with the employee.

Attestation is the same as described in Adding New Employees in the One Identity Manager, steps 4 to 7. The attestation policy "Certification of new users" is run.

Scheduled Attestation

Users are also attested when the certification status for the respective employee in the database is set to "new" at a later data (manually or through import). The schedule "daily" is assigned to the attestation policy "Certification of new users" for this. Attestation of new users is started when the time set in the schedule is reached. Then all employees are determined that have the certification status "new" and are not already pending attestation.

You can assign a custom schedule to the attestation policy if required.

Detailed information about this topic

- Schedules on page 17

Limiting Attestation Objects for Certification

> IMPORTANT: In order to customize default the attestation policy "Certification of new users" 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.

- Attestation policy "Certification of new users"
- Process "VI_Attestation_Person_new_AttestationCase_for_Certification"

- Process "VI_Attestation_AttestationCase_Person_Approval_Granted"
- Process "VI_Attestation_AttestationCase_Person_Approval_Dismissed"

> IMPORTANT: In order for attestation to run correctly in the Web Portal, the default attestation procedure "Certification of users" and the default approval policy "Certification of users" must be assigned to the attestation policy.
>
> The default attestation procedure, the default approval policy and the default approval workflow "Certification of users" must not be changed.

To customize default attestation of new users

1. Copy the attestation policy "Certification of users" and customize it.

   Table 87: Attestation Policy Properties

Property	Value
Attestation procedure	"User certification"
Approval policies	"User certification"
Edit connection...	The default condition must be copied without modification so that the correct attestation object is selected. You can customize the condition to suit your requirements.

2. Create a copy of the process `VI_Attestation_Person_new_AttestationCase_for_Certification` from the base object `Person` in the Designer and customize it.

   Table 88: Process Properties with Modifications

Process Step	Parameter	Modification
`Create attestation instance`	`WhereClause`	Replace the UID of the attestation policy "Certification of new users" with the UID of the new attestation policy.

3. Copy the process `VI_Attestation_AttestationCase_Person_Approval_Granted` of the base object `AttestationCase` in the Designer and customize the copy.

   Table 89: Process Properties with Modifications

Process Step	Modification
Pre-script for generating	Replace the UID of the attestation policy "Certification of new users" with the UID of the new attestation policy.

Process Step	Modification
Generating condition:	

4. Copy the process `VI_Attestation_AttestationCase_Person_Approval_Dismissed` of the base object `AttestationCase` in the Designer and customize the copy.

Table 90: Process Properties with Modifications

Process Step	Modification
Pre-script for generating	Replace the UID of the attestation policy "Certification of new users" with the UID of the new attestation policy.
Generating condition:	

Detailed information about this topic

- General Master Data for Attestation Policies on page 25
- Creating a Copy on page 33
- One Identity Manager Configuration Guide

Recertifying Existing Users

> IMPORTANT: It is possible, that as a result of recertification, access to connected target systems is denied to One Identity Manager users. You can configure this behavior to meet your company’s requirements. Read the following section thoroughly before you use the recertification function.

The One Identity Manager provides an attestation policy for performing cyclical attestation of existing users allowing companies to regularly test and authorize employee master 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. The 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, enabled employees that can access all entitlements in the One Identity Manager assigned to them and the connected target systems.

  Company resources are inherited. Account definitions are assigned.

- OR -

- Denied and permanently deactivated employees.

  Disable employees cannot log onto 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. Set the configuration parameter "QER\Attestation\UserApproval" in the Designer.
2. Create a schedule and assign it to the attestation policy "Recertification of users". By doing this, you replace the schedule assigned by default.
   - Enable the schedule.
3. Assign at least one employee to the application role **Identity Management | Employees | Administrators**.

   All employees with this application role can assign a manager to the employee being attested during the attestation process.

Related Topics

- General Master Data for Attestation Policies on page 25
- Schedules on page 17
- One Identity Manager Application Roles Administration Guide

The Recertification Sequence

The One Identity Manager uses the same method for recertification as for certification of new users. User recertification is triggered when:

- The configuration parameter "QER\Attestation\UserApproval" is set
- No **data source import** is stored with the employee or the **data source import** is not "Oracle"
- The point in time reserved for attestation in the attestation policy "Recertification of user" has been reached.

Employees are attested through their managers. If an employee is not assigned a manager, the employee administrator assigns an initial manager for them. Employee administrators and managers use the Web Portal for attestation.

