DirX Identity V8.7

Identity Management and Governance

User and access management aligned with business processes

The challenge of user and access management

Today's business environment is a challenging one for user and access management in the enterprise. Business relationships are growing more complex, blurring the line between internal and external business processes. They are also more dynamic, requiring greater flexibility and responsiveness in the enterprise's business practices, policies and processes. Companies are under pressure to open their IT infrastructure to an ever-increasing number of users, both inside and outside the company, and to ensure the highest productivity and privacy for these users, all while controlling IT administrative costs and leveraging existing investments wherever possible. To this end, companies are increasingly looking to external cloud services as a way to complement their on-premise IT services and address time-to-market and cost containment concerns. Now more than ever, granting the right people the right access to the right resources at the right time and managing the risks are essential elements of enterprise security as companies strive to protect their corporate data and systems and remain innovative, productive, responsive, compliant and cost-effective business entities.

Several key business objectives are driving governance over the user and access lifecycle on the enterprise IT network:

Regulatory compliance. Secure user access to corporate information has become a major legal issue for business as governments worldwide continue to pass laws intended to ensure the security, privacy, and integrity of sensitive data like consumer and financial records. Domestic and international regulations for financial services, healthcare organizations, pharmaceutical companies and other industries require a secure access control infrastructure, and non-compliance can result in legal action against the enterprise, resulting in heavy financial penalties, even criminal proceedings. The more global a company's reach, the more complex the requirements for regulatory compliance can be and the greater the cost of failure. To prove compliance, companies must be able to show "who did what, and when, with what information", which requires a single view of a user's access rights to all IT systems, a way to track this access automatically on an on-going basis - identity-based audit and access certification - and a way to archive this information securely for long-term access and analysis.

The move to eBusiness. The use of the Internet to provide content and business processes to employees, subscribers, customers, and trading partners is now an essential tool for increasing user productivity and streamlining business-to-business collaboration. Companies are offering Web portals and services for everything from personalized employee access to company information to B2B access to supply chain management processes. As a result, more and more IT applications and content are going online, and access to these applications and content is required by a larger and more varied set of users. And, while consuming the services made available by cloud providers can off-load the need to provide them on premises, it also issues new challenges to maintaining security governance, managing risk, demonstrating accountability and proving regulatory compliance.

Fast and flexible change management. User and access management need to be flexible and responsive to dynamic changes in user populations and business processes brought about by mergers, acquisitions, and the move to eBusiness. To maximize productivity and guard against security risks, companies must be able to react in real time to changes in their users and the access rights these users need to do their jobs. New users and users changing job functions must immediately get the access rights they need to be up and running quickly, while departing users must have their access rights revoked immediately to close security holes. The governance of users and their access rights must remain consistent and effective across the ever-changing business and user landscape.

Bull
atos technologies

Improved information security. Although eBusiness fosters productivity, personalization, and collaboration, it also exposes the corporate infrastructure to greater security threats from malicious users. To combat this problem, companies need to clearly define corporate security policies and implement access governance – "who is allowed to access what information, how and why". The governance of user access is ideally combined with a risk management process that helps to select the adequate level of governance and suggest mitigation actions.

Cost control. Companies need to control or reduce costs to keep competitive, and they are increasingly focusing on IT as an area for cost-cutting. Companies are looking for ways to minimize the number of calls made to their help desks and hotlines for things like forgotten passwords, and they are looking to reduce the administrative costs associated with user management and provisioning - the process that makes the IT resources available to its users. Corporate budgets are cutting investment in IT systems as companies seek to get better returns on the IT systems they already have. Companies also need transparency into the assets they provide to their users and the costs associated with these assets. Service providers need to track the costs associated with users such as disk usage, mailbox size, and application packages used and base remote access fees, while sales organizations need to track the costs of mobile phones, laptops, pagers, and PDAs and retrieve these assets from their users when they leave the organization.

The obstacle to realizing these business objectives is the one function-one system structure of the typical IT network. In the conventional IT infrastructure used in most big companies today, there is a one-to-one correspondence between a function or resource available to users and the IT application/system that provides that function. Consequently, user management, access management, password management and auditing are carried out on a per-IT system basis. IT staff must administer users and their access rights on each IT system in the network or in the cloud, usually by manual administration. Users get one account and one password for each IT system they need to use. Each IT system has its own audit or monitoring function to track changes to users and their access rights on that system.

This structure has negative consequences for user and access management:

- Decentralized user management and provisioning means that user and access data is duplicated across IT systems and usually becomes inconsistent over time, making it difficult to find correct and up-to-date information and to de-provision users.
- Decentralized auditing and monitoring makes it difficult to track changes to users and their access rights. There is no way to tell what a single user's total access rights are across the enterprise - even his account names are different for each IT system he uses - making it very hard to audit for regulatory purposes.
- One password per IT application means that users must remember a lot of different passwords, one for each system they need to use. Password proliferation leads to more help desk calls, lost productivity as users wait for password reset, and increased IT administration costs.
- Manual administration is expensive and error-prone and leads to delays in provisioning and de-provisioning users, which decreases productivity, jeopardizes security and compliance, and introduces data inconsistencies.

To address the key business drivers and overcome the present limitations requires an enterprise-wide, cross-platform, centralized and automated user management, provisioning and access management system that controls access to IT resources based on business roles, policies and processes. The system must provide identity and access governance aligned with business processes and must allow off-loading routine administrative functions and decisions from IT staff to users and their managers so that decisions about what users really need are made by the people who know best. Identity and access management (IAM) technology has evolved to a well-defined market category and has reached the depth and breadth to offer an effective way to satisfy these requirements.

Identity and Access Management

Identity and access management (IAM) is an integrated solution that makes user and access management transparent across the different systems, including cloud solutions, that make up the enterprise's IT infrastructure. IAM is defined as the services, technologies, products, and standards that enable the use of digital identities. Identity management addresses the need to administer users and security policies across the IT infrastructure, while access management addresses the real-time enforcement of the security policies in force for each user of the IT infrastructure. Audit automatically records all identity and access management transactions and stores these records securely.

With the DirX product family an integrated product suite for identity and access management solutions is provided, which consists of

- DirX Identity, a comprehensive identity management and governance solution
- DirX Directory, the standards-compliant LDAP and X.500 directory server
- DirX Audit, providing analytical insight and transparency in the identity and access management processes
- DirX Access, a policy-based Web access management, Web single sign-on and federation product.

The remainder of this document describes the DirX Identity features, functions, and components.

DirX Identity Features

DirX Identity provides a comprehensive, process-driven, customizable, cloud-ready, scalable and highly-available identity management solution for enterprises and organizations. It delivers risk-based identity and access governance functionality seamlessly integrated with automated provisioning. DirX Identity includes powerful, Web-based user self-service and delegated administration, request workflows, password management, user management, cross-platform, real-time provisioning, access certification and metadirectory functionality. The provisioning of users and their access rights in various target systems is driven by powerful, centralized role management supported by flexible policy, workflow and segregation of duty engines. In addition, comprehensive scheduling, monitoring and auditing are available.

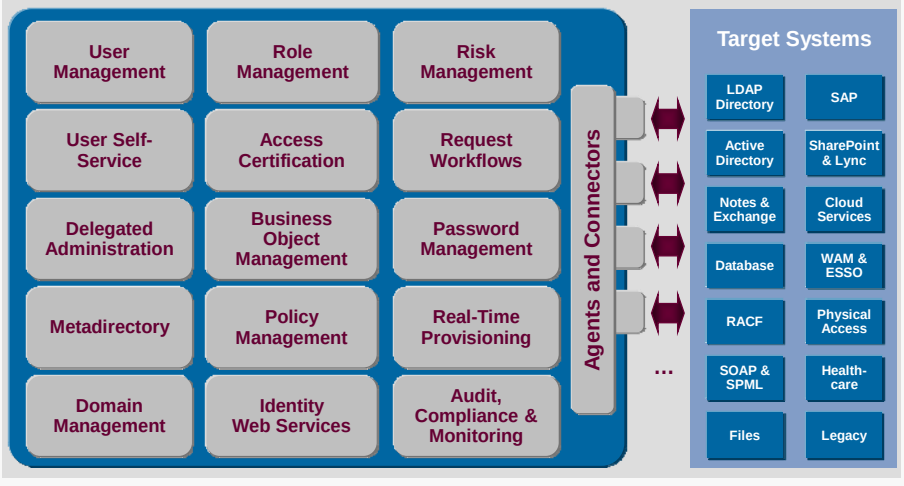


Fig. 1 - DirX Identity Functionality

User Management

User management includes all the activities related to the creation, consolidation, maintenance and use of user accounts, user attributes, roles, entitlements and other data relevant for the lifecycle management of users. DirX Identity supports user management with four types of objects:

- User: A user object in DirX Identity represents the user with its personal attributes, roles, entitlements and accounts. DirX Identity is able to manage multiple accounts per user object, but only one account per target system.
- User facet: User facets are special representations of users. They serve to model multiple privilege profiles for a user, one for each position the user holds within an organization, for example a student who works both as a teaching assistant and as a tutor. User facets share the same accounts with the user. Using user facets one can define and find out which privileges have been granted for which position.
- Persona: Users may also work in different functions in the company, for example as administrators or as project managers. The accounts and the entitlements for each functional representation of a user might be quite different, typically more than one account per target system is required and also auditing should be able to distinguish between these functions. For this purpose, persona objects can be appropriate.
- Functional User: A functional user object represents a resource that is assigned to a responsible user (sponsor). Examples are a global or group mailbox, a physical room with a phone or a working student entry. Such a resource is managed by the user.

User management consists of two main tasks: maintaining an accurate and up-to-date directory of users to be provisioned and assigning users to roles. The user directory is kept up-to-date and consistent through request processes from the users and/or their managers (user self-service and delegated administration) and by data synchronization workflows (for example, with the enterprise HR system) provided by DirX Identity's metadirectory functionality.

In DirX Identity, user management tasks include:

- Adding users, changing the attributes of users and deleting users in the identity store with DirX Identity Web Center or Manager
- Creating and synchronizing users on a regular basis from various sources such as HR, CRM, and ERP systems or from an existing corporate directory master

To reflect an enterprise's Human Resource management process, DirX Identity allows for the maintenance of lifecycle attributes:

- A start date at which the user is to become active; for example, the date at which a new employee starts work
- An end date at which the user is to be removed; for example, the contract end date for an outside contractor
- The start and end date of a leave of absence; for example, a maternity leave

Personas and Functional Users

The lifetime of the user object comprises the lifetime of all associated persona objects. The lifetime of a persona object can be shorter than the user lifetime. This is one possibility to model different contracts for a user that works in the same company but for different organizational units.

