

# One Identity Manager 9.2

## Glossary

### A

#### **Account definition**

Special resource used to automatically create user accounts in the connected target systems. When an account definition is assigned to an identity, One Identity Manager creates a user account in the target system to which the account definition is assigned. The default manage level of an account definition determines which properties of the identity are inherited by the user account.

#### **Active Directory connector**

System connector for connecting to an Active Directory system.

#### **Active Roles connector**

System connector for connecting to an Active Directory system through One Identity Active Roles.

#### **Analyzer**

Program for analyzing data correlations in the database.

#### **API Server**

The API Server provides an API. It also provides the Web Portal, the Password Reset Portal, the Operations Support Web Portal, and your HTML web applications.

#### **Application role**

Functional roles that issue permissions to One Identity Manager functions that are the result of One Identity Manager user tasks within the company. Application roles take into account administrative tasks and approval processes. Application roles are predefined by One Identity Manager, but can be changed and extended.

#### **Application server**

The application server provides a connection pool for accessing the One Identity Manager database and ensures a secure connection to the database. Clients send

their queries to the application server, which processes the objects, for example, by determining values using templates and sending the results back to the clients. The data from the application is sent to the database when an object is saved.

**Approval policies**

Determines which approval workflow is applied to an attestation case or an request, renewal, or unsubscription in the IT Shop.

**Approval procedure**

Determines the attestors for the current attestation case as well as the approvers for the current request, renewal, or unsubscription in the IT Shop.

**Approval process**

Process of granting or denying approval for IT Shop requests. An approval process starts with a product request and ends with the request being finally granted or denied approval. Details of approval processes are specified in approval policies and approval workflows.

**Approval workflow**

Determines which approval procedures are applied in which order in attestation cases or request, renewals or unsubscriptions in the IT Shop. An approval workflow contains at least one approval level with at least one approval step. A different approval procedure can be used in every approval step that determines the approver or attestator.

**Approver**

Identity that can grant or deny a request, renewal, or unsubscription within an approval process.

**Assignment request**

Requests memberships in hierarchical roles or assignment of company resources to hierarchical roles. For example, this allows a business role manager to request in the IT Shop which identities become members of the business role and which company resources are assigned. These requests undergo a defined approval process.

**Assignment table**

Table in which relationships between two tables are established. Both tables' objects are assigned to each other as a many-to-many relationship. For example, assignment tables are PersonInDepartment or ADSAccountInADSGroup.

**Attestation**

Process to authorize data or internal regulations. The attestation function of One Identity Manager allows managers or those responsible to attest to the correctness of edit permissions, system entitlements, requests, or exception approvals on a regular basis or on demand.

**Attestation case**

Object that is created as soon as an attestation is triggered automatically or manually. When attestation is triggered, One Identity Manager creates an attestation case for each attestation object. Information about the attestation is

stored in it. This includes, among others, attestation object, status, and attestation date, attestor.

**Attestation object**

Object in One Identity Manager that is attested.

**Attestors**

Identity who performs an attestation. Attestors grant or deny approval to data submitted in an attestation case.

**Authentication mode**

Mode of logging in to the SharePoint server. SharePoint distinguishes between claim-based authentication and classic Windows authentication.

**Authentication module**

Specify how users log in to the One Identity Manager tools. For example, users can log in with their Active Directory user account or directly as an identity. The authentication module determines the system user assigned to the logged-in user. This assigns the user edit permissions to the user interface of the launched tool and to the database objects.

**Authentication object**

Object by which SharePoint users authenticate themselves when logging in to the SharePoint. For example, an Active Directory group or an LDAP user account.

**Authorization Editor**

Tool for editing the authorization definition of an SAP function.

**Azure Active Directory connector**

System connector for connecting to an Azure Active Directory system.

**B****Base mapping**

Mapping from which another mapping inherits the configuration.

**Base object**

Base objects contain data about the target system to be synchronized, its system connection, and the synchronization server.

**Behavior Driven Governance**

Managing and administration of access to IT system based on usage behavior. Unused entitlements are identified and can be deactivated or deleted after further checks.

**Business role**

Object for mapping custom functions in One Identity Manager. Business roles map company structures with similar functionality that exist in addition to departments, cost centers, and locations. This might be projects groups, for example.

## C

### **Cancellation workflow**

Approval workflow used to cancel IT Shop requests.

