One Identity Manager 8.0.4

Application Roles Administration Guide

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 Application Roles Administration Guide
Updated - September 2019
Version - 8.0.4

Contents

1

One Identity Manager Application Roles

You can use the One Identity Manager role model to control edit permissions for One Identity Manager users. This role model takes into account technical aspects (for example, One Identity Manager tool administrative rights) as well as functional aspects, which result from One Identity Manager user tasks within the company structure (for example, permissions for approving requests). The One Identity Manager makes so-called application roles available.

Application roles have the following aims:

- Program functions, employees, company resources, approval workflows and approval policies are assigned to fixed application roles. Write permissions for these application roles do not need to be defined specifically for the company. This simplifies administration of access permissions.
- Enables audit secure internal administration of One Identity Manager users and their write permissions. Permissions can be granted through assignment, request and approval or by calculation on account of specific properties. Furthermore, issuing permissions with the attestation function is integrated into the attestation process.
- Users are provided with initial permissions, which they required for carrying out their tasks. This is a way, for example, to create initially required user accounts.

Application roles can be limited to permissions groups whose write permissions are predefined by One Identity Manager. Controlling write permissions:

- Navigation configuration in administration tools
- Access to objects and their properties
- Which interface forms and tasks are displayed
- Availability of special program functionality

Users must be role-based to use application roles for logging in to One Identity Manager. Role-based authentications module finds the valid write permissions from all the user's application roles. This provides the One Identity Manager user with permissions corresponding to their application roles for the One Identity Manager functions when they log onto One Identity Manager tools.

Detailed information about this topic

- Application Roles Overview on page 7
- Implementing Application Roles on page 23
- How to Edit Application roles on page 24
- Role Based Authentication Module on page 33

Application Roles Overview

One Identity Manager supplies default application roles whose permissions are matched to the different task and functions. Assign employees to default applications who take on individual tasks and functions. You can also create your won application roles for custom defined tasks.

NOTE: Default application roles are defined in One Identity Manager modules and are not available until the modules are installed. You cannot delete default application roles.

The following default application roles are defined:

- Application Roles for Basic Functions
- Compliance & Security Officer
- Auditors
- Application Roles for Identity Audit
- Application Roles for Company Policies
- Application Roles for Attestation
- Application Roles for Subscribable Reports
- Management Level
- Application Roles for Business Roles
- Application Roles for Organizations
- Application Roles for Employees
- Application Roles for the IT Shop
- Application Roles for Target Systems
- Application Roles for the Universal Cloud Interface
- Application Roles for Custom Tasks

Application Roles for Basic Functions

NOTE: This application role is available if the Identity Management Base Module is installed.

The following application roles are available to you for the basic functionality in One Identity Manager.

Table 1: Application Roles

Application Role	Description
Administrators	Administrators must be assigned to the application role **Base roles | Administrators**. Users with this application role: • Administer application roles for administrators. • Assign employees to administrator application roles. • Can other employees to the application role **Base roles | Administrators** and edit conflicting application roles. • See the master data for the other application roles.
Everyone (change)	The application role **Base roles | Everyone (change)** is automatically assigned to every user. Users with this application role: • Can edit certain employee master data in the Web Portal. Should every user be automatically assigned to a custom permissions group when they log in, then this permissions group can be added to the application role. Members of this application role are determined through a dynamic role.
Everyone (lookup)	The application role **Base roles | Everyone (Lookup)** is automatically assigned to every user. Users with this application role: • Obtain read access to objects in the Web Portal. Should every user be automatically assigned to a custom permissions group when they log in, then this permissions group can be added to the application role. Members of this application role are determined through a dynamic role.
Employee managers	The application **Base roles | Employee managers** is automatically assigned to a user if the user is a manager or supervisor of employees, departments, locations, cost centers, business roles or IT Shops. Users with this application role: • Can edit master data for the objects they are responsible for and assign company resources to them.

Application Role	Description
	• Can edit master data for their employees in the Web Portal. • Can add their staff members to the IT Shop. • Employee and department managers can add new employees in the Web Portal. • Can view their staff's compliance rule violations in the Web Portal. Members of this application role are determined through a dynamic role.
Birthright Assignments	The application role **Base roles | Birthright assignments** is used to provide birthrights to employees which are provided to establish their working environment. The application roles are allocated all the resources marked for automatic assignment to all employees. All internal employees are assigned to this application role and obtain the resources. Internal employees are found through a dynamic role.
Operations support.	Employees that use the Operations Support Web Portal, must be assigned the application role **Base roles | Operations support**. Users with this application role: • Monitor handling of Job queue processes. • Monitor handling of the DBQueue. • Create access codes.

Related Topics

- Customized Extension of Application Role Write Permissions on page 26

Compliance & Security Officer

NOTE: This application role is available if Attestation Module, Compliance Rules Module or Company Policies Module is installed.

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

NOTE: This application role is available if Attestation Module, Compliance Rules Module or Company Policies Module is installed.

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.

Application Roles for Identity Audit

NOTE: This application role is available if the Compliance Rules Module is installed.