In contrast to a functional user, the persona objects normally change their status with the corresponding user object. Re-assignment to another user does not make sense.

In contrast to a persona, the functional user can survive the user and has to be re-assigned to another sponsor (user) if the user is deleted or no longer responsible for it.

In DirX Identity, persona management tasks include:

- Adding personas, deleting personas, and changing the attributes of personas, especially the attributes associated with persona lifetime and deactivation periods.
- Synchronizing the DirX Identity personas with a corporate directory master makes sense if the concept of different user representations is also supported by the corporate directory. Otherwise, only user objects are synchronized, and personas are maintained in DirX Identity.
- Assigning privileges to personas. Assigning privileges is done the same way and follows the same rules for personas as for users.

Note: Most of the tasks described above also apply to user facet management.

Functional user management tasks include:

- Adding functional users, deleting functional users, and changing the attributes of functional users.
- Maintaining the sponsor if the related user for the functional user changes.
- Assigning privileges to functional users. Assigning privileges is done the same way and follows the same rules for functional users as for users.

User Self-Service

DirX Identity makes a number of tasks available for self-service through its Web Center user interface. User-oriented self-service tasks include:

- Registering yourself with one or more of the corporate services available for self-registration
- Making changes to your own data, including your own passwords
- Recovering and resetting forgotten passwords through a challenge-response procedure
- Requesting roles for yourself
- Checking the status of your requests and approvals
- Delegating your access rights (or some of them) for user and role management to other users

Access policies are used to make sure that a user has appropriate access rights for self-service tasks.

Delegated Administration

Administrative access to DirX Identity data is controlled by access policies and by personal delegation. By configuring access policies, administrators grant access rights to DirX Identity data like users, business objects, roles, target system accounts and groups, policies and workflows. For example, an access policy can specify that project team leaders can edit the user data and assign project-specific roles to the members of their project team. Other access policies can specify the approval responsibility for users and roles.

These users in turn can delegate these rights or a subset thereof, to someone else, optionally for a specified period of time. This especially applies to manage users and roles, assign roles to users or approve requests for such assignments from the users. For example, a project leader who is away for two weeks can delegate the rights to assign project-related roles to the members of his team to another person in his group. Optionally the project leader can permit his substitute to assign only some roles which he specifies when he performs the delegation.

Delegated administration tasks in Web Center include:

- Creating new users, roles, groups, business objects and policies
- Making changes to user, role, business object and policy data
- Assigning roles to existing users
- Approving the assignment of roles to users or business objects or the creation of users, roles, and business objects
- Certifying the assignments of roles to users
- Deleting existing users, roles, groups, business objects and policies
- Running status reports

Access policies are used to control which of these administrative tasks a given administrator can perform and on what users and other data he is allowed to perform them.

Password Management

DirX Identity provides a comprehensive password management solution for enterprises and organizations. Providing end users with a quick and flexible way to reset their password based on strong password policies or to unlock their account DirX Identity password management helps organizations to significantly reduce helpdesk costs and to

strengthen security of password-related authentication processes.

The password management feature set includes

- Self-service password reset: Users reset forgotten passwords or unlock accounts using alternative credentials.
- Assisted password reset: Administrators or service desk staff reset forgotten passwords or unlock accounts for users.
- Password expiration: Remind users to change their passwords before they expire.
- User enrollment: Users select and answer security questions (also known as authentication or challenge questions) as alternative credentials.
- Password Listener for Windows: Catch password changes from Windows desktop.
- Password synchronization: Synchronize password changes to target systems in real-time.
- Password policy management: Manage and enforce rules for complexity, expiration and history of passwords.
- Privileged account password management: Manage and control access to passwords for shared privileged accounts.
- Audit and reporting: Keep track records of password-related actions and generate reports.

For a detailed description of the password management features of DirX Identity and their benefits see the datasheet DirX Identity - Secure and flexible Password Management.

Role Management

The goal of role management in DirX Identity is to establish a logical layer for the modelling and management of access control information that is generic enough to cover many of the relevant IT system's authorization/access control methods:

- Group-based IT systems control access rights via account membership in groups. Making an account a member of a group gives it the access rights that have been granted to the group. User groups, profiles, and application-specific roles are examples of group-based methods of access control.
- Attribute-based IT systems control access rights via attributes in the accounts. For example, in Active Directory, a set of account attributes defines a user's mailbox; there is no concept of group membership.
- Some systems, like Microsoft Active Directory, provide both types of access control.

DirX Identity uses a standards-based role management model that supports parameterization for granting different types of access according to contextual information, provides request workflows with approvals and re-approvals and access certification for role authorization and re-authorization and enforces segregation of duties (SoD) policies for regulatory compliance.

The role model used in DirX Identity is based on American National Standards 359-2004, the information technology industry consensus standard for RBAC (ANSI/INCITS 359). The ANSI RBAC reference model organizes the elements of RBAC into four groups of incrementally increasing functionality: core RBAC, hierarchical RBAC, static separation of duty (SSD) relations and dynamic separation of duty (DSD) relations. DirX Identity supports level 3 RBAC, which consists of hierarchical RBAC with SSD. However, while ANSI RBAC includes system resources in its access control model, DirX Identity leaves the management of the individual resources to the local administration of the target systems.

Figure 2 illustrates the relationship between DirX Identity's role model and the access control systems of the IT systems. As shown in the figure:

- A **user** represents a person inside or outside of the enterprise for the purposes of role assignment.
- A **target system** represents an IT system that authenticates and authorizes users. Examples of target systems are operating systems, messaging systems, directories and databases, ERP applications, Web portals and eBusiness applications, groupware applications, and mainframe security systems.
- An **account** represents a user in a target system. Users can have accounts in many different target systems. In addition, DirX Identity can handle privileged accounts that can be temporarily assigned to users.
- A **group** represents a set of access rights in a specific target system. Groups provide the link between the role/permission access model and the target system's access control model. A group can be assigned directly to a user or indirectly through permissions and roles that include the group (entitlement).
- A **permission** represents a set of access rights that is target-system-neutral. A permission can be assigned directly to a user or indirectly through roles that include the permission. A permission aggregates a collection of groups from one or more target systems.
- **Roles** control users' access rights to IT systems and resources. Roles are assigned to users either manually (through user self-service or administrative action) or automatically (via provisioning policies or inheritance from business objects). DirX Identity supports general role hierarchies as defined in ANSI RBAC – roles that correspond to job descriptions can in turn contain (aggregate) simpler roles. Consequently, a role aggregates a collection of roles, a collection of permissions, or both.

When a user is assigned a role, DirX Identity provisions the target systems to which the role ultimately applies with authentication data – the accounts – and the authorization data – the account-group memberships - required to establish the role. This process is called "role resolution" and is discussed in more detail in the "Provisioning" section.

DirX Identity's role model can manage access control for all IT systems that allow for group-based or attribute-based administration of access rights. DirX Identity can also manage roles that are not associated with a physical IT system. The corresponding groups, called virtual lists, are used to support different business processes, for example, lists for facility access.

DirX Identity's role model supports **parameterized RBAC**, where the access rights modeled by a generic role or permission can be customized on assignment to a specific user based on contextual information such as the value of role or permission parameters. A **role parameter** is a variable whose value is provided at role assignment time. For example, one generic role "Project Member" can be assigned multiple times to the same user for several different projects. Each time the role is assigned to the user, a specific project name is given for the role parameter. A **permission parameter** is an attribute in a user entry whose values influences the permission's resolution into groups. For example, suppose a user in the Sales department of an organization is assigned

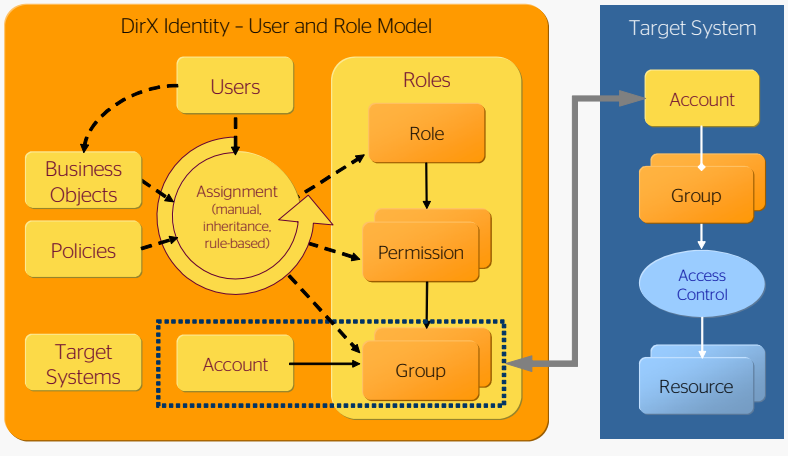


Fig. 2 - DirX Identity User and Role Model

the permission "Departmental File Server". If the permission is parameterized by the "Department" user attribute, DirX Identity can use the "Sales" value of the user's "Department" attribute to resolve the permission into specific target systems and groups that are relevant for the Sales Department File Server. The permission "Departmental File Server" is the same for all employees of the organization, but its resolution to a specific target system depends on the employee's actual department. Role and permission parameters greatly reduce the number of permissions and roles that need to be defined and make role management and assignment based on high-level business roles (role-based assignment) appealing and manageable in the enterprise.

Role-based assignment allows an enterprise to structure access rights to resources according to well-defined business roles derived from the enterprise's business semantics and users. The role-based model works well when access rights are more static – when they depend on the person's job, for example, educational services trainer or quality manager. In this case, roles don't need to change when organizational attributes change. Role parameters and permission parameters can be used to make role-based provisioning more dynamic.

Business Object Management

A business object is a collection of data related to a business structure in the enterprise such as an organizational unit, a cost center or a project. Custom objects can be added easily. Business objects in an identity management system help to automate user-role assignment and reduce identity data redundancy.

In DirX Identity, business objects are used to

- Build any kind of structure like organizational or project structures.
- Manage data consistently. For example, location can be defined with all address data only once and linked automatically to all related user entries. This helps to reduce redundancy of user data in the identity store by providing a single point of control for common user data.
- Automate user-role assignment by allowing the roles referenced by the business object to be inherited by the users linked to it (see figure 2). For example, one can assign roles to an organizational unit. If a user is assigned to this unit, he inherits the roles automatically. If he is removed from the unit, the corresponding roles are also removed from the user. Changes to the information in the business object – including references to roles – are automatically propagated to the users linked to the business object.
- Define parameter structures for related drop-down lists or role parameters.