### **Cart item**

Product assigned to a shopping cart. A cart item shows which product is requested by whom, for whom.

### **cloud application**

Mapping a cloud application in the One Identity Manager's Universal Cloud Interface Module.

### **Cloud target system**

Mapping a cloud application in the One Identity Manager's Cloud Systems Management Module.

### **Company policy**

Object that maps company policies related to identity and access management in One Identity Manager. Attestations and risk assessments can be carried out by company policies. Policy violations can be identified and subsequently approved.

### **Company resource**

Umbrella term for all objects that can be assigned to identities or hierarchical roles or requested through the IT Shop and that are not roles themselves. For example, company resources are software, target system permissions, resources, system roles, devices.

### **Configuration parameters**

Parameters for configuring the basic settings of One Identity Manager's system behavior. Preprocessor relevant configuration parameters are parameters that are linked to preprocessor conditions. If a preprocessor relevant configuration is changed, the database must be compiled.

### **Configuration Wizard**

Program for installing and updating a One Identity Manager database.

### **Connected system**

System the objects and their properties are transferred to during synchronization. The connected system is defined by the synchronization direction. Example of synchronization direction "Target system" (One Identity Manager -> Active Directory): Here Active Directory is the connected system and One Identity Manager is the primary system of synchronization.

### **Connector schema**

The system connector extends the target system schema with additional information which is required for mapping in the Synchronization Editor.

### **Crypto Configuration**

Program for encrypting database contents of a One Identity Manager database.

**CSV connector**

System connector which allow data to be imported from CSV files.

**CUA**

Central user administration of an SAP R/3 system.

**Customer**

Identity that is entitled to request products in the IT Shop. An identity becomes a customer by being assigned to a shop.

**Customizer**

Runs processing logic which would normally be implemented in the object code, such as mutual exclusion of properties. The Customizer contains special methods and has side effects on the table columns. Several customizers can be defined for one table.

**D****Data Import**

Program for importing data into a One Identity Manager database.

**Database connection**

System connection to the One Identity Manager database.

**Database Agent Service**

Controls processing of DBQueue Processor tasks. The Database Agent Service is deployed through the One Identity Manager Service plugin. Alternatively, the Database Agent Service can be started from the command line.

**Database Compiler**

Program for compiling the One Identity Manager database after relevant changes. All VB.NET and C# program parts that are in the One Identity Manager database are compiled. The resulting assemblies are then available to One Identity Manager services and application programs.

**Database Transporter**

Program for exporting objects and custom changes from a One Identity Manager database and importing them into a One Identity Manager database.

**DBQueue**

List of tasks processed by the DBQueue Processor. The tasks queued in the DBQueue are the result of triggering, modifications to configuration parameters (for example, changes to a configuration parameter concerning inheritance) or running scheduled tasks.

**DBQueue Processor**

Component for asynchronous calculation of processing tasks in the DBQueue. The DBQueue Processor also controls cyclically recurring tasks, such as the daily maintenance tasks for calculating statistics or indexing the database.

**Designer**

Tool for configuring the One Identity Manager.

**Dynamic role**

Dynamic roles are used to dynamically assign memberships to departments, cost centers, location, business roles, application roles, and IT Shop nodes.

**E****Entitlement**

Permissions are bound to objects. Permissions are used to grant users and groups access to the objects and object properties. Examples are permissions to display and edit objects, permissions to display UI elements in One Identity Manager tools, or permissions to approve requests. see system authorization; see user permissions

**Exception approver**

Identity that can approve rule violations. Exception approvers belong to the Exception approver role and are assigned to at least one compliance rule through this role.

**Exchange Online connector**

System connector for connecting to an Exchange Online system.

**Extended schema**

A schema can be customized in the Synchronization Editor, for example, to allow or simplify mapping of complex schema properties. Label the modified schema as "extended schema".

**F****Filter**

see revision filter; see object filter; see system filter; see object selection

**G****Generic database connector**

System connector for connecting to an external database.

**Google Workspace connector**

System connector for connecting to a Google Workspace.

**GUID module**

A module GUID (module Globally Unique Identifier) identifies objects as system configuration components. For example, to transport predefined reports, processes, workflows, or mail definitions with a complete system configuration transport, the objects require a primary key with a module GUID.

## H

### **HCL Domino connector**

System connector for connecting to an HCL Domino system.

### **Hierarchical role**

A collection of departments, cost centers, locations, and business roles. Through membership in hierarchical roles, company resources can be inherited by identities.

