DirX Identity V8.7

Identity Management und Governance

Benutzer- und Zugriffsverwaltung ausgerichtet auf Geschäftsprozesse

Herausforderungen für die Benutzer- und Zugriffs-verwaltung

Heutige Geschäftsumgebungen stellen eine Herausforderung für die Benutzer- und Zugriffsverwaltung eines Unternehmens dar. Geschäftsbeziehungen werden immer komplexer, die Grenzen zwischen internen und externen Geschäftsprozessen verwischen mehr und mehr; sie werden dynamischer und erfordern größere Flexibilität und Reaktionsschnelligkeit bei Änderungen der Geschäftsstrategie und Geschäftsprozesse. Die Unternehmen müssen ihre IT-Infrastruktur einer steigenden Zahl von Benutzern zugänglich machen, sowohl innerhalb als auch außerhalb des Unternehmens, dabei höchste Produktivität und Datenschutz für diese Benutzer sicherstellen, gleichzeitig die IT-Administrationskosten in Grenzen halten und existierende Investitionen wo immer möglich wirksam nutzen. Zu diesem Zweck nutzen Unternehmen zunehmend externe Cloud-Dienste, um ihre internen IT-Dienste zu ergänzen und Themen wie Time-to-Market und Kostenbegrenzung zu adressieren. Wenn die Unternehmen den Schutz ihrer Daten und Systeme sicherstellen und gleichzeitig innovative, produktive, reaktionsschnelle, gesetzeskonforme und kosteneffektive Teilnehmer im Wirtschaftsprozess bleiben wollen, ist es für die Sicherheit des Unternehmens mehr denn je essentiell, den richtigen Personen den richtigen Zugriff auf die richtigen Ressourcen zur richtigen Zeit zu gewähren sowie die damit verbundenen Risiken zu beherrschen. Mehrere Hauptziele sind treibende Faktoren für die Governance über den Benutzer- und Zugriffs-Lebenszyklus in einem IT-Unternehmensnetzwerk:

Einhaltung von Vorschriften - Compliance. Gesicherter Benutzerzugriff auf Unternehmensinformationen hat inzwischen eine große rechtliche Bedeutung bekommen, da weltweit die Regierungen Gesetze verabschieden, mit denen die Sicherheit, Geheimhaltung und Integrität von schützenswerten Daten wie Benutzer- und Finanzinformationen sichergestellt werden soll. Nationale und internationale Gesetze für Finanzdienstleister, Organisationen des Gesundheitswesens, Pharmazie-Unternehmen und andere Branchen erfordern eine sichere Infrastruktur für die Zugriffskontrolle. Wenn die gesetzlichen Anforderungen nicht erfüllt sind, kann dies rechtliche Konsequenzen für die betroffenen Unternehmen haben, bis hin zu Gerichtsverfahren und hohen Geldstrafen. Je globaler ein Unternehmen agiert desto größer können die gesetzlichen Anforderungen sein und umso größer die Kosten von Gesetzesverletzungen. Um die Erfüllung der gesetzlichen Anforderungen belegen zu können, müssen die Unternehmen nachweisen können, „wer wann was mit welcher Information gemacht hat". Dies erfordert eine einheitliche Sicht auf die Zugriffsrechte des Benutzers für alle IT-Systeme, eine Möglichkeit, diese Zugriffsrechte kontinuierlich nachzuverfolgen – Identity-basierte Auditmöglichkeiten und regelmäßige Berechtigungsprüfung – und eine Möglichkeit, diese Informationen längerfristig zu archivieren und auszuwerten.

Die Verbreitung des eBusiness. Die Nutzung des Internet, um Inhalte und Geschäftsprozesse Mitarbeitern, Abonnenten, Kunden und Geschäftspartnern zur Verfügung zu stellen, ist heutzutage ein wesentliches Werkzeug zur Steigerung der Benutzer-Produktivität und zur Rationalisierung der geschäftlichen Zusammenarbeit. Unternehmen bieten Web Portale und Web Services an, angefangen vom personalisierten Benutzerzugriff auf Unternehmensinformationen bis hin zu B2B-Zugriff auf Supply Chain Management Prozesse. Als Folge gehen mehr und mehr IT-Applikationen und Inhalte online, und von einer immer größeren Zahl von Benutzern wird der Zugriff auf diese Applikationen und Inhalte benötigt.
Und obwohl die Nutzung von Diensten, die von Cloud-Providern angeboten werden, von der Notwendigkeit befreit, diese Dienste unternehmensseitig zur Verfügung zu stellen, entstehen neue Herausforderungen zur Kontrolle der Sicherheit, zur Handhabung der Risiken, zur Darstellung der Verantwortlichkeiten und zum Nachweis der Einhaltung der regulatorischen Anforderungen.

Bull
atos technologies

Schnelle und flexible Verwaltung von Änderungen. Die Benutzer- und Zugriffsverwaltung muss flexibel und schnell auf die dynamischen Veränderungen der Benutzerzusammensetzung und der Geschäftsprozesse reagieren, die als Folge von Firmenzusammenschlüssen und Firmenübernahmen sowie dem Einsatz von eBusiness auftreten. Um die Produktivität zu maximieren und sich gegen Sicherheitsrisiken zu schützen, müssen die Unternehmen fähig sein, möglichst schnell auf Änderungen bei den Benutzern und den Zugriffsrechten zu reagieren, die diese Benutzer zur Ausübung ihrer Tätigkeiten benötigen. Neue Benutzer sowie Benutzer, die ihre Aufgaben wechseln, müssen schnellstmöglich die von ihnen benötigten Zugriffsrechte bekommen, während ausscheidenden Benutzern die Zugriffsrechte so rasch als möglich wieder entzogen werden müssen, um Sicherheitslücken zu schließen. Die Governance hinsichtlich der Benutzer und ihrer Zugriffsrechte muss konsistent und wirksam über die sich ändernde Geschäfts- und Benutzerlandschaft bleiben.

Verbesserte Informationssicherheit. Obwohl durch eBusiness die Produktivität, Personalisierung und Zusammenarbeit gefördert wird, ist dadurch die IT-Infrastruktur auch größeren Sicherheitsbedrohungen durch böswillige Benutzer ausgesetzt. Um diesen Problemen zu begegnen, müssen die Unternehmen sowohl klare Sicherheitsmaßnahmen definieren als auch Access Governance einführen – „wer darf wann, wie und warum auf welche Informationen zugreifen". Diese Governance von Benutzerzugriffen wird idealerweise mit einem Risikomanagement-Prozess kombiniert, um passende Governance-Maßnahmen bestimmen und Aktionen zur Risikominimierung vorschlagen zu können.

Kostenkontrolle. Unternehmen müssen ihre Kosten kontrollieren oder reduzieren, wenn sie wettbewerbsfähig bleiben wollen, und sie lenken dabei ihre Aufmerksamkeit zunehmend auf die IT. Sie suchen nach Wegen, um die Anzahl der Anrufe bei den Helpdesks und Hotlines zu reduzieren, zum Beispiel für vergessene Passwörter, und sie versuchen, die administrativen Kosten, die mit der Benutzerverwaltung und dem Provisioning verbunden sind, zu reduzieren. Provisioning bezeichnet die Bereitstellung der Zugriffsmöglichkeiten auf IT-Ressourcen für die Benutzer. Die Unternehmen kürzen die Budgets für IT-Systeme, um bessere Renditen ihrer Investitionen in IT-Systeme zu erwirtschaften. Ebenso benötigen die Unternehmen auch eine größere Transparenz für ihre Wirtschaftsgüter, die sie ihren Benutzern zur Verfügung stellen, und für die damit verbundenen Kosten. Service Provider müssen die Kosten ihrer Teilnehmer nachvollziehen können, wie Speicherplatz, Mailboxgrößen, benutzte Applikationen, während Vertriebsorganisationen die Kosten von Mobiltelefonen, Laptops oder PDAs nachvollziehen müssen und diese Arbeitsmittel von den Benutzern zurückfordern müssen, wenn diese das Unternehmen verlassen.

Ein wesentliches Hindernis, diese Ziele zu erreichen, ist die eins-zu-eins Systemstruktur in einem typischen IT-Netzwerk. In der konventionellen IT-Infrastruktur, die in den meisten Unternehmen heutzutage eingesetzt wird, besteht eine eins-zu-eins Beziehung zwischen der Funktion oder Ressource, die einem Benutzer zur Verfügung steht und der IT-Applikation/dem IT-System, das diese Funktion anbietet. Damit werden die Benutzerverwaltung, die Zugriffsverwaltung, das Passwortmanagement und die Auditierung einzeln pro System ausgeführt. Die IT-Administratoren müssen die Benutzer und ihre Zugriffsrechte in jedem einzelnen IT-System des Netzwerks oder in der Cloud – üblicherweise manuell - verwalten. Die Benutzer bekommen eine Benutzerkennung (Account) und ein Passwort für jedes System, das sie benutzen müssen. Jedes IT-System hat seine eigenen Audit- und Monitor-Funktionen, um die Änderungen der Benutzer und ihrer Zugriffsrechte in dem jeweiligen System zu verfolgen.

Diese Struktur hat negative Folgen für die Benutzer- und Zugriffsverwaltung:

- Dezentralisierte Benutzerverwaltung und dezentralisiertes Provisioning haben zur Folge, dass Benutzer- und Zugriffsdaten über die IT-Systeme verteilt gehalten werden und üblicherweise mit der Zeit inkonsistent werden, so dass es schwer wird, aktuelle und richtige Informationen zu finden und Benutzer zu deprovisionieren.
- Dezentralisierte Audit- und Monitor-Funktionen machen es schwierig, Änderungen der Benutzer und ihrer Zugriffsrechte zu verfolgen. Es gibt keine Möglichkeit zu sagen, wie die Zugriffsrechte eines einzelnen Benutzers aussehen – sogar die Accountnamen eines Benutzers können in jedem IT-System unterschiedlich sein -, so dass die Auditierbarkeit für gesetzliche Anforderungen erschwert wird.
- Ein Passwort pro IT-Applikation hat zur Folge, dass sich die Benutzer viele verschiedene Passwörter merken müssen, eines für jedes System, das sie benutzen. Die große Anzahl von Passwörtern führt zu mehr Anrufen bei Helpdesks, reduzierter Produktivität, wenn Benutzer auf das Zurücksetzen der Passwörter warten, und steigenden Administrationskosten.
- Manuelle Administration ist teuer und fehleranfällig und führt zu Verzögerungen beim Provisionieren und Deprovisionieren von Benutzern, was die Produktivität senkt, die Sicherheit und Einhaltung der gesetzlichen Anforderungen gefährdet und zu Dateninkonsistenzen führt.

Um die genannten Geschäftsziele zu adressieren und die vorhandenen Einschränkungen zu überwinden, ist ein unternehmensweites, plattformübergreifendes, zentrales und automatisiertes System für die Benutzerverwaltung, das Provisioning und die Zugriffsverwaltung erforderlich, das den Zugriff auf IT-Ressourcen basierend auf Geschäftsrollen, -regeln und -prozessen steuert. Das System muss an den Geschäftsprozessen ausgerichtete Identity und Access Governance Funktionen bieten und ermöglichen, administrative Routine-Aufgaben und Entscheidungen von den Administratoren auf die Benutzer und ihre Führungskräfte zu verlagern, so dass Entscheidungen darüber, was die Benutzer wirklich benötigen, von Personen getroffen werden, die dies am besten wissen. In diesem Umfeld hat sich die Identity und Access Management (IAM) Technologie zu einem klar abgegrenzten Marktsegment entwickelt und die Tiefe und Breite erreicht, um effiziente Möglichkeiten anbieten zu können, die genannten Anforderungen zu erfüllen.

Identity und Access Management

Identity und Access Management (IAM) ist eine integrierte Lösung, die die Benutzer- und Zugriffsverwaltung über die verschiedenen Systeme der IT-Infrastruktur eines Unternehmens, einschließlich der genutzten Cloud-Lösungen, hinweg transparent macht.

Als IAM werden diejenigen Dienste, Technologien, Produkte und Standards verstanden, die die Nutzung von digitalen Identitäten ermöglichen. Identity Management adressiert den Bedarf, Benutzer und Sicherheitsrichtlinien über alle IT-Systeme zu verwalten, während Access Management die Sicherheitsrichtlinien, die für jeden einzelnen Benutzer einer IT-Infrastruktur in Kraft sind, durchsetzt. Audit-Funktionen zeichnen automatisch die Identity und Access Management Operationen auf und speichern diese Datensätze sicher.