The following application roles are available for managing compliance rule:

Table 2: Application Roles

Application Role	Description
Administrators	Administrators must be assigned to the application role **Identity & Access Governance | Identity Audit | Administrators**. Users with this application role: • Enter base data for for setting up company policies. • Create compliance rules and assign rule supervisors to them. • Can start rule checking and view rule violations as required. • Create reports about rule violations. • Enter mitigating controls. • Create and edit risk index functions. • Monitor Identity Audit functions. • Administer application roles for rule supervisors, exception approvers and attestors. • Set up other application roles as required.
Rule supervisors	Rule supervisors must be assigned to the application role **Identity**

Application Role	Description
	& Access Governance | Identity Audit | Rule supervisors or to a child role. Users with this application role: • Are responsible for compliance rule content, for example, an auditor or a auditing department. • Edit the compliance rule working copies, which are assigned to the application role. • Enable and disable compliance rules. • Can start rule checking and view rule violations as required. • Assign mitigating controls.
Exception approver	Administrators must be assigned to the application role **Identity & Access Governance | Identity Audit | Exception approvers** or to a child role. Users with this application role: • Edit rule violations in the Web Portal. • Can grant exception approval or revoke it in the Web Portal.
Attestors	Attestors must be assigned to the application role **Identity & Access Governance | Identity Audit | Attestors**. Users with this application role: • Attest compliance rules and exception approvals in the Web Portal for which they are responsible. • Can view master data for these compliance rules but not edit them. NOTE: This application role is available if the module Attestation Module is installed.
Maintain SAP Functions	Administrators must be assigned to the application role **Identity & Access Governance | Identity Audit | Maintain SAP functions** or to a child role. Users with this application role: • Are responsible for SAP function contents. • Edit working copies of function definitions for which they are responsible. • Define function instances and variables sets for SAP functions. • Assign mitigating controls.

Application Role	Description
	NOTE: This application role is available if the module SAP R/3 Compliance Add-on Module is installed.

Application Roles for Company Policies

NOTE: This application role is available if the Company Policies Module is installed.

The following application roles are available for managing company policies:

Table 3: Application Roles

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

Application Role	Description
approver	Exception approvers must be assigned to the application role **Identity & Access Governance | Company policies | Exception approvers** or to a child role. Users with this application role: • Edit policy violations. • Can grant exception approval or revoke it.
Attestors	Attestors must be assigned to the application role **Identity & Access Governance | Company policies | Attestors**. Users with this application role: • Attest company policies and exception approvals in the Web Portal for which they are responsible. • Can view the master data for these company policies but not edit them. NOTE: This application role is available if the module Attestation Module is installed.

Application Roles for Attestation

NOTE: This application role is available if the module Attestation Module is installed.

The following application role is available for managing attestation procedures:

Table 4: Application Roles

Application Role	Description
Administrators	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.

Application Role	Description
	• Create and edit risk index functions. • Monitor attestation cases.
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.

NOTE: Attestors in charge are determined through approval procedures. Other application roles may be applied here. Application roles for attestors are defined in different module and are available if the Attestation Module is installed.

Application Roles for Subscribable Reports

NOTE: This application role is available if the module Report Subscription Module is installed.

The following application role is available for managing subscribable reports:

Table 5: Application Roles

Application Role	Description
Administrators	Administrators must be assigned to the application role **Identity & Access Governance | Company policies | Report Subscriptions**. Users with this application role: • Create subscribable reports from existing reports. • Configure report parameters for subscribable reports. • Assign subscribable reports to employees, company structures or IT Shop shelves. • Create custom mail templates for sending subscribed reports by email.

Management Level

NOTE: This application role is available if the Identity Management Base Module is installed.

The user must be assigned to the application role **Identity Management | Management level**.

Users with this application role:

- Can view reports and statistics for management levels in the Web Portal.

Application Roles for Business Roles

NOTE: This application role is available if the module Business Roles Module is installed.

The following application roles are available for the administration of business roles:

Table 6: Application Roles

Application Role	Description
Administrators	Administrators must be assigned to the application role **Identity Management | Business roles | Administrators**. Users with this application role: • Create and edit business roles. • Assign company resources to business roles. • Administrate application roles for role approvers, role approvers (IT) and attestors. • Set up other application roles as required.
Attestors	Attestors must be assigned to the application role **Identity Management | Business roles | Attestors** or a child application role. Users with this application role: • Attest correct assignment of company resource to business roles for which they are responsible. • Can view master data for these business roles but not edit them.

Application Role	Description
	NOTE: This application role is available if the module Attestation Module is installed.
Role approver	Approvers must be assigned to the application role **Identity Management | Business roles | Role approvers** or a child application role. Users with this application role: • Are approvers for the IT Shop. • Approve requests from business roles for which they are responsible.
Role approver (IT)	IT role approvers must be assigned to the application role **Identity Management | Business roles | Role approvers (IT)** or a child application role. Users with this application role: • Are IT role approvers for the IT Shop. • Approve requests from business roles for which they are responsible.

Application Roles for Organizations

NOTE: This application role is available if the Identity Management Base Module is installed.

The following application roles are available for the administration of departments, cost centers and locations:

Table 7: Application Roles

Application Role	Description
Administrators	Administrators must be assigned to the application role **Identity Management | Organizations | Administrators**. Users with this application role: • Set up and edit departments, cost centers and locations. • Assign company resources to departments, cost centers and locations. • Administrate application roles for role approvers, role approvers

Application Role	Description
	(IT) and attestors. • Set up other application roles as required.
Attestors	Attestors must be assigned to the application role **Identity Management | Organizations | Attestors** or a child application role. Users with this application role: • Attest correct assignment of company resources to departments, cost centers and locations for which they are responsible. • Can view master data for departments, cost centers and locations but cannot edit them. NOTE: This application role is available if the module Attestation Module is installed.
Role approver	Approvers must be assigned to the application role **Identity Management | Organizations | Approvers** or a child application role. Users with this application role: • Are approvers for the IT Shop. • Approve request from departments, cost centers and locations for which they are responsible.
Role approver (IT)	IT role approvers must be assigned to the application role **Identity Management | Organizations | Role approvers (IT)** or a child application role. Users with this application role: • Are IT role approvers for the IT Shop. • Approve request from departments, cost centers and locations for which they are responsible.

Application Roles for Employees

NOTE: This application role is available if the Identity Management Base Module is installed.

The following application role is available for employee administration:

Table 8: Application Roles

Application Role	Description
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

Application Roles for the IT Shop

NOTE: This application role is available if the Identity Management Base Module is installed.