### **Hierarchy filter**

Used to limit the number of objects to be loaded directly into the target system. It is built on the basis of the real structural objects of the target system. This filter can be used for defining the scope.

### **History Database**

System for archiving data changes.

## I

### **Identity**

An identity usually represents a real person. In addition, identities that do not represent real people, such as machine identities or service identities, can be mapped in One Identity Manager. (see also virtual identity; see also main identity/subidentity)

### **Intersection**

Objects which occur in both of the connected systems

### **IT Shop**

One Identity Manager components for supplying identities with company resources through defined approval processes. IT Shop solutions are set up in the Manager and can then be used in the Web Portal.

### **IT Shop product**

see product

### **IT Shop request**

see request

### **IT Shop structure**

Role class that groups together the components (shopping center, shop, shelf, product, customer) of an IT Shop solution.

## J

### **Job queue**

Central store for generating and running process component actions.

**Job server**

Server with the One Identity Manager Service installed.

**Job Queue Info**

Tool for controlling services running in the One Identity Manager network. It enables a detailed and comprehensive overview of the requests in the Job queue and the process history. The tool provides on-the-fly status information and makes fast error detection possible.

**Job Service Configuration**

Program for configuring the One Identity Manager Service.

**Job Service Updater**

Program for updating the One Identity Manager Service on Job servers.

**JobDestination**

One Identity Manager Service components. The Job destination component handles the process steps and returns a result to the Job provider.

**Jobprovider**

One Identity Manager Service components. A Job provider provides a Job destination process step and evaluates the result.

**L****LDAP connector**

System connector for connecting to an LDAP system.

**License Meter**

Program for maintaining and tracking One Identity Manager database licenses.

**M****Machine role**

Describes the role that a computer or server plays in One Identity Manager. You can give each computer or server several roles. This means, one, or more machine roles can be assigned. You select machine roles when One Identity Manager components are installed. The installation packages and files to be installed on the computer or server are specified in a machine role.

**Main identity/subidentity**

Describes how an identity is associated to another identity. Here, the main identity is the parent identity and the subidentity is the child identity. A main identity is a primary identity and always represents a real person. A subidentity is a virtual identity that is set up for a specific purpose.

**Maintenance**

Post processing of data that could not be saved during synchronization.

**Manage level**

The user account's manage level specifies the extent of the identity's properties that are inherited by the user account. One Identity Manager provides a default configuration for the "Unmanaged" and "Full managed" manage levels. You can define further manage levels.

**Manager (1)**

Administration tool for setting up all the information about identities. It displays and maintains all the data required for the administration of identities, their user accounts, permissions, and company-specific roles in a One Identity Manager network. Company resources identities require can be entered and assigned to them. Manager functionality can be provided by web applications.

**Manager (2)**

Identity that supervises or is responsible for identities or hierarchical roles.

**Mapping**

List of object matching rules and property mapping rules which map the schema properties of two connected systems to one another.

**Mapping direction**

Direction in which schema property data is transferred. The mapping direction determines the primary system for the schema property.

**Microsoft Exchange connector**

System connector for connecting to a Microsoft Exchange system.

**Mitigating control**

Measures to be taken to prevent a compliance rule from being violated (for example). Mitigating control Mitigating controls reduce risk by a fixed value (significance reduction). Mitigating controls are independent on One Identity Manager's functionality. For example, by frequent manual checking for irregular permissions, mitigating controls can reduce the risk posed by a rule violation.

**Module**

A module is a closed unit with a defined functionality. A module includes descriptive information, the binaries (exe, DLL), the documentation, and information about the database (see also One Identity Manager schema).

**O****Object definition**

View of database objects that allows them to be distinguished by specific properties and thus provide additional control.

**Object filter**

Filter to limit an object list that is already loaded. All schema properties of the schema (also virtual) can be used as filter criteria and linked with logical operators.

**Object matching rule**

Specifies how a concrete object of a target system schema class can be set in relation to a concrete schema class object of a One Identity Manager schema. An object matching rule encompasses the target system schema property based on which the target system objects can be uniquely identified. A distinction is made between primary and alternative object matching rules.

**Object property**

Value of a schema property for a specific object.

**Object selection**

Filter for limiting the number of objects to synchronize. For example, the system objects of an Active Directory domain are limited to one container. You can also filter single objects.