Mit der DirX-Produktfamilie steht ein integriertes Produktangebot für Identity und Access Management Lösungen zur Verfügung, bestehend aus

- DirX Identity, einer umfassenden Identity Management und Governance Lösung
- DirX Directory, dem standardkonformen LDAP und X.500 Directory Server
- DirX Audit, das analytische Einblicke und Transparenz für die Identity und Access Management Prozesse liefert
- DirX Access, das Policy-basiertes Web Access Management, Web Single Sign-On und Federation bietet.

Die folgenden Abschnitte dieses Dokuments beschreiben die Eigenschaften, Funktionen und Komponenten von DirX Identity.

DirX Identity Funktionen

DirX Identity stellt eine umfassende, prozessgesteuerte, kundenspezifisch anpassbare, Cloud-fähige, skalierbare und hochverfügbare Identity Management Lösung für Unternehmen und Organisationen zur Verfügung. Es stellt risikobasierte Identity und Access Governance Funktionalität bereit, die nahtlos mit automatisiertem Provisioning integriert ist.

DirX Identity bietet leistungsstarke, Web-basierte Self-Service-Funktionen für Endbenutzer, delegierte Administration, Antrags-Workflows, Passwortmanagement, Benutzerverwaltung sowie plattformübergreifendes Provisioning in Echtzeit, periodische Berechtigungsprüfung und Metadirectory-Funktionalität. Das

Provisioning von Benutzern und ihrer Zugriffsrechte in verschiedenen Zielsystemen wird von einer leistungsstarken, zentralen Rollenverwaltung gesteuert, die durch flexible Policy-, Workflow- und Segregation of Duty- Engines unterstützt wird. Darüber hinaus sind umfangreiche Funktionen zur Ablaufsteuerung, zum Monitoring und für Audit-Zwecke enthalten.

Benutzerverwaltung

Die Benutzerverwaltung umfasst alle Aktivitäten, die die Erzeugung, die Konsolidierung, die Pflege und die Nutzung von Benutzer-Accounts, Benutzer-Attributen, Rollen und Berechtigungen und anderer Daten betreffen, die für die Verwaltung des Lebenszyklus von Benutzern relevant sind. DirX Identity unterstützt die Benutzerverwaltung mit vier Typen von Objekten:

- Benutzer: Ein Benutzerobjekt in DirX Identity repräsentiert den Benutzer mit seinen persönlichen Attributen, Rollen, Berechtigungen und Accounts. DirX Identity kann mehrere Accounts pro Benutzerobjekt verwalten, aber nur einen Account pro Zielsystem.
- User-Facet: User-Facets bieten die Möglichkeit, mehrere Rechte-Profile für einen Benutzer zu modellieren, eines für jede Position, die ein Benutzer in einer Organisation innehat; zum Beispiel ein Student, der sowohl als wissenschaftlicher Mitarbeiter als auch als Tutor arbeitet. User-Facets haben dieselben Accounts wie der Benutzer. Mittels User-Facets kann man festlegen und herausfinden, welche Rechte einem Benutzer aufgrund welcher Position zugewiesen wurden.
- Persona: Benutzer können auch in verschiedenen Funktionen in einem Unternehmen arbeiten, zum Beispiel als Administrator oder als Projektmanager. Die Accounts und die Berechtigungen für jede dieser Funktionen eines Benutzers können recht unterschiedlich sein; typischerweise ist mehr als ein Account pro Zielsystem erforderlich und auch das Audit muss zwischen den unterschiedlichen Funktionen unterscheiden können. Zu diesem Zweck sind Persona-Objekte geeignet.
- Funktionsbenutzer: Ein Funktionsbenutzerobjekt repräsentiert eine Ressource, die einem Benutzer (Sponsor) zugewiesen ist. Beispiele sind globale oder Gruppenmailboxen, ein Raum mit einem Telefon oder ein Eintrag für einen Werkstudenten. Eine derartige Ressource wird von dem Benutzer verwaltet.

Die Benutzerverwaltung umfasst zwei Hauptaufgaben: die Pflege eines konsistenten und aktuellen Benutzerverzeichnisses und das Zuweisen von Rollen an Benutzer. Die Pflege eines konsistenten Benutzerverzeichnisses wird von den Benutzern selbst und/oder von ihren Managern gesteuert (über den Benutzer-Self-Service oder die delegierte Administration) und/oder über Datensynchronisations-Workflows (zum Beispiel mit dem HR-System des Unternehmens) über die Metadirectory-Funktionalität.

Die Aufgaben der Benutzerverwaltung in DirX Identity umfassen:

- das Hinzufügen von Benutzern, das Ändern von Benutzerattributen und das Löschen von Benutzern im Identity Store über das DirX Identity Web Center oder den DirX Identity Manager
- das Erzeugen und regelmäßige Synchronisieren von Benutzern aus verschiedenen Quellen wie HR, CRM oder ERP Systemen oder einem existierenden Corporate Directory Master

DirX Identity ermöglicht die Verwaltung von Gültigkeitsdaten für die Benutzer, um die Personalmanagementprozesse eines Unternehmens widerzuspiegeln:

- Startdatum, zu dem ein Benutzer aktiv wird, zum Beispiel das Anfangsdatum eines neuen Mitarbeiters
- Enddatum, zu dem einem Benutzer seine Zugriffsrechte entzogen werden sollen, zum Beispiel das Vertragsende eines externen Vertragspartners
- das Start- und Enddatum einer längeren Abwesenheit, zum Beispiel bei einem Erziehungsurlaub

Personas und Funktionsbenutzer

Die Lebensdauer eines Benutzerobjekts umfasst die Lebensdauer aller zugehörigen Persona-Objekte. Die Lebensdauer eines Persona-Objekts kann kürzer als die Lebensdauer des Benutzers sein. Personas bieten somit eine Möglichkeit, unterschiedliche Verantwortungsbereiche eines Benutzers zu modellieren, der für verschiedene Organisationseinheiten in einem Unternehmen arbeitet.

In Gegensatz zu einem Funktionsbenutzer ändern die Persona-Objekte ihren Status mit dem entsprechenden Benutzerobjekt. Eine Zuweisung zu einem anderen Benutzer macht keinen Sinn.

Im Gegensatz zu einer Persona kann ein Funktionsbenutzer den Sponsor überdauern und muss einem anderen Sponsor (Benutzer) zugewiesen werden, wenn der ursprüngliche Sponsor gelöscht wird oder nicht mehr für den Funktionsbenutzer zuständig ist.

Die Aufgaben der Persona-Verwaltung in DirX Identity umfassen:

- das Hinzufügen und Löschen von Personas, das Ändern von Persona-Attributen, speziell von Attributen, die sich auf die Lebensdauer von Personas oder auf Zeiträume ihrer Deaktivierung beziehen
- das Synchronisieren von DirX Identity Personas mit einem Corporate Directory Master. Dies macht Sinn, wenn das Konzept unterschiedlicher Benutzer-Repräsentationen auch vom Corporate Directory unterstützt wird. Andernfalls werden nur die Daten der Benutzerobjekte synchronisiert und die Persona-Daten werden in DirX Identity verwaltet.
- das Zuweisen von Rollen zu Personas. Dies geschieht auf die gleiche Art und Weise wie für Benutzer.

Hinweis: Viele der vorgehend beschriebenen Aufgaben treffen in analoger Weise auch auf die User-Facets zu.

Die Aufgaben der Verwaltung der Funktionsbenutzer in DirX Identity umfassen:

- das Hinzufügen und Löschen von Funktionsbenutzern und das Ändern ihrer Attribute
- das Verwalten des Sponsors, wenn der für den Funktionsbenutzer zuständige Benutzer wechselt
- das Zuweisen von Rollen zu Funktionsbenutzern. Diese Zuweisung erfolgt auf die gleiche Art und Weise wie für normale Benutzer.

Benutzer-Self-Service

Dirx Identity stellt über seine Web Center Benutzerschnittstelle eine Reihe von Funktionen für den Self-Service der Benutzer zur Verfügung. Dazu gehören:

- Anmeldung für Services, die für die Selbstregistrierung über das Intranet oder das Extranet im Unternehmen zur Verfügung stehen
- Änderung eigener Daten inklusive Änderung eigener Passwörter
- Zurücksetzen vergessener Passwörter mittels Challenge-Response-Verfahren

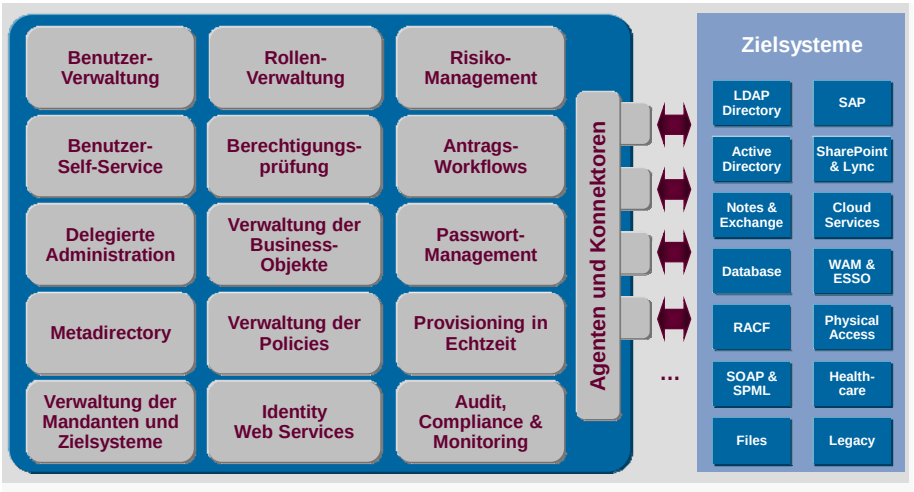


Abb. 1 - DirX Identity Funktionalität

- Beantragung von Rollen für sich selbst
- Überprüfen des Status eigener Anträge und Genehmigungen
- Delegation von Zugriffsrechten oder Teilen davon für die Benutzer- und Rollenverwaltung an andere Benutzer

Access Policies werden benutzt, um sicherzustellen, dass ein Benutzer nur für seine eigenen Aufgaben Zugriffsrechte hat.

Delegierte Administration

Der administrative Zugriff auf DirX Identity Daten wird über Zugriffsrechte und persönliche Delegation kontrolliert. Durch die Konfiguration von Access Policies gewähren die Administratoren Zugriffsrechte auf DirX Identity Daten wie Benutzer, Business Objekte, Rollen, Zielsystem-Accounts, Gruppen, Policies und Workflows. Beispielsweise kann eine Access Policy spezifizieren, dass Projektleiter die Benutzerdaten ihrer Projektmitarbeiter bearbeiten können und diesen projektspezifische Rollen zuweisen können. Andere Access Policies können die Zuständigkeit für die Genehmigung von Benutzern und Rollen festlegen.

Diese Benutzer können diese Zugriffsrechte oder einer Untermenge davon an jemand anderen delegieren, optional auch für einen festgelegten Zeitraum. Dies betrifft speziell die Rechte, Benutzer und Rollen zu verwalten, Rollen an Benutzer zuzuweisen oder Anträge für derartige Zuweisungen von Benutzern zu genehmigen. Zum Beispiel kann ein Projektleiter, der zwei Wochen abwesend ist, die Zugriffsrechte, die ihm erlauben, projektbezogene Rollen an die Mitglieder seines Teams zu vergeben, an eine andere Person seines Teams übertragen. Optional kann eine Auswahl der Rollen, die für die delegierte Administration durch einen Stellvertreter freigeschaltet wird, vom Projektleiter spezifiziert werden.

Die Aufgaben der delegierten Administration innerhalb des DirX Identity Web Center umfassen:

- Anlegen neuer Benutzer, Rollen, Gruppen, Business-Objekte und Policies
- Ändern von Daten von Benutzern, Rollen, Business-Objekten und Policies
- Zuweisung von Rollen an existierende Benutzer
- Genehmigung der Zuweisung von Rollen oder Business-Objekten an Benutzer oder des Anlegens von Benutzern, Rollen und Business-Objekten
- Regelmäßige Überprüfung und Bestätigung der Rollenzuweisungen
- Löschen existierender Benutzer, Rollen, Gruppen, Business-Objekte und Policies
- Erzeugen von Status-Reports

Access Policies werden benutzt, um zu steuern, welche dieser administrativen Aufgaben ein bestimmter Administrator ausführen darf und für welche Benutzer und für welche anderen Daten er sie ausführen darf.

