EVIDEN

Identity and Access Management

DirX Identity

Introduction

Version 8.10.13, Edition October 2025

Table of Contents

Preface

This manual is an introduction to DirX Identity. It consists of the following sections:

- Chapter 1 provides information about the challenge of user and access management.
- Chapter 2 provides a DirX Identity overview.
- Chapter 3 provides a glossary that defines terms and concepts that relate to identity and access management and DirX Identity.

DirX Identity Documentation Set

The DirX Identity document set consists of the following manuals:

- *DirX Identity Introduction*. Use this book to obtain a description of DirX Identity architecture and components.
- *DirX Identity Release Notes*. Use this book to understand the features and limitations of the current release. This document is shipped with the DirX Identity installation as the file **release-notes.pdf**.
- *DirX Identity History of Changes*. Use this book to understand the features of previous releases. This document is shipped with the DirX Identity installation as the file **history-of-changes.pdf**.
- *DirX Identity Tutorial*. Use this book to get familiar quickly with your DirX Identity installation.
- *DirX Identity Provisioning Administration Guide*. Use this book to obtain a description of DirX Identity provisioning architecture and components and to understand the basic tasks of DirX Identity provisioning administration using DirX Identity Manager.
- *DirX Identity Connectivity Administration Guide*. Use this book to obtain a description of DirX Identity connectivity architecture and components and to understand the basic tasks of DirX Identity connectivity administration using DirX Identity Manager.
- *DirX Identity User Interfaces Guide*. Use this book to obtain a description of the user interfaces provided with DirX Identity.
- *DirX Identity Application Development Guide*. Use this book to obtain information how to extend DirX Identity and to use the default applications.
- *DirX Identity Customization Guide*. Use this book to customize your DirX Identity environment.
- *DirX Identity Integration Framework*. Use this book to understand the DirX Identity framework and to obtain a description how to extend DirX Identity.
- *DirX Identity Web Center Reference*. Use this book to obtain reference information about the DirX Identity Web Center.
- *DirX Identity Web Center Customization Guide*. Use this book to obtain information how to customize the DirX Identity Web Center.
- *DirX Identity Meta Controller Reference*. Use this book to obtain reference information about the DirX Identity meta controller and its associated command-line programs and files.
- *DirX Identity Connectivity Reference*. Use this book to obtain reference information about the DirX Identity agent programs, scripts, and files.
- *DirX Identity Troubleshooting Guide*. Use this book to track down and solve problems in your DirX Identity installation.
- *DirX Identity Installation Guide*. Use this book to install DirX Identity.
- *DirX Identity Migration Guide*. Use this book to migrate from previous versions.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

userID_home_directory
The exact name of the home directory. The default home directory is the home directory of the specified UNIX user, who is logged in on UNIX systems. In this manual, the home pathname is represented by the notation *userID_home_directory*.

install_path
The exact name of the root of the directory where DirX Identity programs and files are installed. The default installation directory is *userID_home_directory*/**DirX Identity** on UNIX systems and **C:\Program Files\DirX\Identity** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

dirx_install_path
The exact name of the root of the directory where DirX programs and files are installed. The default installation directory is *userID_home_directory*/**DirX** on UNIX systems and **C:\Program Files\DirX** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathname is represented by the notation *dirx_install_path*.

dxi_java_home
The exact name of the root directory of the Java environment for DirX Identity. This location is specified while installing the product. For details see the sections "Installation" and "The Java for DirX Identity".

tmp_path

The exact name of the tmp directory. The default tmp directory is /tmp on UNIX systems. In this manual, the tmp pathname is represented by the notation *tmp_path*.

tomcat_install_path
The exact name of the root of the directory where Apache Tomcat programs and files are installed. This location is defined during product installation.

mount_point
The mount point for DVD device (for example, **/cdrom/cdrom0**).

1. 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 for the right reasons is an essential element 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 a way to archive this information securely for long-term access and analysis.

The move to e-business. 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 enterprise 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 e-business. 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.

Improved information security. Although e-business 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 - "who is allowed to access what information, and how" - and consistently enforce them across the heterogeneous systems in the enterprise IT infrastructure. This task becomes even a bigger challenge when cloud services are used.

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 enterprise's 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, 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 enterprise 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 and hotline 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.
- Security administration on a per IT system basis means that access policies are designed from the bottom up instead of being modeled according to business practices and processes. Decentralized, ad hoc security policies make it difficult to assign the right access to the right users given their function in the organization, increasing risk, decreasing productivity, and making it hard to prove compliance with enterprise security policies and external regulations on access.

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 governs access to IT resources according to business roles, policies and processes. The system must provide ways to be aligned with business processes and off-load routine administrative functions and decisions from IT staff to users and their managers so that requests and decisions about what users really need are made by the people who know best. Identity and access management (IAM) technology offers an effective way to satisfy these requirements.

1.1. What Is Identity and Access Management?

Identity and access management (IAM) provides for a process-driven, centralized, automated, and integrated solution, making user and access management transparent across the different systems in the enterprise's IT infrastructure. **Identity management** processes address the administration of users and their access rights across the IT infrastructure according to business principles, practices, policies and processes. **Access management** processes address the real-time enforcement of user access to the systems, services, and applications that make up the enterprise IT infrastructure according to their established access rights. **Audit** processes running outside of the IAM process stream address the need to record, review, analyze and report on the IAM processes themselves to mitigate risk, demonstrate accountability, prove compliance and provide feedback for corporate decision-making on IAM design and performance.

1.1.1. Identity Management

Identity management processes work to align enterprise business interests with lower-level IT operations for user management and provisioning. **Identity governance** functions provide a high-level, transparent way to define, create, manage, assign, review and remove users (who are represented in the IAM system as digital identities) and their access rights to resources according to business security objectives and compliance requirements. **Identity provisioning** functions dynamically and automatically realize the results of identity governance operations into the necessary entitlements (for example, accounts and groups) in the systems, applications, and services that make up the enterprise IT infrastructure.

Identity governance and provisioning processes include user self-service and delegated

administration, password management, user management, role, policy and business object management, request workflow, certification campaigns, real-time provisioning and reconciliation and metadirectory.

1.1.1.1. User Self-Service

User self-service allows users to perform simple user-oriented identity management tasks that must typically be carried out by technical IT administrators in the traditional enterprise IT infrastructure. With self-service, users can register themselves with enterprise services, manage their own data, including their own passwords, and request roles, which model user access rights to enterprise resources for themselves. User self-service allows the enterprise to put common, frequently recurring identity management tasks like password resets and user profile updates into the hands of the users themselves, rather than IT, hotline, and help desk staff.

1.1.1.2. Delegated Administration

Delegated administration allows users to grant other users the right to perform their identity management tasks (or a subset of these tasks). Delegation allows an enterprise to distribute identity management tasks according to business functions and to create a hierarchy for identity management that reflects its business structure. The enterprise can use delegated administration to balance the user management and access rights administration load across both IT and non-IT departments according to areas of responsibility and expertise.

1.1.1.3. Password Management

Password management allows users to maintain a single password that will automatically be synchronized to all relevant IT systems in the enterprise. Password management functions permit users to reset forgotten passwords themselves through challenge-response procedures (or request an administrator reset), change their passwords in one or more systems, for example, in an LDAP directory or in Windows, notify users when they need to change their passwords to comply with password policies established for the enterprise (for example, expiration of a password's lifetime), and synchronize these password changes in real time to all the relevant IT systems.

1.1.1.4. User Management

User management includes all the activities related to the creation, maintenance and use of user accounts, user attributes, roles, entitlements and other data encompassing the different directories, user databases, and application-specific repositories that make up the fragmented, heterogeneous enterprise IT environment. 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. Maintaining a consistent user directory is handled by request processes from the users themselves and/or their managers (user self-service and delegated administration) and by data synchronization workflows (for example, with the enterprise HR system) provided by the metadirectory. User facets, personas and functional users extend the user for alternative representations of users and assigned resources.

1.1.1.5. Role Management

A **role** is a set of access rights based on either business semantics or on IT-system specific semantics that permits users to access enterprise IT resources. In a role-based access control (RBAC) model, access rights to IT systems and resources are controlled by roles, which in turn are associated with or assigned to users. The enterprise can structure its roles in a hierarchical model according to its business roles and functions or other considerations. The role concept establishes a logical layer for the modeling and management of access control information that is generic enough to cover many IT systems' access control methods, such as:

- Group-based IT systems, which 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, which 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.
- Systems that use both group-based and attribute-based access control methods, like Microsoft Active Directory.

Role-based access management allows access control on each IT system to be managed in a uniform way. Role management also simplifies and structures access rights administration. High-level managers can assign roles to their staff without needing to know the IT-specific details, and IT personnel can administer the access rights in the IT systems without needing to know the business details. The assignment of roles to users can be partially automated with the help of security policies and their associated rules.

1.1.1.6. Certification Campaigns

A **certification campaign** is the identity governance process of periodically checking user-privilege and privilege-user assignments to ensure that these assignments continue to comply with enterprise business policies. Certification campaigns specify the privileges or users and assignments to be certified, how often the certification is to take place, and who is to perform the certification. Compliance officers can monitor the certification campaign's progress and generate reports on the completed campaign. Certification campaigns allow the enterprise to verify that access rights to its IT systems - especially security-sensitive systems - remain properly granted to its user community over time, satisfying compliance regulations and mitigating risk.

1.1.1.7. Business Object Management

A business object is a collection of data related to a business structure in the enterprise such as an organization, a cost center or a project. Business objects in an identity management system serve two main functions:

- They help to automate user-role assignment by allowing the roles referenced by the business object to be inherited by the users linked to it.
- They help to reduce redundancy of user data in the identity store by providing a single

point of control for common user data. For example, an organization's street address and postal code can be kept in a business object and associated with all users linked to it.

Changes to the information in the business object – including references to roles – are automatically propagated to the users linked to the business object.

Business objects offer a way to view identities from different perspectives: for example, all people in a particular location, all members of a specific organizational unit, or all people that belong to a particular cost center. Because business objects locate data centrally instead of at individual user entries, they allow for easier data cleansing and maintenance. Finally, automatic user-role assignment via links to business objects has become a popular method for role assignment.

1.1.1.8. Policy Management

Policy management refers to the creation and maintenance of policies that reflect the enterprise's security and administrative policies and their associated rules and which help to govern, automate and control identity management processes. A policy is composed of one or more rules; each rule identifies the entities - for example, a set of users, or a set of resources - to which the rule applies, the action to be taken, such as assigning one or more roles, and a priority level that is used to resolve conflicts with other rules. Policies can be applied to governance-level functions such as password creation and maintenance, role assignment, and segregation of duties (user-role assignments that constitute conflicts of interest), to provisioning-level functions like user data consolidation and reconciliation (periodic comparison of IT system data and its representation in the IAM system) and to audit-level functions to control how identities and their access rights are monitored. Policies help to control and automate identity management tasks, reducing error-prone manual administration and help to guarantee compliance with internal and external regulations.

1.1.1.9. Request Workflow and Approval

Request workflows provide the process control mechanism that supports user self-service and delegated administration activities. Request workflows allow users to create identity management data like users or roles, request or assign resources, such as access to a company newsletter or a file share, and optionally authorize these requests according to the access policies in force in the enterprise. When a request needs approval, the request workflow notifies each person in the defined approval path - for example, by email - and each approver uses a Web browser to access a Web interface to accept or reject the request. When access policies require re-authorization of a resource at a given interval, for example, quarterly re-approval of a financially sensitive role assignment, request workflows automatically enforce compliance by re-notifying the appropriate approvers; failure to re-approve leads to automatic unassignment. Request workflows allow the enterprise to handle all of the business processes associated with identity management in a well-defined, controlled and automated way.

1.1.1.10. Provisioning

Provisioning is the fully automated, real-time process of calculating user access rights and

distributing them to IT systems based on the roles assigned to the user. The provisioning process automatically and instantaneously grants, changes, and revokes access rights in IT systems in response to role assignment, re-assignment, and revocation. Provisioning automates the time-consuming process of managing access rights across many different IT systems over the user life-cycle and permits fast activation and de-activation of access rights across these systems for multiple user identities.

Provisioning provides a single point of administration for the enterprise's total identity and access control information and implements the services that keep the identity and access control data in the IT systems consistent and up-to-date, allowing the enterprise to ensure the security of its data, reduce administration overhead, accelerate its business processes and improve its customer service, and protect its investments in existing IT systems.

1.1.1.11. Reconciliation

Reconciliation is the process of periodically comparing the access rights data in an IT system to the IAM system's central repository - its identity store - to detect local changes to the IT system data that have occurred independently of changes initiated by the IAM system. Deviations can be explicitly reconciled by hand or automatically and periodically by reconciliation policies. Reconciliation ensures the integrity of access rights data across the enterprise, a key element of compliance.