The following application roles are available for the IT Shop administration:

Table 9: Application Roles

Application Role	Description
Administrators	Administrators must be assigned to the application role **Request & Fulfillment | IT Shop | Administrators**. Users with this application role: • Create the IT Shop structure with shops, shelves, customers, templates and service catalog. • Create approval policies and approval workflows. • Specify which approval procedure to use to find attestors. • Create products and service items. • Set up request notifications. • Monitor request procedures. • Administrate application roles for product owners and attestors. • Set up other application roles as required. • Create extended properties for company resources of any type.

Application Role	Description
	• Edit the resources and assign them to IT Shop structures and employees. • Assign system authorizations to IT Shop structures.
Product owners	The product owners must be assigned to the application roles **Request & Fulfillment | IT Shop | Product owners** or an application role below that. Users with this application role: • Approve through requests. • Edit service items and service categories under their management.
Attestors	Attestors must be assigned to the application role **Request & Fulfillment | IT Shop | Attestors**. Users with this application role: • Attest correct assignment of company resource to IT Shop structures for which they are responsible. • Can view master data for these IT Shop structures but not edit them. NOTE: This application role is available if the module Attestation Module is installed.
Chief approval team	The chief approver must be assigned to the application **Request & Fulfillment | IT Shop | Chief approval team** Users with this application role: • Approve through requests. • Assign requests to other approvers.

NOTE: Approvers in charge are determined through approval procedures. Other application roles may be applied here. Application roles for approvers are defined in different modules and are available there.

Application Roles for Target Systems

NOTE: Application roles are dependent on the target system and are contained in One Identity Manager modules. Application roles are not available until the modules are installed.

The following application roles are available for target system administration:

Table 10: Application Roles

User	Task
Target system administrators	Target system administrators must be assigned to the application role **Target system | Administrators**. Users with this application role: • Administrate application roles for individual target systems types. • Specify the target system manager. • Set up other application roles for target system managers if required. • Specify which application roles are conflicting for target system managers • Authorize other employee to be target system administrators. • Do not assume any administrative tasks within the target system.
Target system managers	Target system managers must be assigned to the application role **Target systems | <target system>** or a sub application role. NOTE: There is at least one application role per target system for target system managers. This application role is available if the target system module is installed. Target system managers must be assigned to the application role **Target systems | G Suite** or a sub application role. Target system managers must be assigned to the application role **Target systems | SharePoint Online** or a sub application role. Users with this application role: • Assume administrative tasks for the target system. • Create, change or delete target system objects, like user accounts or groups. • Edit password policies for the target system. • Prepare system entitlements for adding to the IT Shop. • Configure synchronization in the Synchronization Editor and defines the mapping for comparing target systems and One Identity Manager. • Edit the synchronization's target system types and outstanding objects.

User	Task
	• Authorize other employees within their area of responsibility as target system managers and create child application roles if required.
Target system managers for Unified Namespace	Target system managers must be assigned to the application role **Target systems | Unified Namespace** or a sub application role. Users with this application role: • Obtain view of the objects in the connected target systems across all target systems. • Can create reports across all target systems. If the users are also target system managers of the basic underlying target systems, you can manage these target systems through the Unified Namespace.

Application Roles for the Universal Cloud Interface

NOTE: Application roles are available if the Universal Cloud Interface Module is installed.

The following application roles are available for managing cloud systems.

Table 11: Application Roles

User	Task
Cloud administrators	Administrators must be assigned to the application **Universal Cloud Interface | Administrators** or a sub application role. Users with this application role: • Manage application roles for the Universal Cloud Interface. • Set up other application roles as required. • Configure synchronization in the Synchronization Editor and define the mapping for comparing tcloud applications and One Identity Manager. • Edit cloud application in the Manager. • Edit pending, manual provisioning processes in the Web Portal and obtain statistics.

User	Task
	• Obtain information about the cloud objects in the Web Portal and the Manager.
Cloud operators	Operators must be assigned to the application role **Universal Cloud Interface | Operators** or a sub application role. Users with this application role: • Edit pending, manual provisioning processes in the Web Portal and obtain statistics.
Cloud auditors	Auditors must be assigned to the application role **Universal Cloud Interface | Auditors** or a sub application role. Users with this application role: • Can view manual provisioning processes in the Web Portal and obtain statistics.

Application Roles for Custom Tasks

NOTE: This application role is available if the Identity Management Base Module is installed.

The following custom functions are available for application roles:

Table 12: Application Roles

Application Role	Description
Administrators	Administrators must be assigned to the application role **Custom | Administrators**. Users with this application role: • Administrate custom application roles. • Set up other application roles for managers, if required.
Managers	Managers must be assigned to the application role **Custom | Managers** or a subordinate role. Users with this application role: • Add custom task in the One Identity Manager. You can use these application roles, for example, to guarantee One Identity Manager users write permissions on custom tables or columns. All application roles that you define here must obtain their write permissions through custom permissions groups.

Implementing Application Roles

IMPORTANT: To use application roles you must add one employee to the application role **Base roles | Administrators**. This employee is the authorized to assigned administrative One Identity Manager application roles to other employees.

Only run this task once.

To initially add an employee to the application role Base roles | Administrators

1. Log into the Manager as a non role-based administrative user.
2. Select the **Employees | Employees**.
3. Select the employee to be assigned to the application role **Base role | Administrators**.
4. Select **Authorize as One Identity Manager administrator** in the task view.

NOTE: As soon as you refresh the Manager view, the task **Authorize as One Identity Manager Administrator** is no longer shown in the task view. That means that the task can only be run when there are no other employees assigned to this application role.

It is possible that no more employees assigned to the application role **Base roles | Administrators** after you have been working with the One Identity Manager for a while. In this case, proceed as described above in order to reassign an employee to this application role.

The One Identity Manager user with the application role **Base roles | Administrators** can now add more employees to application roles and edit the application role master data.