Passwort-Management

DirX Identity stellt eine umfassende Passwortmanagement-Lösung für Unternehmen und Organisationen zur Verfügung. Dadurch, dass Endbenutzer ihre Passwörter schnell und flexibel basierend auf starken Passwortrichtlinien zurücksetzen oder ihren Account entsperren können, hilft das DirX Identity Passwortmanagement Organisationen dabei, ihre Help-Desk-Kosten signifikant zu reduzieren und die Sicherheit bei der Authentifizierung mittels Passwörtern zu stärken.

DirX Identity Passwortmanagement bietet folgende Funktionalitäten:

- Self-Service Passwort Reset: die Benutzer setzen vergessene Passwörter selbst zurück oder entsperren ihre Accounts. Dabei nutzen sie verschiedene Alternativen zur Authentifizierung.
- Unterstütztes Zurücksetzen von Passwörtern: Administratoren oder Service-Desk-Mitarbeiter setzen für die Benutzer Passwörter zurück oder entsperren deren Accounts.
- Abgelaufene Passwörter: Benutzer werden darauf hingewiesen, ihre Passwörter zu ändern, bevor sie ablaufen.
- Erstmalige Registrierung von Benutzern: Die Benutzer wählen Sicherheitsfragen und zugehörige Antworten, die alternativ als Zugangsdaten genutzt werden können, was auch unter dem Begriff Challenge-Response-Verfahren bekannt ist.
- Passwort Listener für Windows: Dieser erkennt die Passwortänderungen, die vom Benutzer am Windows Desktop durchgeführt werden.
- Passwort-Synchronisation: Synchronisiert geänderte Passwörter in Real-Time zu angeschlossenen Zielsystemen.
- Passwortrichtlinien-Management: Verwaltet Regeln zur Komplexität, Ablauf und Historie von Passwörtern und setzt diese Regeln durch.
- Passwortmanagement für privilegierte Accounts: Verwaltet und steuert den Zugriff auf Passwörter für gemeinsam genutzte, privilegierte Accounts.
- Audit und Reports: Führt Aufzeichnungen und erzeugt Reports zu Passwort-bezogenen Aktionen.

Eine detaillierte Beschreibung der Passwortmanagementfunktionen von DirX Identity sowie der daraus resultierenden Vorteile findet sich im separaten Datenblatt DirX Identity - Sicheres und flexibles Passwortmanagement.

Rollenverwaltung

Das Ziel der Rollenverwaltung ist es, eine logische Schicht für die Modellierung und Verwaltung von Zugriffskontroll-Informationen einzuführen, die generisch genug ist, um möglichst viele der Autorisierungs- und Zugriffskontrollmethoden der relevanten IT-Systeme abzudecken:

- Gruppen-basierte IT-Systeme steuern die Zugriffsrechte mittels der Gruppenzugehörigkeiten der Accounts. Wenn ein Account ein Mitglied einer Gruppe wird, hat er die Zugriffsrechte, die dieser Gruppe gewährt wurden. Benutzergruppen, Profile und anwendungsspezifische Rollen sind Beispiele von Gruppen-basierten Methoden der Zugriffskontrolle.
- Attribut-basierte IT-Systeme steuern die Zugriffsrechte mittels Attributen innerhalb der Accounts. Beispielsweise definiert in Microsoft Active Directory ein Satz von Attributen eine Benutzer-Mailbox in Microsoft Exchange.
- Einige Systeme, zum Beispiel Microsoft Active Directory, stellen beide Arten der Zugriffskontrolle zur Verfügung.

DirX Identity nutzt ein standardbasiertes Rollenverwaltungsmodell, das Parametrisierung unterstützt, um unterschiedliche Zugriffsrechte abhängig von Kontextinformationen zu gewähren. DirX Identity unterstützt Antrags-Workflows mit Genehmigungsschritten und regelmäßige Berechtigungsprüfungen zur Autorisierung und Re-Autorisierung von Rollenzuweisungen und setzt die Regeln für Funktionstrennungen (Segregation of Duties, SoD) durch, um gesetzlichen Anforderungen oder Unternehmensrichtlinien zu genügen.

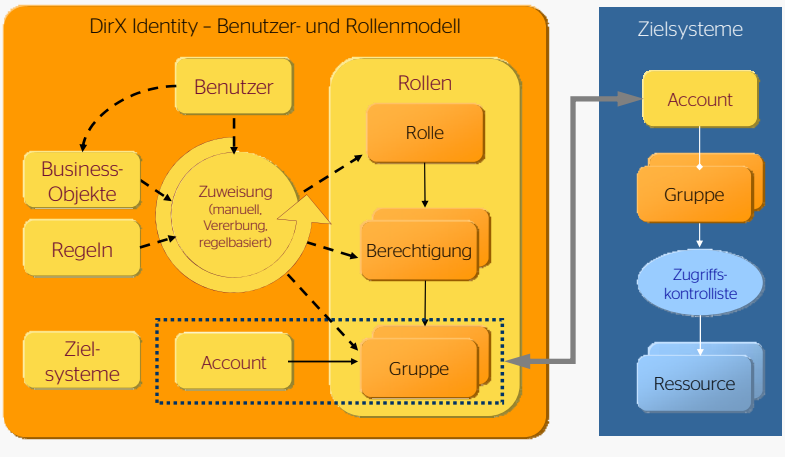


Abb. 2 - DirX Identity Benutzer- und Rollenmodell

Das Rollenmodell in DirX Identity basiert auf dem RBAC-Standard ANSI/INCITS 359. Das ANSI RBAC Referenzmodell organisiert die RBAC-Elemente in vier Gruppen mit jeweils erweiterter Funktionalität: Core RBAC, hierarchisches RBAC, statische Funktionstrennungen (SSD) und dynamische Funktionstrennung (DSD).

DirX Identity unterstützt Level 3 RBAC, also hierarchisches RBAC mit statischer Funktionstrennung. Während ANSI RBAC auch Systemressourcen in seinem Zugriffkontrollmodell einschließt, überlässt DirX Identity die Verwaltung der individuellen Ressourcen der jeweiligen lokalen Administration des Zielsystems.

Abbildung 2 stellt die Beziehungen zwischen dem Rollenmodell in DirX Identity und den Zugriffskontrollsystemen der IT-Systeme dar:

- Ein **Benutzer** repräsentiert eine Person innerhalb oder außerhalb des Unternehmens, dem Rollen zugewiesen werden.
- Ein **Zielsystem** repräsentiert ein IT-System, das Benutzer authentifiziert und autorisiert. Beispiele von Zielsystemen sind Betriebssysteme, Messaging Systeme, ERP-Applikationen, Web-Portale und eBusiness-Anwendungen sowie Groupware Applikationen und Mainframe Security Systeme.
- Im jeweiligen Zielsystem wird ein Benutzer durch eine **Benutzerkennung (Account)** repräsentiert, wobei jeder Benutzer Accounts in mehreren Zielsystemen haben kann. Zusätzlich kann DirX Identity privilegierte Accounts verwalten, die temporär Benutzern zugewiesen werden können.
- Eine **Gruppe** repräsentiert einen Satz von Zugriffsrechten in einem spezifischen Zielsystem. Gruppen stellen die Beziehung zwischen dem Rollen/Berechtigungs-Zugriffsmodell und dem Zugriffskontrollmodell der Zielsysteme her. Eine Gruppe kann direkt einem Benutzer zugewiesen werden oder indirekt durch Berechtigungen (Permissions) und Rollen, die diese Gruppe einschließen.
- Eine **Berechtigung (Permission)** repräsentiert einen Satz von Zugriffsrechten, die Zielsystem-neutral sind. Eine Berechtigung kann direkt einem Benutzer zugewiesen werden oder indirekt durch Rollen, die diese Berechtigung einschließen. Eine Berechtigung vereinigt Gruppen eines oder mehrerer Zielsysteme.
- **Rollen** steuern die Zugriffsrechte von Benutzern zu IT-Systemen und Ressourcen. Rollen werden Benutzern entweder manuell (mittels Benutzer-Self-Service oder Administratoren) oder automatisch (über Provisioning-Policies oder Vererbung von Business-Objekten) zugewiesen. DirX Identity unterstützt generelle Rollenhierarchien, wie in NIST RBAC definiert – Rollen können einfachere Rollen beinhalten. Folglich vereinigen Rollen eine Sammlung von Rollen, eine Sammlung von Berechtigungen oder beides.

Wenn einem Benutzer eine Rolle zugewiesen wird, provisioniert DirX Identity die Zielsysteme, für die die Rolle zutrifft, mit den Authentifizierungsdaten – den Accounts - und den Autorisierungsdaten – den Account-Gruppen-Beziehungen - , die diese Rolle repräsentieren. Dieser Prozess wird als „Rollenauflösung" bezeichnet und wird weiter unten im Abschnitt über "Provisioning" beschrieben.

Das Rollenmodell von DirX Identity kann die Zugriffskontrolle für all diejenigen IT-Systeme verwalten, die eine Gruppen-basierte oder Attribut-basierte Verwaltung der Zugriffsrechte erlauben. DirX Identity kann auch Rollen verwalten, die nicht direkt mit einem IT-System verknüpft sind. Die zugehörigen Gruppen, so genannte virtuelle Listen, dienen zur Unterstützung verschiedener Geschäftsprozesse, zum Beispiel Listen von Zutrittsberechtigten für Gebäude, die zur manuellen Prüfung benötigt werden.

Das Rollenmodell von DirX Identity unterstützt **parametrisiertes RBAC**, bei dem die Zugriffsrechte, die von einer generischen Rolle oder Berechtigung modelliert werden, bei der Zuweisung zu einem spezifischen Benutzer basierend auf Kontextinformationen wie zum Beispiel den Werten von Rollen- oder Berechtigungsparametern angepasst werden. Ein **Rollenparameter** ist eine Variable, deren Wert zum Zuweisungszeitpunkt zur Verfügung gestellt wird. Zum Beispiel kann der Benutzer die Rolle "Projektmitglied" für mehrere verschiedene Projekte haben. Ein generische Rolle „Projektmitglied" kann mehrfach einem Benutzer zugewiesen werden; für jedes einzelne Projekt wird der spezifische Projektname als Rollenparameter mitgegeben, wenn die Rolle einem Benutzer zugewiesen wird.

Ein **Berechtigungsparameter** ist ein Attribut in einem Benutzereintrag, dessen Wert die Berechtigungsauflösung in Gruppen beeinflusst. Zum Beispiel angenommen, ein Mitarbeiter der Vertriebsabteilung hat die Berechtigung "Abteilungs-File-Server". Dies ist eine generische, unternehmensweite Berechtigung, die mit dem Benutzerattribut „Abteilung" parametrisiert ist. DirX Identity kann den Wert „Vertrieb" aus dem Benutzerattribut „Abteilung" dazu nutzen, die Berechtigung in bestimmte Zielsysteme und Gruppen aufzulösen, die dem Benutzer Zugriffsrechte zu dem Abteilungs-File-Server der Vertriebsabteilung dieses Benutzers zu gewähren. Die Berechtigung "Abteilungs-File-Server" ist für alle Mitarbeiter einer Organisation gleich, die Auflösung in ein spezielles Zielsystem hängt jedoch von der aktuellen Abteilung des Mitarbeiters ab.

Rollen- und Berechtigungsparameter führen zu einer starken Reduzierung der Anzahl der Berechtigungen und Rollen, die definiert werden müssen, und machen die Rollenverwaltung, die auf Geschäftsrollen basiert, einfacher handhabbar (Rollen-basierte Zuweisung).