**One Identity Manager connector**

System connector that connects to a One Identity Manager database.

**One Identity Manager schema**

The One Identity Manager data model. The data model is grouped logically in modules. The modules are linked through predecessor relationships. A module can have one or more predecessors. Each module extends the schema by its own tables and columns and installs its own default objects, such as, templates, scripts, or processes. The functions of a module are not available until the module is installed in the database.

**One Identity Manager Service**

System service on servers that handle One Identity Manager processes.

**One Identity Safeguard connector**

System connector that connects to a One Identity Safeguard appliance.

**OneLogin connector**

System connector for connecting to a OneLogin system.

**Operations Support Web Portal**

Web application for help desk staff. The Operations Support Web Portal can be used to control handling of processes and DBQueue processing. In addition, passcodes can be generated for employees.

**Oracle E-Business Suite connector**

System connector for connecting to an Oracle E-Business Suite.

**Organization**

Groups hierarchical roles department, cost center, and location together.

## P

### **Password Reset Portal**

Web application that allows users to reset passwords for the user accounts they manage.

### **Peer group analysis**

Procedure to approve requests or attestation cases automatically. Identities that belong together organizationally often need the same system entitlements or company resources for their work. Requests or attestations for such objects are automatically approved or denied by the peer group analysis.

### **Performance/memory factor**

Percentage with which the reload threshold, partition size and bulk level are applied to an object type.

### **Permissions group**

Different permissions of One Identity Manager functions are grouped together in permissions groups. Permissions groups are allocated to system users and application roles. Thus, users of One Identity Manager tools obtain their permissions to One Identity Manager functions. Some permissions groups are part of the One Identity Manager installation. Other permissions groups can be custom defined in the Designer.

### **PowerShell connector**

System connector for connecting non-directly supported target systems. PowerShell cmdlets are used to run read/write operations in the target system.

### **Preprocessor condition**

Condition that limits compilation of program code. Conditional compilation allows parts of the program code to be parsed whereas other parts remain untouched. Possible preprocessor conditions are defined by configuration parameters and their options.

### **Process**

Sequence of process steps for mapping an operational workflow. The process steps are connected to one another by predecessor/successor relationships. This functionality allows flexibility when linking up actions and sequences on object events.

### **Process component**

Component available for use in process steps.

### **Process parameter**

Parameter that is permitted for a single task of a process component.

### **Process plan**

Contains the basic configuration for automatically running a process.

**Process step**

Represents one processing task in a process.

**Process task**

Task to be run by a process.

**Processing method**

Method used to process objects within a synchronization step. Example: Add object (insert), update object (update), delete object (delete). Processing methods and their mandatory parameters are define with the schema type.

**Product**

Company resource that is assigned to an IT Shop shelf and can therefore be requested. Only company resource assigned to service items can be added to the IT Shop as products.

**Product bundle**

Template for a shopping cart which groups together cart items that are frequently requested together. Public product bundles are available to all users as soon as they are released. Non-public product bundles can be used only by the owners of the product bundle.

**Project template**

Template used by the project wizard to create a preconfigured synchronization project.

**Project wizard**

Wizard which aids configuration of synchronization projects.

**Property mapping rule**

Describes how a target system schema property is mapped in the One Identity Manager schema.

**Provisioning**

Actual changes to an object in the One Identity Manager database (added, modified, deleted) are made immediately written to the target system.

**Provisioning workflow**

Specifies the order in which the synchronization steps are provisioned.

**Q****Quota**

A maximum set of system objects that can be processed in a synchronization step with a particular processing method. If the quota is exceeded during synchronization, none of the object of this schema class with this processing method are handled and synchronization is stopped.

## R

### **Reference scope**

Used to resolve reference between objects of different systems. The reference scope specifies the system in which objects for resolving references may be found.

### **Relative complement**

Objects that only occur in one of the two system systems involved in synchronizing.

### **Remote connection server**

Job server installed with the RemoteConnectPlugin and the target system connector is installed. If direct access to the target system is not possible, a remote connection can be set up. Communication between the Synchronization Editor and Target System is done through a remote connection server.

### **Renewal workflow**

Approval workflow that can be used to extend a temporary request. If approved, the new expiration date will be applied to the existing request.

### **Request**

Request for products in the IT Shop. Products can be company resources, such as system roles or system entitlements, or membership in hierarchical roles. Requests follow a defined approval process that determines whether a product may be assigned or not.