Related Topics

- Assigning Employees to Application Roles on page 26
- How to Edit Application roles on page 24
- Role Based Authentication Module on page 33

How to Edit Application roles

To set up your first application roles you need to add an employee to the application role **Base roles | Administrators**. This employee is authorized to add more employees to different administration application roles. For more information, see Implementing Application Roles on page 23.

NOTE: To edit the application role, log on to the Manager using a role-based authentication module.

Administrators can edit child application roles, set up more application roles and assigned employees.

To edit attestation roles

1. Select the category **One Identity Manager administration**.
2. Select a category in the navigation view.
3. Select the application role in the result list. Select **Change master data** in the task view.

   - OR -

   Click in the result list toolbar.
4. Edit the application role's master data.
5. Save the changes.

NOTE: You cannot delete default application roles.

Related Topics

- Application Role Master Data on page 24
- Assigning Employees to Application Roles on page 26
- Customized Extension of Application Role Write Permissions on page 26
- Role Based Authentication Module on page 33

Application Role Master Data

If you add a new application role, you must fill out the compulsory fields.

Table 13: Application Role Properties

Property	Meaning
Application role	Application role name.

Property	Meaning
Internal name	Empty text field for a internal company identifier
Full name	Full name of application role. Is made up automatically from the application role name and the parent application role.
Parent application role	Application role to which the application role being edited is subordinate.
Department, location, cost center	Additional information for the application role definition. These input fields are only used for information. They do not indicate for which department, cost center or location the application roles are responsible.
Permissions group	Permissions group for determining write permissions on role-based login. The application role is given access permissions of the associated permissions group. If there is no permissions group assigned, the application role gets write permissions from the parent application role. Administrators can assign the rest of the application roles to custom defined permissions groups. For more information, see Customized Extension of Application Role Write Permissions on page 26. NOTE: Permissions groups for default administrator application roles for cannot be edited.
Description	Spare text box for additional explanation.
Comment	Spare text box for additional explanation.
Certification status	Status of the application role's certification. You can select the following certification statuses: • New - The application role has been added to the One Identity Manager database. • Certified - The application role's master data has been granted approval by a manager. • Denied - The application role's master data has been denied approval by a manager.
Block inheritance	Specifies whether employees from parent application roles can also be determined as approvers for requests in the IT Shop that use the approval methods RD, RL, RO or RP. If this option is set, only employee that are assigned to exactly this application can be determined as approvers. NOTE: This option available on compatibility grounds with older versions of the program. It is recommended that you set this option.
Dynamic roles not	Specifies whether a dynamic role can be created for the application role.

Property	Meaning
allowed	
Spare fields no. 01.....spare field no. 10	Additional company specific information. Use the Designer to customize display names, formats and templates for the input fields.

Assigning Employees to Application Roles

Assigned employees obtain all the write permissions of the permission group to which the application role (or a parent application role) is assigned. In addition, employees obtain the company resources assigned to the application role. Employees of the parent application role are inherited if no employees are directly assigned to an application role.

NOTE: The application role **Base roles | Everyone (Change)**, **Base roles | Everyone (Lookup)**, **Base roles | Employee Managers** and **Base roles | Birthright Assignments** are automatically assign to employees. Do not make any manually assignments to these application roles.

To assign employees to an application role

1. Select the category **One Identity Manager administration**.
2. Select a category in the navigation view.
3. Select an application role in the result list.
4. Select **Assign employees** in the task view.
5. Assign employees in **Add assignments**.

   - OR -

   Remove employees from **Remove assignments**.
6. Save the changes.

Customized Extension of Application Role Write Permissions

For role-based login, the application roles require a link to a permissions group in which write permissions for One Identity Manager are defined. The application role is given access permissions of the associated permissions group. If there is no permissions group assigned, the application role gets write permissions from the parent application role.

Different role-based authentication modules are available for role-based login on One Identity Manager tools. First, the employee memberships in application roles are determined during log in with role-based authentication. Assignments of permissions group

to application roles are used to determine which permissions groups apply to the employee. A dynamic system user is determined from these permissions groups that will be used for the employee's login.

Some of the default application roles are already assigned permissions groups. The permissions groups have write permissions to tables and columns and are equipped with menu items, forms, methods and program functions for editing application data with the Manager and the Web Portal.

You can assign customized permissions groups to application roles so that the write permissions for application roles meet your company requirements. You need to ensure that your custom permissions groups contain all the write permissions of the default permissions groups for these application roles. This allows users with these application roles to use all default One Identity Manager functionality.

NOTE: You can simplify grouping of permissions by using hierarchical linking of permissions groups. Permissions from hierarchical permissions groups are inherited from top to bottom. That means that a permissions group contains all the permissions belonging parent permissions groups.

Proceed as follows:

1. Create a new permissions group in the Designer.

   NOTE: Set the option **Only use for role-based authentication**.

2. Set up dependencies for the new permissions group to the default permissions group for the application role.

   The default permissions group must be assigned as a subgroup. This means that the new permissions group inherits the properties.

3. Allocate additional write permissions for menu items, forms, tables and columns.
4. Assign the permissions group to the application role in the Manager.

If a user logs into the Manager or the Web Portal with this type of altered application role they get, in additional to the default permissions for this application role, the custom defined edit permissions.

For detailed information about creating permissions groups and editing entitlements, see the One Identity Manager Configuration Guide.

Related Topics

- Application Role Master Data on page 24

Additional Tasks for Managing Application Roles

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.

Creating Dynamic Roles for Application Roles

Use this task to assign employees to an application role through dynamic roles. For more detailed information about using dynamic roles, see the One Identity Manager Identity Management Base Module Administration Guide.

NOTE: The task **Create dynamic role** is only available for application roles, which do not have the option **Dynamic roles not allowed** set.