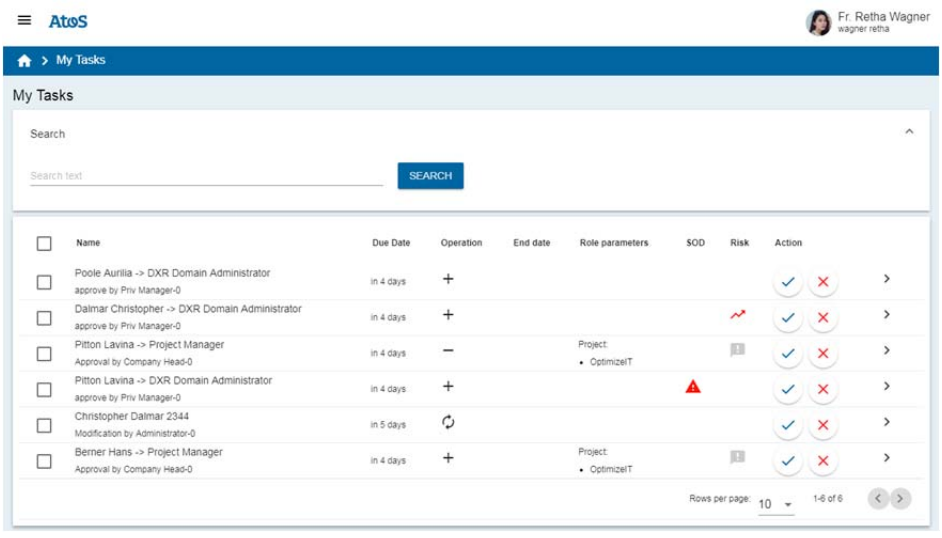
Die Rollen-basierte Zuweisung ermöglicht dem Unternehmen, die Zugriffsrechte zu Ressourcen nach wohldefinierten Geschäftsrollen, die aus dem Geschäftsmodell abgeleitet werden, und nach Benutzern zu strukturieren. Das Rollen-basierte Provisioning-Modell ist besonders geeignet, wenn die Zugriffsrechte relativ statisch sind, wenn sie zum Beispiel von der Tätigkeit der Person abhängen. In diesem Fall ändern sich die Privilegien nicht unbedingt, wenn sich organisatorische Attribute ändern. Rollen- und Berechtigungsparameter können eingesetzt werden, um das Rollen-basierte Provisioning dynamischer anzuwenden.

Verwaltung von Business-Objekten

Ein Business-Objekt ist eine Sammlung von Daten zu einer Geschäftsstruktur in einem Unternehmen, wie Organisationseinheit, Kostenstelle oder ein Projekt. Kundenspezifische Objekte können einfach hinzugefügt werden. Business-Objekte in einem Identity Management System dienen zur automatischen Rollenzuweisung und der Reduzierung von redundanten Identity-Daten.

In DirX Identity werden Business-Objekte genutzt,

- um Organisations- oder Projektstrukturen abzubilden,



DirX Identity Business User Interface Beispiel – Genehmigung von Rollenzuweisungen

- um Daten konsistent bereitzustellen; zum Beispiel wird der Unternehmensstandort mit all seinen Adressen nur einmal definiert und diese Information automatisch mit allen relevanten Benutzerinformationen verlinkt. Dies dient zur Reduzierung von redundanten Daten in der Identity-Datenhaltung, da gemeinsame Benutzerdaten nur an einer Stelle verwaltet werden.
- um automatisch Rollen an Benutzer zuzuweisen. Die Benutzer, die mit den Business-Objekten verbunden sind, erhalten die Rollen, die mit den Business-Objekten verbunden sind (siehe Abbildung 2).
  Beispielsweise können Rollen einer Organisationseinheit zugewiesen werden. Wenn dann ein Benutzer dieser Organisationseinheit zugewiesen wird, erbt er automatisch die entsprechenden Rollen. Wenn er die Einheit wieder verlässt, verliert er die entsprechenden Rollen wieder. Änderungen der Informationen in den Business-Objekten – inklusive der Referenzen zu Rollen – werden automatisch an diejenigen Benutzer weitergegeben, die mit den Business-Objekten verbunden sind.
- um Parameterstrukturen für zugehörigen Drop-Down-Listen oder Rollenparameter zu definieren.

Die Verwaltungsaufgaben für Business-Objekte in DirX Identity beinhalten:

- das Hinzufügen von Business-Objekten zu einer hierarchischen Struktur, das Ändern von Attributen von Business-Objekten und das Löschen von Business-Objekten in der Identity Datenhaltung mittels DirX Identity Manager oder Web Center
- das Zuweisen/Verbinden von Benutzern zu entsprechenden Business-Objekten
- das Zuweisen von Rollen (oder Berechtigungen oder Gruppen) zu Business-Objekten, so dass Benutzer, die mit den Business-Objekten verbunden sind, diese Rollen automatisch erben
- das Erzeugen und regelmäßige Synchronisieren von Business-Objekten aus verschiedenen Quellen wie zum Beispiel HR-, CRM- oder ERP-Systemen oder aus einem existierenden Corporate Directory Master
- das Definieren von Vorschlagslisten auf Basis von Business-Objekten

Verwaltung privilegierter Accounts

In Ergänzung zu Accounts, die genau einem festgelegten Benutzer zugeordnet sind, wird in Zielsystemen typischerweise eine kleine Anzahl von privilegierten Accounts verwaltet, die für die Verwaltung der Zielsysteme berechtigt sind. Solche Accounts, zum Beispiel der Root-Account in Unix-Systemen können in den Zielsystemen kritische Aktionen mit hohen Sicherheitsrisiken durchführen. Privilegierte Accounts sind nicht mit einem spezifischen Benutzer verbunden. Eine Reihe von Personen kann sie parallel benutzen.

DirX Identity stellt Mittel zur Verfügung, um privilegierte Accounts zu kontrollieren und auditieren:

- Jedem Benutzer kann durch Zuweisung einer entsprechenden Rolle ein privilegierter Account zugewiesen werden, wobei alle Funktionen der Rollenverwaltung inklusive Antrags-Workflows, regelmäßige Berechtigungsprüfung und Segregation of Duties zur Verfügung stehen.
- Benutzer, denen ein privilegierter Account zugewiesen wurde, können das Passwort in Klartext lesen, um das Login durchführen zu können.
- Sie haben die Berechtigung, das Passwort privilegierter Accounts zu löschen.
- Wird einem Benutzer ein privilegierter Account entzogen, wird automatisch das Passwort geändert.
- Alternativ kann festgelegt werden, dass bei der Zuweisung eines Benutzers zu einem privilegierten Account die Zertifikate des Benutzers zum Account kopiert werden. Dies ermöglicht im Zielsystem die Authentifizierung mittels Zertifikat.
- DirX Identity ändert automatisch die abgelaufenen Passwörter privilegierter Accounts.

Funktionstrennungen / Segregation of Duties

In einem rollenbasierten System können Interessenskonflikte entstehen, wenn einem Benutzer Zugriffsrechte aus Rollen zugewiesen werden sollen, die miteinander in Konflikt stehen. Mit der ANSI RBAC Komponente SSD werden diese Interessenkonflikte vermieden, indem Beschränkungen bei der Rollenzuweisung durchgesetzt werden. DirX Identity unterstützt dieses Modell von Funktionstrennungen, auch **Segregation of Duties** oder Separation of Duties (SoD) genannt. Mit entsprechenden SoD-Regeln wird festgelegt, welche Benutzer-Rollen-Zuweisungen Interessenskonflikte erzeugen oder nicht akzeptierbare Sicherheitsrisiken bilden können. DirX Identity setzt diese Regeln bei der Benutzer-Rollen-Zuweisung durch und lässt bei erkannten Verletzungen eine Rollenzuweisung nur zu, falls eine entsprechende Sondergenehmigung eingeholt wird. SoD-Regeln können auch für Benutzer-Permission- und Benutzer-Gruppen-Zuweisungen definiert werden.

Alternativ oder zusätzlich ermöglicht DirX Identity die Anbindung von anderen GRC-Systemen wie zum Beispiel SAP BusinessObjects GRC (Access Control) zur externen SoD-Prüfung.

Policy Management

Eine **Policy** ist eine übergeordnete Regel, die intern benutzt wird, um die Entscheidungen des DirX Identity Systems zu steuern.

DirX Identity unterstützt das Anlegen von **Sicherheits-Policies** und **administrativen Policies** zur Steuerung seiner Abläufe. Sicherheits-Policies steuern den Zugriff auf Ressourcen, während administrative Policies die Integrität der DirX Identity Daten für Benutzer, Rollen und Zielsysteme verwalten.

Zu den DirX Identity Policies gehören:

- **Access Policies** zur Steuerung des Zugriffs für den Self-Service und die delegierte Administration auf die DirX Identity Daten. Eine Access Policy definiert einen Satz von Zugriffsrechten auf DirX Identity Daten wie beispielsweise Benutzer, Business-Objekte oder Rollen. Zum Beispiel kann eine Access Policy festlegen, dass ein Projektleiter Benutzerdaten bearbeiten darf und projektspezifische Rollen an die Mitglieder seines Projektteams vergeben darf. Mittels der Access Policies kann das Unternehmen seine Administrationsaufgaben gemäß seinem Geschäftsmodell oder seiner Organisation strukturieren und die Operationen auf den DirX Identity Benutzer- und Rollendaten, die ein bestimmter Benutzer ausführen darf, einschränken. Ebenso kann die Sichtbarkeit der zugewiesenen Berechtigungen eingeschränkt werden. Access Policies werden auch genutzt, um zu steuern, welche Menüeinträge im DirX Identity Web Center für Benutzer sichtbar und nutzbar sind.
- **Audit Policies** um festzulegen, welche Attributänderungen welcher Objekte in Bezug auf unternehmensinterne Sicherheitsrichtlinien und gesetzliche Regelungen Compliance-relevant sind und daher aufgezeichnet werden müssen.
- **Passwort Policies** zur Steuerung der Anforderungen von DirX Identity an Benutzerpasswörter: Komplexität, Gültigkeitsdauer, Verhalten nach fehlgeschlagenen Login-Versuchen, etc.
- **Provisioning Policies**, um Rollen automatisch, basierend auf den Werten von Benutzerattributen, zu gewähren und zu entziehen. Diese wiederum steuern die Zugriffsrechte für die Zielsysteme. Provisioning Policies werden über Provisioning Regeln definiert. Zum Beispiel kann eine Provisioning Regel festlegen, dass eine bestimmte Anwendung nur von Mitarbeitern der Vertriebsabteilung genutzt werden darf. Der Wert des Benutzerattributs „Abteilung“ wird mit der Regel ausgewertet und denjenigen Mitarbeitern, für die der Wert von „Abteilung“ gleich „Vertrieb“ ist, wird die Rolle zur Nutzung der Vertriebsanwendung gewährt. Sobald der Wert des Benutzerattributs nicht mehr den Bedingungen der Regel genügt, in diesem Fall „Vertrieb“, wird dem Benutzer die Rolle automatisch entzogen und der Benutzer wird deprovisioniert.
- **Attribut-Policies**, um Änderungen kritischer Attribute zu verfolgen und ggfs. automatisch Antrags-Workflows zur Genehmigung zu

starten.

- **SoD Policies** spezifizieren, welche Kombination von Rollen, Berechtigungen und Gruppen einem Benutzer nicht gleichzeitig ohne spezielle Genehmigung zugewiesen sein dürfen.
- **Validation Policies** vergleichen Daten der Zielsysteme mit den in DirX Identity gespeicherten Daten, um Abweichungen zwischen den Accounts, Gruppen und Account-Gruppen-Beziehungen in den Zielsystemen und der zugehörigen Information in DirX Identity zu erkennen und die Werte abzugleichen. Diese Policies werden mittels Validierungsregeln definiert.
- **Konsistenz Policies** zur Überprüfung der Konsistenz von Benutzer- und Rollendaten innerhalb DirX Identity und zur Reparatur von Inkonsistenzen, um zum Beispiel Account- und Benutzerdaten konsistent zu halten. Diese Policies werden mittels Konsistenzregeln definiert.

Die DirX Identity Policy Engine verarbeitet die administrativen Policies entweder dynamisch oder periodisch (abhängig von der Art der Policy), während der DirX Identity Security Manager die Security Policies dynamisch verarbeitet.