In DirX Identity, business object management tasks include:

- Adding business objects in a hierarchical structure, changing the attributes of business objects and deleting business objects in the identity store with DirX Identity Manager or Web Center
- Assigning/linking users to the appropriate business objects
- Assigning roles (or permissions or groups) to business objects so that users linked to the business objects can automatically inherit them
- Creating and synchronizing business objects on a regular basis from various sources such as HR, CRM, and ERP systems or from an existing corporate directory master
- Defining proposal lists that use the business objects

Privileged Account Management

In addition to accounts that are related to just one specified identity (user), target systems typically hold a small number of privileged accounts that are entitled to target system management. Such accounts, as for example the root account in UNIX systems, are allowed to perform critical actions in the target system with a high security risk. Privileged accounts are not related to a specific user. A number of persons can use them in parallel.

DirX Identity provides means to control and audit privileged accounts:

- Any user can be assigned to a privileged account by assigning a role. All features of role management like request workflows with approvals and re-approvals, access certification or SoD are available.
- Users that are assigned to privileged accounts can read the password in clear text to perform the login action.
- They are also entitled to change the password of privileged accounts.
- Removal of a user from a privileged account automatically enforces a password change.
- Alternatively one can define that assignment of a user to a privileged account copies his certificates to the account. This allows authentication via certificates at the target system side.
- DirX Identity automatically changes all expired privileged account passwords.

Segregation of Duties

In a role-based system, conflicts of interest can occur as the result of a user receiving access rights associated with conflicting roles. The ANSI RBAC SSD component prevents this type of conflict by enforcing constraints on the assignment of users to roles. DirX Identity implements this model of separation of duties - also called **Segregation of Duties** (SoD). Enterprise SoD policies specify which user-role assignments constitute conflicts of interest or pose unacceptable security risks. DirX Identity enforces these policies during user-role assignment and will not make a user-role assignment that it determines to be an SoD violation unless special approval has been performed. SoD policies can also be defined for user-permission and user-group assignments.

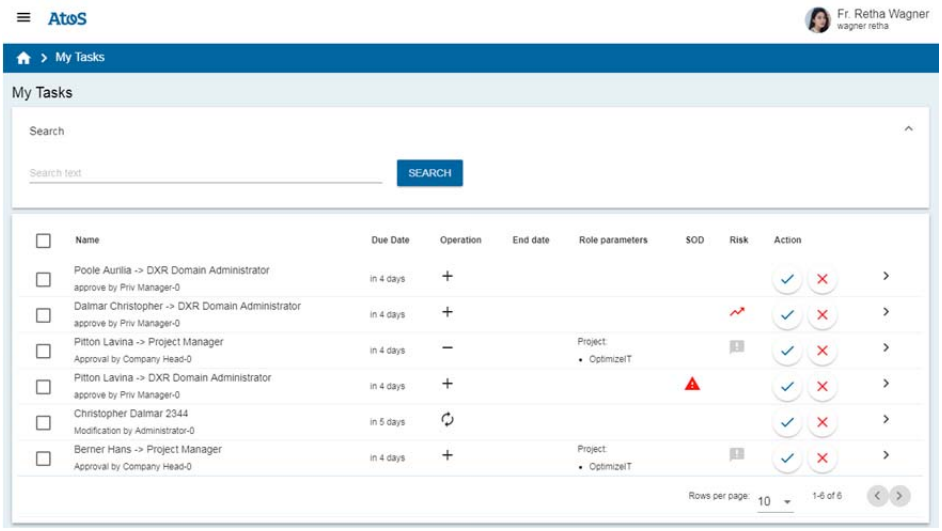
Alternatively or additionally, DirX Identity allows interfacing with third-party GRC systems such as SAP BusinessObjects GRC (Access Control) for external SoD checks.

Policy Management

A **policy** is a high-level directive that is used to control the decision-making behaviour of the DirX Identity system.

DirX Identity supports the creation of **security policies** and **administrative policies** to control its operations. Security policies manage access to resources, while administrative policies manage the integrity of DirX Identity user, role, and target system data. DirX Identity policies include:

- **Access policies** to control self-service and delegated administrative access to DirX Identity data. An access policy defines a set of



DirX Identity Business User Interface Sample – Approve Roles - Overview

access rights to DirX Identity data like users, business objects or roles. For example, an access policy can specify that project team leaders can edit the user data and assign project-specific roles to the members of their project team. Access policies allow the enterprise to structure administration tasks according to its business or organizational model and to restrict the operations on DirX Identity user and role data that particular users can perform as well as the visibility of role assignments. Access policies are also used to control, which menu entries are visible/usable for users in the DirX Identity Web Center user interface.

- **Audit policies** to define which attribute changes of which objects are relevant to compliance with corporate security policies and government regulations and which therefore should be tracked.
- **Password policies** to control the requirements placed by DirX Identity on user passwords, such as password complexity, expiration dates, the behavior of the system after failed logins, etc.
- **Provisioning policies** to grant and revoke roles automatically based on the values of user attributes against the conditions of the policy, which in turn controls the access rights received in the target systems. Provisioning rules are used to define this type of policy. For example, a provisioning rule might specify that a certain application can only be used by employees in the Sales department. The value of the user attribute "Department" is evaluated against the rule, and those employees whose "Department" value is "Sales" are granted the role to use the Sales application. When the value of the user attribute - in this case, "Department" - no longer matches the condition of the rule - in this case, "Sales" - the "Sales application" role is automatically revoked and the user is de-provisioned.
- **Attribute policies** to track changes to critical attributes and automatically trigger request workflows for approval.
- **SoD policies** to specify the combination of roles, permissions and groups that cannot be assigned to a user in parallel without special approval.
- **Validation policies** to compare target system data against the information within DirX Identity to detect and reconcile deviations between the target system's accounts, groups, and account-group memberships and the same information in DirX Identity. Validation rules are used to define this type of policy.
- **Consistency policies** to check the consistency of user and role data within DirX Identity and repair any inconsistencies, for example, to keep account and user data consistent. Consistency rules are used to define this type of policy.

The DirX Identity policy engine processes administrative policies either dynamically or periodically (depending on the kind of policy), while the DirX Identity security manager processes security policies dynamically.

Request Workflows

DirX Identity provides several types of workflows that support user self-service and delegated administration activities:

- Request workflows that create new identity management data (creation workflows), like users, roles, permissions, policies, and so on including global id generation for user creation workflows
- Request workflows that change existing identity management data (modification workflows). Examples are attributes of users, roles or business objects. Attribute policies govern which attribute changes have to be approved and which workflow for which attribute is to be started.
- Request workflows that create and maintain relationships between identity management data (assignment workflows); for example, assigning a role to a user or assigning a role to another role (role hierarchies).
- Request workflows that delete existing identity management data (deletion workflows), like users, roles, permissions, policies, and so on.

DirX Identity allows requestors and approvers to digitally sign their requests and approvals respectively.

DirX Identity provides template request workflows. Customers can make copies of these templates and then use DirX Identity's graphical workflow editor to tailor them to their requirements.

Management of request workflows is protected by access policies and comprises start, stop, suspend and resume operations as well as change participant functionality.

Approval

Request workflows can contain optional approval steps that manage the authorization requirements for the request.

A user-role assignment, for example, can require initial approval and can also require re-approval after a specified period of time (for example, every 6 months) or on a specified date and time. **Approval** and **re-approval** steps can be defined for these roles to carry out the approval and/or re-approval process automatically. The approval process supports a variety of models for determining participants, including single individual approver, static and dynamic approver groups, and policy-driven calculation. If required, additional methods can be implemented via Java extensions.

Users request an approval via the Web Center or the Business User Interface. The workflow then notifies each person in the approval path – for example by e-mail – that an approval request is to be handled. The approver uses either Web Center, the Business User Interface or the Approval App to accept or reject the request. Escalation mechanisms help to cope with problems such as timeouts, etc. In addition to individual approvers, one can assign a group of approvers, e.g. helpdesk personnel, to handle an approval request. In this case, the approval is performed by one member of the group on a first-served basis.

Risk Management

DirX Identity provides risk assessment for identities based on an extensible set of risk factors.

To classify users into risk categories from low to high, risk factors for users are regularly calculated and aggregated into a compound risk according a customizable configuration. Examples for risk factors are: SoD violations, imported accounts and group memberships and total number of group memberships or privileged accounts. For any user, Web Center displays its risk category. DirX Identity Manager additionally displays all individual risk factors. Compliance officers, line managers or administrators can then monitor the risk values and plan actions to reduce the number of high risk users e.g. by running appropriate certification campaigns or by enforcing additional approval steps.

For any requested change in a user's privilege assignments, DirX Identity can compare the compound risk before and after. If the risk category would increase by the requested privilege assignment, additional approval steps may be required.

Access Certification

Access certification allows attesting that access rights are assigned to users in compliance with internal security policies and legal regulations. DirX Identity supports certification campaigns for users and privileges, e.g. roles or groups, to support such compliance processes:

- A certification campaign performs access certification for a selectable subset of users or privileges, e.g. for all users in the HR department or for all sensitive privileges. For each user or privilege, one or more approvers e.g. line managers or role owners are automatically defined. For each user or privilege to be certified, the approvers can see all assignments and can decide whether to accept or reject each individual assignment. As an option, privileges that have been assigned manually and were rejected in the campaign are revoked automatically and corresponding users are notified. DirX Identity supports both one-time and periodic certification campaigns. Certification campaign phases are controlled via start date, due date, end date and expiration date. When a certification task is approaching the due date, reminder notifications are sent to the approvers.
- DirX Identity also supports access certification of an individual privilege assignment by the re-approval feature. In this case the approval for selected and critical privileges is repeated after a specified time interval. Re-approval is done either by running the same workflow as for the initial

privilege approval or by a specific one. If an approver rejects the assignment, the privilege is immediately revoked. Re-approval for selected privileges can be enabled together with timing conditions.