To create a dynamic role

1. Select the category **One Identity Manager administration**.
2. Select a category in the navigation view.
3. Select an application role in the result list.
4. Select **Create dynamic role** in the task view.
5. Enter the required master data. The following applies to dynamic roles for application roles:
   - Object class

     "Person"
   - Application role

     This is preset with the selected application role. If these objects fulfill the dynamic role conditions, they become members in the application role.
   - Dynamic role

     The dynamic role identifier is made up by default of the object class and the full name of the application role.
6. Save the changes.

To edit a dynamic role

1. Select the category **One Identity Manager administration**.

   Application roles are grouped by category in the navigation. Those application roles are shown corresponding to the application roles you are allowed to edit
2. Select a category in the navigation view.
3. Select an application role in the result list.

4. Select **Application role overview** in the task view.
5. Select the form element "dynamic roles" and click on the dynamic role.
6. Select **Change master data** in the task view.
7. Edit the dynamic role.
8. Save the changes.

Related Topics

- Application Role Master Data on page 24

Define Inheritance Exclusion for Application Roles

It is possible that employees cannot own certain system roles at the same time. Thus, for example, exception approvers for rule violations may not be rule supervisors at the same time. You can specify mutually exclusive (conflicting) application roles to achieve this behavior. Then you cannot assign these application roles to the same person anymore.

NOTE: Only system roles, which are defined directly as conflicting application roles cannot be assigned to the same employee. Definitions made on parent or child application roles do not effect the assignment.

To define conflicting application roles

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

To define conflicting application roles

1. Select the category **One Identity Manager administration**.
2. Select a category in the navigation view.
3. Select the application role in the result list for which you want to define conflicting application roles.
4. Select **Edit conflicting application roles** in the task view.
5. Assign the application roles that are mutually exclusive to the selected application role in **Add assignments**.

   - OR -

   Remove the application roles that are no longer mutually exclusive in **Remove assignments**.
6. Save the changes.

Assign subscribable reports

NOTE: This function is only available if the Report Subscription Module is installed.

Use this task to assign subscribable reports to selected application roles. All employee in this application role can subscribe to reports in the Web Portal.

NOTE: This task is only available if the application roles (or a parent application role) is assigned to a permissions group.

NOTE: You cannot assign subscribable reports to the application roles **Base roles | Employee managers**, **Base roles | Everyone (Lookup)** and **Base roles | Everyone (Change)**.

1. Select the category **One Identity Manager administration**.
2. Select a category in the navigation view.
3. Select an application role in the result list.
4. Select **Assign subscribable reports** in the task view.
5. Assign reports in **Add assignments**.

   - OR -

   Remove the reports in **Remove assignments**.
6. Save the changes.

For more detailed information about report subscriptions, see the One Identity Manager Report Subscriptions Administration Guide.

Assign Extended Properties to Application Roles

Extended properties are meta objects that cannot be mapped directly in the One Identity Manager, for example, operating codes, cost codes or cost accounting areas.

To specify extended properties for an application role

1. Select the category **One Identity Manager administration**.
2. Select a category in the navigation view.
3. Select an application role in the result list.
4. Select **Assign extended properties** in the task view.
5. Assign extended properties in **Add assignments**.

   - OR -

Remove extended properties from **Remove assignments**.

6. Save the changes.

For more detailed information about using extended properties, see the One Identity Manager Identity Management Base Module Administration Guide.

Reports about Application Roles

One Identity Manager makes various reports available containing information about the selected base object and its relations to other One Identity Manager database objects. The following reports are available for application roles.

Table 14: Reports about Application Roles

Report	Description
Overview of all Assignments	This report finds all the roles in which employees from the selected application roles are also members.
Show historical memberships	This report lists all members of the selected application role and the length of their membership.

Related Topics

- Analyzing Role Memberships and Employee Assignments on page 31

Analyzing Role Memberships and Employee Assignments

The report "Overview of all Assignments" is displayed for certain objects, for example, permissions, compliance rules or roles. The report finds all the roles, for example, departments, cost centers, locations, business roles and IT Shop structures in which there are employee who own the selected base object. In this case, direct as well as indirect base object assignments are included.

Example

- If the report is created for a resource, all roles are determined in which there are employees with this resource.
- If the report is created for a group, all roles are determined in which there are employees with this group.
- If the report is created for a compliance rule, all roles are determined in which there are employees with this compliance rule.

- If the report is created for a department, all roles are determined in which employees of the selected department are also members.
- If the report is created for a business role, all roles are determined in which employees of the selected business role are also members.

To display detailed information about assignments

- To display the report, select the base object from the navigation or the result list and select the report **Overview of all assignments**.
- Use the **Used by button** in the report's toolbar to select the role class (department, location, business role or IT Shop structure) for which you determine if roles exist in which there are employees with the selected base object.

  All the roles of the selected role class are shown. The color coding of elements identifies the role in which there are employees with the selected base object. The meaning of the report control elements is explained in a separate legend. In the report's toolbar, click to open the legend.
- Double-click a control to show all child roles belonging to the selected role.
- By clicking the button in a role's control, you display all employees in the role with the base object.
- Use the small arrow next to to start a wizard that allows you to bookmark this list of employee for tracking. This creates a new business role to which the employees are assigned.

Figure 1: Toolbar for Report "Overview of all assignments"

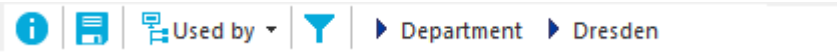

Table 15: Meaning of Icons in the Report Toolbar

Icon	Meaning
	Show the legend with the meaning of the report control elements
	Saves the current report view as a graphic.
	Selects the role class used to generate the report.
	Displays all roles or only the affected roles.

Role Based Authentication Module

IMPORTANT: Users must be role-based to use application roles for logging in. Role-based login is provided for the Manager and the Web Portal. To use role-based login with other One Identity Manager tools, you should ensure that users determined through the authentication module, own the required permissions.