Antrags-Workflows

DirX Identity stellt verschiedene Typen von Workflows zur Verfügung, die die Aktivitäten beim Self-Service und der delegierten Administration unterstützen:

- Antrags-Workflows zur Erzeugung neuer Identity Management Daten (Creation Workflows), wie Benutzer, Rollen, Berechtigungen, Regeln, inklusive der Erzeugung globaler Ids bei Workflows zum Anlegen neuer Benutzer
- Antrags-Workflows zum Ändern existierender Daten (Änderungs-Workflows); Beispiele sind Attribute von Benutzern, Rollen oder Business-Objekten. Attribut-Policies legen fest, welche Attributänderungen genehmigt werden müssen und welche Workflows für welches Attribut gestartet werden müssen.
- Antrags-Workflows zum Erzeugen und Pflegen von Zuweisungen von Identity Management Daten (Zuweisungs-Workflows), zum Beispiel das Zuweisen einer Rolle zu einem Benutzer oder das Zuweisen einer Rolle zu einer anderen Rolle (Rollenhierarchien).
- Antrags-Workflows zum Löschen von Identity Management Daten (Lösch-Workflows), wie Benutzer, Rollen, Berechtigungen, Policies, etc.

DirX Identity ermöglicht den Antragstellern und den genehmigenden Personen das digitale Signieren ihrer Anträge bzw. Genehmigungen.

DirX Identity stellt Vorlagen für Antrags-Workflows bereit, die von den Kunden mittels des grafischen Workflow-Editors gemäß ihren Anforderungen angepasst werden können.

Die Verwaltung von Antrags-Workflows wird durch Access-Policies geschützt und umfasst sowohl Start-, Stop-, Unterbrechungs- und Fortsetzungsoperationen als auch Teilnehmeränderungen.

Genehmigungen

Antrags-Workflows können optional Genehmigungsschritte erfordern, um die Genehmigung für den Antrag zu erteilen.

Beispielsweise kann eine Rollenzuweisung eine Erstgenehmigung voraussetzen sowie eine Wiedergenehmigung nach einer festgelegten Zeitperiode (zum Beispiel nach 6 Monaten) oder zu einem bestimmten Zeitpunkt. Um die automatische Durchführung dieser Prozesse zu unterstützen, können entsprechende Workflows zur Genehmigung und Wiedergenehmigung definiert werden. Für den Genehmigungsprozess werden eine Reihe von Modellen zur Ermittlung der beteiligten Personen unterstützt, wie einzelne genehmigende Personen, statische und dynamische Gruppen von genehmigenden Personen und regelbasierte Ermittlung von genehmigenden Personen. Falls diese Standardmethoden nicht ausreichen, können beliebige Algorithmen über Java-Erweiterungen definiert werden.

Benutzer beantragen eine Genehmigung für eine Rolle über die Web Center Benutzerschnittstelle oder das Business User Interface. Der Workflow benachrichtigt dann jede Person in dem Genehmigungspfad, zum Beispiel mittels E-Mail, dass ein Antrag zur Genehmigung vorliegt. Die genehmigende Person nutzt dann entweder ebenfalls die Web Center Benutzerschnittstelle, das Business User Interface oder alternativ die Approval App, um den Antrag zu genehmigen oder abzulehnen. Eskalationsmechanismen unterstützen bei Problemen wie Zeitüberschreitungen, etc. Zusätzlich zu einzelnen Genehmigern kann einem Genehmigungsschritt auch eine Gruppe von Genehmigern zugeordnet werden, zum Beispiel Mitarbeiter eines Helpdesks. In diesem Fall wird die Genehmigung von demjenigen Mitarbeiter durchgeführt, der als erster den Genehmigungsschritt bearbeitet.

Risikomanagement

DirX Identity stellt eine Risikobewertung für Identitäten basierend auf einem erweiterbaren Satz von Risikofaktoren zur Verfügung.

Um die Benutzer in Risikoklassen einzuordnen, wie zum Beispiel risikoreiche und risikoarme Benutzer, werden regelmäßig Risikofaktoren berechnet und gemäß einer kundenspezifisch anpassbaren Konfiguration zu einem Gesamtrisiko zusammengefasst. Beispiele für Risikofaktoren sind: Verletzungen von Funktionstrennungen, importierte Accounts und Gruppenmitgliedschaften oder die Gesamtanzahl von Gruppenmitgliedschaften oder privilegierter Accounts eines Benutzers.
Für jeden Benutzer kann Web Center dessen Risikoklasse anzeigen. Zusätzlich zeigt DirX Identity Manager die individuellen Risikofaktoren an. Compliance Manager, Vorgesetzte oder Administratoren können die Risikowerte überwachen und Aktionen zur Reduzierung der Anzahl der mit hohem Risiko bewerteten Benutzer planen, beispielsweise die Durchführung von Kampagnen zur Berechtigungsprüfung oder zusätzliche Genehmigungsschritte.

Für jeden Antrag zur Zuweisung von Benutzerprivilegien kann DirX Identity das Gesamtrisiko vor und nach der Änderung vergleichen. Falls die Risikoklasse durch die beantragte Zuweisung erhöht wird, können zusätzliche Genehmigungsschritte erforderlich werden.

Periodische Berechtigungsprüfung

Periodische Berechtigungsprüfung, die auch als Access Certification bezeichnet wird, ermöglicht die Bestätigung, dass Benutzern Zugriffsrechte in Übereinstimmung mit internen Sicherheitsrichtlinien und gesetzlichen Bestimmungen zugewiesen sind. Zur Unterstützung derartiger Compliance-Prozesse bietet DirX Identity Kampagnen zur Berechtigungsprüfung sowohl für Benutzer als auch für Privilegien, zum Beispiel für Rollen oder Gruppen:

- Eine Kampagne zur Berechtigungsprüfung führt die Access Certification für eine auswählbare Untermenge von Benutzern oder Privilegien durch, zum Beispiel für alle Benutzer der Personalabteilung oder für alle kritischen Privilegien. Für jeden Benutzer oder jedes Privileg können ein oder mehrere Genehmiger automatisch festgelegt werden, z.B. Vorgesetzte oder Rollenverantwortliche. Für jeden zu prüfenden Benutzer oder jedes zu prüfende Privileg können die Genehmiger alle Zuweisungen sehen und für jede einzelne Zuweisung entscheiden, ob sie diese akzeptieren oder ablehnen. Optional werden Privilegien, die manuell zugewiesen und in einer Kampagne abgelehnt wurden, automatisch entzogen und die betroffenen Benutzer werden benachrichtigt. DirX Identity unterstützt sowohl einmalige als auch periodische Kampagnen zur Berechtigungsprüfung. Die Phasen der Kampagnen werden mittels Startdatum, Fälligkeitsdatum, Enddatum und Ablaufdatum gesteuert. Wenn sich ein Auftrag zur Berechtigungsprüfung seinem Fälligkeitsdatum nähert, werden Erinnerungsnachrichten an die Genehmiger gesendet.
- DirX Identity unterstützt auch die Access Certification einer individuellen Zuweisung eines Privilegs mittels erneuter Genehmigung (Re-Approval). In diesem Fall ist die Genehmigung für ausgewählte und kritische Privilegzuweisungen nach einem festgelegten Zeitintervall zu wiederholen. Für die erneute Genehmigung kann entweder derjenige Workflow genutzt werden, der schon zur erstmaligen Genehmigung genutzt wurde, oder ein spezieller Workflow. Wenn der Genehmiger die Zuweisung eines Privilegs ablehnt, wird dem Benutzer das Privileg sofort entzogen. Diese Methode arbeitet individuell pro Zuweisung. Die erneute Genehmigung für ausgewählte Privilegzuweisungen kann in Verbindung mit Terminvorgaben eingestellt werden.

Real-Time Provisioning

Provisioning ist der Prozess, die Zielsystem-spezifischen Zugriffsrechte einzurichten, in die die Benutzer-Rollenzuordnung aufgelöst wird. Es nutzt dabei die beschriebenen Prozesse der Benutzer-, Rollen- und Policy-Verwaltung. Provisioning ist ein zweistufiger Prozess:

- Bestimmen der Accounts und Gruppen sowie der Account-Gruppen-Zuordnung pro Zielsystem im Identity Store basierend auf der vorher erfolgten Zuweisung von Rollen zu Benutzern. Dieser Prozessschritt wird als Rollenauflösung bezeichnet und kann optional Rollen- und Berechtigungsparameter einschließen.
- Nutzen der Connectivity Infrastruktur, um die berechneten Zugriffsrechtsdaten sofort vom Identity Store in die Zielsysteme zu übertragen und sicherstellen, dass die Konsistenz der Daten mit den Zugriffsrechten, die aus der Rollenauflösung abgeleitet wurden, gewährleistet ist. Um zum Beispiel in Outsourcing-Einsatzszenarien eine sehr große Anzahl von Zielsystemen (bis zu 10.000) optimal zu unterstützen, ermöglicht DirX Identity das Clustern von Zielsystemen, d.h. ein Workflow kann mehrere Zielsysteme provisionieren.

Für Benutzer-Rollen-Zuweisungen, die Genehmigungen erfordern, wird das Provisioning erst durchgeführt, wenn alle Genehmigungen vorliegen.

Es ist zu beachten, dass der Administrator des jeweiligen Zielsystems die Zugriffsrechte für die Ressourcen für die jeweilige Gruppe im Zielsystem zuweist. Dieser Vorgang liegt außerhalb von DirX Identity und erfolgt mit den Administrationstools des jeweiligen Zielsystems. Die Zugriffskontrollkomponenten des jeweiligen Zielsystems sorgen auch für die Einhaltung der Zugriffsrechte. Das Unternehmen sollte einen Organisations-Prozess installieren, der sowohl das Einrichten der Policies und Rollenstrukturen als auch die Zuweisung der Ressourcen-spezifischen Zugriffsrechte zu Gruppen in den Zielsystemen steuert.

Wenn sich die Benutzerrollen, Berechtigungsparameter oder Rollenparameter ändern oder wenn sich ein Benutzerattribut ändert, das eine Provisioning-Policy steuert, führt DirX Identity sofort automatisch eine neue Rollenauflösung durch und provisioniert alle Änderungen in die Zielsysteme.

Die Provisioning Services von DirX Identity stellen eine zentrale, konsistente und automatisierte Administration von Benutzern und ihrer Zugriffsrechte in der IT-Infrastruktur des Unternehmens zur Verfügung.

DirX Identity unterstützt die Ausführung beliebiger Programme oder Skripte über die Java-basierten Workflow User Hooks. Dies ermöglicht beispielsweise die Verwaltung von Home-Verzeichnissen für Microsoft Active Directory Accounts oder die sofortige Aktivierung von Mailboxen in Microsoft Exchange mit den Mitteln von Windows PowerShell.

Service Management Unterstützung

DirX Identity unterstützt die Integration mit Service Management Systemen wie zum Beispiel Support-Ticket-Systeme sowohl als Quell- als auch als Zielsysteme:

- Service Management als Quelle:
  Wenn ein Kunde bereits ein Ticket-System zur Bearbeitung von Anfragen oder Anträgen einsetzt, ist es sinnvoll, dieses System als Quelle für Aufträge zu nutzen. Ein Ticket kann genutzt werden, um Identity Management Aktionen zu starten. Beispiele derartiger Tickets sind Aufträge zum Anlegen oder Ändern von Benutzereinträgen oder Anträge für die Zuweisung von Rollen.
- Service Management als Ziel:
  Wenn der Kunde bereits ein Ticketsystem zum Starten von manuellen Provisioning von Zielsystemen einsetzt, kann DirX Identity über ein Ticket einen Auftrag übergeben. Lokale Administratoren bearbeiten die Tickets aus dem Ticket-System und bestätigen den Abschluss ihrer Aufträge. Konnektoren für allgemein verbreitete Ticket-Systeme (Remedy, HP OpenView) können mittels kundenspezifischer Konnektoren im Rahmen von Kundenprojekten implementiert werden.
- Manuelles Provisioning von nicht angeschlossenen Systemen:
  Wenn der Kunde kein Ticket-System einsetzt und wenn es Systeme gibt, die noch nicht automatisch mit DirX Identity verwalten werden, d.h. das Zielsystem ist noch nicht angeschlossen, kann man einen manuellen Ansatz zum Provisoning mittels DirX Identity Antrags-Workflows nutzen. In diesem Fall richten die Provisioning-Workflows zur Synchronisation einen Antrags-Workflow für jedes Ereignis ein. Die Administratoren der Zielsysteme erhalten die Aufträge zum Erzeugen, Modifizieren und Löschen per Email, führen die Arbeiten manuell durch und Bestätigen den Abschluss ihrer Arbeiten.