Real-Time Provisioning

Provisioning is the process of establishing the target system-specific access rights to which a user-to-role assignment ultimately resolves. Provisioning makes use of all the processes of user, role and policy management discussed in earlier topics. Provisioning is a two-step process:

- Calculating the accounts, the groups, the target systems to which the accounts and groups belong, and the account-group memberships that result from the role assignments to users and creating the account, group, and group membership data in the identity store – this process is called role resolution and can involve the matching of user attributes to provisioning policies, permission parameters or role parameters where appropriate.
- Using the connectivity infrastructure to physically transfer the access rights data immediately from the identity store to the target systems and ensure the consistency of the target system data with the access rights derived from the role resolution. To optimize support of a huge number of target systems (up to 10.000), e.g. in outsourced environments, DirX Identity allows clustering target systems, i.e. one workflow can provision many target systems.

User-to-role assignments that require approval are not provisioned until every approval has been received.

Note that it is the administrator of the target system who assigns access rights to the resources on the system for a given group. This process is outside of DirX Identity and is accomplished using the target system's administrative tools and enforced by the access control components of the target system. The enterprise needs to have an organizational process in place that controls both the set-up of policies and the role structure and the assignment of access rights to groups in target systems.

When there is a change in the user's roles, permission parameters, or role parameters, or when there is a change in a user's attribute that controls a provisioning policy, DirX Identity automatically and immediately performs a new role resolution and provisions all changes to the target systems.

DirX Identity provisioning services provide centralized, consistent, single-point and fully automated administration of users and their access rights within the enterprise IT infrastructure.

DirX Identity supports the execution of any executable or script from Java-based workflow user hooks. This allows for example via the PowerShell technology the management of home folders for Microsoft Active Directory accounts or immediate mailbox enabling for Microsoft Exchange.

Service Management Support

DirX Identity supports the integration of service management systems such as support ticket systems or action request systems both as source systems and as target systems:

- Service Management as a source:
  If a customer has a ticket system already in place that is used for any type of request, it makes sense to reuse that system as a source for orders. A ticket can be used to trigger specific identity management actions. Examples of such tickets are requests for user creation or modification or for role assignments.
- Service Management as a target:
  If the customer has a ticket system in place that is already used to initiate manual provisioning of target systems, DirX Identity can place an order by means of a ticket. Local administrators work on these tickets from the ticket system and confirm the completion of their tasks. Connectors to commonly used ticket systems (Remedy, HP OpenView) can be implemented via custom connectors within a customer project.
- Manual provisioning of offline systems: If the customer has no ticket system in place and if there are target systems that are not managed by DirX Identity, i.e. the target system is offline, one can use a manual provisioning approach via DirX Identity request workflows. In this case, the provisioning workflows for synchronization establish a request workflow for each event. The administrators of the target systems get these add, modify or delete requests via email, perform the actions manually and confirm the completion of their tasks.

Scheduled Change Management

It allows managing changes that become effective in the future, e.g. a move of a person to another department scheduled for July 1st. Consequently, such a change may lead to changes of assigned privileges. At the effective date, DirX Identity changes the person's data and processes subsequent changes that are mandated by policies and privilege resolution, Administrators can view pending and processed change orders made on DirX Identity objects to track the order status and results.

Metadirectory

DirX Identity metadirectory is the set of services that integrates the disparate directories, user databases, and application-specific information repositories into a centralized data store and provides the connectivity, management and interoperability functions that unify the user data ("join") and ensure the bidirectional attribute flow (synchronization) in this fragmented environment. The metadirectory provides:

- **Integration services** that collect and integrate user data from multiple authoritative sources - human resources directories, enterprise resource planning (ERP) systems, customer relation management (CRM) and Supply Chain Management (SCM) databases - into a single, **unique digital identity** that represents the user to be provisioned in the IT systems.
- **Synchronization services** that maintain an accurate and up-to-date identity store of these identities and synchronize identity data from the identity store back into the authoritative sources.

For both integration and synchronization services:

- DirX Identity agents and connectors enable data exchange between the different target systems and the identity store
- Execution can be scheduled, triggered by specific events, or initiated by hand by an administrator and can be monitored and logged for auditing purposes.
- Flexible data flow and ownership models allow the enterprise to control who owns the data, what data is synchronized, and how update operations on the data are carried out, including authoritative control, filtering, and operations mapping.

Default applications

A powerful set of default applications are delivered with DirX Identity. They hold ready-to-use examples for typical identity creation, maintenance and synchronization processes that can be easily tailored to set up customer solutions.

The default applications

- Provide applications for all supported connected directories and agents
- Are based on a unique architecture with a standard set of control parameters and scriptable extensions accessible via wizards
- Can easily be upgraded due to a clear separation of standard script code and customer extensions.

Audit and Compliance

DirX Identity provides configurable, customizable, and comprehensive audit trail, status reporting and query mechanisms to help ensure and document regulatory compliance.

The audit trail mechanism can track all relevant identity management events, recording information such as the date/time the event occurred, the identity that initiated it, the users who approved it, and whether it was carried out by hand or automatically by a policy. The audit trail mechanism allows backtracking of an event to the causing event within a hierarchical event chain. DirX Identity supplies a set of pre-configured audit policies and permits customers to define their own audit policies to satisfy individual corporate requirements. If the audit logs are not directly supplied to DirX Audit, they are stored in log files in XML format to a central location for centralized visibility and traceability. The files can be optionally secured

with a system-specific digital signature to make them tamper-proof. A command-line tool allows for verifying these signatures.

The status reporting mechanism can generate regulation-specific and custom status reports in XML, HTML, or pure text format on all DirX Identity objects on demand or at scheduled intervals. Customers can use DirX Identity reporting to create reports on specific objects, object lists or object collections and their attributes, user-role, permission, and group assignments, delegated users and administrators, unused roles, the entire role catalogue, the complete role hierarchy, and provisioning workflow hierarchies. DirX Identity provides pre-configured reports for common regulations and allows customers to use Extensible Stylesheet Language Transformations (XSLT) to customize them or create their own reports to meet specific requirements. Access policies can be applied to reports to safeguard their security.

While a status report typically comprises the content of many related DirX Identity objects and shows them as a whole, a query typically runs on a specific type of object - for example, a user or a role - with a specific search filter and returns a set of objects to examine. A query can be used, for example, to return a list of objects in an error state. An administrator can examine each object, fix the error, then run the query again to make sure the object is no longer returned in the list.

DirX Identity provides for seamless integration with DirX Audit. DirX Audit also belongs to the DirX product suite. It provides for centralized, secure storage, analysis, correlation and review of identity-related audit logs via a single user interface providing auditors, security compliance officers, and audit administrators with the answers to the "what, when, where, who and why" of user access and entitlements.

DirX Identity auditing, status reporting and query work in concert with other DirX Identity services to permit fast, cost-effective deployment of regulatory compliance controls:

- Metadirectory services allow identities and their access rights to be centrally managed, providing greater transparency into identity management activities and tighter administrative control with fewer administrators
- Automated role- and policy-based user provisioning ensures that corporate security policies are consistently enforced across all points in the corporate IT infrastructure, avoiding error-prone, ad hoc application of access rights by many different IT administrators working in different parts of the enterprise
- Request workflows with approval and re-approval steps automate the application of corporate authorization policies, ensuring that they are applied consistently rather than on a case-by-case basis

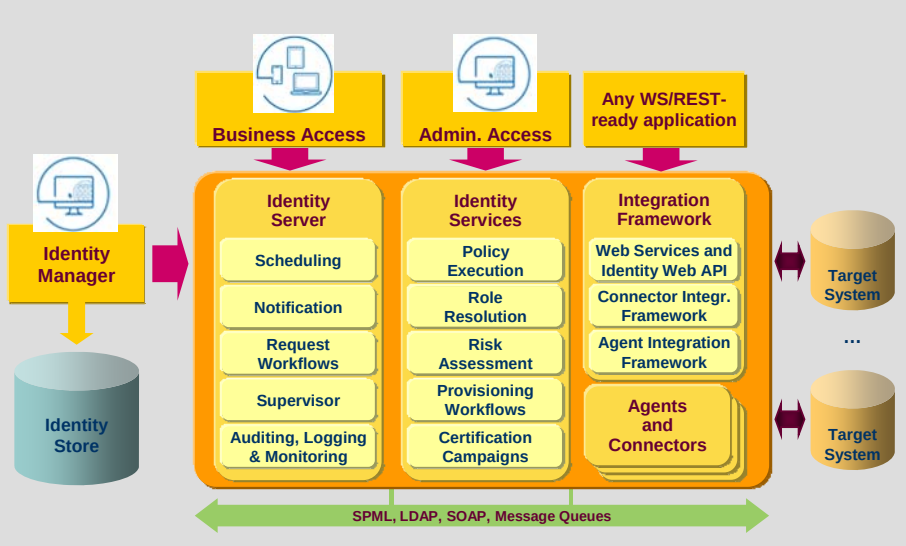


Fig. 3 - DirX Identity – Service Architecture

- An additional level of compliance control is added by allowing requestors and approvers to digitally sign their actions in the workflow
- Automated, real-time user de-provisioning ensures that access rights of terminated employees and contractors are immediately and accurately revoked on all affected IT systems
- Automated reconciliation services can detect suspicious accounts and access rights on corporate IT systems and eliminate them automatically or report them to the appropriate administrator for handling
- Segregation of duties enforcement by user provisioning services prevents user-role assignments that violate corporate security policies or create unacceptable risks
- Pre-configured audit policies and reports help to jump-start regulatory compliance efforts

Domain Management

Multi-tenant support is provided by the concept of DirX Identity domains.

A DirX Identity domain is a high-level separation of DirX Identity data that can be used to establish different policies and role models in a single DirX Identity system. Domain management tasks consist of:

- Setting up a domain
- Managing DirX Identity administrators
- Generating information about a domain (reports)
- Maintaining database consistency

Several sample domains are delivered with DirX Identity which illustrate the typical way to work with DirX Identity in a customer environment and show most of the features DirX Identity provides. The sample domains can be automatically installed with DirX Identity.

DirX Identity Components

The main components of DirX Identity include

- Identity Business Access
- Identity Administration Access
- Identity Manager
- Identity Store
- Identity Server
- Identity Services
- Agents and Connectors
- Identity Web Services
- Identity REST Services
- Identity Integration Framework
- Messaging Service

Figure 3 illustrates these components and the relationships between them.

Identity Business Access

The Identity Business Access provides different user interfaces for administering the business features of DirX Identity:

- Identity Business User Interface
- Identity Web Center
- Identity Approval App

Identity Business User Interface

The features provided by the DirX Identity Business User Interface focus on the most common use cases of business users. Following the mobile first approach, the user interface is designed for tablets and smartphones as well as for desktop computers. The Business User Interface is based on HTML5. It supports the following use cases:

- Login with password
- Display and edit own profile
- Request a new role
- Display and edit role parameters of assigned roles
- Show pending role requests
- Approve single/bulk role requests

Identity Web Center

The Identity Web Center is the component that enables user self-service and delegated administration from a Web browser. Customers can integrate some or all of the Web Center's functions into their Web portals, and they can customize the layout of the Web Center's HTML pages.