Different role-based authentication modules are available for role-based login on One Identity Manager tools. First, the employee memberships in application roles are determined during log in with role-based authentication. Assignments of permissions group to application roles are used to determine which permissions groups apply to the employee. A dynamic system user is determined from these permissions groups that will be used for the employee's login.

NOTE: Authentication modules are defined in the One Identity Manager modules and are not available until the modules are installed.

Following role-based authentication modules are available:

Generic single sign-on (role based)

Login Data	The authentication module uses the Active Directory login data of user currently logged in on the workstation.
Prerequisites	The employee exists in the One Identity Manager database. The employee is assigned at least one application role. The user account exists in the One Identity Manager database and the employee is entered in the user account's master data.
Set as default	No
Single Sign-On	Yes
Front-end login allowed	Yes
Web Portal	Yes

login allowed

Remarks

One Identity Manager searches for the user account according to the configuration and finds the employee assigned to the user account.

If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication.

- If this configuration parameter is set, the employee's main identity is used for authentication.
- If the parameter is not set, the employee's subidentity is used for authentication.

A dynamic system user determined from the employee's application roles. The user interface and the write permissions are loaded through this system user.

Changes to the data are assigned to the logged in employee.

Modify the following configuration parameters in the Designer to implement the authentication module.

Table 16: Configuration Parameters for the Authentication Module

Configuration parameter	Meaning
QER\Person\OAuthAuthenticator	This configuration parameter specifies whether authentication through single sign-on is supported.
QER\Person\GenericAuthenticator\SearchTable	This configuration parameter contains the table in the One Identity Manager schema in which user information is stored. The table must contain a foreign key with the name `UID_Person`, which points to the table `Person`. Example: `ADSAccount`
QER\Person\GenericAuthenticator\SearchColumn	This configuration parameter contains the column from the One Identity Manager table (SearchTable), which is used to search for the user name of the current user. Example: `CN`
QER\Person\GenericAuthenticator\EnabledBy	This configuration parameter contains a pipe (|) delimited list of Boolean columns from the One Identity Manager table (SearchTable) enabled by the user account for the login.
QER\Person\GenericAuthenticator\DisabledBy	This configuration parameter contains a pipe (|) delimited list of Boolean columns from the One Identity Manager table (SearchTable) disabled by the user account for the login. Example: `AccountDisabled`

Employee (role based)

Login Data	Employee's central user account and password.
Prerequisites	The employee exists in the One Identity Manager database. • The central user account is entered in the employee's master data. • The password is entered in the employee's master data. The employee is assigned at least one application role.
Set as default	Yes
Single Sign-On	No
Front-end login allowed	Yes
Web Portal login allowed	Yes
Remarks	If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication. • If this configuration parameter is set, the employee's main identity is used for authentication. • If the parameter is not set, the employee's subidentity is used for authentication. A dynamic system user determined from the employee's application roles. The user interface and the write permissions are loaded through this system user. Changes to the data are assigned to the logged in employee.

User Account (role based)

Login Data	The authentication module uses the Active Directory login data of user currently logged in on the workstation.
Prerequisites	The employee exists in the One Identity Manager database. • Permitted logins are entered in the employee's master data. The logins are expected in the form: `domain\user`. The employee is assigned at least one application role.
Set as default	No
Single Sign-	Yes

On	
Front-end login allowed	Yes
Web Portal login allowed	Yes
Remarks	All employee logins saved in the One Identity Manager database are found. The employee whose login data matches that of the current user is used for logging in. If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication. • If this configuration parameter is set, the employee's main identity is used for authentication. • If the parameter is not set, the employee's subidentity is used for authentication. A dynamic system user determined from the employee's application roles. The user interface and the write permissions are loaded through this system user. Data modifications are attributed to the current user account.

Active Directory user account (role based)

Login Data	The authentication module uses the Active Directory login data of user currently logged in on the workstation.
Prerequisites	The employee exists in the One Identity Manager database. The employee is assigned at least one application role. The Active Directory user account exists in the One Identity Manager database and the employee is entered in the user account's master data.
Set as default	Yes
Single Sign-On	Yes
Front-end login allowed	Yes
Web Portal login allowed	Yes
Remarks	The appropriate user account is found in the One Identity Manager database through the user's SID and the domain given at login. One Identity Manager determines which employee is assigned to the user account.

If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication.

- If this configuration parameter is set, the employee's main identity is used for authentication.
- If the parameter is not set, the employee's subidentity is used for authentication.

A dynamic system user determined from the employee's application roles. The user interface and the write permissions are loaded through this system user.

Data modifications are attributed to the current user account.

NOTE: If the option **Connect automatically** is set, authentication is no longer necessary for subsequent logins.

Active Directory user account (manual input/role based)

Login Data	Login name and password for registering with Active Directory. You do not have to enter the domain.
Prerequisites	The employee exists in the One Identity Manager database. The employee is assigned at least one application role. The Active Directory user account exists in the One Identity Manager database and the employee is entered in the user account's master data. The domain for logging in are entered in the configuration parameter "TargetSystem\ADS\AuthenticationDomains".
Set as default	Yes
Single Sign-On	No
Front-end login allowed	Yes
Web Portal login allowed	Yes
Remarks	The user‘s identity is determined from a predefined list of permitted Active Directory domains. The corresponding user account and employee are determined in the One Identity Manager database, which the user account is assigned to. If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication.

- If this configuration parameter is set, the employee’s main identity is used for authentication.
- If the parameter is not set, the employee’s subidentity is used for authentication.

A dynamic system user determined from the employee's application roles. The user interface and the write permissions are loaded through this system user.

Data modifications are attributed to the current user account.