Zeitgesteuerte Änderungen

Dies ermöglicht die Verwaltung von Änderungen, die in der Zukunft wirksam werden sollen, zum Beispiel der Wechsel eines Mitarbeiters von einer Abteilung zu einer anderen Abteilung am 1. Juli. Dies kann Änderungen der zugewiesenen Berechtigungen zur Folge haben. Am festgelegten Datum ändert DirX Identity die Daten der Person und führt weitere Änderungen aus, die aus der Anwendung von Policies und aus Rollenauflösungen resultieren. Die Administratoren können die ausstehenden und bereits abgearbeiteten Änderungsaufträge ansehen, um den Auftragsstatus und die Ergebnisse zu verfolgen.

Metadirectory

DirX Identity Metadirectory ist ein Satz von Diensten, der die unterschiedlichen Directories, Benutzerdatenbanken und anwendungsspezifischen Datenhaltungen in einer zentralen Datenhaltung integriert. Er bietet die notwendigen Anschlussmöglichkeiten, Management- und Interoperabilitätsfunktionen, die die Benutzerdaten zusammenführt (Join) und den bidirektionalen Datenfluss (Synchronisation) in einer heterogenen Infrastruktur gewährleistet. Die Metadirectory Services umfassen:

- **Integrationsdienste:** sie sammeln und integrieren Benutzerdaten von verschiedenen maßgeblichen Quellen wie zum Beispiel Human Ressource Directories, Enterprise Resource Planning (ERP) Systemen, Customer Relation Management (CRM) und Supply Chain Management (SCM) Datenbanken in einer einzigen einheitlichen digitalen Identität. Diese repräsentiert den Benutzer, für den das Provisioning in die angeschlossenen Systeme durchgeführt werden soll.
- **Synchronisationsdienste**: sie pflegen einen konsistenten und aktuellen Identity Store für diese Identitäten und synchronisieren Benutzerdaten vom Identity Store zurück in die maßgeblichen Quellen.

Sowohl für die Integrations- als auch für die Synchronisationsdienste

- ermöglichen die DirX Identity Agenten und Konnektoren den Datenaustausch zwischen den verschiedenen Zielsystemen und dem Identity Store
- kann die Ausführung automatisch zeitgesteuert erfolgen, durch entsprechende Events ausgelöst werden oder manuell gestartet werden; für Audit-Zwecke kann dies automatisch überwacht und protokolliert werden
- ermöglichen flexible Datenfluss- und Daten-Ownership-Modelle dem Unternehmen zu kontrollieren, welches die maßgebliche Quelle der Daten ist, welche Daten synchronisiert werden, wie Änderungsoperationen auf den Daten ausgeführt werden, inklusive Datenfilterung und Mapping von Operationen.

Default Applications

Eine umfangreiche Sammlung von Anwendungen, die sogenannten Default Applications, wird mit DirX Identity geliefert. Sie enthalten Beispiele für typische Prozesse zum Erzeugen, Pflegen und Synchronisieren von Identitäten, die einfach angepasst werden können, um kundenspezifische Lösungen aufzubauen.

Die Default Applications

- stellen Anwendungen für alle unterstützten angeschlossenen Directories und Agenten zur Verfügung,
- basieren auf einer einheitlichen Architektur, mit standardisierten Kontrollparametern und mit programmierbaren Erweiterungsmöglichkeiten über Wizards,
- können wegen der klaren Trennung von Standard-Programmcode und kundenspezifischen Erweiterungen leicht beim Upgrade auf neue Versionen hochgerüstet werden.

Audit und Compliance

DirX Identity stellt umfassende, konfigurierbare und kundenspezifisch anpassbare Mechanismen für Audit Trails, Status-Reports und Queries zur Verfügung, um die Einhaltung von Vorschriften sicherzustellen und zu dokumentieren.

Mittels Audit Trails können alle relevanten Identity Management Ereignisse zurückverfolgt werden; es werden Informationen wie Datum/Uhrzeit des Ereignisses aufgezeichnet, die Identität, die das Ereignis initiiert hat, die Benutzer, die es genehmigt haben, und ob es manuell oder automatisch durch eine Policy ausgelöst wurde. Die Audit Trail Mechanismen ermöglichen das Zurückverfolgen eines Ereignisses zu seinem zugehörigen auslösenden Ereignis in einer hierarchischen Ereigniskette. DirX Identity stellt einen Satz vorkonfigurierter Audit Policies zur Verfügung und ermöglicht die Definition kundenspezifischer Audit Policies, um individuelle, unternehmensspezifische Anforderungen zu berücksichtigen. Wenn die Audit Log-Dateien nicht direkt an DirX Audit übergeben werden, werden sie im XML-Format zentral in Log-Dateien zur weiteren Auswertung gespeichert. Die Log-Dateien können optional mit einer systemspezifischen, digitalen Signatur versehen werden, um sie vor Manipulationen zu sichern. Ein Kommandozeilen-Tool ermöglicht die Verifikation dieser Signaturen.

Mit den Status-Report-Funktionen können vorschriften- oder kundenspezifische Status-Reports im XML-, HTML- oder reinem Textformat für alle DirX Identity Objekte in festgelegten Zeitintervallen oder auf Anfrage erstellt werden. Damit können Kunden Reports über ausgewählte Objekte und Objektlisten und ihre Attribute sowie Zuweisung zu Rollen, Berechtigungen und Gruppen, delegierte Benutzer und Administratoren, nicht benutzte Rollen, den gesamten Rollenkatalog, die Rollenhierarchie und Provisioning Workflows erzeugen.

DirX Identity stellt vorkonfigurierte Reports für verbreitete Vorschriften zur Verfügung und ermöglicht es durch Verwendung von Extensible Stylesheet Language Transformations (XSLT), diese kundenspezifisch für spezielle Anforderungen anzupassen. Zur Absicherung von Reports können Access Policies eingerichtet werden.

Während Statusreports typischerweise den Inhalt mehrerer miteinander in Beziehung stehender DirX Identity Objekte darstellen, werden Queries (Abfragen) mit einem spezifischen Suchfilter für bestimmte Objekttypen – zum Beispiel Benutzer oder Rollen – gestellt. Die Abfragen liefern eine Menge von Objekten zur weiteren Analyse zurück, zum Beispiel eine Liste von Objekten mit einem Fehlerstatus. Ein Administrator kann jedes Objekt analysieren, den Fehler beheben und die Abfrage neu ablaufen lassen, um sicherzustellen, dass das Objekt nicht mehr in der Ergebnisliste zurückgeliefert wird.

DirX Identity arbeitet nahtlos mit DirX Audit zusammen. DirX Audit gehört ebenfalls zur DirX Produktfamilie. DirX Audit stellt Funktionen für die zentrale, sichere Speicherung, die Analyse, die Korrelation und das Review Identitätsbezogener Audit-Daten über eine gemeinsame Benutzerschnittstelle zur Verfügung, die Auditoren, Audit-Administratoren und Sicherheitsbeauftragten die Antworten zu den „Was, Wann, Wo, Wer und Warum"-Fragen in Bezug auf Benutzerzugriffe und -berechtigungen liefert.

Die DirX Identity Audit Trails, Status Reports und Queries führen zusammen mit anderen DirX Identity Diensten zu einem schnellen, kostengünstigen Einsatz von Überwachungsmöglichkeiten für die Einhaltung von Vorschriften (Compliance):

- Metadirectory Dienste ermöglichen die zentrale Verwaltung von Benutzern und ihrer Zugriffsrechte und ermöglichen somit eine größere Transparenz von Identity Management Aktivitäten und eine stärkere administrative Kontrolle mit weniger Administratoren.
- Automatisches Rollen- und Policy-basiertes User Provisioning stellt sicher, dass unternehmensweite Sicherheits-Policies konsistent über alle Systeme in der IT-Infrastruktur des Unternehmens durchgesetzt werden. Dadurch wird die fehleranfällige Ad-Hoc-Zuweisung von Zugriffsrechten durch die vielen verschiedenen IT-Administratoren in den einzelnen Unternehmenseinheiten vermieden.
- Antrags-Workflows mit Genehmigungsschritten automatisieren die Anwendung von Autorisierungsregeln des Unternehmens und stellen somit sicher, dass sie konsistent angewendet werden.
- Ein zusätzlicher Level zur Sicherstellung von Compliance wird erreicht, indem Antragstellern und genehmigenden Personen das digitale Signieren ihrer Aktionen im Workflow ermöglicht wird.
- Sofortiges, automatisches Deprovisionieren von Benutzern stellt sicher, dass Zugriffsrechte von ausgeschiedenen Mitarbeitern auf betroffene IT-Systeme sofort entzogen werden.
- Mittels des automatischen Abgleichs können verdächtige Accounts und Zugriffsrechte in IT-Systemen entdeckt und entweder automatisch entfernt oder an die zuständigen Administratoren zur weiteren Bearbeitung gemeldet werden.
- Die Durchsetzung von Funktionstrennungen durch die Provisioning Dienste vermeidet Rollenzuweisungen, die die Sicherheitsrichtlinien des Unternehmens verletzen oder nicht akzeptable Risiken verursachen.
- Vorkonfigurierte Audit Policies und Reports bieten eine Starthilfe für Compliance.

Domänen-Management

Mandantenfähigkeit wird in DirX Identity durch das Domänenkonzept unterstützt: Eine DirX Identity Domäne ermöglicht eine Trennung der DirX Identity Daten und ihrer Verwaltung auf einer hohen Ebene, so dass unterschiedliche Policy- und Rollenmodelle in jeder einzelnen Domäne angewendet werden können. Folgende Aufgaben zur Verwaltung von Domänen werden unterstützt:

- Einrichten von Domänen
- Verwalten von DirX Identity Administratoren
- Erzeugen von Reports über Domänen
- Aufrechterhalten der Konsistenz der Datenhaltung

Mit DirX Identity werden verschiedene Beispieldomänen zur Verfügung gestellt, die den typischen Umgang mit DirX Identity in einer Kundenumgebung illustrieren und viele der Eigenschaften von DirX Identity zeigen. Die Beispieldomänen können automatisch mit DirX Identity installiert werden.

DirX Identity Komponenten

Die Hauptkomponenten von DirX Identity sind

- Identity Business Access
- Identity Administration Access
- Identity Manager
- Identity Store
- Identity Server
- Identity Services
- Agenten und Konnektoren
- Identity Web Services
- Identity REST Services
- Identity Integration Framework
- Messaging Service

Abbildung 3 stellt diese Komponenten sowie die Beziehungen zwischen ihnen dar.

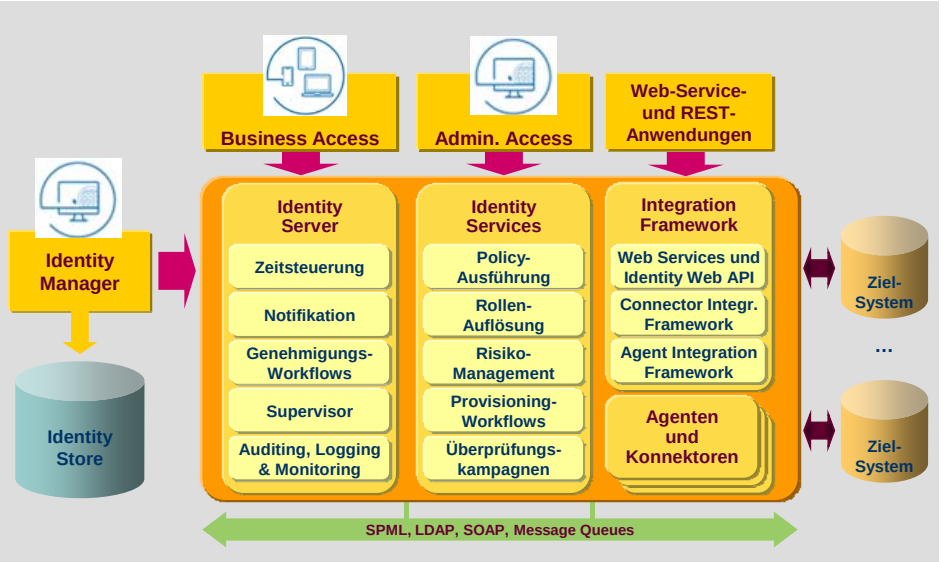


Abb. 3 - DirX Identity - Service-Architektur

Identity Business Access

Mit Identity Business Access stehen verschiedene Benutzerschnittstellen zur Administration der Business-Funktionalität von DirX Identity zur Verfügung:

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

Identity Business User Interface

Die Funktionen, die über das DirX Identity Business User Interface angeboten werden, decken die wesentlichen Anwendungsfälle eines Business Users ab. Basierend auf HTML5 wurde es unter Berücksichtigung des „Mobile First" Ansatzes sowohl für Tablets und Smartphones als auch für Desktop-Rechner entworfen. Zu den unterstützten Anwendungsfällen gehören:

- Login mit Passwort
- Anzeigen und Bearbeiten des eigenen Profils
- Anfordern von neuen Rollen
- Anzeigen und Bearbeiten von Rollenparametern zugewiesener Rollen
- Anzeigen offener Rollenanforderungen
- Genehmigen von Rollenanforderungen

Identity Web Center

Das DirX Identity Web Center ist die Komponente, die den Benutzer-Self-Service und delegierte Administration aus einem Web-Browser ermöglicht. Kunden können die Web Center Funktionalität oder Teile davon in ihre Web-Portale integrieren und sie können das Layout der Web Center HTML-Seiten kundenspezifisch anpassen.