1.1.1.12. Metadirectory

Metadirectory is the set of services that integrates the disparate directories, user databases, and application-specific information repositories in the enterprise IT network 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.

In an IAM system, the metadirectory provides an infrastructure for automated enterprise-wide user management that addresses the problem of decentralized multiple user identities and user administration functions. Metadirectory services:

- 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
- 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

1.1.2. Access Management

Access management processes control the real-time access by user identities to systems, services, and applications in the IT infrastructure according to the entitlements established for them by IM processes. Access management processes include authentication, authorization and federation.

1.1.2.1. Authentication

Authentication is the process of identifying users and validating their identity. Various authentication methods can be used, including basic authentication using username/password, secure tokens, digital certificates and smart cards. Authentication ensures that users are properly identified and that these identities are validated to the enterprise's resources. **Single sign-on (SSO)** permits a user to access multiple IT systems and applications after being authenticated just one time. Web SSO uses encrypted cookies to store user authentication and session information, which permits users to access enterprise resources over Web-based applications without the need to re-authenticate.

1.1.2.2. Authorization

Authorization is the real-time enforcement of user access requests to the enterprise resources. Authorization ensures that users can only access the IT systems in the enterprise and the corresponding resources according to their access rights. Access decisions can be based on centralized access control policies.

1.1.2.3. Federation

Identity **federation** permits an enterprise to share trusted identities with autonomous organizations outside of the enterprise, like trading partners or suppliers. The goal of federation is to integrate identity information across enterprise boundaries to allow the enterprise to build business communities.

1.1.3. Audit and Compliance

Audit is an identity and access "intelligence" process that provides a window into IAM process functioning and complements the real-time monitoring and reporting capabilities provided by the IAM processes themselves.Audit functions include:

- Automatically logging information about all identity and access management transactions and storing these records, called audit trails, securely in an audit log repository for subsequent analysis and report.
- Generating reports, either automatically or on demand, about the status of identity management data in the identity store

An **identity-based audit trail** automatically collects information about all user and role transactions, and can provide information about who has access to what, when access to something was granted, who granted that access, and which policy permitted it.An **access-based audit trail** automatically collects information from all enforcement points in the access management process, and can provide information about which operations were performed by administrators and identities, which events have occurred, and which operations succeeded or failed. **Status reports** provide information about the current state of identity management data, for example, which users have which roles, which roles are unused, and which users have been given delegated administrative tasks.

Audit ensures that the activities associated with identity and access management are logged for day-to-day monitoring, to prove regulatory compliance, and for input to corporate decision-making and continuous improvement processes.

1.2. How Does IAM Work?

Here are some real-life user and access management scenarios that illustrate how IAM works.We'll discuss how to use IAM to:

- Make a new employee productive quickly
- Change an employee's job function
- Change a user password
- Authorize a request
- Self-register for services
- Certify assignments to a role

1.2.1. Making a New Employee Productive Quickly

This example shows how the IAM system works when a new employee is hired, as illustrated in the following figure.

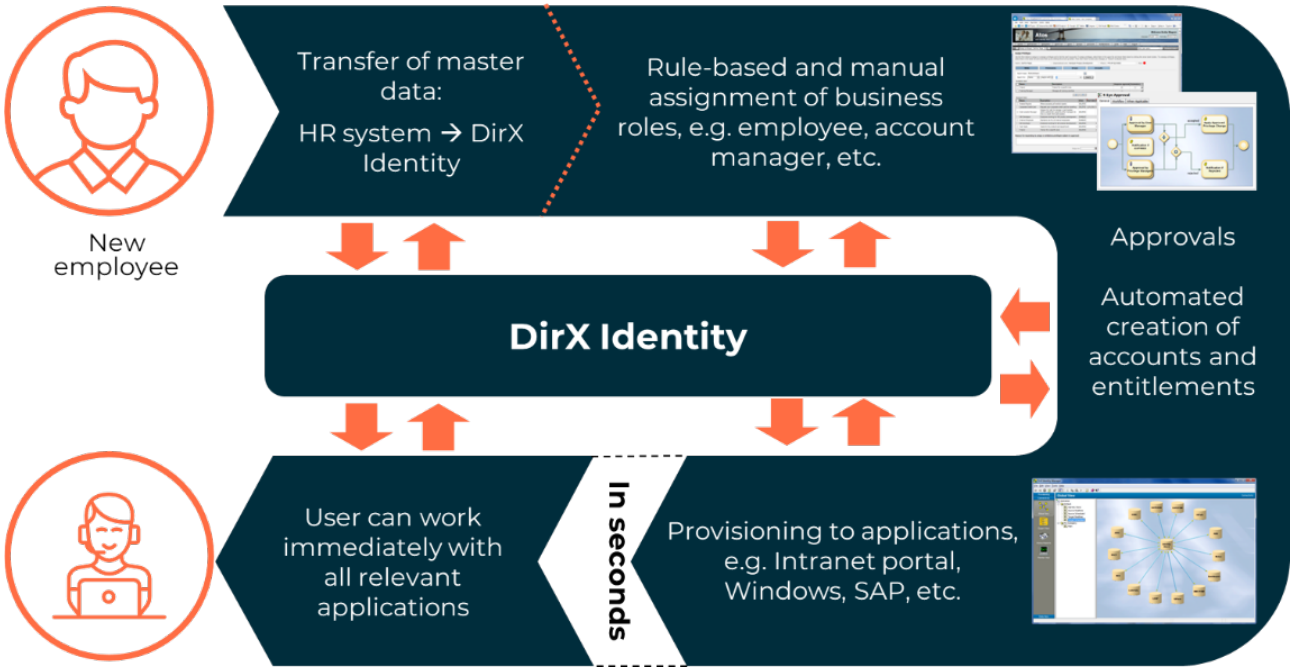

Figure 1. Making a New Employee Productive Quickly

As shown in the figure:

1. The ERP system generates the master data for the employee from the human resources database or the order processing system (the authoritative sources) and automatically synchronizes it to the IAM system's identity store, creating a centralized unique digital identity for the employee.
2. The IAM system automatically assigns the appropriate roles to the employee's entry following the security policies administered in the identity store.
3. The IAM system automatically calculates the access rights for the employee that result from the roles assigned to him.

4. An administrator enters individual data about the employee, such his employment start date, into the employee's entry in the identity store.
5. IAM provisioning processes automatically generate accounts and access rights in the intranet and extranet access servers, email servers, and the other IT resources assigned to the employee.
6. IAM provisioning processes set the employee's access rights in the central access management system which protects the enterprise portals he will use.

The employee now has the access rights defined in the roles assigned to him and is ready to work productively.

1.2.2. Changing an Employee's Job Function

In this scenario, an employee is switching from the Sales department to the Marketing department effective February 1st. He is currently authorized to perform sales activities in the sales portal, but will need to use the marketing portal as of February 1st. The following figure illustrates how the IAM system handles the access rights changes required.

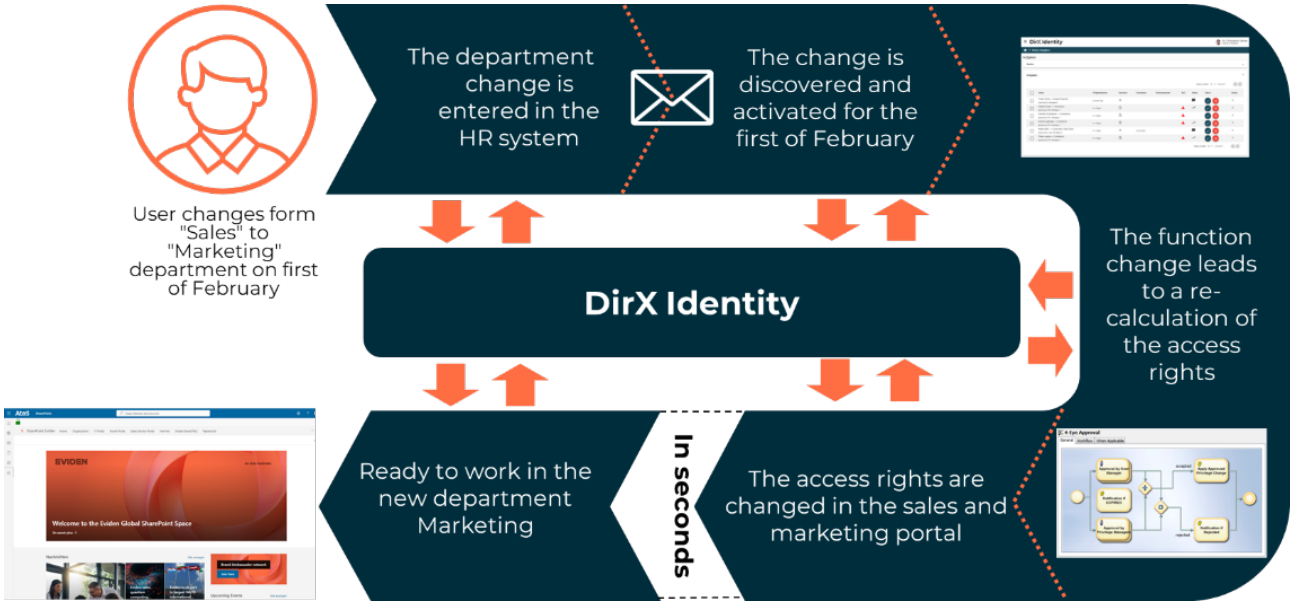

Figure 2. Changing an Employee's Job Function

As shown in the figure:

1. The Human Resources department enters the change in department and the effective date of the change into the HR system and provisions the changes to the IAM system via "department" and "start date" user attributes.
2. The IAM system records the departmental change in the entry for the employee in the identity store (in the "department" user attribute) and automatically recalculates the employee's access rights based on the new value.
3. The IAM system revokes the access rights associated with the role "Sales".
4. The IAM system calculates the access rights associated with the "Marketing" role.
5. The IAM system synchronizes the "Marketing" access rights on the Sales and Marketing portals.

6. The Marketing Portal is made available to the employee, and the Sales Portal is no longer accessible to the employee.

1.2.3. Changing a User Password

This example illustrates what happens in the IAM system when a password that can be used for several applications is changed.

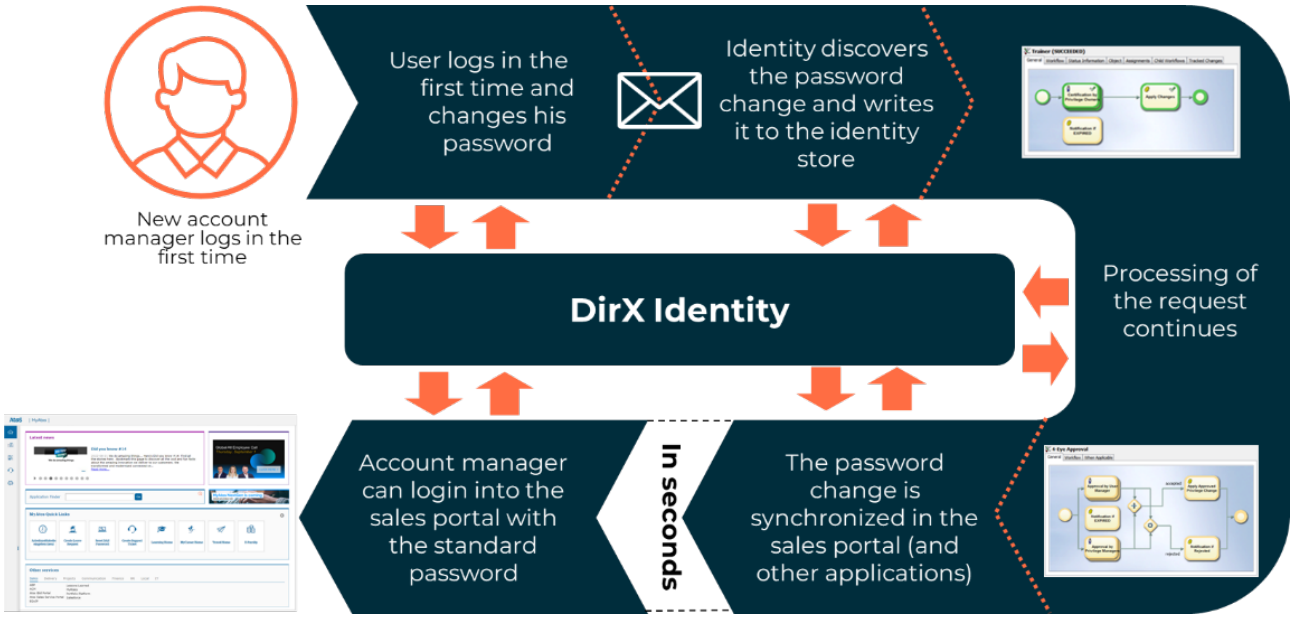

Figure 3. Changing a User Password

As shown in the figure:

1. A user changes his password on his first login to a Windows system.
2. The IAM system discovers the password change, saves the password securely in the entry for the employee in the identity store, and records this operation in the audit store.
3. The IAM system synchronizes the changed password on the Employee Portal and records this operation in the audit store.
4. The changed password is available to authenticate against the Employee Portal.