LDAP user account (role based)

Login Data	Login name, identifier, distinguished name or user ID of an LDAP user account. LDAP user account's password.
Prerequisites	The employee exists in the One Identity Manager database. The employee is assigned at least one application role. The LDAP user account exists in the One Identity Manager database and the employee is entered in the user account's master data. The configuration data for dynamically determining the system user is defined in the application. Thus, an employee can, for example, be assigned a system user dynamically depending on their department membership.
Set as default	No
Single Sign-On	No
Front-end login allowed	Yes
Web Portal login allowed	Yes
Remarks	If you log in using a login name, identifier or user ID, the corresponding user account is determined in the One Identity Manager database through the container's domain. Logging in with a distinguished name is done directly. One Identity Manager determines which employee is assigned to the LDAP user account. If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication. - If this configuration parameter is set, the employee’s main identity is used for authentication.

- If the parameter is not set, the employee's subidentity is used for authentication.

A dynamic system user determined from the employee's application roles. The user interface and the write permissions are loaded through this system user.

Data modifications are attributed to the current user account.

Modify the following configuration parameters in the Designer to implement the authentication module.

Table 17: Configuration Parameters for the Authentication Module

Configuration parameter	Meaning
TargetSystem\LDAP\Authentication	The configuration parameter allows configuration of the LDAP authentication module.
TargetSystem\LDAP\Authentication\Authentication	The configuration parameter specified the authentication mechanism. Permitted values are "Secure", "Encryption", "SecureSocketsLayer", "ReadonlyServer", "Anonymous", "FastBind", "Signing", "Sealing", "Delegation" and "ServerBind". The value can be combined with commas (,). For more information about authentication types, see the MSDN Library. Default is ServerBind.
TargetSystem\LDAP\Authentication\Port	LDAP server's port. Default is port 389.
TargetSystem\LDAP\Authentication\RootDN	The configuration parameter contains the root domain's distinguished name. Syntax: `dc=MyDomain`
TargetSystem\LDAP\Authentication\Server	The configuration parameter contains the name of the LDAP server.

HTTP header (role based)

The authentication module support authentication through Web Single Sign-On solutions that work with proxy-based architecture.

Login Data	Employee's central user account or personnel number.
Prerequisites	The employee exists in the One Identity Manager database. • The central user account or personnel number is entered in the employee's master data. The employee is assigned at least one application role.
Set as default	Yes
Single Sign-On	Yes
Front-end login allowed	No
Web Portal login allowed	Yes
Remarks	You must pass the user (in the form: `UserName =<user name of authenticated user>`) in the HTTP header. The employee is found in the One Identity Manager database whose central user account or personnel number matches the user name passed down. If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication. • If this configuration parameter is set, the employee's main identity is used for authentication. • If the parameter is not set, the employee's subidentity is used for authentication. A dynamic system user determined from the employee's application roles. The user interface and the write permissions are loaded through this system user. Changes to the data are assigned to the logged in employee.

OAuth 2.0/OpenID Connect (role-based)

The authorization module supports the authorization code for OAuth 2.0 and OpenID Connect. For more detailed information about the authorization code flow, see, for example, the OAuth Specification or the OpenID Connect Specification.

This authentication module uses a Secure Token Service for logging in. This login procedure can be used with every Secure Token Service which can return an OAuth 2.0 token.

Login Data	Dependent on the authentication method of the secure token service.
Prerequisites	The employee exists in the One Identity Manager database.

	The employee is assigned at least one application role. The user account exists in the One Identity Manager database and the employee is entered in the user account's master data.
Set as default	No
Single Sign-On	No
Front-end login allowed	Yes
Web Portal login allowed	Yes
Remarks	One Identity Manager determines which employee is assigned to the user account. If an employee owns more than one identity, the configuration parameter "QER\Person\MasterIdentity\UseMasterForAuthentication" controls which employee is used for authentication. • If this configuration parameter is set, the employee's main identity is used for authentication. • If the parameter is not set, the employee's subidentity is used for authentication. A dynamic system user determined from the employee's application roles. The user interface and the write permissions are loaded through this system user. Data modifications are attributed to the current user account. To do this, the claim type whose value is used for labeling data changes must be declared.

The respective user interface prompts for the authorization code. The configuration parameter "QER\Person\OAuthAuthenticator\LoginEndpoint" is used to open an extra login dialog box for determining the authorization code. The authentication module requires an access token from the token endpoint and the certificate is required to check the security token. In the process, an attempt is made to find the certificate from the web application configuration. If this is not possible, configuration parameters are applied. To find the certificate for testing the token, the certificate stores are queries in the following order:

1. Web application configuration (table `QBMWebApplication`)
    a. Certificate text (`QBMWebApplication.CertificateText`) .
    b. Subject or finger print from the local store (`QBMWebApplication.OAuthCertificateSubject` and `QBMWebApplication.OAuthCertificateThumbPrint`).

c. Certificate endpoint (`QBMWebApplication.CertificateEndpoint`).

   In addition, the subject or finger print is used to check certificates from the server if they are given and do not exist locally on the server.

2. Configuration Parameter

   a. Certificate text (configuration parameter "QER\Person\OAuthAuthenticator\CertificateText").

   b. Subject or finger print from the local store (configuration parameter "QER\Person\OAuthAuthenticator\CertificateSubject" and "QER\Person\OAuthAuthenticator\CertificateThumbPrint").

   c. Certificate endpoint (configuration parameter "QER\Person\OAuthAuthenticator\CertificateEndpoint").

      In addition, the subject or finger print is used to check certificates from the server if they are given and do not exist locally on the server.

   d. JSON Web Key endpoint (configuration parameter "QER\Person\OAuthAuthenticator\JsonWebKeyEndpoint").

A claim type is required to find the user account from the user information. In addition, it is specified which One Identity Manager schema information should be used to search for the user account.

Authentication through OpenID is built on OAuth. OpenID Connection authentication uses the same mechanisms, but make user claims available either in an ID token or through a UserInfo endpoint. Other configuration settings are required for using OpenID Connect. If the configuration parameter "QER\Person\OAuthAuthenticator\Scope" contains the value "openid", the authentication module uses OpenID Connect.