Das DirX Identity Web Center stellt Web Single Sign-On Integration mit SAP NetWeaver und mit anderen führenden Web Access Control Lösungen, zum Beispiel mit DirX Access oder GetAccess von Entrust, bereit. Generische Mechanismen ermöglichen die Single Sign-On Integration mit vielen anderen Web Access Management Produkten. Zusätzlich unterstützt Web Center Microsoft Windows Single Sign-On.

Für die Integration mit SAP NetWeaver Portal wird DirX Identity Web Center als komplettes URL-iView zur Verfügung gestellt.

Das DirX Identity Web Center for Password Management (verfügbar mit der Password Management Option) stellt eine für die Passwortmanagement-Funktionalität erweiterte und spezialisierte Benutzerschnittstelle zur Verfügung.

Approval App

DirX Identity bietet eine Approval-App, genannt DirX Identity Approvals, die speziell für iOS-basierte mobile Endgeräte wie Smartphones oder Tablets entworfen wurde. Sie bietet Benutzern die Möglichkeit, ihre Genehmigungsaufgaben schnell und komfortabel von ihren mobilen Endgeräten aus durchführen zu können. Die App kommuniziert mit DirX Identity mittels REST-basierter Services.

DirX Identity Approvals ist zum Download im iTunes Store von Apple verfügbar.

Identity Administration Access

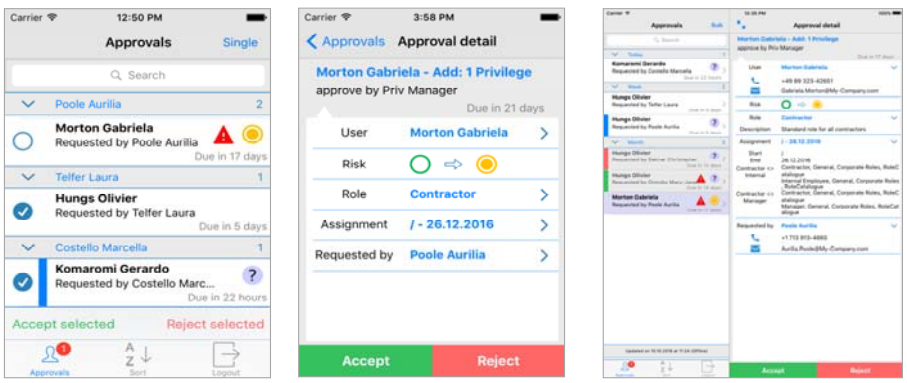
Zum Verwalten und Überwachen der DirX Identity Server stehen im Rahmen des Identity Administration Access zwei Benutzerschnittstellen zur Verfügung:

- Identity Web Admin
- Identity Server Admin

Identity Web Admin

Der DirX Identity Web Admin ist ein Web-basiertes Management-Interface für den Identity Server basierend auf der Java Management Extensions (JMX) Technologie, die zur Entwicklung von Management- und Monitoring-Tools dient. Web Admin oder jeder andere JMX Client – zum Beispiel Oracle's JConsole – kann eingesetzt werden, um den Java-basierten Identity Server über das Web zu überwachen und zu konfigurieren. Zu den Web-basierten Administrationsaufgaben gehören das Überwachen des Server-Status, der Server-Statistiken und der Prozess-Instanzen sowie das Optimieren von Lastverteilung und Performanz.

Der Java-basierte Identity Server führt eine so genannte Dead Letter Queue, die fehlerhafte (dead) Messages und Events, die Fehler verur-



DirX Identity Mobile Access – DirX Identity Approvals App

sacht haben, speichert. Die Administratoren können Web Admin nutzen, um die Informationen in der Queue auszuwerten, um die Fehlerursache zu finden, den Server oder die Umgebung entsprechend umzukonfigurieren, und die Nachrichten oder die Events erneut abzuarbeiten oder zu löschen, falls sie nicht länger benötigt werden.

Spezielle Web-Schnittstellen ermöglichen es, die Workflow Engines und den Java-basierten Identity Server zu steuern und zu überwachen wie beispielsweise die Workflow-Statistiken.

Identity Server Admin

Die Server Admin Web-Anwendung wird zur Überwachung des Zustands der DirX Identity Server genutzt und um zur Lastverteilung oder zur Gewährleistung von Business Continuity Aufgaben zwischen Servern zu verlagern. Server Admin wird mit der High-Availability Option von DirX Identity zur Verfügung gestellt.

Identity Manager

Der Identity Manager stellt eine einfach zu nutzende, Java-basierte grafische Benutzerschnittstelle zur Verwaltung und Konfiguration der verschiedenen Teile von DirX Identity zur Verfügung inklusive der Verwaltung von

- Benutzern und Services
- Rollen und Policies
- Integration, Synchronisation und Workflows
- Zielsystemen und maßgeblichen Datenquellen

Der Identity Manager kann auch dazu genutzt werden, Provisioning Workflows, die Rollenauflösung und die Ausführung der Policies zu überwachen.

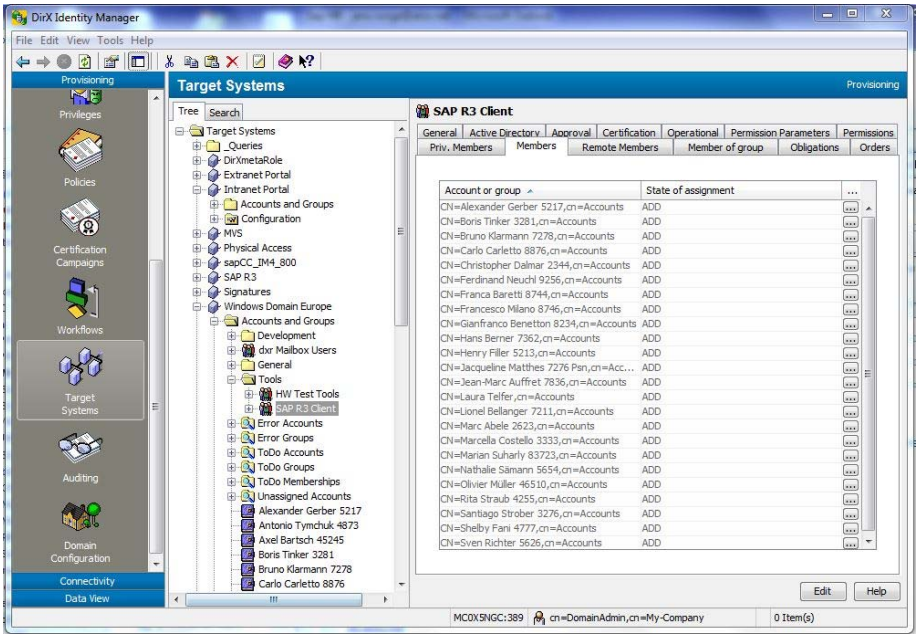
Der Identity Manager unterstützt das SSL-Protokoll (Secure Socket Layer) für authentifizierte, verschlüsselte Kommunikation mit dem Identity Store.

Der Identity Manager unterstützt starke Authentifizierung mittels Smartcards. Es bietet Authentifizierung/Login über alle CardOS Smartcards, die von Atos CardOS API V5.3 unterstützt werden.

Identity Store

Der Identity Store ist ein LDAPv3-Directory, zum Beispiel der DirX Directory Server oder ein Sun Java System Directory Server, der als Konsolidierungspunkt (dem Directory "Join") für die Identity-Integration aus den maßgeblichen Datenquellen und als Verteilungspunkt für das Provisioning und die Synchronisation der Zielsysteme der IT-Infrastruktur des Unternehmens dient.

Der Identity Store ist die Datenhaltung für die Konfigurationsdaten von DirX Identity, für die Benutzerdaten, die Business-Objekte, die Rollen, die Policies, die Daten über die Accounts, Gruppen, und Account-Gruppen-Zugehörigkeiten der Zielsysteme sowie die Konfigurations- und Betriebsdaten, die von den Metadirectory Integrations- und Synchronisationsdiensten benötigt werden. Der Identity Store stellt die zentrale



DirX Identity Manager Beispiel – Account-Gruppen-Mitgliedschaft

Drehscheibe für die Verwaltung dieser Daten sowie für ihre Synchronisation zurück in die Zielsysteme und Datenquellen zur Verfügung. Zur Verteilung und Skalierbarkeit können Teile der Konfigurationsdaten auf mehrere Directory Server verteilt werden.

Identity Server

Der Identity Server stellt die Laufzeitumgebung für die Event- und Zeit-gesteuerten Provisioning Workflows zur Verfügung. Der Server enthält Komponenten

- zur Abarbeitung von Event-gesteuerten Provisioning-Aufgaben wie die Passwort-Synchronisation oder den Real-Time Abgleich von Provisioning Events
- zur Terminplanung von Provisioning-Workflow-Läufen, inklusive Operationen zur Wiederherstellung und Wiederholung bei aufgetretenen Problemen
- zur Benachrichtigung der Administratoren via E-Mail und SMS über Ereignisse bei den Provisioning-Workflows
- für Messaging Services, die Message Queues und JMS Clients unterstützen
- für Audit-, Logging- und Statistik-Zwecke, um Administratoren und Auditoren bei der Analyse und Steuerung der Laufzeitumgebung von DirX Identity zu unterstützen.

Die Server-Komponenten können zum Zwecke der Lastverteilung, Hochverfügbarkeit und Skalierbarkeit auf verschiedene Systeme im Unternehmensnetzwerk verteilt werden.

DirX Identity stellt zwei Arten von Identity Servern zur Verfügung: einen Java-basierten Identity Server zur Behandlung von Java APIs und einen C++-basierten Identity Server zur Behandlung von C und C++ APIs.

Der **Java-basierte Identity Server** bearbeitet hauptsächlich Event-gesteuerte Provisioning Prozesse, wie sie zum Beispiel beim Passwort-Management erforderlich sind. Wenn ein Benutzer sein Passwort ändert, sorgt der Java-basierte Identity Server dafür, dass das neue Passwort sofort mit den Benutzerkennungen der entsprechenden Zielsysteme synchronisiert wird.

Der Java-basierte Identity Server unterstützt auch das Real-Time Provisioning bei Änderungen, die zum Beispiel aus einer Rollenauflösung resultieren. Änderungen an der Benutzer-Rollen-Zuweisung oder an Parameterwerten haben Änderungen bei den Accounts oder Account-Gruppen-Beziehungen in einem oder mehreren Zielsystem zur Folge. Das DirX Identity System sendet diese Änderungen als Events an Java-basierte Identity Server Workflows, die diese Information sofort an die Zielsysteme übertragen.

Ein anderes Beispiel ist die Änderung eines Business-Objekts, zum Beispiel einer Organisationseinheit. Geänderte Attribute werden über Events an alle Benutzer weitergegeben, die dieser Organisationseinheit angehören. Die Zuweisung von Rollen an die Organisationseinheit hat eine unmittelbare Vererbung der Rollen an alle zugehörigen Benutzer zur Folge.

Diese Technologie basiert auf dem Service Provisioning Markup Language (SPML) Standard. Java-basierte Identity Server Workflows können auch zeitgesteuert ablaufen, zum Beispiel um die Konsistenz des Identity Stores zu gewährleisten.

Der Java-basierte Identity Server bietet Möglichkeiten zur Lastverteilung und zur Skalierbarkeit, Funktionen zur Fehlerbehandlung inklusive Benachrichtigungsfunktionen und konfigurierbares Audit und Logging.