### **Request parameters**

Parameters describing additional features such as color, size, or equipment of the product to be requested. Requesters specify the required parameter value when they make the request.

### **Request property**

Collection of request parameters that can be additionally specified for a product. Request properties are assigned to service items or service categories.

### **Resource**

Equipment that is necessary for an identity's work efficiency, for example, mobile phones, desks, company cars, or keys. Resources can be any equipment that is not system entitlements, devices, or software.

### **Resource type**

Customer-specific criteria for grouping resources.

### **Revision**

Highest value of the revision counters of all a schema type's objects that are synchronized during a synchronization run. This value is stored in the DPRRevisionStore table, in the Value column. It is used as a comparison value for revision filtering when the same workflow is synchronized the next time.

**Revision counter**

Information about the last change to a system object. The revision counter is used to determine the objects that have changed since the last synchronization.

**Revision filter**

Filters all system objects not changed since the last synchronization. The deciding factor being the revision property modification. Synchronization can be speeded up with revision filtering.

**Revision filtering**

Method for accelerating synchronization. Only objects that have changed since the last synchronization are fully loaded and synchronized. Revision filtering can only be used if the target system supports it.

**Revision property**

Schema property containing the revision counter of a system object. Example for revision properties of Active Directory groups: in the target system schema - UNS-Changed; in the One Identity Manager schema - Revision date.

**Risk index**

Security risk for the company if a company resource is assigned to an identity or a compliance rule, company policy, or attestation policy is violated. A risk index can be entered for any company resource, SAP function, attestation policy, company policy, or compliance rule. An identity's risk index is determined by the risk indexes of their directly and indirectly assigned company resources. It is given as a value between 0 (no risk) and 1 (problem).

**Risk index function**

Method used to calculate risk indexes. The risk index function defines the data sources, the objects to be included, the calculation type, and the table column of the function's target object.

**Rogue Detection**

See rogue modification

**Rogue modification**

Discrepancy in the data between object properties of two connected system that is detected when the direction of mapping of the associated property mapping rule is opposite to the direction of synchronization.

**Role**

see: hierarchical role

**Role assignment**

Assignment of SharePoint user accounts or groups to a SharePoint role.

**Role class**

Criteria for grouping similar hierarchical role together, such as departments or cost centers. To differentiate between different business roles, define company specific role classes. Role classes are used to specify which company resource assignments are possible through roles in a role class.

**Role definition**

Assignment of SharePoint permissions to a permission level.

**Role type**

Customer-specific criteria for classifying hierarchical roles. Role types are mainly used to regulate approval policy inheritance within an IT Shop structure. Furthermore, role types can be used to structure hierarchical roles or shops in the IT Shop by customer-specific criteria.

**S****SAP function**

Definition of selected transactions and permissions objects that can be used to test which SAP authorizations SAP user accounts can have in an SAP client.

**SAP function categories**

Criteria for grouping SAP functions.

**SAP R/3 connector**

System connector for connecting to an SAP R/3 system.

**Schedule**

Task to run on a cyclical basis. Schedules control regular running of processes, calculation tasks, and other scheduled tasks. You define the start and interval times for the scheduled tasks. The activation time can be given in local time or Universal Time Code. A schedule can be in control of several tasks.

**Schema**

Data model of a connected system. The schema describes all the main data from the connected system. see target system schema; see One Identity Manager schema; see connector schema; see extended schema

**Schema browser**

Synchronization Editor components, in which details of the entire schema of the connected target system and the details of the entire One Identity Manager schema are mapped.

**Schema class**

Subset of a schema type. The result list of a schema type is filtered by defined criteria. Example: Active Directory contacts are Active Directory user accounts with the property objectclass = "CONTACT".

**Schema editor**

Schema browser components that can be used to edit user-specific virtual schema properties.

**Schema property**

Property of a schema type. Refers to exactly one column of a table or view of the database based schema or exactly one object type property of the non-database based schema.

**Schema type**

Defines an object type within a schema. Refers to exactly one table or view of the database based schema or exactly one object type of the non-database based schema.

**Schema Extension**

Program for extending One Identity Manager schema by custom tables, columns, database view and indexes.

**SCIM connector**

System connector, which connects a cloud application using the System for Cross-domain Identity Management specification.

**Scope**

Section of a connected system which should be synchronized. The scope is defined with a filter.