NOTE: Only employee administrators can ultimately deny recertification. If a manager denies recertification, the case is returned to the employee administrators for approval in any case.

Attestation is the same as described in Adding New Employees in the One Identity Manager, steps 4 to 7. The attestors are determined using the approval policy "Certification of users".

Related Topics

- One Identity Manager Web Portal User Guide

Limiting Attestation Objects for Recertification

IMPORTANT: In order to customize default the attestation policy "Recertification of users" you must make changes to One Identity Manager objects. Always use a custom copy of the respective object to make changes.

All employees in the saved in the database are recertified using the attestation policy "Recertification of users" supplied in the 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.

- Attestation policy "Recertification of users"
- Process `VI_Attestation_AttestationCase_Person_Approval_Granted`
- Process `VI_Attestation_AttestationCase_Person_Approval_Dismissed`

IMPORTANT: In order for recertification to run correctly in the Web Portal, the default attestation procedure "Certification of users" and the default approval policy "Certification of users" must be assigned to the attestation policy.

The default attestation procedure, the default approval policy and the default approval workflow "Certification of users" must not be changed.

To customize default recertification of users

1. Copy the attestation policy "Recertification of users" and customize it.

   Table 91: Attestation Policy Properties

Property	Value
Attestation procedure	"User certification"
Approval policies	"User certification"
Edit connection...	The default condition must be copied without modification so that the correct attestation object is selected. You can customize the condition to suit your requirements.

2. Copy the process `VI_Attestation_AttestationCase_Person_Approval_Granted` of the base object `AttestationCase` in the Designer and customize the copy.

   Table 92: Process Properties with Modifications

Process property	Modification
Generating pre-script	Replace the UID of the attestation policy "Certification of new users" with the UID of the new attestation policy.
Generating condition:	

3. Copy the process `VI_Attestation_AttestationCase_Person_Approval_Dismissed` of the base object `AttestationCase` in the Designer and customize the copy.

   Table 93: Process Properties with Modifications

Process property	Modification
Generating pre-script	Replace the UID of the attestation policy "Certification of new users" with the UID of the new attestation policy.
Generating condition:	

Detailed information about this topic

- General Master Data for Attestation Policies on page 25
- Creating a Copy on page 33
- One Identity Manager Configuration Guide

Mitigating Controls

Table 94: Configuration Parameter for Risk Assessment

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

Violation of regulatory requirements can harbor different risks for companies. To evaluate these risks, you can apply risk indexes to compliance rules and company policies. These risk indexes provide information about the risk involved for the company in violating the respective rule functionpolicy. 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

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

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

General Master Data for a Mitigating Control

To edit mitigating controls

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

   - OR -

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

Enter the following master data for mitigating controls.

Table 95: General Master Data for a Mitigating Control

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

Additional Tasks for Mitigating Controls

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

The Mitigating Controls Overview

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

To obtain an overview of a mitigating control

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

Assigning Attestation Policies

Use this task to specify for which attestation policies the mitigating control is valid.

To assign attestation policies to mitigating controls

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

   - OR -

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

Calculating Mitigation

The significance reduction of a mitigating control supplies the value by which to reduce an attestation's risk index if the control is implemented. One Identity Manager calculates a reduced risk index based on the risk index and the significance reduction. One Identity Manager supplies default functions for calculating reduced risk indexes. These functions cannot be edited with One Identity Manager tools.

The reduced risk index is calculated from the attestation 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.

Appendix: 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 96: 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.
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\AutoCloseInactivePerson	If this configuration parameter is set, pending attestation cases for an employee are closed, when this employees is permanently deactivated.
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\	If this configuration parameter is set, ends the application role delegation if attestation approval

Configuration parameter	Description
RemoveDelegatedRole	is not granted.
QER\Attestation\AutoRemovalScope\AERoleMembership\RemoveDirectRole	If this configuration parameter is set, employee membership in the application role will be removed if attestation approval is not granted.
QER\Attestation\AutoRemovalScope\AERoleMembership\RemoveRequestedRole	If this configuration parameter is set, the requested application role membership is canceled 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.
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveDelegatedRole	If this configuration parameter is set, ends the role delegation through which the employee obtained the system role if attestation approval is not granted. This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveDirect	If this configuration parameter is set, direct user account membership in the system role will be removed if attestation approval is not granted. This removes all indirect assignments the employee obtained through the system role.
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveDirectRole	If this configuration parameter is set, the system role assignment to roles (organizations and business roles) is removed if attestation approval is not granted. This removes the system entitlement assignment to all user accounts whose associated employees are members of these roles. IMPORTANT: Employees whose attestation has been approved can lose the system role through this.
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 if attestation approval is not granted. This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveRequested	If this configuration parameter is set, the requested system role is canceled if attestation