1.2.4. Approving a Request

In this example, a sales employee needs access to an analyst report, and this access must be approved. The following figure illustrates how the IAM system handles this case using a request workflow.

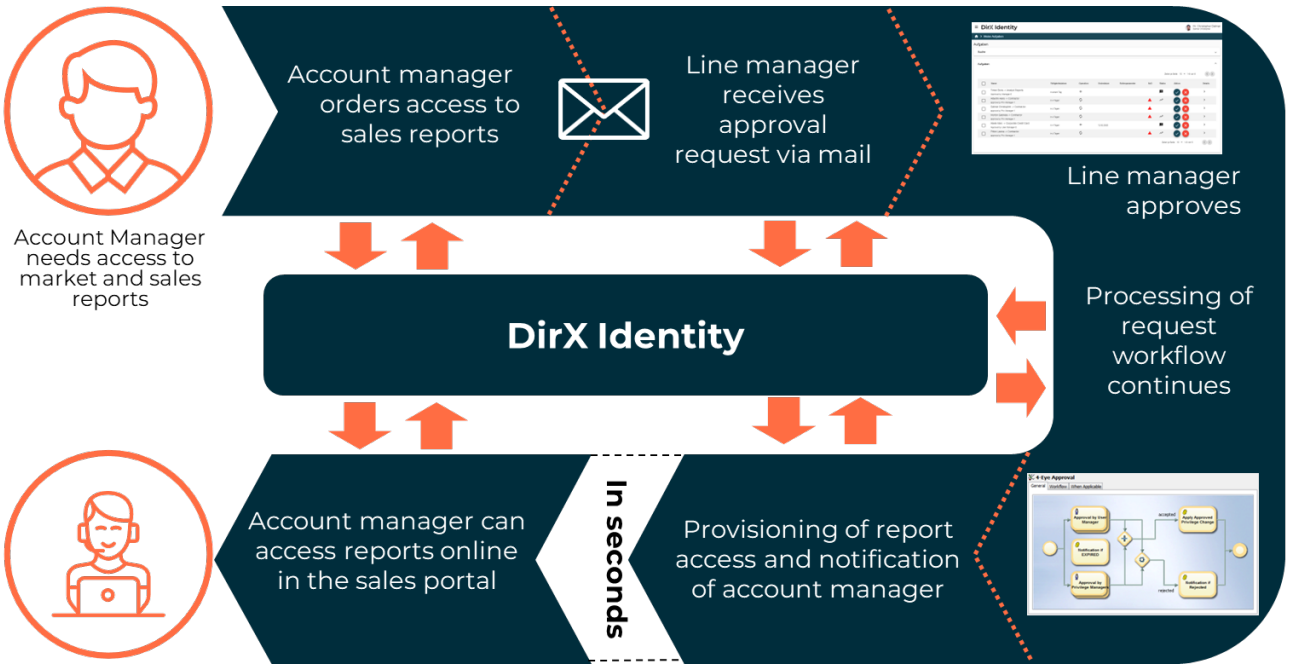

Figure 4. Approving a Request

As shown in the figure:

1. The Sales employee submits a request for the analyst reports.
2. The IAM system runs a request workflow that handles the approval process and automatically forwards the request to Sales management.
3. Once Sales management has approved the request, the IAM system synchronizes the changes in access rights in the Sales portal.
4. The IAM system informs the Sales employee via email that access to the analyst report has been granted.
5. The employee then obtains the analyst report from the Sales Portal.

1.2.5. Self-Registering for Services

In this example, an outside consultant who works for the Marketing department needs access to the Marketing portal and requests that he be registered as a new Marketing user via the Internet.

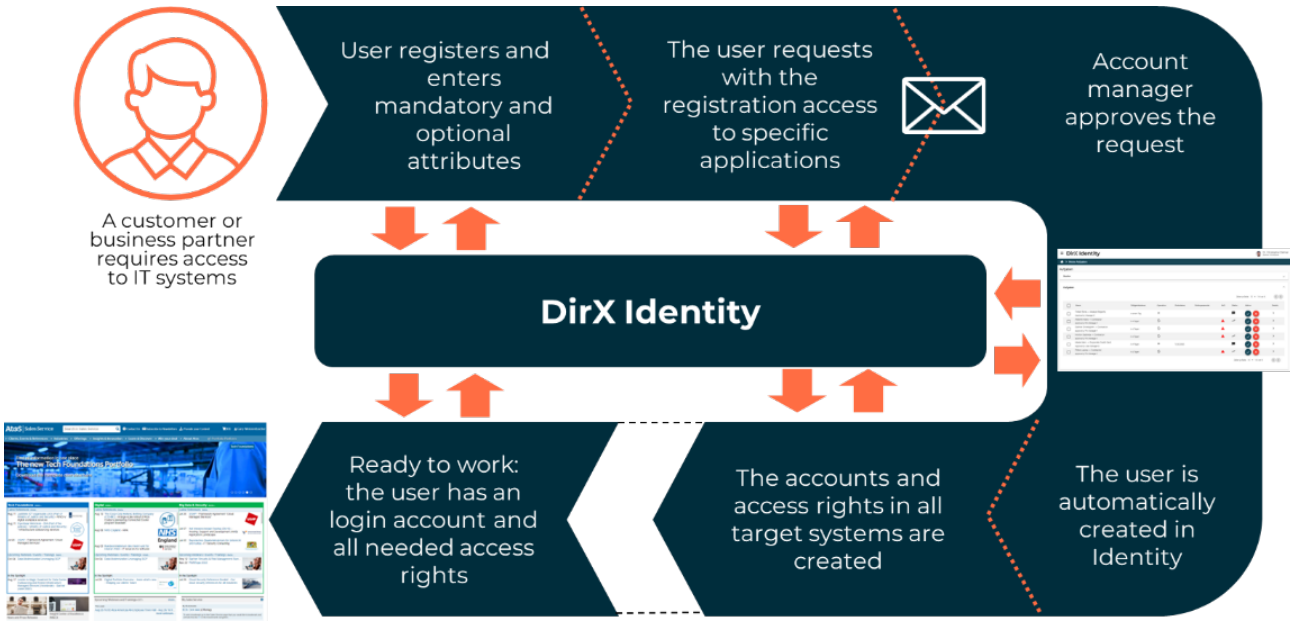

Figure 5. Self-Registering for Services

As shown in the figure:

1. The consultant uses his Web browser to go to the URL of the company's Web-based user self-registration interface and clicks "Register". The IAM system automatically starts a user creation workflow, which displays a registration page that requests more information.
2. The consultant fills out the website's registration page with his name, his company's name and address, and other required and optional attributes, and then clicks "Save".
3. The Web interface presents the consultant with a selection of job-related roles from which he can choose. The consultant chooses the "New Marketing Info" and "Download Marketing Material" roles and then clicks "Save".
4. Because the "Download Marketing Material" role requires approval from the Marketing Download manager, the user creation workflow automatically notifies the manager about the request and asks him to accept or reject it.
5. Once the manager approves the request, the IAM system automatically calculates the consultant's access rights based on the information he supplied in the registration page and the roles he requested.
6. The IAM system immediately provisions accounts and access rights in the relevant IT systems.
7. The IAM system automatically notifies the consultant via email that he is now a registered Marketing user.

The consultant can now access the requested resources defined in the roles assigned to him and is ready to work productively.

1.2.6. Certifying a User's Assignments

In this example, compliance requirements dictate that privilege assignments to users in the Finance department must be certified by the users' managers.

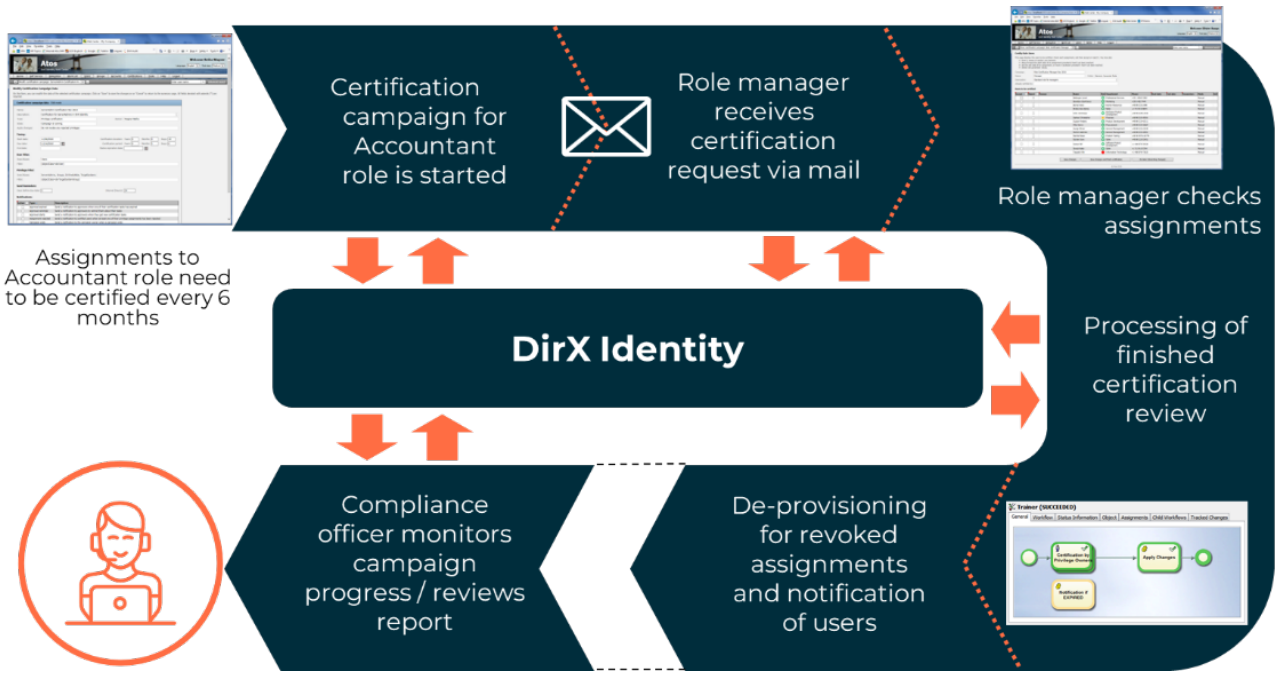

Figure 6. Certifying User or Privilege Assignments

As shown in the figure:

1. A compliance officer sets up a certification campaign for the Finance department to start at the beginning of next month and finish at the end of the next month.
2. When the start date arrives, the IAM system starts the certification campaign.It creates a certification task for every user in the department, identifies all privileges to be certified, assigns the user's manager as the responsible approver and informs them via email.
3. The user manager verifies - sometimes by consulting role managers, human resources representatives, and other people in the organization - that the user's assignment to each privilege complies with the business policies given the user's function in the organization.If the user-privilege assignment complies with regulations, the user manager indicates to the IAM system that the assignment should remain in force.If it does not comply, he indicates to the IAM system that the assignment should be removed.
4. At the end of the campaign, the IAM system processes the results of the certification review.It revokes the access rights that were rejected by the approvers, and then informs the affected users about the change.
5. The compliance officer uses the IAM system to monitor the certification campaign and generate a report on the results.

1.3. What is DirX?

The DirX suite of highly scalable and automated IAM solutions allow customers to choose from on-premise, managed and cloud-based delivery models and to benefit from enhanced regulatory compliance and audit capabilities, greater security, higher efficiency and reduced overall costs.The DirX portfolio ranges from identity management and access governance, identity analytics and intelligence to Web access management and single

sign-on, authorization, identity federation, and directory services.Analysts recognize Atos as a world leader in role management and SAP integration.