The Identity Web Center provides Web single sign-on integration with SAP NetWeaver and leading Web access management products, e.g. DirX Access and Entrust GetAccess. Generic mechanisms allow single sign-on integration with many other Web access management products. In addition, DirX Identity Web Center supports Microsoft Windows single sign-on.

For integration with SAP NetWeaver Portal, the Identity Web Center is provided as a complete URL-iView.

The Identity Web Center for Password Management (available with the Password Management Option) provides an enhanced and specialized interface for password management functionality.

Approval App

DirX Identity provides an approval application called DirX Identity Approvals which is specifically designed for iOS-based mobile devices such as smartphones and tablets. It provides users with a fast and comfortable way of carrying out approval tasks from their mobile devices. The app communicates with DirX Identity using REST-based services.

DirX Identity Approvals is available for download from Apple's iTunes store.

Identity Administration Access

The Identity Administration Access provides different user interfaces for managing and monitoring the DirX Identity servers:

- Identity Web Admin
- Identity Server Admin

Identity Web Admin

Identity Web Admin is a Web-based management interface for the Identity Server built on the Java Management Extensions (JMX) technology for creating management and monitoring tools. Customers can use Web Admin or any other JMX client - for example, Oracle's JConsole - to monitor and tune the Java-based Identity Server from the Web. Web-based administration tasks include supervising server status, observing server statistics, viewing process instances, and optimizing for load distribution and performance.

The Java-based Identity server maintains a dead letter queue that stores erroneous ("dead") messages and events that have encountered problems. Administrators can use Web Admin to examine the information about an item in the queue, determine the cause of the problem, re-configure the server accordingly, and process the message (or event) again. Administrators can also use Web Admin to delete messages in the queue that are no longer needed.

Special Web interfaces allow controlling and monitoring the workflow engines, e.g. monitoring workflow statistics, and the Java-based identity server.

Identity Server Admin

The Web application Server Admin allows to monitor the health state of DirX Identity servers and to move tasks between servers for load balancing or ensuring business continuity. The Server Admin is available with the High Availability Option of DirX Identity.

Identity Manager

The Identity Manager provides an easy-to-use, Java-based graphical user interface for transparently configuring and managing all aspects of DirX Identity, including:

- Users and services
- Roles and policies
- Integration, synchronization, and request workflows
- Target systems and authoritative sources

Identity Manager can also be used to monitor provisioning, all types of workflows, role resolution and policy execution.

Identity Manager supports the SSL (Secure Socket Layer) protocol for authenticated, encrypted communication with the Identity Store.

Identity Manager supports strong authentication with smart cards. It provides authentication/ login via all CardOS smart cards that are supported by Atos CardOS API V5.3.

Identity Store

The Identity Store is an LDAPv3 directory – for example, a DirX directory server or a Sun Java System Directory Server - that serves as the consolidation point (the directory "join") for identity integration from authoritative sources and as the distribution point for provisioning and synchronization of the target systems in the enterprise IT infrastructure.

The Identity Store is the repository for all DirX Identity configuration data, including user data, business objects, roles, policies, target system account, group, and account-group membership data and the configuration and operational data required by the metadirectory integration and synchronization services. The Identity Store provides the central point for management of this data and for its synchronization back to the target systems and authoritative sources. To provide for distribution and scalability, parts of the configuration and monitoring data can be distributed to other directory servers.

Identity Server

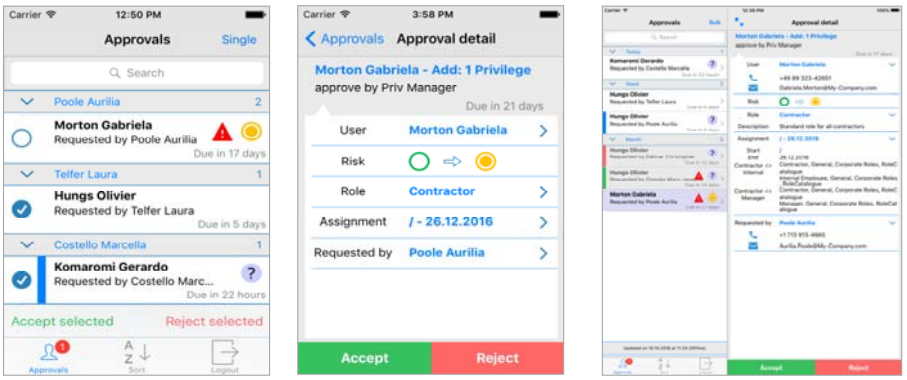
The Identity Server provides a comprehensive runtime environment for event-triggered and scheduled provisioning workflows. The server provides components for:

- Handling event-triggered provisioning tasks like the real-time synchronization of provisioning events or password synchronization
- Scheduling provisioning and real-time workflow runs, including recovery and retry operations in the event that problems occur
- Notifying administrators via email and SMS about provisioning workflow events
- Messaging services, message queue support and JMS clients
- Auditing, logging, and collecting statistics to help administrators and auditors to analyze and control DirX Identity's execution environment

Server components can be distributed across different systems in the enterprise network to provide for load-balancing, high availability and scalability.

DirX Identity provides two types of Identity Server: a Java-based Identity Server that handles Java application programming interfaces (APIs) and a C++-based Identity Server that handles C and C++ APIs.

The **Java-based Identity Server** is designed to handle primarily event-triggered provisioning processes. These types of processes are required, for example, by password management: the real-time provisioning of user password changes made through the Identity Web Center or coming from the Windows Password Listener. When a user changes his or her password, the Java-based Identity Server ensures that the new password is synchronized



DirX Identity Mobile Access – DirX Identity Approvals App

immediately with the user's accounts in the appropriate target systems.

The Java-based Identity Server also supports the real-time provisioning of changes that are calculated, for example, by role resolution. Changes to a user's role assignments or parameters may require changes to accounts and account-group memberships in one or more target systems. The DirX Identity system sends these changes as events to Java-based Identity Server workflows, which transfer the information immediately to the target systems.

Another example is the change of a business object, for example an organizational unit. Changed attributes are propagated via events to all users that are assigned to this unit. Assignment of roles to the unit results in immediate inheritance of these roles to all of these users.

This technology is completely built on the Services Provisioning Markup Language (SPML) standard. Java-based Identity Server workflows can also run in scheduled mode, mainly to guarantee the Identity Store's consistency.

The Java-based Identity Server offers features for load distribution and scalability, error handling - including notification services - and configurable auditing and logging.

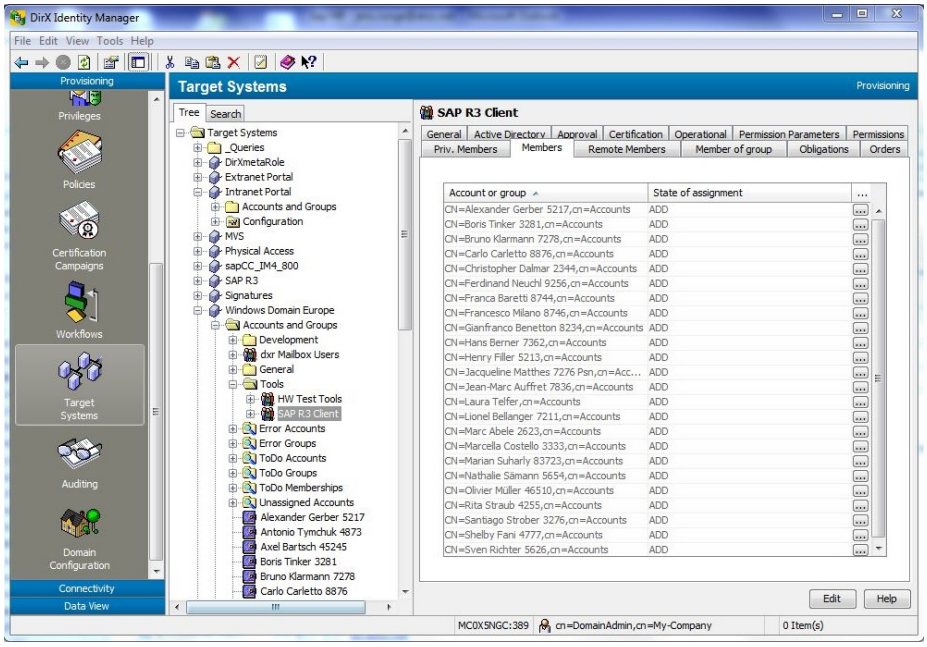
The **C++-based Identity Server** is designed to handle provisioning in full and delta mode: the provisioning of complex objects or a large number of objects at a scheduled time, for example, a group of new employees all hired on the same date, a group of new employees that have moved from one department to another, or a new subscriber database that needs to be integrated and provisioned.

The C++-based Identity Server is the runtime environment for executing workflows that use the DirX Identity meta controller and agents. It can also host connectors that handle C++-based interfaces to target systems that are used by the Java-based Identity Server's event-triggered and scheduled workflows. The C++-based Identity Server supports distributed and nested workflow runs in a heterogeneous network as well as exception handling and recovery mechanisms including restart of workflows according to previously automatically set checkpoints.

Identity Services

DirX Identity Services run in the Identity Server environment and include:

- The policy execution service, which runs rules against various objects for automated role assignment and consistency and validation checks, including automatic reconciliation.
- The role resolution service, which calculates from abstract role structures the detailed access rights required in the necessary target systems.
- The request workflow service, which handles actions related to configured request workflow activities; for example, attribute input from users and approval of role assignments or objects by the people in an approval list or by calculated approvers.



DirX Identity Manager Sample – Account-Group-Membership

- Event-triggered provisioning workflow services, which perform fast, immediate real-time provisioning or password synchronization.
- Scheduled provisioning workflow services, which perform complex identity creation, maintenance, and target system provisioning tasks.
- A campaign generator to run and monitor certification campaigns.

Agents and Connectors

DirX Identity agents and connectors enable data exchange between the different target systems and the identity store during integration and synchronization operations.

A **connector** is a Java component that implements the connector interface and performs update and search operations for a specific kind of target system. It runs in the Identity Server and is called by the provisioning real-time workflow to exchange data between a target system and the identity store.