Configuration parameter	Description
	approval is not granted. This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\ESetAssignment\RemoveRequestedRole	If this configuration parameter is set, the requested role through which the employee obtained the system role, is canceled if attestation approval is not granted. This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\GroupMembership	Determines default behavior for automatic removing of united namespace system entitlements if attestation approval is not granted.
QER\Attestation\AutoRemovalScope\GroupMembership\RemoveDelegatedRole	If this configuration parameter is set, ends the role delegation through which the employee obtained the system role if attestation approval is not granted. This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\GroupMembership\RemoveDirect	If this configuration parameter is set, 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, system entitlement assignment to roles (organizations and business roles) is removed if attestation approval is not granted. This removes the system entitlement assignment to all user accounts whose associated employees are members of these roles. IMPORTANT: Employees whose attestation has been approved can lose the system entitlement through this.
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 if attestation approval is not granted. This removes all indirect assignments the employee obtained through this role.
QER\Attestation\AutoRemovalScope\	If this configuration parameter is set, the

Configuration parameter	Description
GroupMembership\ RemoveRequested	requested system entitlement is canceled if attestation approval is not granted.
QER\Attestation\AutoRemovalScope\ GroupMembership\ RemoveRequestedRole	If this configuration parameter is set, the requested role through which the employee obtained the system entitlement, is canceled if attestation approval is not granted. This removes all indirect assignments the employee obtained 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 if attestation approval is not granted. This removes all indirect assignments the employee obtained through this system role. NOTE: This configuration parameter is only available if the System Roles Module is installed.
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, 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, 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\ RemoveRequestedRole	If this configuration parameter is set, the requested application role membership 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.

Configuration parameter	Description
QER\Attestation\AutoRemovalScope\UNSGroupInUNSGroup\RemoveDirect	If this configuration parameter is set, the system entitlement assignment to a system entitlement is removed when attestation approval is not granted.
QER\Attestation\DefaultSenderAddress	This configuration parameter contains the sender email address for messages automatically generated for attestation.
QER\Attestation\MailApproval\Account	Name of user account for authentication of "Approval by mail" mailbox.
QER\Attestation\MailApproval\DeleteMode	Specifies the way emails are deleted from the inbox.
QER\Attestation\MailApproval\Domain	Domain of user account for authentication of "Approval by mail" mailbox.
QER\Attestation\MailApproval\ExchangeURI	Specifies the Microsoft Exchange Web Service URL. AutoDiscover mode is used to find the URL if it is not given.
QER\Attestation\MailApproval\Inbox	This Microsoft Exchange mailbox is used for "Approval by mail" processes.
QER\Attestation\MailApproval\Password	Password of user account for authentication of "Approval by mail" mailbox.
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	This mail template is used for attestation made through "Approval 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\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

Configuration parameter	Description
	set, a "Mail template demand" or "Mail template reminder" for single attestation cases can be entered to send an email for each request. If this configuration parameter is set, single mails are not sent.
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\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\CalculateRiskIndex	Preprocessor relevant configuration parameter controlling system components for calculating an employee's risk index. Changes to the parameter require recompiling the database. If the parameter is set, values can be entered and calculated for the risk index.
QER\Person\Defender	This configuration parameter specifies whether Starling Two-Factor Authentication is supported.
QER\Person\Defender\ApiEndpoint	This configuration parameter contains the URL of the Starling 2FA API end point used to register new users.
QER\Person\Defender\ApiKey	This configuration parameter contains your company's subscription key for accessing the Starling Two-Factor Authentication interface.

Configuration parameter	Description
QER\Person\Defender\DisableForceParameter	This configuration parameter specifies whether Starling 2FA is forced to send the OTP by SMS or 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.
Common\MailNotification\DefaultCulture	This configuration parameter contains the default language culture for email notifications if no language culture 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 company 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 the configuration parameter is not set, the login data stored in the parameters "Common\MailNotification\SMTPDomain", "Common\MailNotification\SMTPAccount" and "Common\MailNotification\SMTPPassword" is

Configuration parameter	Description
	used.
Common\ProcessState\PropertyLog	When this configuration parameter is set, changes to individual values are logged and shown in the process view.

About us

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

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

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

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

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

Index