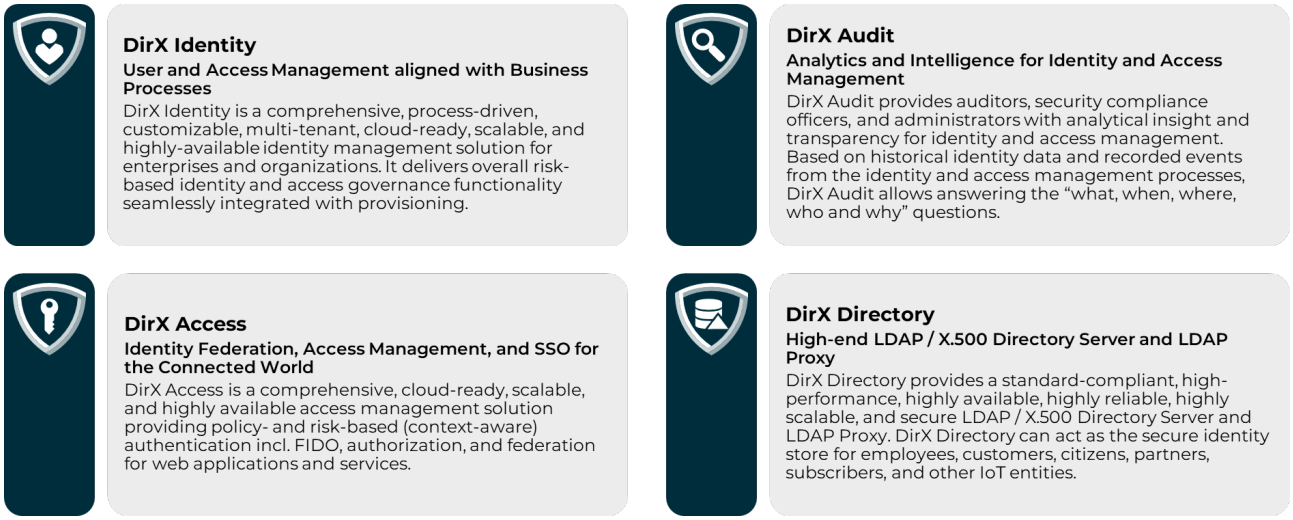

Figure 7. DirX: The integrated product suite for Identity and Access Management

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 / X.500 directory server and LDAP Proxy
- 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, Authorization, and federation product.

The DirX products provide full coverage of the four core IAM processes

- Identity Administration Process
  The DirX Identity Business Suite delivers lifecycle management of users and organizational data, administrative and self-service management interfaces, metadirectory and provisioning capabilities.
- Entitlement Administration Process
  The DirX Identity Pro Suite includes all the features of the Business Suite plus lifecycle management of roles and entitlements, request and approval workflows, delegated administration and access certification.
- Access Process
  DirX Access protects access to resources by providing central security services for authentication, authorization, single sign on, identity federation, and Web services security.
- Intelligence Process
  DirX Audit delivers analytical insight and transparency in the identity and access management processes.

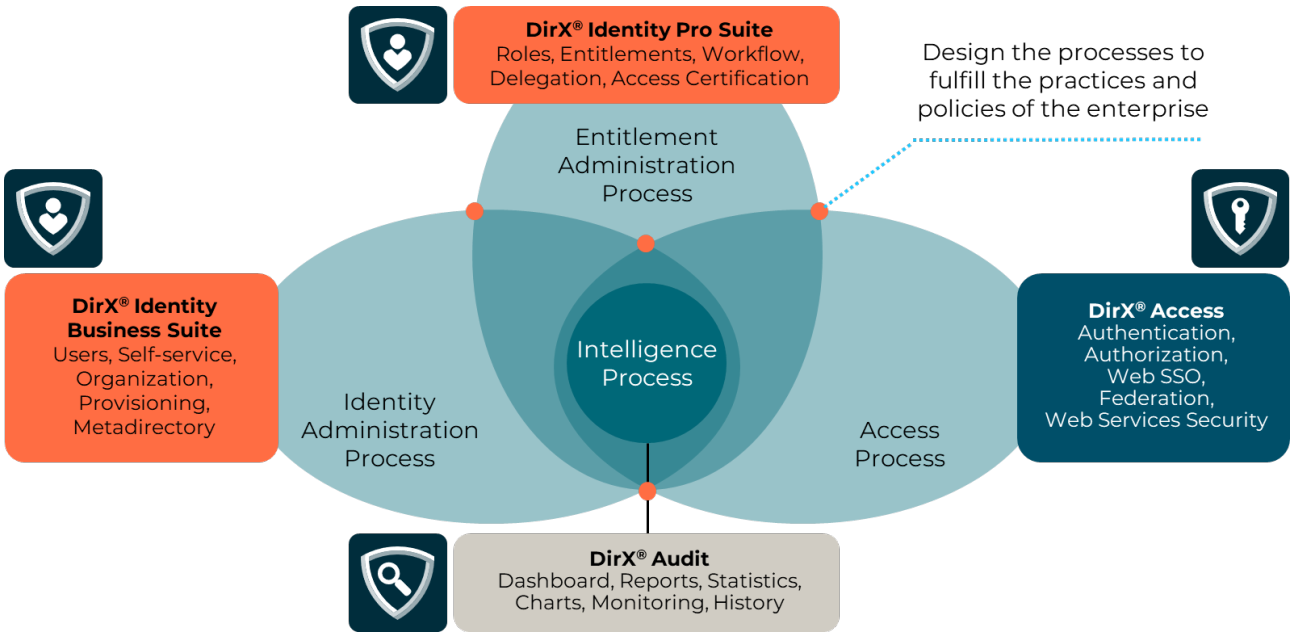

Figure 8. The DirX products provide full coverage for all 4 IAM core processes

The rest of this document describes DirX Identity features, functions, and components. See the user documentation for DirX Audit, DirX Directory and DirX Access for detailed information about these products.

2. DirX Identity Overview

DirX Identity provides the functionality and the corresponding building blocks for a complete identity management solution. Its key features include:

- User management for an integrated user creation and change management process containing both manual and automatic steps
- User facets, personas and functional users for extended representation of a user or for modeling a resource
- Access management modeled on role, permission, and group representations of access rights including automatic assignment to users through security policies and their associated rules
- Certification of user-privilege and privilege-user assignments for risk management and compliance
- Configurable, extensible request workflows for controlling user self-service and delegated administration activities
- Web-based user self-service and delegated administration for structuring and load-partitioning identity management tasks
- Business object management for maintaining common data in structural hierarchies; for example, organizational data or location data
- Instantaneous, automated provisioning and de-provisioning of users and their access rights to resources in the target systems
- A complete password management solution with self-service password administration and automatic password synchronization
- Policies and rules for tailoring the entire identity management solution
- Metadirectory functionality for bidirectional synchronization of identity and access control data between various sources and consolidation of digital identities into the central identity store
- Multi-tenant domain management capabilities and support for any IT system with its own user management and integrated access control
- Web services that can be easily integrated into a service-oriented architecture (SOA) environment
- Auditing of all relevant identity management operations and reporting on the status of all relevant identity management objects for regulatory compliance and investigative purposes
- Monitoring the state of the identity management system to ensure optimal performance
- Scheduled change management for applying changes to DirX Identity data at the right time in the future
- Integration of IT service management systems into DirX Identity's governance and provisioning processes to preserve business and user investments in the existing systems

The following figure illustrates the main functional blocks of DirX Identity.

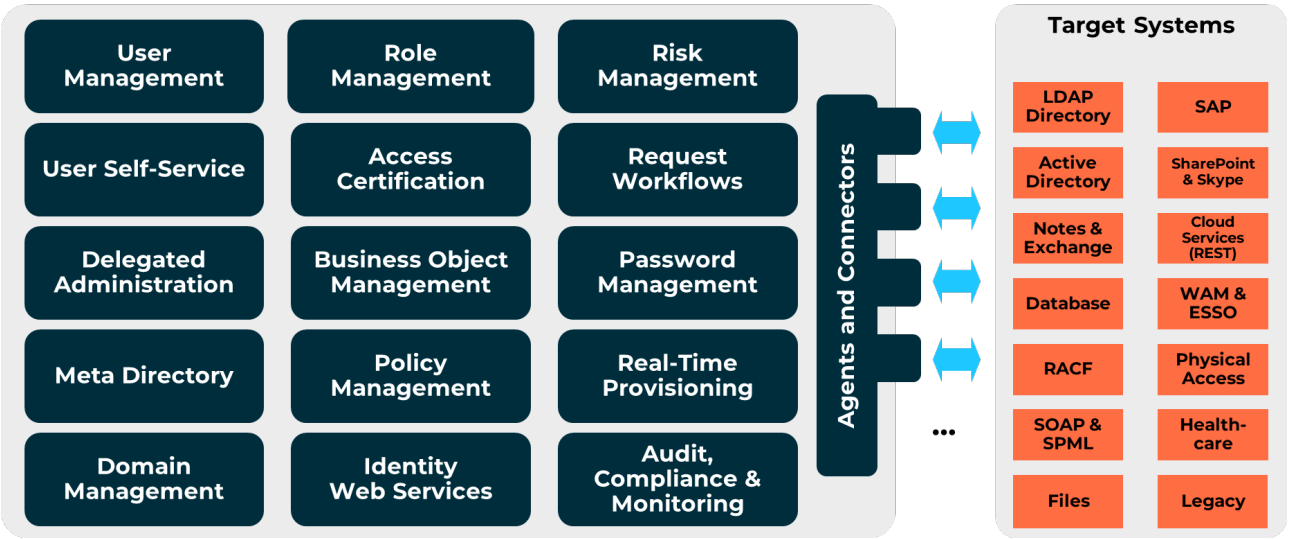

Figure 9. DirX Identity Functionality

The rest of this chapter describes the core mechanisms and features of each function block and how it implements an identity management function. The chapter also provides a brief description of DirX Identity's architectural components.

2.1. 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 encompassing the different directories, user databases, and application-specific repositories that make up the fragmented, heterogeneous IT environment relevant for the lifecycle management of users.DirX Identity supports user management with three types of objects:

- The **user**.A user object in DirX Identity represents the user with its personal attributes, roles, entitlements and accounts.DirX Identity can manage multiple accounts for each user object, but only one account for each target system.
- The **user facet**.A user may hold different positions within an organization that require different roles; for example, a student who works as a tutor and a teaching assistant.A user facet represents the rights that are relevant to a particular job or position – student, tutor, teaching assistant – while the user object represents all access rights and the resulting accounts.User facet objects allow for modeling multiple profiles that share the same accounts as the user; for example, for multiple job profiles within the same organizational unit.
- The **persona**.Users may perform 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 may be quite different, more than one account per target system is typically required, and auditing should be able to distinguish between these functions.Persona objects can be used to extend a user object to address these requirements.Persona objects allow for modeling multiple jobs that require separate accounts for the user; for example, for multiple job profiles within different

organizational units.

- The **functional user**.A functional user object represents a resource that is assigned to a responsible user (called the **sponsor**); for example, a global or group mailbox, a physical room with a phone or a working student entry.These types of resources are managed by the sponsoring user and require accounts that are independent of the sponsoring 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.User directory consistency can be handled by request processes initiated from the users themselves and/or their managers (user self-service and delegated administration) and by data synchronization workflows (for example, with the enterprise HR system) provided by the metadirectory.These processes and workflows can automatically generate global unique identifiers (GUIDs) during user creation, which are essential for maintaining data consistency in large identity databases.

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 DirX Identity 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
- Assigning roles to users to provide them with the necessary access to target system resources.

To reflect an enterprise's Human Resource management process, DirX Identity allows for the maintenance of a user's lifetime with:

- 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

To ensure consistency throughout the user update process, DirX Identity provides a mechanism called a "user LDAP lock" to prevent two or more applications, programs, or threads from updating the same user in parallel.The use case document *DirX Identity Java Programming* provides more information about this mechanism.

2.2. User Facet, Persona and Functional User Management

The user object's lifetime comprises the lifetime of all its associated persona objects.A user facet or a persona object's lifetime can be shorter than the user's lifetime.For a user facet, this provides a way to model different positions within an organization, where each position may have a different lifetime.A user facet might be the right model to apply if the user works in different jobs for one organization and can login under the same accounts for these jobs.For a persona, this provides a way to model different contracts for a user who, for

example, works in the same company but for several different organizational units.

A user facet or a persona object usually changes its status with the corresponding user object, and is not reassigned to another user.A functional user, however, can survive the user object and must be re-assigned to another sponsor (user) if the user is removed or is no longer responsible for the resource that the functional user represents.

In DirX Identity, user facet management tasks include:

- Adding user facets, deleting user facets, and changing the attributes of user facets to be managed with DirX Identity, especially the attributes associated with user facet lifetime and deactivation periods (if DirX Identity masters the user facet data).
- Synchronizing the DirX Identity user facets with a corporate directory master, if the corporate directory supports the concept of different user representations and masters the user facet data.If it does not, only the user objects are synchronized, and the user facets are maintained in DirX Identity.
- Assigning roles and groups to user facets.Role assignment for user facets follows the same procedures and rules as for users.Roles assigned to a user facet are automatically inherited by the user who owns the user facet.

Persona management tasks include:

- Adding personas, deleting personas, and changing the attributes of personas to be managed with DirX Identity, especially the attributes associated with persona lifetime and deactivation periods (if DirX Identity masters the persona data).
- Synchronizing the DirX Identity personas with a corporate directory master, if the corporate directory supports the concept of different user representations and masters the persona data.If it does not, only the user objects are synchronized, and the personas are maintained in DirX Identity.
- Assigning roles and groups to personas.Role assignment for personas follows the same procedures and rules as for users.