Modify the following configuration parameters in the Designer to implement the authentication module.

Table 18: Configuration Parameters for the Authentication Module

Configuration Parameter	Meaning
QER\Person\OAuthAuthenticator	This configuration parameter specifies whether authentication is supported through security tokens.
QER\Person\OAuthAuthenticator\CertificateEndpoint	The configuration parameter contain the certificate endpoint's Uniform Resource Locator (URL) on the authorization server. Example: `https://localhost/RSTS/SigningCertificate`
QER\Person\OAuthAuthenticator\CertificateSubject	The configuration parameter contain the subject of the certificate to use for testing. Either subject or finger print must be set.
QER\Person\OAuthAuthenticator\CertificateThumbPrint	This configuration parameter contains the fingerprint of the certificate used to verify the security token.

Configuration Parameter	Meaning
QER\Person\OAuthAuthenticator\ClientID	This configuration parameter specifies whether the client application supports this authentication.
QER\Person\OAuthAuthenticator\ClientID\Web	This configuration parameter contains the web application's Uniform Resource Name URN, which supports this authentication. Example: `urn:OneIdentityManager/Web`
QER\Person\OAuthAuthenticator\ClientID\Windows	This configuration parameter contains the native application's Uniform Resource Name URN, which supports this authentication. Example: `urn:OneIdentityManager/WinClient`
QER\Person\OAuthAuthenticator\DisabledByColumns	This configuration parameter contains a pipe (|) delimited list of Boolean columns from the One Identity Manager table (SearchTable) disabled by the user account for the login. Example: `AccountDisabled`
QER\Person\OAuthAuthenticator\EnabledByColumns	This configuration parameter contains a pipe (|) delimited list of Boolean columns from the One Identity Manager table (SearchTable) enabled by the user account for the login.
QER\Person\OAuthAuthenticator\IssuerName	This configuration parameter contains the certificate issuer's Uniform Resource Name (URN) for verifying the security token. Example: `urn:STS/identity`
QER\Person\OAuthAuthenticator\LoginEndpoint	This configuration parameter contains the Uniform Resource Locator (URL) of the Secure Token Service login page. Example: `http://localhost/rsts/login`
QER\Person\OAuthAuthenticator\Resource	This configuration parameter contains the Uniform Resource Name (URN) of the resourec to be queried, for example ADFS.
QER\Person\OAuthAuthenticator\SearchClaim	This configuration parameter contains the claim type's Uniform Resource Identifier (URI) found from the login data. Example: name of an entity http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
QER\Per-	This configuration parameter contains the column from the

Configuration Parameter	Meaning
son\OAuthAuthenticator\ SearchColumn	One Identity Manager table (SearchTable), which is used to search for user data. Equivalent to the claim type (SearchClaim) in the One Identity Manager schema. Example: `ObjectGUID`
QER\Per-son\OAuthAuthenticator\ SearchTable	This configuration parameter contains the table in the One Identity Manager schema in which user information is stored. The table must contain a foreign key with the name `UID_Person`, which points to the table `Person`. Example: `ADSAccount`
QER\Per-son\OAuthAuthenticator\ TokenEndpoint	This configuration parameter contains the token endpoint's Uniform Resource Identifier (URL) of the authorization server for returning the access token to the client for logging in. Example: `https://localhost/rsts/oauth2/token`
QER\Per-son\OAuthAuthenticator\ UserNameClaim	This configuration parameter contains the claim type's Uniform Resource Identifier (URL) used to label change data (`XUserInserted`, `XUserUpdated`).. Example: User Principle Name (UPN) http://s-chemas.xmlsoap.org/ws/2005/05/identity/claims/upn
QER\Per-son\OAuthAuthenticator\ InstalledRedirectUri	This configuration parameter contains the Uniform Resource Identifier (URL) for forwarding to installed applications. Example: `urn:InstalledApplication`
QER\Per-son\OAuthAuthenticator\ AllowSelfSignedCertsForTL-S	The configuration parameter specifies whether self-signed certificates are allowed for connecting to the token and UserInfo endpoint.
QER\Per-son\OAuthAuthenticator\ CertificateText	This configuration parameter contains the contents of the certificate as a Base64 coded string. It is used if no certi-ficate is configured.
QER\Per-son\OAuthAuthenticator\ JsonWebKeyEndpoint	This configuration parameter contains the Uniform Resource Identifier (URL) of the JSON Web Key endpoint, which supplies the signature key. At the moment, only JWK files, which contain the certificate in the x5c field are supported.
QER\Per-son\OAuthAuthenticator\ LogoutEndpoint	This configuration parameter contains the Uniform Resource Identifier (URL) of the log off end point. Example: `http://localhost/rsts/login?wa=wsignout1.0`

Configuration Parameter	Meaning
QER\Person\OAuthAuthenticator\SharedSecret	This configuration parameter contains the Shared-Secret value used for authenticating at the token endpoint.
QER\Person\OAuthAuthenticator\TokenEndpointAuthentication	This configuration parameter contains the authentication methods to use for the token end point. It specifies how the Shared-Secret is transferred. Permitted values are: • client_secret_basic (default value) HTTP basic authentication method. The shared secret is passed in the HTTP header. • client_secret_post The shared secret is passed in the value "client_secret" of the POST body.

Table 19: Additional Configuration Parameters for OpenID Connect

Configuration Parameter	Meaning
QER\Person\OAuthAuthenticator\Scope	This configuration parameter specifies the authentication log. If the configuration parameter has the value "openid", OpenID Connect is used and otherwise OAuth2.
QER\Person\OAuthAuthenticator\UserInfoEndpoint	This configuration parameter contains the Uniform Resource Locator (URL) of the OpenID Connection UserInfo endpoint.

About us

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

Contacting us

For sales or other inquiries, such as licensing, support, and renewals, 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

A

D

E