**Script property**

Schema property whose value is determined by a script.

**Script variable**

Variable whose value is determined by a script.

**Server function**

Defines the function of a server in One Identity Manager. Depending on the server function, processes are handled. When installing a server, the possible server functions are predefined based on the selected machine role.

**Service category**

Criteria for grouping service items. For a product from the service catalog to be select, its service item must be assigned to a service category.

**Service item**

Objects that are required for requesting company resources as products in the IT Shop and for internal invoicing.

**Shadow copy**

Configuration data of a synchronization project stored as an XML definition in the database. If a shadow copy is present, loading a synchronization project is significantly accelerated.

**SharePoint connector**

System connector for connecting to a SharePoint farm.

**SharePoint role**

A permission level linked to a specific SharePoint site.

**SharePoint Online connector**

System connector for connecting to a SharePoint Online farm.

**Shelf**

IT Shop structure that is part of a shop and can have products assigned to it. Shelves make up a hierarchically structured IT Shop solution together with shops, shopping centers, and products.

**Shelf template**

Templates for automatically setting up shelves in the IT Shop and adding company resources to them. Shelf templates can be used if shelves with the same products are set up in more than one shop. One Identity Manager distinguishes between global shelf templates, special shelf templates and shopping center templates.

**Shop**

IT Shop structure to which shelves and customers are assigned. Together with shelves, products, and shopping centers, shops form a hierarchically structured IT Shop solution.

**Shopping center**

IT Shop structure under which you can group shops together. Together with shelves, shops, and products, shopping centers form a hierarchically structured IT Shop solution.

**Significance reduction**

Value by which the risk index of a compliance rule, SAP function, attestation policy, or company policy is reduced when a mitigating control is assigned. The risk index (reduced) is calculated from the risk index and the significance reduction.

**Snapshot**

Snapshot of an object at a certain point in time, optionally with dependent objects.

**SoD**

Segregation of Duty (separation of functions)

**SoD Conflict**

Non-compliant combination of authorizations in SAP roles or profiles that can lead to compliance rule violations. SoD conflicts are identified through SAP functions.

**Software**

Software application managed in One Identity Manager. Software can be assigned directly to identities, inherited via hierarchical roles, or requested from the IT Shop.

**Software Loader**

Program for loading new or modified files into the One Identity Manager database in order to distribute them in the One Identity Manager network using automatic software update.

**SQL processing server**

Job server that handles SQL processes.

**Start configuration**

Specifies which synchronization configuration components are used for a specific synchronization. Specifies the synchronization schedule.

**Start up sequence**

Sequence of start up configurations that are automatically run one after the other. By default, a start up sequence is started by a schedule.

**Start up sequence instance**

Maps a start up sequence while it is running. As soon as a start sequence is run, an instance of the start sequence is created in the DPRStartSequence table. This instance contains information about the runtime status and errors of the entire start up sequence. Likewise, an instance is stored in the DPRStartSequenceHasProjection table for each startup configuration that is run. This instance contains information about the runtime status and errors of the current synchronization.

**Subidentity**

A subidentity is a virtual identity that is set up for a specific purpose, such as for an administrative user account or to map different roles in the company. A subidentity is always connected to a main identity.

**Synchronization**

The process of comparing data between One Identity Manager and a target system. Objects and their properties are compared by fixed rules. Synchronization results in the identical data situation in the target system and One Identity Manager database.

**Synchronization buffer**

One Identity Manager table with information about referenced objects which could not be assigned by synchronization.

**Synchronization engine**

One Identity Manager component which runs synchronization and provisioning tasks.

**Synchronization in direction**

Direction in which synchronization is run. The primary system is defined by the direction of synchronization.

**Synchronization of single objects**

Current changes of an object in the target system (change, delete) are immediately written to the One Identity Manager database.

**Synchronization primary**

System that has data sovereignty during synchronization. The primary system is specified by the direction of synchronization. Example of synchronization direction "Target system" (One Identity Manager -> Active Directory): Here Active Directory is the connected system and One Identity Manager is the primary system of synchronization.

**Synchronization project**

A collection of all data required for synchronizing and provisioning a target system. Connection data, schema classes and properties, mappings, and synchronization workflows all belongs to this.

**synchronization server**

Job server installed with the target system connector. All One Identity Manager actions are run against the target system environment on the synchronization server.

**Synchronization step**

Specific rule for processing exactly two schema classes.