Functional user management tasks include:

- Adding functional users, deleting functional users, and changing the attributes of functional users to be managed with DirX Identity.
- Maintaining the sponsor if the related user for the functional user changes.
- Assigning roles and groups to functional users.Role assignment for functional users follows the same procedures and rules as for users.

2.3. Role Management

DirX Identity uses a standards-based role management model that supports parameterization for granting different types of access according to parameterized input, provides approval and re-approval workflows 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 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.The following figure illustrates the relationship between DirX Identity's role model and the access control systems of the IT systems.

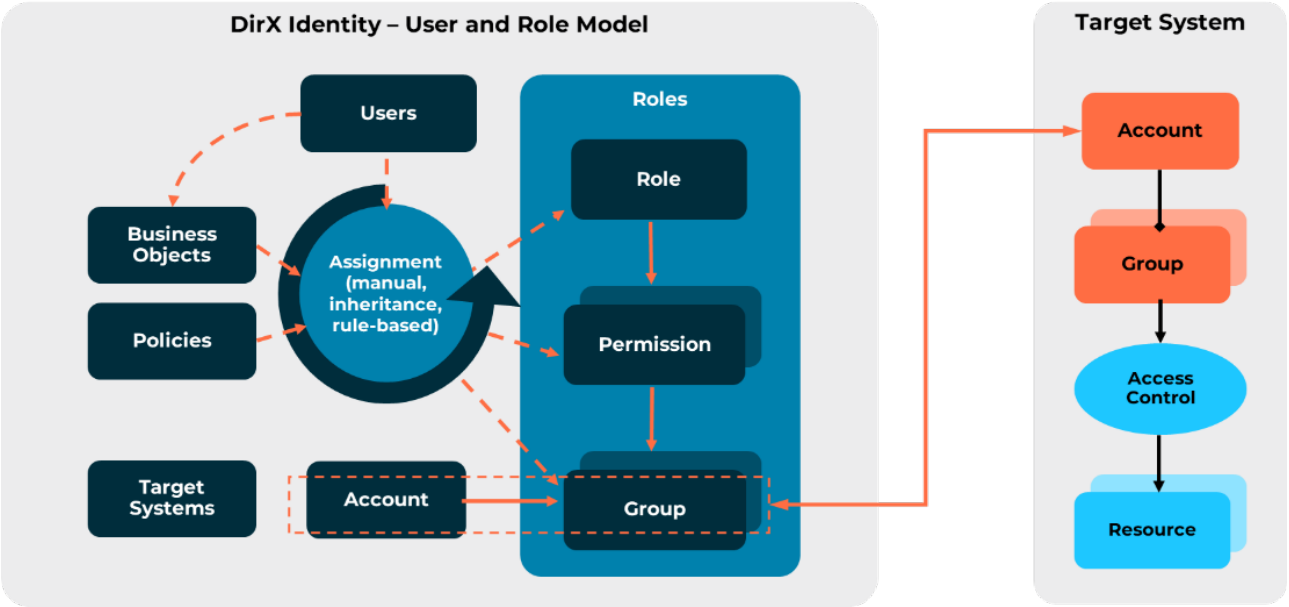

Figure 10. DirX Identity User and Role Model

As shown in the figure:

- A user represents a person inside or outside 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 e-business 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.
- 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.
- 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 by hand (through user self-service or administrative action) or automatically

via provisioning policies or business object inheritance. 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 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.Like roles, role parameter values can be organized into a hierarchical tree.

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 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 appealing and manageable in the enterprise.

A user-role assignment 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 (November 3, 2011 at 5PM). **Approval** and **re-approval workflows** 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 calculating participants in the approval process, including single individual approver, static and dynamic approver groups, policy-driven and even programmed approver calculation.

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 defined in DirX Identity 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 is in violation unless special approval has been performed.

2.4. Certification Campaigns

DirX Identity provides a comprehensive role model for controlling access rights to resources in connected target systems.Features such as access policies, SoD and approval workflows help to secure the assignment of access rights.However, compliance requirements can mandate certification or re-certification of assignments on a regular basis when they are made explicitly by managers or administrators instead of through business objects or rules.DirX Identity provides several mechanisms to support these compliance processes:

- **Manual access certification campaigns for users**.This mechanism allows a campaign manager to define the users that require certification and set up start and end dates for the campaign.When the certification start date arrives, the certification campaign controller starts the campaign.For every user to be certified, it discovers the user's privileges, determines the approver (normally the user's manager), and informs the approver via email.The approvers are notified by the certification campaign controller and they can view each user and his or her privilege assignments.They must decide whether to accept or reject each privilege assignment.They can even change an assignment's end date or a role parameter.When the campaign's end date arrives, DirX Identity removes all rejected assignments and notifies the affected users.Additionally, when a certification task is approaching the due date, reminder notifications are sent to the approvers.The campaign manager can produce a report on the entire campaign.
- **Manual certification campaigns for privileges**.This mechanism allows a campaign manager to define the privileges that require certification and then schedule (or run explicitly) the certification campaign controller to start the campaign.The controller discovers the set of privileges that have been selected for certification and their current assignments and then runs a certification campaign entry for each one.The approvers are notified by the certification campaign controller and they can view the privilege and all of the users to which it is assigned.They must decide whether a user keeps the privilege or whether the privilege is to be removed or modified (change end date or remove role parameters).When approver attestation is complete, DirX Identity removes all rejected assignments to the privilege and notifies the affected users.Additionally, when a certification task is approaching the due date, reminder notifications are sent to the approvers.
- **Continuous access certification via re-approval**: This method uses DirX Identity's re-approval feature on a per-assignment basis.In this scenario, the approval for selected or critical roles is repeated at a specified time.The workflow used for the original approval of the role assignment can be used again, or a special re-approval workflow can be created for the re-approval task.If the notified approvers reject the assignment, the role is removed from the user.Re-approval can be set up so that all critical roles are scheduled for re-approval at the same time.

2.5. Request Workflow

DirX Identity provides several types of request workflow 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
- Request workflows that change and delete existing identity management data (modification workflows), like the attributes of users, roles or business objects.Attribute policies govern which attribute changes must 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)

Each of these workflows can contain optional approval steps that manage the authorization requirements for the request.

DirX Identity allows requesters and approvers to sign their requests and approvals digitally; the digital signature is stored with the request workflow audit trail in the central audit store, and this audit information, including the signed requests, can optionally be protected by system digital signature for compliance purposes.

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.The following figure illustrates the "create user" request workflow template.

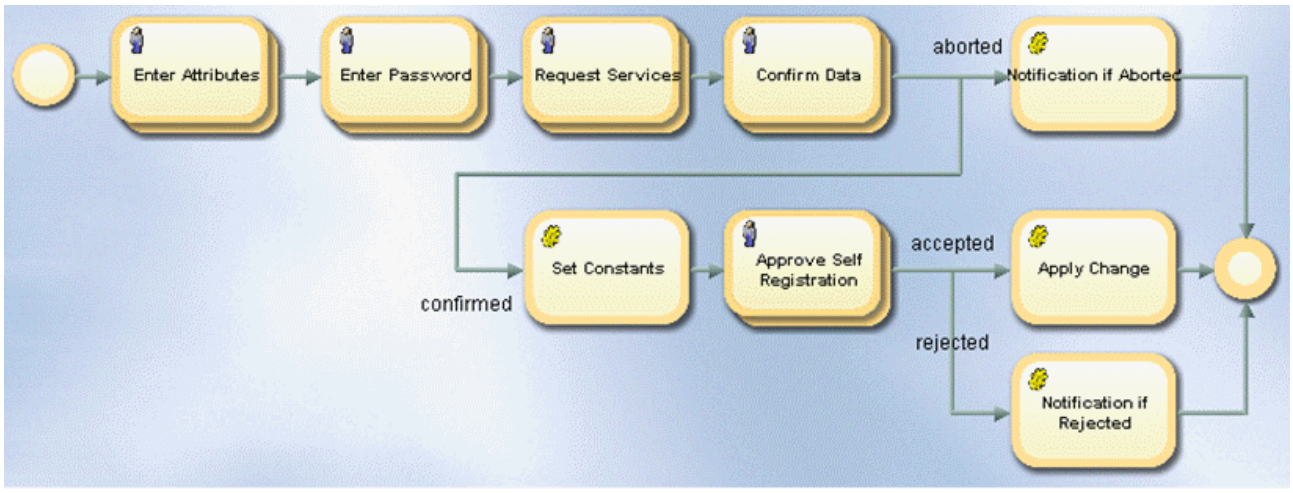

Figure 11. "Create User" Request Workflow Template

The management of request workflows is protected by access policies and comprises start, stop, suspend and resume operations as well as a "change participant" feature to react to real-life situations in which approvers are temporarily unavailable (or permanently unavailable because they have left the company) or are incorrectly assigned to the approval task at hand.Users can approve with DirX Identity's Business User Interface or with DirX Identity's Web Center interface.

2.6. Self Service and Delegated Administration

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 over the intranet or extranet
- Making changes to your own data, including your own passwords
- Recovering and re-setting forgotten passwords through a challenge-response procedure
- Requesting a password reset
- Requesting roles for yourself
- Checking the status of your requests and approvals
- Delegating your access rights (or some of them) to other users

Access policies are used to make sure that a user has access at least to his own data. Access policies are discussed in more detail in the "Policy Management" section.

Delegated administration in DirX Identity is the process of assigning the access rights you have within DirX Identity, or a subset of your access rights, to someone else, optionally for a specified period of time. These access rights include the rights to manage users and roles, assign roles to users or approve requests for such assignments. For example, a project leader who is away for two weeks can delegate the access rights that allow him to assign project-related roles to the members of his team to another person in his group who will then be able to assign roles to these users during these two weeks. And, instead of allowing his substitute to assign all of the available project roles, the project leader can permit his substitute to assign only one or two basic roles; he specifies the roles that can be assigned when he makes the delegation.

Delegated administration tasks in Web Center include:

- Creating new users, roles and rules
- Making changes to user, role and rule data
- Assigning roles to existing users
- Approving the assignment of roles to users or the creation of users, roles, and rules
- Deleting existing users, roles and rules
- Running status reports

Delegated administration tasks in the Business User Interface include:

- Making changes to users and privileges
- Requesting privileges for other users (team members)
- Approving privilege assignments
- Assigning privileges
- Delegating rights to other users

Access policies are used to control which of these administrative tasks a given administrator can perform and on what users and/or roles he is allowed to perform them.Access policies are described in more detail in the "Policy Management" section.

2.7. Business Object Management

Business objects are collections of business-related data that can be used to automate user-role assignment and reduce the redundancy of user data in the identity store.DirX Identity provides a default set of business objects that can be used to build organizational business structures, project structures, and other kinds of structures.Customers can create their own business objects for complete flexibility.

In DirX Identity, business objects are commonly used to:

- Automate user-role assignment by allowing the roles referenced by the business object to be inherited by the users linked to it.For example, an "organizational unit" business object can reference a set of roles that control resources within the organizational unit; when a user is linked to the organizational unit business object, he automatically inherits the roles that allow him access to these resources.Any new roles linked to the business object are automatically inherited by those users assigned/linked to the business object.
- Manage user data centrally and consistently across a set of users; for example, a "location" business object defines all address data only once and can then be linked to related user entries.An update to the business object’s addressing information is then automatically propagated to the linked users.
- Define the contents of proposal lists.A **proposal list** is a list of selections displayed in a drop-down list when a user clicks the drop-down list icon for an attribute value field.Proposal lists can be simple; for example, a proposal list can display a list of locations derived from "location" business objects.Proposal lists can also be complex and interlinked; for example, selecting from a "country" list leads to selecting from an "available locations" list, which leads to selecting from an "available buildings" list, which leads to selecting from an "available rooms" list.

Business object management includes all the activities related to the creation, maintenance and use of business objects, business object attributes and relationships to other objects.Business objects include organizations, organizational units, locations, cost locations and projects.

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 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

2.8. Real-Time Provisioning

Provisioning is the dynamic 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:

1. 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.
2. 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.

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 re-provisions (or de-provisions) the target systems.

DirX Identity's provisioning services provide centralized, consistent, single-point and fully automated administration of users and their access rights within the enterprise IT infrastructure.However, integrating a target system completely with these provisioning services does not always make sense - for example, when the system's user population is small or frequent user or role maintenance is not an issue.These types of systems can be loosely integrated via DirX Identity's manual provisioning feature, allowing them to remain "offline" to its full set of provisioning processes but still benefit from DirX Identity processes that monitor provisioning events to the offline systems and dispatch them to the responsible administrators for manual implementation.