An **agent** is a stand-alone executable that supports the interfaces to a specific target system to enable data exchange between that target system and the identity store. It may be realized by a connector embedded in the Identity connector framework.

Agents can only work with scheduled provisioning services, while connectors can work with both scheduled and event-triggered provisioning services.

In addition to native DirX Identity connectors, DirX Identity provides connector bundles that run in OpenICF connector servers. DirX Identity leverages an OpenICF connector server as **provisioning proxy**. The integration of DirX Identity with OpenICF connector server is accomplished by the native DirX Identity OpenICF proxy connector.

Identity Web Services

The Identity Web Services are used to integrate DirX Identity's provisioning features into SOA-compliant application environments. One can handle users, roles, permissions, groups, accounts, target systems and business objects completely via DirX Identity's Web Services interface. They implement the OASIS SPML standard. In addition to the SPML standard operations (add, modify, delete, lookup, search) the services support the following capabilities:

- User: add including global id generation, role assignment, disable/enable, password change
- Role: role parameters
- Permission: match rules
- Group: account-group memberships.
- Account: disable/enable and set password, account-group memberships, read password policy, authentication via security questions or signature of requests
- Target system: tombstone feature and references
- Business objects: references to roles and other business objects.

For all object types a user hook can intercept requests and responses and perform custom operations such as moving entries, creating or checking unique identifiers.

DirX Identity also provides SOAP-based workflow services to control the execution of request workflows: methods to create, modify and manage workflows are provided. Clients can retrieve worklists and information about workflow definitions and instances and approve their tasks.

The SOAP-based Identity Web Services provide Web single sign-on integration with SAP NetWeaver and leading Web access management products, e.g. DirX Access and Entrust GetAccess.

Identity REST Services

The Identity REST Services are used to integrate DirX Identity into application environments which want to use the standard HTTP protocol and the performance and scalability advantages of REST-based services. Especially, they can be used by modern, HTML5-based Single-Page applications; one example is the DirX Identity Business User Interface.

The REST services adhere to SCIM 2, the System for Cross-domain Identity Management. They provide the following functionality with JSON as data format:

- Approval – Users can approve their tasks and accept or refuse them either task-by-task or in bulk mode.
- Self Service – Users can request roles and view and edit their profile.

Identity Integration Framework

The Identity Integration Framework comprises the public interfaces of DirX Identity. This framework allows customers to:

- Use the Identity Web Services or REST Services.
- Use the SPML-standardized set of interfaces and common utilities in the connector integration framework to implement custom connectors to access target systems via Java or C++ based interfaces.
- Use the agent integration framework to integrate executables or batch files as agents into batch-oriented workflows
- Integrate parts of the Identity Web Center into their portal applications or use the Identity Web API to add extra functionality.

Supervisor

With the High Availability Option each Java-based Identity Server hosts a supervisor that can monitor another Java-based Identity Server or several C++-based servers. The supervisor provides for automatic fail-over between servers if a monitored server is down.

Messaging Service

The messaging service provides reliability features such as store and forward and automatic redelivery of messages. It is Java Message Service-compliant. DirX Identity leverages Apache ActiveMQ as messaging service.

Standards support

DirX Identity components support several standards for connectivity, storage and data formatting:

- The identity store and configuration repositories use Lightweight Directory Access Protocol (LDAP) and the connectivity services use LDAP to communicate with LDAP-enabled target systems
- The role management model implements the ANSI RBAC reference model (ANSI/INCITS 359).
- All provisioning components work with Services Provisioning Markup Language (SPML) 1.0 requests and responses internally: data exported and imported from/to external systems are converted to and from SPML.
- Identity Web Services implement the OASIS SPMLv2 specification using the SPMLv2-DSML profile.
- The Identity Integration Framework (Java, C++, C#) supports SPML 1.0 for the construction of custom connectors that transform internal requests to proprietary APIs.
- The Identity Services and Identity Server messaging queues comply with Java Messaging Service (JMS).
- The Identity Web Admin is built on Java Management Extensions (JMX) technology. As a JMX agent the Identity Java Server can be managed via JMX.
- DirX Identity connectors provision target systems via Simple Object Access Protocol (SOAP) version 1.2 and SPML version 1.0 and 2.0, and workflow and provisioning services are called via SOAP.

Security

The authentication and authorization mechanisms of the respective LDAP directory allow protecting attributes and passwords. DirX Identity provides additional security features:

- All components can optionally work in SSL/TLS mode when using LDAP connections.
- Data transfer via the messaging service can be optionally encrypted to provide high security during network transfer.
- Most attributes, especially passwords can be stored in strong encrypted mode in the Identity store. DirX Identity guarantees that data transfer and logging is secure up to the interface of the connected target directory.

Scalability

To achieve scalability in a DirX Identity deployment, one can set up multiple instances of Java-based and C++-based servers.

DirX Identity provides features for static and dynamic load balancing on these instances:

- For static load balancing, Java-based Workflows can be assigned to selected Java-based server instances according to their type: Request Workflows, Provisioning, Password Change and Event Maintenance.
- For dynamic load balancing, Java-based Workflows can be dispatched among multiple Java-based server instances that have been statically assigned for the respective workflow type.
- Classic, Tcl-based batch workflows can be distributed to all installed C++-based DirX Identity servers to distribute load.

Deployment

DirX Identity provides mechanisms to reduce deployment time ensuring smooth transition from one environment to another, e.g. from staging systems such as development or test systems to production systems as well as configuration management systems. This also allows for rapid deployment of multiple DirX Identity instances.

Business Continuity

With the High Availability Option DirX Identity supports continued operations for the message service, for Tcl-based workflows, and for Java-based workflows.

The Server Admin Web application provides an overview of the state of all Java- and C++-based servers as well as the message brokers and allows moving functionality between them. DirX Identity supports both administrative failover and automatic failover. In case of administrative failover administrators can move

- A Java JMS adaptor and thus the associated workflows to another Java-based Identity Server.
- The request workflow processing to another Java-based Identity Server.
- The scheduler service to another Java-based Identity Server
- The Tcl-based workflows to another C++-based Identity Server

DirX Identity supports automatic failover via circular monitoring: each Java-based Identity Server monitors the state of another one, altogether building a circle. If the monitored server is not available any more, the monitoring server takes over its functionality. One of the Java-based Identity Servers monitors the C++-based servers. If it is not available any more, it moves the workflows to another C++-based Identity Server.

The automatic failover solution is controlled by a Groovy Script that can be adapted to project specific needs.

DirX Identity provides backup and restore capabilities to help ensure data availability and reliability. This includes a synchronized, joint backup and restore for the Java-based Identity Server and the DirX Directory Server.

Nagios Support

DirX Identity provides a set of specialized Nagios plugins and commands for the JNRPE Nagios add-on that can be used in an existing Nagios environment to monitor the status of DirX Identity service resources and operations and to collect statistics about these items for later analysis.

The DirX Identity Nagios plugins allow monitoring:

- All information provided via JMX, especially from Java-based Identity Server and other JMX-enabled programs such as Apache ActiveMQ and Tomcat

- The C++-based server using internal DirX Identity interfaces.

The DirX Identity Nagios plugins provide input parameters for specifying warning and critical thresholds to be monitored for DirX Identity service operations, offering DirX Identity administrators the opportunity to respond to problems detected by the plugins and displayed by the Nagios server before they become severe, and to track their resolution.

DirX Identity provides commands for the Nagios JNRPE add-on to check:

- The state of the Java-based Identity server
- The outstanding responses of a specific JMS adaptor
- A statistics attribute of a specified workflow
- JVM memory usage
- The state of the C++-based server

Customization

DirX Identity is designed to be highly customizable with regard to its functions, objects and to the display of its objects in its user interfaces. Customization includes

- Configuration via LDAP, XML, flags, parameters, etc.
- Extensibility using JavaScript, Java, C++ or by integrating other processes

License Options

DirX Identity is available with two options for the base license: **Business Suite** and **Pro Suite**. The **Pro Upgrade** option allows a customer to extend the Business Suite license to a Pro Suite license. The base licenses can be extended by the following add-on license options: **Connectivity Packages**, **Password Management Option** and **High Availability Option**.

Table 1 and table 2 at the end of this document provide an overview of the main features of the Business Suite, the Pro Suite and the Password Management Option.

DirX Identity Business Suite

DirX Identity Business Suite provides user lifecycle management, rule-based provisioning of accounts and groups in target systems, validation and reconciliation of target systems, metadirectory functionality, Web-based user self-service to manage own data, business object management, domain management and default connectivity. It also provides report functionality on users, accounts groups, target systems, and access policies.

DirX Identity Pro Suite

DirX Identity Pro Suite is based on the Business Suite and additionally provides Identity and Access Governance (IAG) functionality such as role management with associated policy management and reporting functionality, segregation of duty support, request workflows, approval and re-approval, access certification, rule-based and manual assignment of roles to users, password management functionality, audit services to audit password changes and administrative changes in DirX Identity

DirX Identity Password Management Option

In addition to the basic password management functionality provided with the Pro Suite, the Password Management Option provides a specialized Web Center for Password Management that allows password change by end-users for a subset of their accounts, display of the password change status, and challenge/response procedures to reset forgotten passwords by administrators or help desk. This option also includes the Password Reset Client for Windows.

DirX Identity High Availability Option

The High Availability Option supports continued operations with automatic and administrative failover. The supervisor monitors the servers and allows for automatic failover. The Web application Server Admin provides for administrative failover by manually moving tasks between servers.

DirX Identity Connectivity Packages

DirX Identity provides connectivity to many target systems that are structured in connectivity packages.

Default Connectivity

DirX Identity provides default connectivity to DirX Access, to SPML-enabled applications, to LDAP directories, to DirX Identity domains and to Unix systems (Linux) based on PAM as part of the basic system.

DirX Access

- Supports DirX Access V8.4 or higher
- Seamless integration by shared LDAP user repository
- Real-time provisioning and password synchronization
- Runs on Microsoft Windows and all supported Linux platforms

SPML-enabled Applications

- Supports SPML V1.0 and V2.0
- Supports add, modify, delete, search and getSchema operations
- Real-time provisioning and password synchronization
- Agent and agentless mode possible (in this case the connector runs in the Java Server)
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

LDAP Directories

- Connectivity to any LDAPv2 or LDAPv3 compliant system
- Full and delta import and export of all object classes and all attributes
- Real-time provisioning and password synchronization
- Support of LDAP filters and multi value attributes
- Agent and agentless mode possible (in this case the connector runs in the Java Server)
- Customization / extension possible
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

DirX Identity Domain

A specialized real-time connector supports the provisioning of a DirX Identity domain. It leverages directly the features of the service layer, namely the rules of the object descriptions, assignment of roles even with role parameters and the direct role resolution. This connector especially simplifies importing of users by calculating default values for attributes, applying provisioning rules for automatic role assignment and requesting approvals where necessary.