**Synchronization workflow**

Specifies the order of all the synchronization steps to be run during synchronization.

**Synchronization Editor**

One Identity Manager tool for configuring target system synchronization.

**Synchronization Editor Command Line Interface**

Synchronization Editor components with which synchronization projects can be created on the command line.

**Synchronization Editor Module for Windows PowerShell**

Synchronization Editor components with which synchronization projects can be created by PowerShell CmdLet.

**System connector**

Software interface for accessing a connected system.

**System entitlement**

Object used in the target system to control access to target system resources. A user account obtains the required permissions for accessing target system resources through its memberships in system entitlements. Examples: Active Directory group, SAP R/3 role, SharePoint Online group see permission

**System filter**

Used to limit the number of objects to synchronize in the connected system. The connector only loads the object found through this filter.

**System object**

Object from the target system. A system object always belongs to a schema class.

**System role**

Combines company resources that must always be assigned together to identities, into a single package. Different types of company resources can be grouped into one system role, for example Active Directory groups, software and resources. System roles can be assigned directly to identities requested through the IT Shop, or inherited via hierarchical roles.

**System user ID**

User ID with which a user logs in to the One Identity Manager tools. The system user ID depends on the selected authentication module. For example, it can be a central user account, a login name for an Active Directory domain, or a system user.

## T

### **Target system**

An instance of a target system in which the identities managed by One Identity Manager have access to network resources. Example: An Active Directory domain X for target system type "Active Directory", a directory Y for target system type "LDAP", a client Z for target system type "SAP R/3".

### **Target system browser**

Synchronization Editor components, with which objects in the connected system can be viewed and edited.

### **Target system schema**

Data model of a specific target system. Describes all the data originating from the target system.

### **Target system synchronization**

Post processing of objects that were marked as outstanding by synchronization.

### **Target system type**

Grouping similar target systems. Examples: Active Directory, LDAP, SharePoint.

### **Template**

Rule for mapping object properties. Templates can be applied to an object and also have a cross-object effect.

### **TimeTrace**

One Identity Manager function you can use to track changes to an object that were made up to any point in the past. In its analysis, the TimeTrace function includes the data changes saved to the One Identity Manager database as well as the records stored in a History Database. You can use this to find out who had which permissions at which point in time. You can apply historical data to the current object and restore the object to the status prior to the change.

## U

### **UID**

Artificial primary key generated by One Identity Manager as soon as the object is inserted into the One Identity Manager database. The UID is a unique value, which does not change even if the properties of an object change. An object is identified by a UID and can be uniquely referenced by it.

### **Unified Namespace (UNS)**

Virtual system in which different target systems can be mapped with their structures, user accounts, system entitlements, and memberships. Target systems such as Active Directory domains can be mapped in just the same way as custom target systems. Through the Unified Namespace a general, cross-target system mapping of all connected target systems is achieved. Other core functions of

One Identity Manager, such as identity audit, attestation, or reporting, can be used across target systems.

**Universal Cloud Interface connector**

System connector for connecting to the Universal Cloud Interface.

**Unix connector**

System connector that connects to a Unix host.

**UNS**

see Unified Namespace

**Update server**

Job server that provides automatic software update of the other servers.

**User account**

A user account represents access to a target system. A user account has permissions to perform actions in a target system. A user account is usually linked to an identity.

**User permissions**

Permit users to perform an operation that affects an entire computer rather than a specific object on the computer. Examples are logging in as a service or changing the system time. see permissions

**V**

**Variable set**

Used to configure synchronization configuration for different systems. Each variable set contains at least the variables for the system connection parameter. The value of the variables are redefined for different uses.

**Virtual schema properties**

Schema class property added by the system connector or the user.

**W**

**Web Installer**

Program for simplifying installation and configuration of web-based applications created with the Web Designer.

**Web Portal**

Web-based application that provides various workflows. In the Web Portal, users can change their own main data, edit employee data, request company resources in the IT Shop, delegate their own responsibilities, edit approvals, attestations, or rule violations.

**Workflow**

see decision workflow, see provisioning workflow, see synchronization workflow,

**Workflow wizard**

Wizard which aids configuration of synchronization workflows.

# 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.

**Copyright 2024 One Identity LLC.**

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

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 website (<http://www.OneIdentity.com>) for regional and international office information.



**Patents**

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

**Trademarks**

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

**Legend**

-  **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.
  
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.