2.9. Password Management

DirX Identity supports a complete password management solution that allows users to maintain a single password that will be automatically synchronized to all relevant IT systems in the enterprise.Password management functions allow users to change and reset their password in one or more systems (for example, in an LDAP directory or in a Windows domain), notify users when they need to change their passwords to comply with

password policies established for the enterprise (for example, expiration of a password's lifetime), and synchronize in real time the password changes to all the relevant IT systems.Users can reset forgotten passwords themselves through a challenge-response procedure or request that an administrator reset them.

Through the Web Center interface, users can:

- Change their own passwords
- Recover/reset forgotten passwords through a challenge-response procedure

From the Web Center interface, administrators can:

- Reset other users' passwords on request
- Create and maintain password policies that control how passwords are used and administered in the enterprise, such as password length and complexity, password aging, and password re-use after expiration

Through the Business User Interface, users can:

- Change their own passwords

Administrators can also:

- Reset other users' passwords

With the Atos Password Reset Client (APRC), users can reset their Active Directory password from their Windows login dialog.They authenticate with their certificate, with a challenge-response procedure, or with a one-time password (OTP) that is sent via SMS.

DirX Identity provides an event-driven password synchronization service that ensures that password changes made from the Web Center interface in the identity store, or from the Windows system in the domain controller, are immediately synchronized to the users' accounts in the appropriate target systems.The service can audit password changes and output the audit information into XML format or provide the data directly to DirX Audit.

2.10. Policy Management

A **policy** is a high-level directive that helps to govern, automate and control identity management processes according to business practices, policies and processes.Policies are composed of one or more **rules**; each rule implements a part of the policy.

DirX Identity supports the creation of identity management policies for governing access to enterprise resources, for ensuring the integrity of DirX Identity user, role and target system data and for acquiring intelligence on DirX Identity data and operations for compliance and continuous process improvement initiatives.These policies include:

- **Access policies** to control self-service and delegated administrative access to DirX Identity's internal resources.An access policy defines a set of access rights to almost any kind of DirX Identity object; for example, users, roles, business objects, user-role assignments, request workflow instances, reports, and even DirX Identity Web Center

menus.For example, an access policy can specify that project team leaders can edit the user data of and assign project-specific roles to the members of their project team, or specify that only certain users are allowed to view certain security-sensitive roles or accounts.Access policies allow the enterprise to structure administration tasks according to its business or organizational model and to restrict the operations on DirX Identity data that particular users can perform.

- **Attribute policies** to track and control changes to specific object attributes like a user's organization or location.Changes to these attributes automatically trigger an approval workflow so that the changes will be authorized.
- **Deletion policies** to track and optionally control the deletion of complete objects.For example, a deletion policy can specify that users and roles are not to be deleted without approval.
- **Event policies** to track creation of and changes to certain types of object; for example, users, accounts, or "organization" business objects.Creating a new object or changing an existing object of the indicated type triggers an event-based workflow that stores information about the creation or change event for compliance purposes.
- **Assignment 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.
- **SoD policies** to specify the combinations of roles, permissions and groups that cannot be assigned to a user at the same time unless approval is obtained under mitigating controls.
- **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, and so on.
- **Reconciliation 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.
- **Audit policies** to define the DirX Identity objects and object attributes that are relevant to compliance with corporate security policies and government regulations and which therefore should be monitored for change.

DirX Identity processes policies either dynamically or periodically, depending on the kind of policy.

2.11. Metadirectory

DirX Identity metadirectory is the set of services that integrates the disparate directories, user databases, and application-specific information repositories in the enterprise IT network 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.

2.12. Domain and Target System Management

Multi-tenant support is provided through 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.Users and administrators from one domain cannot see and handle objects from another domain, and all roles, rules, policies and workflows are completely separated.You can use domain specific set-up parameters to define different behavior for different domains.

DirX Identity delivers several sample domains – for example, a sample domain for a company that provides software and hardware products and a sample domain for a healthcare organization - that illustrate the typical ways to work with DirX Identity in a customer environment and show most of the features that DirX Identity provides.These domains can be automatically installed on request during DirX Identity installation.

A target system is any system that DirX Identity is to control.Examples of target system types are Active Directory (AD), databases or applications that contain their own user management with integrated access control.You can define any number of target system instances for one type, for example, you can model the domains of an AD forest as different AD target systems.Administrators can set specific set-up parameters according to each

target system type and instance.

Target systems typically contain accounts and groups that are kept synchronized between the connected system and the target system.Target systems usually have a small number of privileged accounts that allow users to perform high-risk, security-critical operations on the target systems and can be used by different users in parallel.DirX Identity allows privileged accounts to be modeled as roles so that they can be controlled and audited as identity management elements.Privileged accounts then become eligible for assignment to users and for the application of SoD, re-approval, and other role-related policies.DirX Identity also applies automatic controls to privileged account passwords, such as automatically enforcing a password change when a user assignment is removed from the role and automatically changing expired privileged account passwords.

2.13. Web and REST Services

Service-oriented architecture (SOA) is a methodology for structuring functional elements as modular, interoperable services.SOA can be an effective way for an enterprise to bring its internal assets online as re-usable, interoperable business services that can be quickly and easily integrated and re-integrated to respond to changing business processes and new market opportunities.Web Services is one way to implement an SOA, and it has become a popular technology for connecting the business services deployed in enterprise SOA environments

The Identity Web Services can be used to integrate DirX Identity's provisioning features into SOA-compliant application environments.The Identity Web Services interface can handle users, roles, permissions, groups, accounts, target systems and business objects.The Identity Web Services implement the OASIS Service Provisioning Markup Language (SPML) standard and support the standard SPML operations add, modify, delete, lookup and search.Depending on the object type, additional capabilities may be offered; for example, assignment of roles to users or password changes.

For all object types, a **user hook** - an extension made by the customer to DirX Identity common code that is protected from product updates - can intercept requests and responses and perform custom operations such as moving entries and creating or checking unique identifiers.

In the area of access management, the Identity Web Services provide Web single sign-on integration with SAP NetWeaver and leading Web access management products such as DirX Access and Entrust GetAccess.

With the Representational State Transfer (REST) paradigm becoming more and more popular, DirX Identity provides a REST service which is used to integrate DirX Identity into application environments that want to use the standard HTTP protocol and the performance and scalability advantages of RESTful services.In particular, they can be used by modern, HTML5-based Single-Page applications; one example is the new DirX Identity Business User Interface.

The REST services adhere to SCIM 2, the System for Cross-domain Identity Management.They provide the following features with JavaScript Object Notation (JSON) as the 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.
- User Service - users can request roles for other users, view and edit the profiles of other users, and reset their passwords.
- Delegation Service - users can delegate tasks to other users.
- Domain Service - users can manage any type of objects in a generic way.

2.14. 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.DirX Identity supplies a set of pre-configured audit policies and permits customers to define their own audit policies to satisfy individual corporate requirements.Audit logs are archived in XML format to a central audit store for centralized visibility and traceability and can be optionally secured with a system-specific digital signature to make them tamper-proof.

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 or object collections and their attributes, user-role, permission, and group assignments, delegated users and administrators, unused privileges, the entire role catalog, 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 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

- Approval and re-approval workflows automate the application of corporate authorization policies, ensuring that they are applied consistently rather than on a case-by-case basis
- 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

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

2.15. Risk Management

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

When risk assessment is enabled at the domain and a risk policy is defined, a risk calculation workflow regularly calculates the risk factors for every user in the domain and then aggregates them into a compound risk according to a customizable configuration, thus classifying users into risk categories from low to high.DirX Identity Web Center displays a user’s risk category, while DirX Identity Manager displays a user’s individual risk factors as well.Risk factors include SoD violations, imported accounts and group memberships and total number of group memberships or privileged accounts.

For any requested change in a user’s privilege assignments, a customizable assignment request workflow can compare the compound risk before and after privilege assignment.If the risk category increases as the result of the requested privilege assignment, additional approval steps can be required before the privilege can be assigned.Compliance officers, line managers and administrators can use DirX Identity’s risk assessment feature to monitor the risk values in the domain and plan actions to reduce the number of high risk users; for example, by running appropriate certification campaigns or by enforcing additional approval steps.

2.16. Monitoring

Running complex provisioning and request workflows can result in a heavy load on DirX

Identity's servers.You can use DirX Identity's specially tailored user interfaces to check the state of the system and to observe running processes and threads.You can use this information to optimize the system; for example, you can add or remove threads for specific tasks, or you can change relevant parameters that affect system performance.

DirX Identity provides a set of specialized Nagios plugins and commands for the Java-based Nagios Remote Plugin Executor (JNRPE) add-on that can be used in an existing Nagios® Core™ Open Source monitoring 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 for monitoring:

- All information provided via Java Management Extensions (JMX), especially from the Java-based Identity Server and other JMX-enabled programs such as Apache ActiveMQ and Apache Tomcat.
- The C++-based Identity 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 JNRPE add-on to check:

- Java-based Identity Server state
- The outstanding responses of a specific Java Messaging Service (JMS) adaptor
- A statistics attribute of a specified workflow
- Java Virtual Memory (JVM) usage
- C++-based Identity Server state

The DirX Identity servers attempt to handle each event properly.Nevertheless, errors in messages and events can occur as the result of incorrectly configured server processes.These messages and events are stored in a dead letter queue which DirX Identity's monitoring interface allows you to examine.You can then correct the configuration and process the event again.You can also delete saved messages or events that you no longer need to track.

You can also use the LDAP session tracking information generated by DirX Identity components in conjunction with DirX Directory's audit record decoding tools to pinpoint DirX Identity component operation and correlate activities across LDAP servers and clients.

2.17. Scheduled Change Management

By default, DirX Identity processes updates to its identity management data immediately.For example, when an administrator changes a user's department attribute, the change is applied right away (or when approval is obtained).In some cases, however, administrators may want to delay the application of a change and schedule it for a future

date.For example, suppose a company employee is transferring from Sales to Marketing, but not until the end of the month, which is a few weeks away.The employee’s department information should not change until his transfer is complete, but it should be scheduled to change on the date that coincides with his transfer.

DirX Identity provides a ticketing feature that allows administrators to specify due dates for changes to any DirX Identity object - user, role, policy, and so on - and thus schedule the change to occur on the right date.A ticket process runs on a daily basis to check these due date "tickets", and then automatically initiates the change when a ticket’s due date arrives.In this way, the administrator can schedule the employee’s department attribute change from "Sales" to "Marketing" now, and know that it will be carried out automatically at the end of the month.Administrators can view pending and processed ticket orders made on DirX Identity objects to track the order status and results.

2.18. DirX Identity Components

The main components of DirX Identity include:

- Identity Business User Interface
- Identity Web Center and Identity Web Center for Password Management
- Identity Manager
- Identity Store
- Identity Server
- Identity Services
- Agents and connectors
- Identity Integration Framework
- Identity Server Admin
- Identity Web Admin
- Atos Password Reset Client

The following figure illustrates these components and the relationships between them.

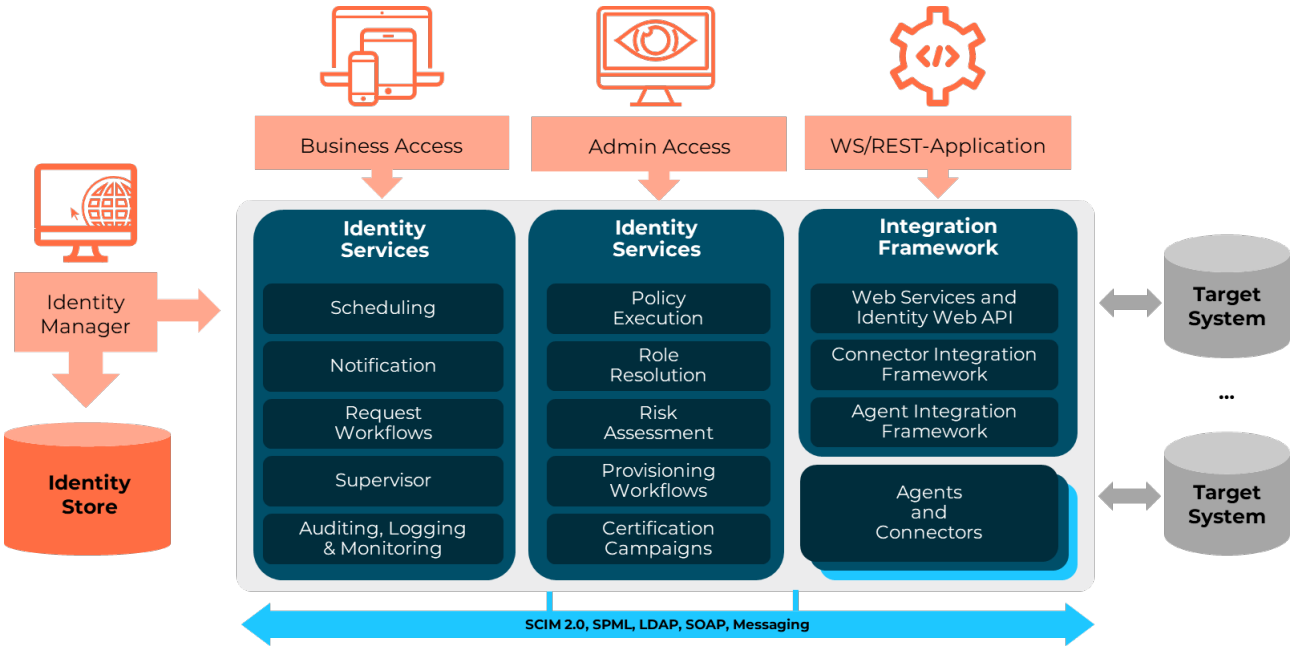

Figure 12. DirX Identity Component Architecture

2.18.1. 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. Web Center also supports various types of single sign-on; for example, for Microsoft Windows, SAP NetWeaver and generic configurable mechanisms.