- Connectivity to a DirX Identity domain
- Support of all entry types from users to business objects, roles, groups and accounts
- Evaluates object descriptions and processes their rules to calculate default values and values of dependent attributes
- Assignment of privileges with start and end date and of roles with parameters
- Password changes for users and accounts
- Searches paged and non-paged
- Applies provisioning and consistency rules after all changes.
- Performs role resolution immediately after entitlement-relevant changes

Unix PAM

- Supports UNIX PAM LDAP structures according to RFC2307 on the supported Linux platforms
- Full and delta import and export of accounts, groups and group memberships
- Real-time provisioning and password synchronization
- Agent and agentless mode possible (in this case the connector runs in the Java Server)
- Customization / extension possible
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Note: Provisioning of Unix accounts can also be done with the OpenICF connector bundle for Unix which is available in the Proxy Connectivity Package.

CSV export/import

- Full import and export of CSV files

Connectivity Package for Microsoft AD

Active Directory / Exchange / Lync

- Supports Microsoft Active Directory for Windows Server 2008 R2, Windows Server 2012 / 2012 R2 and Windows Server 2016 via the Microsoft ADSI LDAP provider as agent and via LDAP interface as connector
- Integrated handling of Exchange 2000/2003/2007/2010/2013/2016 mailboxes
- Integrated handling of Microsoft Lync 2013
- Integrated post-processing, e.g. creation of shares
- Full and (native) delta import and export of all ADS object classes (e.g. users and groups)
- Real-time provisioning and password-synchronization (connector)
- Supports serverless binding, paging on export (for large amounts of entries), LDAP filters, multi-value attributes and move of objects between different trees
- Delta support for deleted entries
- Ready-to-use management of home folders for Microsoft Active Directory accounts or immediate mailbox enabling for Microsoft Exchange via PowerShell technology
- Error reporting and tracing
- Agent runs on Microsoft Windows platforms; connector runs on all supported platforms

Note: Provisioning of local Windows accounts can be done with the OpenICF connector bundle for Windows Local Accounts which is available in the Proxy Connectivity Package.

SharePoint

- Supports Microsoft Office SharePoint Server 2007, 2010 and 2013
- The solution uses the Windows Active Directory accounts
- Provisioning of groups and group memberships in SharePoint
- Import of groups and group memberships from SharePoint sites, used for initial load and target system validation
- Handles SharePoint's organization of sites and groups i.e. each SharePoint site has an own set of groups with a different set of access rights (called roles in SharePoint)
- Real-time provisioning
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Windows Password Listener

The Windows Password Listener catches the user password changes in a Windows domain, encrypts the information and generates password change events. These trigger the event manager and the corresponding password change workflows.

The Windows Password Listener is suitable for Microsoft Windows 2012 R2 / 2016 servers and is provided as a separate installation unit.

Connectivity Package for Database systems

ODBC

- Supports ODBC (without cursors) and accesses any ODBC-accessible source/destination
- Uses and requires an ODBC driver installation
- Requires DataDirect ODBC 4.0 or higher on Linux platforms
- Full and delta export of selected rows from a table or a join of tables
- Full and delta import to a single table, (limited import facility for joined tables). Relationships of tables can be followed (referential integrity)
- Support of stored procedures for import operations
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

JDBC

- Supports JDBC and accesses any JDBC-accessible source/destination
- Uses and requires a JDBC driver installation
- Full export of selected rows from table
- Full and delta import to a single table. Relationships of tables can be followed (referential integrity)
- Support of stored procedures for import and export operations
- Real-time provisioning and password synchronization
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Connectivity Package for HiPath

HiPath 4000 Manager / Hicom DMS

- Supports HiPath 4000 Manager V3.0 and V3.1 and Hicom DMS V3.1 and 3.6 using the XIE interface (request / response files)
- Full and delta import and export of the PERS table, with insert, update, delete operations
- Supports join with unique ID or best-guess match as well as delta export with native SELECT_UPDATES query
- Supports referential integrity with COMPIMP, ORGIMP, LOCIMP and BUILDIMP tables
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Connectivity Package for Healthcare systems

Health Enterprise Dashboard

- Supports Health Enterprise Dashboard with implemented BatchXML API (version 1.0)
- Uses standard HTTP connection to connect to the URL of the Dashboard servlet
- Is built on DirX Identity's SPML-based connector integration framework
- Full and delta import of users and accounts for external applications with creation, modification and deletion operation
- Real-time password synchronization
- Creation of backchannel information to support automatic status handling of DirX Identity
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

medico//s

- Supports medico//s release 16 with appropriate service pack/patch
- Uses the standard DirX Identity SPML connector
- Full and delta import of loginIds and Persons with creation, modification and deletion operation
- Full and delta import of groups, profiles and roles with creation, modification and deletion operation
- Handling of memberships between loginIds and groups, profiles and roles
- Real-time provisioning
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Connectivity Package for Physical Security systems

SiPass

- Supports SiPass 2.4, 2.5 and 2.6 and uses the SiPass Human Resources Interface (COM technology)
- Full export of card holders and workgroups from a SiPass system
- Delta import of users with creation, modification and deletion operation including assignment to workgroups
- Error reporting and tracing
- Runs on Microsoft Windows
- Requires the .NET framework to be correctly installed on the machine

Connectivity Package for SAP systems

SAP ERP HR and OM

- Compliant to SAP ECC 6.0 respectively SAP ERP 6.0 and higher
- Implemented as an ERP application with GUI components (for the SAPgui)
- Integrated usage of ERP batch jobs for ad-hoc and scheduled execution
- Full and delta export of data from SAP HR and SAPoffice components
- Full and delta export of data from SAP OM (Organizational Management) with data either integrated into HR data or provided separately
- Supports Unicode
- Supports multiple, criteria-based selection of data records and record fields (Infotypes) as well as multi-valued attributes
- Client-specific configuration and execution
- Configurable advanced data security constraints
- Error reporting and tracing
- Runs on all NetWeaver (ABAP stack) platforms

SAP ECC User Management

- Compliant to SAP ECC respectively SAP ERP 6.0 and higher
- Uses and requires a SAP Java Connector installation (SAP JCo 3.0.10 or higher for Windows/Linux systems)
- Is built on DirX Identity's SPML-based connector integration framework
- Supports stand-alone systems and Central User Administration (CUA)
- Full and delta synchronization of user, profile (read only) and SAP role (read only) data to the SAP ECC user management
- Support of user hooks to trigger custom ABAP extensions
- Real-time provisioning and password synchronization
- Error reporting and tracing
- Runs on all platforms that are supported by both SAP JCo and DirX Identity

SAP NetWeaver User Management

- Compliant to SAP NetWeaver and Enterprise Portal 6
- Is built on DirX Identity's SPML-based connector integration framework
- Full and delta synchronization of user and role information (read only) to the SAP NetWeaver and Enterprise Portal user management
- Real-time password synchronization
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Connectivity Package for IBM systems

Lotus Notes / Domino

- Supports V8.5 and V9.0 using Notes C++ and C APIs
- Remote Access to Lotus Notes Directory Server
- Requires co-located Notes Client
- Full and delta export of addresses, groups and other forms with specification of search filters and attribute selection
- Full and delta import of addresses, groups and other forms including creation of mailboxes (optionally with replicas) and user registration in Notes
- Supports AdminP functionality
- Real-time provisioning and password synchronization for the Internet password
- Support of multi-valued attributes
- Error reporting and tracing
- Runs on Microsoft Windows platforms

IBM RACF

- Supports z/OS and OS/390 V2R8 using the LDAP interface of IBM's LDAP server to access RACF
- Full and delta export of all RACF object classes
- Full and delta import of RACF users and groups
- Real-time password synchronization
- Support of LDAP filters and multi value attributes
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Connectivity Package for Enterprise Single Sign-On systems

Evidian Enterprise SSO

- Supports Evidian Enterprise SSO 9.01b5901 or newer
- Evidian Enterprise SSO user data can be stored either in Microsoft Active Directory or in an LDAP directory
- Evidian Enterprise SSO is provisioned via the Evidian User Access Web Service
- Handles Evidian Enterprise SSO account objects, i.e. application/login name/password tuples
- Add, modify and delete operations are supported
- Full export of accounts from DirX Identity to Evidian Enterprise SSO
- Real-time provisioning for account objects
- Error reporting and tracing
- Runs on Microsoft Windows platforms

Imprivata OneSign

- Supports Imprivata OneSign 4.1 SP1 or above
- Imprivata OneSign is provisioned via SPMLv1 messages being sent to an enabled Provisioning System Adaptor in the Imprivata OneSign appliance
- Handles subscriber und application account objects
- Add and delete operations are supported, modify operations are limited by capabilities of Imprivata SPMLv1 API
- Supports one-to-one relationship between a subscriber object and an application account object in an application
- Full and delta export of subscriber and account objects from DirX Identity to Imprivata OneSign
- Real-time provisioning and password synchronization for subscriber and account objects
- Runs on Microsoft Windows and all supported Linux platforms

Connectivity Package for Cloud systems

Google Apps

- Connector uses the Google Directory API
- Connectivity is based on HTTP protocol
- Full import of accounts, groups and group memberships
- Real-time provisioning of accounts, groups and group memberships
- Real-time password synchronization
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Citrix ShareFile

- Connector uses the Citrix ShareFile API
- Connectivity is based on HTTP protocol
- Full import of accounts, groups and group memberships
- Real-time provisioning of accounts, groups and group memberships
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Microsoft Office 365

- Connector uses the Microsoft Graph API version 2013-11-08 on URL https://graph.windows.net
- Connectivity is based on HTTP protocol.
- Full import of users, groups, roles, service plans with assignments
- Real-time provisioning of users, groups, roles, with assignments
- Assignment of users to plans – this enables users to use the licensed Office 365 features like Office applications, Exchange, Skype for Business, etc.