2.18.2. 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 or PKI card
- Manage team members (including profile changes, requesting new privileges, and resetting passwords)
- Display and edit a user's own profile
- Request a new privilege
- For requests, edit the participants list and cancel a user's own requests
- Display and edit role parameters of assigned roles
- Show pending role requests
- Approve single/bulk role requests
- Create, edit and modify delegations (new style)
- Change and reset passwords for team members

2.18.3. Identity Web Center for Password Management

The Identity Web Center for Password Management is a Web application that provides the subset of Identity Web Center functions that support the password management solution described in "Password Management". Identity Web Center for Password Management allows users to change the passwords of some or all of their accounts in the target systems and permits administrators to reset user passwords, manage password policies and run specialized reports on password management-related activities.

2.18.4. 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 (Metadirectory), provisioning, and request workflows
- Target systems and authoritative sources

Identity Manager can also be used to monitor provisioning workflows, role resolution and policy execution. Identity Manager supports the SSL (Secure Socket Layer) protocol for authenticated, encrypted communication with the Identity Store.

2.18.5. Identity Store

The Identity Store is an LDAPv3 directory - a DirX Directory Server - that serves as the consolidation point (the directory "join") for identity integration from authoritative sources and as the distribution point for provisioning 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, request workflow definitions, target system account, group, and account-group membership data and the configuration and operational data required by the metadirectory integration and provisioning 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.

2.18.6. Identity Server

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

- Handling event-triggered provisioning tasks like password synchronization or the real-time synchronization of provisioning events
- Scheduling provisioning workflow runs, including recovery, retry, and checkpointing

operations in the event that problems occur

- Notifying administrators via e-mail about provisioning workflow events
- Messaging services, messaging queue support and Java Messaging Service (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 and scalability and high availability scenarios.

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.

2.18.6.1. Java-based Identity Server

The **Java-based Identity Server** is designed to handle event-triggered provisioning processes and request workflows. 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 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 a change to a business object, for example, an organizational unit. Changes to the organizational unit's attributes are propagated by events to all users that are assigned to this unit. When a role is assigned to the unit, it is immediately inherited by all of the users assigned to the unit.

Java-based Identity Server 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 can also process request workflows. Request workflows are used to protect unauthorized object changes, for example, user or role creation, critical user attribute modification or assignment of security-related roles to users.

Each Java-based Identity Server hosts its own embedded messaging service, an Apache ActiveMQ Message Broker. This messaging service supports not only local consumers and producers from the same server, but also external ones such as Web Center and Identity Manager. With appropriate configuration, the messaging service improves overall scalability by forwarding messages to other Java-based Identity Servers.

Client applications can use the Java-based Identity Server's Web Services to manage users, roles, and user-role assignments without the need to change proprietary client interfaces.

The Java-based Identity Server offers features for load distribution and scalability, automatic fail-over from failed to working Identity servers, escalation, error handling - including notification services - and configurable auditing and logging.

2.18.6.2. C++-based Identity Server

The **C++-based Identity Server** is designed to handle scheduled 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 workflows. The C++-based Identity Server supports distributed and nested workflow runs in a heterogeneous network as well as exception handling and recovery mechanisms.

2.18.7. 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
- The REST service, which handles the approval of user-role assignments and self-service.
- Event-triggered provisioning workflow services for fast, immediate real-time provisioning and password synchronization and scheduled provisioning workflow services for complex identity creation, maintenance, and target system provisioning tasks
- The certification campaign controller, which starts, monitors and finishes user or privilege certification campaigns.

2.18.8. Connectors and Agents

DirX Identity connectors and agents 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 type of target system. A connector 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. An agent can be implemented by a connector that is 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.

2.18.9. Identity Integration Framework

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

- Use the Identity **Web 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 abstract REST connector to implement a custom connector to any RESTful API or use the System for Cross-domain Identity Management (SCIM) connector to access any RESTful API using the SCIM standard.
- 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.

2.18.10. Identity Server Admin

The Identity Server Admin is a Web application that allows DirX Identity administrators to perform **administrative fail-over** of Identity server operations: the ability to move server functions manually from a failed Identity server to a working Identity server. Identity Server Admin gives an overview of all Java-based Identity Servers, C++-based Identity Servers and Message Brokers and allows you to move:

- The Java-based Identity Server's Java Messaging Service (JMS) publish / subscribe adaptors to another Java-based Identity Server.
- The responsibility for request workflow processing to another Java-based Identity Server.
- The Java-based workflow scheduler to another Java-based Identity Server.

2.18.11. Identity Web Admin

The 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, Jconsole - to monitor and tune Java-based Identity Servers from the Web or from a program. Web-based administration tasks include supervising server status, observing server statistics, viewing process instances, optimizing for load distribution and tuning for performance. Identity Web Admin can help DirX Identity administrators manage server crashes and prevent data loss.

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.

2.18.12. DirX Password Reset Client

The DirX Password Reset Client (DPRC) is a Windows client that is deployed on a user's Microsoft Windows system.

DPRC can be accessed and used before logging into Windows (after CTRL-ALT-DEL) via an additional option in the login dialog.The advantage of this user interface is that the password reset can be done directly from the user's workstation.It can be used from within the corporate network or from outside the network by roaming users.

The DirX Password Reset Client offers a configurable deployment mode for selecting alternative authentication methods:

- Smart card authentication
- Security questions
- Mobile OTP
- Any combination of these options

2.19. Integration with Service Management Systems

Many companies have IT service management systems in place to help manage the company's assets - for example, hand-held devices, software licenses, computer and printer supplies - and dispatch requests for access to these assets to the appropriate IT service technicians and administrators.Some of these requests involve identity management-related actions, like requesting access to a file share or to a specialized function in a software system like Active Directory or SAP.While these systems can be tightly integrated into DirX Identity's automatic provisioning process, it is often easier and more cost-effective to integrate these external systems loosely as source or target systems for identity management actions.

In the source configuration, the service management system is connected to DirX Identity - for example, through a Web Services interface - and issues identity management-related requests - for example, to create or change a user, or assign a role to a user - to DirX Identity, which then processes these requests.The service management system can issue status update requests to track the request processing.

In the target configuration, the service management system is connected to DirX Identity through a customer-written connector, and DirX Identity issues identity management requests to the system - specifically, provisioning requests.Administrators for the target service management system process the DirX Identity requests and then confirm the completion of their tasks to DirX Identity.

Sometimes there is no external service management system in place for target system provisioning, but connecting the system tightly to DirX Identity's automated provisioning feature isn't a good option.Perhaps the target system has a very small number of users, or requires very little ongoing maintenance.DirX Identity's **manual provisioning** process allows these systems to remain "offline" to its automated provisioning process but monitors provisioning events to these systems - add, modify or delete requests - and dispatches them to the responsible system administrators via email notifications sent by request workflows.The administrators perform the indicated synchronizations at the target system by hand and then confirm the completion of their tasks to DirX Identity.

2.20. Standards Support in DirX Identity

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.
- DirX Identity Web Services implement the OASIS SPMLv2 specification using the SPMLv2-DSML profile.
- DirX Identity REST Services adhere to the SCIM 2 specification.They are described in the Open API V3 specification.
- 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 and Server Admin are 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.

2.21. DirX Identity Default Applications

DirX Identity delivers a powerful set of default applications that hold ready-to-use examples for typical identity creation, maintenance and synchronization workflows.These applications can easily be tailored to 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 that are accessible via wizards

- Can be easily upgraded due to the clear separation of standard script code and customer extensions

2.22. Deployment

DirX Identity has three deployment phases: the planning phase, the initial phase and the production phase.

In the planning phase, you define your approach to DirX Identity deployment given your IT environment: In this phase, the steps are to:

- Collect information about your current IT environment and document it.
- Define your target DirX Identity deployment architecture.Think about component distribution, operation, and performance enhancements.

In the initial phase, you install and configure DirX Identity according to your target deployment architecture.Decentralized security administration is in place: the target systems already have accounts and groups, but security administration is not role-based.In this phase, the steps are to:

- Build your own connector to the target system, if necessary. Configure the workflows that are required to perform synchronization and validation to this target system.
- Collect all of the account and group information from the target systems and consolidate it in the DirX Identity store using the target system validation workflow in "initial load" mode.
- Determine whether the target system groups are acceptable as they are for role-based administration.
- If necessary, restructure the target system groups based on the role definition information, or use groups and map them to permissions.

In the production phase: (the target system integration section in the *DirX Identity Tutorial* shows how to get to this phase)

- Access control is centrally administered
- All target systems are managed from DirX Identity
- All namespaces, account and group names are centrally administered from DirX Identity

You can add additional target systems step by step using the last two steps for each target system that needs to be connected.

Glossary

This glossary defines terms and concepts that relate to identity and access management and DirX Identity.

A

abstract class

In object-oriented programming, a class that is designed only as a parent class from which sub-classes may be derived but which is not itself suitable for instantiation. Abstract classes define special features to be included in all inherited classes. Also called interface.

access management

The part of an IAM system that performs real-time enforcement of the security policies established for each user of the enterprise IT infrastructure. Access management processes include authentication, authorization, and audit.

access policy

A policy that defines access rights within DirX Identity itself. Access policies form the basis of delegated administration and can be optionally controlled through privileges. See also delegated administration, privileges.

access rights

The rights granted to a user that define how that user is allowed to access a resource on an IT system (a connected system or DirX Identity itself). In DirX Identity:

- Account-group memberships in target system groups determine a user's access rights in that specific connected system. See also privilege, group.
- Access policies determine a user's access rights to resources (user, privilege, and password policy data) in DirX Identity itself; for example, the set of privileges a user is allowed to assign, and to which users he is allowed to assign them.

account

A user's representation in a target system. A user can have accounts in many different target systems. See also personal account and privileged account.

administrative fail-over

The process of monitoring Identity Server operation in a high availability scenario and then manually transferring functions from a failed Identity Server to a working Identity Server. DirX Identity administrators can use the Identity Server Admin tool to perform these tasks.

agent

A DirX Identity component that enables data exchange between a specific connected system and the target system in the identity store during meta directory integration and synchronization operations. Agents work with batch-oriented metadirectory synchronization and provisioning services.

application programming interface (API)

The interface (functions and classes) that an application presents to developers for adding new features or changing existing ones. See also connector server API.

approval workflow

A type of request workflow that handles approvals of user-role assignments by requesting authorization of these assignments by various approvers according to the access policies in force. See also request workflow.

audit

The process of producing, collecting, cleansing and correlating data about IAM administration, authentication and authorization events and then transforming this data into actionable intelligence with respect to compliance regulations, business security policies and corporate risk management objectives. Identity audit provides the means to analyze and report on IAM functioning and deliver the information necessary to support IAM governance of users and their entitlements. "Audit" is called "identity audit" in the context of IAM.

audit message

A message in an audit trail that DirX Audit has extracted, transformed into DirX Audit data format and stored in the DirX Audit Database. The data in the audit message includes the original message in the format of the audit producer plus the "who", "what" and "where from" information and a message identification.

audit trail

A chronological sequence of audit messages, where each message contains evidence that directly pertains to and results from the execution of an IAM transaction. See also audit message.

authentication

The process of identifying users and validating their identity.

authorization

The real-time enforcement of user access requests to the enterprise resources. Authorization ensures that users can only access the IT systems in the enterprise and their corresponding resources according to their access rights.

automatic fail-over

The process of monitoring Identity Servers in a high availability scenario and then automatically transferring functions from a failed Identity Server to a working Identity Server. Administrators configure Identity Servers to perform these tasks.

B

business object

A collection of data related to a business structure in the enterprise such as an organizational structure, a cost center structure or a project structure. Business objects in an identity management system help to automate user-role assignment and reduce

identity data redundancy.

C

c++ connector

A connector written in the C++ programming language. See also connector.

certification campaign

The process of periodically checking user-privilege assignments to ensure that these assignments continue to comply with business policies.

collection

A set of objects and subtrees within a domain that can be exported to an LDIF file for subsequent transfer to another domain.

compliance

The clear and demonstrable observation of legal regulations.

connected system

An IT system in an enterprise that authenticates and authorizes users and is provisioned by DirX Identity according to identity information about the system which is stored in the Identity store. Examples of connected systems are operating systems, messaging systems, directories and databases, ERP applications, Web portals and e-business applications, groupware applications, and mainframe security systems. DirX Identity represents connected systems as target systems in its Identity store.

connectivity

The ability to connect to a connected system for provisioning or to handle a connected system through its API. In DirX Identity, connectivity is accomplished through agents or connectors.

connector

A DirX Identity component that enables data exchange with a specific connected system. Connectors are used by event-triggered provisioning services. Agents can be built by integrating a specific connector with the identity integration framework to a stand-alone program.

connector server API

The interface classes, macros and libraries that third-party developers can use to create customer-specific connectors.

D

delegated administration

The process of permitting users to assign their access rights to data in DirX Identity's identity store (or a subset of these access rights) to other users through a Web-based interface.

domain

An isolated area under DirX Identity control that has its own set of users, roles, and policies. DirX Identity can support several domains (called "multi-tenant capability").

E

entitlement

The access right of a user in a target system; for example, a group assignment. Identity governance functions discover entitlements in target systems and then use them to create aggregated privileges like permissions and business roles. Privilege resolution determines, as a consequence of role assignment and user context information like attributes and role parameters, the set of entitlements that need to be provisioned. See also group, privilege.

exception

An error condition that changes the normal flow of control in a program. In the C programming language, an exception is a special C construct that allows developers to define specific error-handling for an application, called "throwing an exception". The C++ connector server expects a connector to throw an exception when an error occurs.

F

factory method

A method that defines an interface for creating objects but allows a class to defer instantiation to subclasses. A factory method creates instances of the class in which it is declared, as opposed to creating a class instance by calling its constructor after the new operator, for example.

federation

An application of authentication that permits an enterprise to share trusted identities with autonomous organizations outside the enterprise, like trading partners or suppliers. Also, called federated identity.

functional user

A method for modeling a resource that can be assigned to a user; for example, a global mailbox, a group mailbox, a physical room with a phone connection or a working student entry. A functional user represents the resource and is managed by the user who sponsors it. See also user and persona.

G

group

A set of access rights in a specific target system. The group is the basic building block in the DirX Identity privilege model. Its semantic is specific for each connected system; more generic privileges are built by aggregating groups. See also entitlement, privilege.

I

identity

A single unique view of a user to be provisioned in the enterprise IT infrastructure that is aggregated from multiple authoritative sources of user data in the enterprise IT infrastructure by the IAM system's metadirectory services. Also called digital identity. The representation of an identity in a connected system is an account.

identity and access management (IAM)

An integrated solution for user and access management across the heterogeneous systems that constitute the IT infrastructure of an enterprise.

identity governance

The functions in identity management that provide a high-level, transparent business-oriented way to define, create, manage, assign, review and remove digital identities and their entitlements to resources.

identity Integration Framework

The set of interfaces and common utilities that permit customers to extend DirX Identity connectivity to new connected systems and to customize the Identity Web Center.

identity management

The part of an IAM system that ensures a consolidated, enterprise-wide view and way to manage user access to resources in the enterprise IT infrastructure. Identity management processes include user self-service and delegated administration, password management, user management, privilege and policy management, provisioning, and metadirectory.

identity Manager

The DirX Identity component that provides a graphical user interface (to the configuration information in the identity store) to manage DirX Identity connectivity and provisioning.

identity provisioning

The functions in identity management that dynamically and automatically realize the results of identity governance functions into entitlements in the IT infrastructure.

identity Server

The runtime environment for all DirX Identity services and workflows.

identity Server Admin

The DirX Identity Web application that allows DirX Identity administrators to perform administrative fail-over of Identity server operations. See also administrative fail-over.

identity Store

An LDAP-enabled directory in the enterprise IT infrastructure that is used as the identity consolidation and distribution point for the other connected IT systems in the enterprise. The identity store contains consolidated identity data from different authoritative sources and connected systems and manages DirX Identity's configuration data in a

separate tree.

identity Web Admin

A Web-based DirX Identity component for monitoring server processes, including status, logging, and statistics. Web Admin also permits server optimization and error-handling via a dead letter queue.

identity Web Center

The DirX Identity component that provides a Web interface for self-service user management and selected administrative tasks - for example, privilege management, password policy management and delegation - from a Web browser.

internal SPML representation (ISR)

The set of classes that implement the SPML constructors for use in C++ connectors. These classes form the connector server API and carry the data that is delivered to and from the connectors. See also Service Provisioning Markup Language, connector server API.

M

manual provisioning

The process of provisioning a target system that is not directly connected to DirX Identity 's provisioning processes via event-triggered request workflow notifications sent to the target system’s administrator, who then performs the provisioning by hand. See also provisioning.

meta agent

See agent.

metadirectory

The identity management component that integrates the different directories, user databases, and application-specific repositories in the enterprise IT network. It provides the connectivity, management and interoperability functions that unify the user data ("join") and ensures the bidirectional attribute flow (synchronization) in this fragmented, heterogeneous environment.

multithreaded application

An application whose program execution consists of multiple threads executing in a shared address space. The C++ connector server is a multithreaded application: its components (for example, its connectors) run independently of each other but share the same application resources (for example, memory space). See also threads.

P

parameterized RBAC

An aspect of role-based access control (RBAC) that permits the access rights modeled by a generic role or permission to be customized on assignment to a specific user. See also role parameter, permission parameter, role-based access control.

password management

A specialized application of an identity management system that allows users to maintain a single password that is automatically synchronized to all relevant IT systems in the enterprise, to change and reset their passwords in one or more systems (for example, an LDAP directory or in Windows) and to notify users when they need to change their passwords to comply with password policies established for the enterprise (for example, expiration of a password's lifetime).

password policy

A policy for controlling the requirements that DirX Identity places on user passwords, such as password complexity, expiration dates, and the behavior of the system after failed logins.

permission

A connected-system-neutral set of access rights that aggregates a collection of groups from one or more connected systems. The permission is the intermediate building block of the DirX Identity privilege model. See also privilege.

permission parameter

A critical attribute in a user entry that indirectly influences the user's access rights via rules or other mechanisms. Because permission parameters have system-wide effects on user access rights, the ability to change permission parameters should be secured by approval processes.

persona

A method for modeling a user's different functions in an enterprise - for example, "system administrator" or "project manager" - where each function requires a different set of accounts and entitlements. See also user and functional user.

personal account

An account in a target system that is related to one specific identity (user). See also account and privileged account.

policy

A high-level directive that is used to control the decision-making behavior of the DirX Identity system. Policies are composed of one or more rules; each rule implements a part of the policy.

policy parameters

The parameters used in DirX Identity that affect the assignment of access rights or privileges, especially permission and role parameters.

privilege

Any set of access rights modeled and used in DirX Identity. The term "privilege" is used as a generic designation for group, permission, or role. In this model, access rights to IT systems and resources are controlled by privileges, which in turn are associated/assigned to users. See also group, permission, role.

privileged account

An account in a target system that entitles users to perform high-risk, security-critical operations on the target system. An example of a privileged account in a UNIX operating system is the "root" account. An example of a privileged account in a Windows operating system is the "Administrator" account. See also account and personal account.

proposal list

A list of selections displayed in a drop-down list when a user clicks the drop-down list icon for an attribute value field. The content of a proposal list can be derived from business object structures.

provisioning

The process of automatically calculating user access rights and distributing them to IT systems based on the privileges assigned to the user. The provisioning process automatically grants, changes, and revokes access rights in IT systems in response to privilege assignment, re-assignment, and revocation.

Q

query

A search filter that is intended for dynamic, frequent use for auditing purposes, such as searching for unassigned accounts (accounts that have no user assigned to them). Queries are stored as query folders in the DirX Identity store.

R

reconciliation

The periodic comparison of connected system accounts and group data to the identity store to detect local changes to the connected system’s data that have occurred independently of the changes initiated by DirX Identity. Deviations can be reconciled by hand or through automated policy-driven workflows.

request workflow

A workflow that handles self-service and delegated administration requests that may require authorization by one or more approvers.

role

A set of access rights based on business semantics that allows the enterprise to structure access to resources according to job descriptions and functions. The role is the top-most building block of the DirX Identity privilege model and is based on the National Institute of Standards and Technology (NIST) role-based access control (RBAC) standard.

role-based provisioning

The process of assigning, either manually or with rules, a user one or more roles in order to implement a security policy. Role-based provisioning requires the existence of a role catalog and a role engineering process that reflects the enterprise business processes. Assigning a role to a user results in group memberships in various target systems.

rule

A lower-level directive that implements a part of a policy.

rule-based privilege assignment

The process of automatically assigning privileges (roles, permissions, but mostly groups) to a user based on one or more rules that implement a security policy. Also called policy-based privilege assignment.

S

segregation of duties (SoD)

The process of placing constraints on role assignment to enforce "conflict of interest policies", for example, a user with the role "accounts payable" cannot be assigned the role "accounts receivable". Also called separation of duties.

self-registration

A form of self-service in which a user makes a request from the intranet or Internet for membership in an enterprise service.

self-service

The process of allowing users to manage their own data, passwords, and delegations and to request privileges for themselves through a Web-based interface.

separation of duties

See segregation of duties (SoD).

service management system

A platform for structuring information technology (IT) operations and IT-related activities such as problem resolution and change control according to business processes and user requirements. Also called IT service management (ITSM).

service Oriented Architecture (SOA)

A methodology for defining functional elements as modular, interoperable services. Web Services are one method for implementing an SOA.

services Provisioning Markup Language (SPML)

A standard XML-based language designed for use in provisioning databases. SPML is based on request-response scenarios; for more information on SPML, see http://www.oasis-open.org/specs/#spmlv1.0.

simple Object Access Protocol (SOAP)

The standard protocol for calling network services and transmitting data between them. SOAP is based on request-response scenarios; for more information about SOAP, see http://www.w3.org/2000/xp/Group/2/06/LC/soap12-part1.html.

single sign-on (SSO)

A component of Web access management that permits a user to access multiple IT systems and applications after being authenticated just once. Similar to Web SSO for the

access of Web-based applications.

soD policy

A policy that specifies the roles that cannot be assigned to a user at the same time. See also segregation of duties (SoD).

sponsor

The user who is assigned to manage the resource represented by a functional user. See also functional user.

synchronization

The process of extracting, transforming, and loading data from one repository to another, especially identity and access control data in the case of identity management systems, for example, from the authoritative sources of identity information to the identity store and vice-versa.

T

target system

The representation of a connected system within DirX Identity. A target system is a partial copy of the data in a connected system that DirX Identity keeps synchronized with the actual data in the connected system. This data includes accounts (the users in the connected system) and groups (a representation of the access control objects or resources in the connected system).

thread

The part of an application that can run independently of and concurrently with other parts of the application. See also multithreaded application.

ticket

A record of a service management request. See also service management system.

U

user

A person inside or outside the enterprise for the purposes of privilege assignment.

user facet

A method for modeling a user's different positions within an organization - for example, "student", "tutor" or "teaching assistant" - where each position requires a different set of roles. See also user, persona and functional user.

user hooks

Extensions made by customers to DirX Identity common code that are independent of this code and which therefore do not change with product updates. The DirX Identity default application code is divided into common code (control and central scripts that can change with product updates) and user hooks (customer routines that are protected from product updates).

user management

The activities related to the creation, maintenance, and use of user accounts, user attributes, privileges, and so on that encompass the different directories, user databases, and application-specific repositories that make up the fragmented, heterogeneous enterprise IT environment. User management consists of two main tasks: maintaining an up-to-date and accurate directory of users to be provisioned and assigning users to privileges.

V

validation

The process of comparing a connected system with its representation - the target system - in the Identity store to determine any deviations. The reconciliation process consists of a validation that is followed by manual or automatic handling of the detected deviations.

W

Web access management

Access management for users and applications that attempt to access IT resources via a Web browser and/or Web protocols. See also access management.

Web Services

(W3C definition) A software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically Web Services Description Language (WSDL)). Other systems interact with the Web Service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards. DirX Identity Web Services expose important identity management functionality for SOA environments.

workflow

An IT processing activity built from successive and parallel steps. Examples include request workflows, data synchronization workflows, event-triggered workflows, scheduled workflows, and so on.

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, 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-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit 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 with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.