- Real-time password synchronization
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Salesforce

- Connector uses the Force.com REST API
- Connectivity is based on HTTP protocol
- Full import of users and profiles
- Real-time provisioning of users including assigned ProfileId
- Real-time password synchronization
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

Proxy Connectivity Package

Remote Upload Connector

- Supports scenarios where DirX Identity is deployed as part of a cloud service infrastructure such as IDMaaS (Identity Management as a Service) and Active Directory or any other LDAP directory is available at a remote customer site to upload identities
- Connectivity is based on HTTP protocol
- Connector uses native LDAP to access on-site Active Directory of Microsoft Windows Server 2008 R2, Windows Server 2012 R2 and Windows Server 2016 or any other LDAP directory
- Requires Java Runtime Environment 8 or newer and Apache Tomcat 8 or newer at the service site
- Requires Java Runtime Environment 8 or newer at the remote customer site
- Full import of accounts (identities)
- Error reporting and tracing
- Runs on Microsoft Windows and all supported Linux platforms

OpenICF Proxy Connector

- The Java-based OpenICF proxy connector runs inside the Identity Java Connector Integration Framework.
- It communicates with an OpenICF connector server (Java- or .NET-based) using an internal OpenICF protocol.
- The connector can dynamically obtain information about required configuration parameters and data schema from that connector server.
- The connector converts provisioning operations and data between DirX Identity and OpenICF formats.
- The connector is required to integrate any of the OpenICF connector bundles with DirX Identity.

Note: In addition to provisioning with the delivered OpenICF-based workflows, provisioning of other target systems that are supported by OpenICF connector bundles is also supported. This requires customization of the delivered workflows.

OpenICF Connector Bundle for Unix

- Real-time provisioning of Unix accounts, groups and group memberships
- Real-time password synchronization
- Full import of Unix accounts, groups and group memberships
- Error reporting and tracing
- The connector bundle is deployed in a Java-based OpenICF connector server.
- Runs on all Microsoft Windows and Linux platforms that are supported by the OpenICF connector server.

OpenICF Connector Bundle for Windows Local Accounts

- Real-time provisioning of accounts, groups and group memberships that are located in a local SAM database of a Microsoft Windows computer
- Real-time password synchronization
- Full import of accounts, groups and group memberships
- Works with Microsoft Windows Server 2008 R2, Windows Server2012 R2, Windows Server 2016 and Windows 7 (64-Bit) and Windows 10
- Error reporting and tracing
- The connector bundle is deployed in a .NET-based OpenICF connector server running on any Windows server.
- Runs on all Microsoft Windows platforms that are supported by the OpenICF connector server.

Other DirX Products

The following products also belong to the DirX product suite and can be ordered separately; DirX provides the basis for totally integrated identity and access management:

- DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable and secure LDAP and X.500 directory server with very high linear scalability. DirX Directory can act as the identity store for employees, customers, trading partners, subscribers, and other e-business entities.
- DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy-based authentication, authorization and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premise.
- DirX Audit provides auditors, security compliance officers and administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the "what, when, where, who and why" questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard, a monitor for identity-related events and job management for report generation. With its analytical features, DirX Audit helps enterprises and organizations to ensure sustainable compliance and provide business intelligence for the identity and access management processes.

Table 1 - DirX Identity Business Suite, Pro Suite, Password Management Option Overview

	Pro Suite	Business Suite	Password Management Option
Web-based User Self-Service via Web Center	**Yes**	**Yes**	**-**
- Managing own data	Yes	Yes	-
- Managing own passwords	Yes	1)	-
- Managing delegations	Yes	-	-
- Requesting roles	Yes	3)	-
Delegated Administration via Web Center	**Yes**	**-**	**-**
Password Management	**Yes**	**Yes**	**Yes**
- Password policies	Yes	-	Yes
- Password change by end-user via Web Center	Yes	-	Yes
- Password change by end-user for a subset of their accounts	-	-	Yes
- Display the password change status	-	-	Yes
- Challenge/response procedures to reset forgotten passwords (self-service)	Yes	-	Yes
- Challenge/response procedures to reset forgotten passwords (via administrators or service desk)	-	-	Yes
- Administrative password reset	Yes	-	Yes
- Windows Password Listener	2)	2)	2)
- Real-time password synchronization	Yes	Yes	Yes
- Password Reset Client for Windows	-	-	Yes
User Management	**Yes**	**Yes**	**-**
- Managing users	Yes	Yes	-
- Managing personas	Yes	-	-
- Managing user facets	Yes	-	-
- Managing functional users	Yes	-	-
Role Management	**Yes**	**Yes**	**-**
- Managing accounts	Yes	Yes	-
- Managing groups	Yes	Yes	-
- Managing permissions and permission parameters	Yes	-	-
- Managing roles and role parameters	Yes	-	-
- Segregation of duties	Yes	-	-
Business Object Management	**Yes**	**Yes**	**-**
Request workflows, approval and re-approval	**Yes**	**-**	**-**
Risk Management	**Yes**	**-**	**-**
Access Certification	**Yes**	**-**	**-**
Support for outsourced environments	**Yes**	**Yes**	**-**
- Privileged account management	Yes	Yes	-
- Workflows for clustered target systems	Yes	Yes	-
Policy Management	**Yes**	**Yes**	**-**
- Access policies	Yes	Yes	-
- Audit policies	Yes	-	-
- Provisioning policies for groups	Yes	Yes	-
- Provisioning policies for roles and permissions	Yes	-	-
- Validation policies	Yes	Yes	-
- Consistency policies	Yes	Yes	-
Provisioning	**Yes**	**Yes**	**-**
- Policy-/Rule-based assignment of groups to users	Yes	Yes	-
- Policy-/Rule-based assignment of permissions and roles to users	Yes	-	-
- Manual assignment of groups to users	Yes	Yes	-
- Manual assignment of permissions and roles to users	Yes	-	-
- Inheritance of groups from business objects to users	Yes	Yes	-
- Inheritance of permissions and roles from business objects to users	Yes		-
- Real-time provisioning of accounts and groups to target systems	Yes	Yes	-

1) In conjunction with Windows Password Listener over Microsoft Windows native tools/interfaces, not via Web Center
2) Requires DirX Identity Microsoft Connectivity Package
3) Groups instead

Table 2 - DirX Identity Business Suite, Pro Suite, Password Management Option Overview - continued

	Pro Suite	Business Suite	Password Management Option
Service Management Support	Yes	Yes	-
Metadirectory	Yes	Yes	-
- Default Applications	Yes	Yes	-
- Bi-directional synchronization of structured files (XML, LDIF, DSML, CSV)	Yes	Yes	-
Auditing Services	Yes	Yes	-
- Reports on users, accounts, groups	Yes	Yes	-
- Reports on target systems, delegations, access policies, rules	Yes	Yes	-
- Reports on roles and permissions	Yes	-	-
- Audit trail of administrative changes in DirX Identity	Yes	-	-
- Audit trail of password changes and password lookup	Yes	-	-
- Audit trail of Web Center login/logout	Yes	-	-
- Validation and reconciliation of target systems	Yes	Yes	-
Domain Management	Yes	Yes	-
Default Connectivity	Yes	Yes	-
Identity Manager	Yes	Yes	-
Business User Interface	Yes	Yes	-
Web Center	Yes	Yes	4)
Java- and C++-based Identity Server and Web Admin	Yes	Yes	-
Web Services	Yes	Yes	-
Identity Integration Framework	Yes	Yes	-

4) Password Management functionality only

System Requirements for DirX Identity V8.7

Hardware

- Intel server platform for Microsoft Windows Server 2012 R2/ 2016 (LTSC), Red Hat Enterprise Linux, SUSE Linux Enterprise Server

Memory requirements:

Main memory: minimum 8 GB

Disk Space: minimum 4 GB plus disk space for data

Software

DirX Identity is supported on the following platforms with latest patches/service packs for the selected platform:

- Microsoft Windows Server 2012 R2 (x86-64 Intel architecture)
- Microsoft Windows Server 2016 LTSC (x86-64 Intel architecture)
- Red Hat Enterprise Linux 7 (x86-64)
- SUSE Linux Enterprise Server 12 (x86-64)
- Microsoft Windows 7, Microsoft Windows 10 (x86-64) , client components Identity Manager, client signature only

- Java SE Runtime Environment (JRE) 8
- Apache Tomcat 8 or 8.5

Virtual Machine Support:

- VMWare ESXi 6.0, in combination with guest operating systems listed above that are supported by VMWare ESXi 6.0

Note: C++-based components of DirX Identity run as 32-bit application on 64-bit platforms. Java-based components run as 64-bit application on 64-bit platforms.

For the DirX Identity Data Store

- DirX Directory V8.5/V8.6

For the DirX Identity Web Center/Web Admin

- Microsoft Internet Explorer 11
- Mozilla Firefox 52 or newer
- Google Chrome 62 or newer (Request signing via Java applet is not supported)
- Microsoft Edge 40 or newer (Request signing via Java applet is not supported)

For DirX Identity Approvals App

- iOS 9/10/11

For DirX Identity Business User Interface

- Mozilla Firefox 52 or newer
- Google Chrome 62 or newer
- Microsoft Edge 40 or newer

For DirX Identity Manager

- For smart card support: Atos CardOS API V5.3 in combination with CardOS smart cards that are supported by Atos CardOS API V5.3.

For OpenICF connector bundles

- For Unix: An OpenICF Java Connector Server installation, version 1.1.1.0 or newer
- For Windows Local Accounts. An OpenICF .NET Connector Server installation, version 1.4.0.0 or newer

For Nagios support

- Nagios Core, version 4.0.8
- JNRPE Server, version 2.0.5
- JNRPE plugins, version 2.0.3

User interface

English

Web Center: English/German/customizable

Documentation

Manuals and Use Case documents are provided in English.

Manuals

- Installation Guide
- Migration Guide
- Introduction
- Tutorial
- Provisioning Administration Guide
- Connectivity Administration Guide
- User Interface Guide
- Application Development Guide
- Customization Guide
- Integration Framework
- Web Center Reference
- Web Center Customization Guide
- Meta Controller Reference
- Connectivity Reference
- Troubleshooting Guide
- Business User Interface User Guide
- Business User Interface Configuration Guide

Use Case documents

- Configuring the Maintenance Workflows for User Facets
- Creating a Custom Target System Type
- Enabling Smart Card Login for Identity Manager
- High Availability
- Java Programming in DirX Identity
- Monitoring DirX Identity Servers with Nagios
- Password Management
- Real-time Synchronization within an Identity Domain
- Service Management
- Certification Campaigns
- Configuring User-specific Proposal Lists for Role Parameters
- Using Domains
- Using Segregation of Duties
- Web Center File Upload

www.evidian.com

Atos