Der **C++-basierte Identity Server** bearbeitet zeitgesteuerte Provisioning-Aufgaben im Voll- oder Delta-Modus, wie sie beispielsweise beim Provisioning komplexer Objekte oder für das Provisioning einer großen Anzahl von Objekten zu einem bestimmten Zeitpunkt erforderlich

sind; zum Beispiel eine Gruppe neuer Mitarbeiter, die alle am gleichen Datum anfangen, eine Gruppe von Mitarbeitern, die alle am gleichen Datum die Abteilung wechseln, oder eine Datenbank mit neuen Benutzern, die integriert und provisioniert werden müssen.

Der C++-basierte Identity Server ist die Laufzeitumgebung zur Ausführung von Workflows, die den DirX Identity Meta Controller und die Agenten benutzen. Ebenso unterstützt er auch Konnektoren, die C++-basierte Schnittstellen zu Zielsystemen nutzen, die wiederum von den Java-basierten Identity Server Workflows genutzt werden. Der C++-basierte Identity Server unterstützt verteilte und verschachtelte Workflow-Abläufe in einem heterogenen Netz inklusive Ausnahmebehandlung und Wiederanlauffähigkeit sowie den Neustart von Workflows bei Checkpunkten, die vorher automatisch vom System gesetzt wurden.

Identity Services

Die DirX Identity Services laufen in der Identity Server Umgebung und beinhalten:

- den Service für die Policy-Ausführung, der Regeln für verschiedene Objekte für die automatische Rollenzuweisung sowie Konsistenz- und Validierungsprüfungen inklusive automatischem Abgleich ausführt
- den Service für die Rollen-Auflösung, der aus den abstrakten Rollenstrukturen die konkreten Zugriffsrechte für die Zielsysteme errechnet
- den Service für die Aktionen, die mit den Antrags-Workflows verbunden sind, zum Beispiel die Genehmigung von Rollenzuweisungen durch Mitglieder der Genehmigerliste
- den Service für Event-gesteuerte Provisioning Workflows, die die sofortige, schnelle Passwortsynchronisation oder Real-Time Provisioning durchführen
- den Service für zeitgesteuerte Provisioning Workflows, die komplexe Operationen zur Erzeugung und Pflege von Identitäten und für das Provisioning von Zielsystemen durchführen
- den Kampagnen-Generator zur Durchführung und Überwachung von Überprüfungskampagnen.

Agenten und Konnektoren

Die DirX Identity Agenten und Konnektoren ermöglichen den Datenaustausch zwischen den verschiedenen Zielsystemen und dem Identity Store bei den Integrations- und Synchronisationsoperationen.

Ein **Konnektor** ist eine Java-Komponente, die eine Konnektorschnittstelle implementiert und Änderungs- und Suchoperationen für Zielsysteme eines bestimmten Typs durchführt. Sie läuft im Identity Server ab und wird von den Echtzeit-Provisioning-Workflows aufgerufen, um Daten zwischen einem Zielsystem und dem Identity Store auszutauschen.

Ein **Agent** ist ein eigenständig ausführbares Programm, das die Schnittstellen eines bestimmten Zielsystems unterstützt, um den Datenaustausch zwischen dem Zielsystem und dem Identity Store zu ermöglichen. Er kann auch mittels eines Konnektors realisiert sein, der in das Identity Integration Framework eingebettet ist.

Agenten arbeiten nur mit zeitgesteuerten Provisioning Services, während Konnektoren sowohl mit den Event-gesteuerten als auch mit den zeitgesteuerten Provisioning Services arbeiten.

Zusätzlich zu den Konnektoren stellt DirX Identity Connector Bundles zur Verfügung, die in OpenICF Connector Servern laufen. DirX Identity nutzt einen OpenICF Connector Server als **Provisioning Proxy**. Die Integration von DirX Identity mit dem OpenICF Connector Server wird mittels des DirX Identity OpenICF Proxy Connectors durchgeführt.

Identity Web Services

Die DirX Identity Web Services können genutzt werden, um Provisioning-Funktionen in Anwendungsumgebungen von Service-orientierten Architekturen (SOA) zu integrieren. Sowohl Benutzer-Objekte als auch Rollen-, Gruppen-, Account-, Zielsystem- und Business-Objekte können komplett über die Web Services Schnittstellen bearbeitet werden. Sie implementieren den OASIS SPML Standard. Neben den SPML-Standardoperationen (hinzufügen, ändern, löschen, nachschlagen und suchen) werden für die einzelnen Objekte zusätzlich folgende Funktionen angeboten:

- Benutzer: hinzufügen inklusive Erzeugen von globalen Ids, Rollenzuweisung, aktivieren/deaktivieren, Passwortänderungen
- Rollen: Rollenparameter
- Berechtigungen: Match Rules
- Gruppen: Account-Gruppen-Mitgliedschaften
- Accounts: aktivieren/deaktivieren und Passwort setzen, Gruppenmitgliedschaft zuweisen/ entfernen, Lesen der Passwort Policy; die Authentifizierung erfolgt mittels Sicherheitsfragen oder der Signatur der Requests
- Zielsysteme: Tombstone-Feature und Referenzen
- Business-Objekte: Referenzen zu Rollen und anderen Business-Objekten

Bei allen Objekttypen können sogenannte User Hooks die Anforderungen (Requests) und zugehörigen Antworten (Responses) abfangen und kundenspezifische Operationen ausführen, wie das Verschieben von Einträgen oder das Erzeugen und Prüfen von eindeutigen Identifikatoren.

DirX Identity stellt auch SOAP-basierte Workflow-Services, die die Ausführung von Antrags-Workflows steuern, zur Verfügung: enthalten sind Methoden zum Erzeugen, Modifizieren und Verwalten von Workflows. Clients können Worklisten sowie Informationen über Workflow-Definitionen und –Instanzen abrufen und ihre Aufgaben genehmigen.

Die SOAP-basierten Identity Web Services stellen eine Web Single Sign-On Integration mit SAP NetWeaver und führenden Web Access Management Produkten, zum Beispiel DirX Access und Entrust GetAccess, zur Verfügung.

Identity REST Services

Die Identity REST Services können dazu genutzt werden, DirX Identity in Anwendungsumgebungen zu integrieren, die das HTTP-Protokoll und die Performance- und Skalierungsvorteile von REST-basierten Services nutzen wollen. Dies gilt speziell für moderne, HTML5-basierte Single-Page Anwendungen; ein Beispiel ist das DirX Identity Business User Interface:
Die REST Services folgen dem SCIM 2 Standard: System for Cross-domain Identity Management. Sie stellen folgende Funktionen mit JSON als Datenformat zur Verfügung:

- Genehmigen – Benutzer können ihre Tasks genehmigen und sie einzeln oder insgesamt genehmigen.
- Self-Service – Benutzer können Rollen anfordern und ihr eigenes Profil anzeigen und bearbeiten.

Identity Integration Framework

Das Identity Integration Framework enthält die öffentlichen Schnittstellen von DirX Identity. Das Framework ermöglicht den Kunden,

- die DirX Identity Web oder REST Services zu nutzen
- das SPML-Standard-Set von Schnittstellen und Werkzeugen im Connector Integration Framework zu nutzen, um kundenspezifische Konnektoren zu implementieren, die auf die Zielsysteme mittels Java- oder C++-basierter Schnittstellen zugreifen
- ausführbare Programme oder Batch-Files als Agenten mit dem Agent Integration Framework in Batch-orientierte Workflows zu integrieren
- Teile des DirX Identity Web Centers in ihre Portal-Applikationen zu integrieren oder die DirX Identity Web-API zu nutzen, um zusätzliche Funktionen hinzuzufügen.

Supervisor

Mit der High Availability Option stellt jeder Java-basierte Identity Server einen Supervisor zur Verfügung, der andere Java-basierte Identity Server oder mehrere C++-basierte Identity Server überwacht. Der Supervisor sorgt für automatischen Failover zwischen Servern, sobald ein überwachter Server nicht mehr verfügbar ist.

Messaging Service

Der Messaging Service stellt Funktionen für die Ausfallsicherheit zur Verfügung wie "Store and Forward" und automatische Wiederzustellung von Nachrichten. Er ist konform zum Java Message Service. DirX Identity nutzt Apache ActiveMQ als Messaging Service.

Unterstützung von Standards

Die DirX Identity Komponenten unterstützen verschiedene Standards für die Konnektivität, die Datenspeicherung und Datenformatierung:

- Der Identity Store und die Konfigurationsdatenhaltung nutzen das Lightweight Directory Access Protocol (LDAP), ebenso die Verbindungen zu Zielsystemen, die LDAP unterstützen.
- Das Rollenmanagementmodell basiert auf dem ANSI RBAC Referenzmodell (ANSI/INCITS 359).
- Alle Provisioning-Komponenten arbeiten intern mit SPML Requests und Responses nach dem Services Provisioning Markup Language (SPML) 1.0 Standard.
  Daten, die von/zu externen Systemen exportiert/importiert werden, werden nach und von SPML konvertiert.
- Die Identity Web Services implementieren die OASIS SPMLv2 Spezifikation mit dem SPMLv2-DSML Profile.
- Das Identity Integration Framework (Java, C++, C#) unterstützt SPML 1.0 zur Erstellung von kundenspezifischen Konnektoren, die interne Requests in proprietäre APIs umwandeln.
- Die Identity Services und die Identity Server Messaging Queues entsprechen dem Java Messaging Service (JMS).
- DirX Identity Web Admin baut auf Java Management Extensions (JMX) auf. Als JMX-Agent kann der DirX Identity Java-Server mittels JMX verwaltet werden.
- Die DirX Identity Konnektoren können Zielsysteme via Simple Object Access Protocol (SOAP) Version 1.2 und SPML V1.0 und V2.0 provisionieren; Workflow und Provisioning Services werden über SOAP aufgerufen.

Sicherheit

Die Authentifizierungs- und Autorisierungs-Mechanismen des zugrunde liegenden LDAP Directory Servers ermöglichen es, Attribute und Passwörter zu schützen. DirX Identity stellt zusätzliche Sicherheitsfunktionen zur Verfügung:

- Alle Komponenten können optional im SSL/TLS-Modus arbeiten, wenn sie LDAP-Verbindungen benutzen.
- Der Datenaustausch über den Messaging Service kann optional verschlüsselt werden, um hohe Sicherheit bei dem Datentransfer über das Netzwerk zu ermöglichen.
- Die meisten Attribute, speziell auch die Passwörter, können stark verschlüsselt im Identity Store gespeichert werden. DirX Identity sorgt dafür, dass der Datentransfer und die Protokollierungen bis an die Schnittstelle des angeschlossenen Zielsystems gesichert sind.

Skalierbarkeit

Um Skalierbarkeit in einer DirX Identity Einsatzumgebung zu erreichen, können mehrere Instanzen der Java-basierten und C++-basierten Server eingesetzt werden.

DirX Identity stellt Funktionen zur statischen und dynamischen Lastverteilung für diese Instanzen zur Verfügung:

- Zur statischen Lastverteilung können Java-basierte Workflows gemäß ihres Typs auf ausgewählte Java-basierte Server-Instanzen verteilt werden: Antrags-Workflows, Provisioning-, Passwortänderungs- und Event Maintenance-Workflows.
- Zur dynamischen Lastverteilung können Java-basierte Workflows an verschiedene Java-basierte Server-Instanzen verteilt werden, die statisch für den entsprechenden Workflow-Typ zugewiesen wurden.
- Klassische Tcl-basierte Batch-Workflows können auf alle installierten C++-basierten DirX Identity Server verteilt werden, um die Last zu verteilen.

Einsatzunterstützung

DirX Identity stellt Mechanismen zur Verfügung, mit denen die Vorbereitungszeit für den Produktiveinsatz reduziert wird. Sie ermöglichen die leichte Übertragung von einem System zu einem anderen, zum Beispiel von einem Test- oder Entwicklungssystem zu einem Produktivsystem oder zu Konfigurationsmanagementsystemen. Dadurch wird auch der schnelle Einsatz mehrerer DirX Identity Instanzen ermöglicht.

Business Continuity

Mit der High Availability Option unterstützt DirX Identity den kontinuierlichen Betrieb für den Message Service, für die Tcl-basierten Workflows und für die Java-basierten Workflows.

Die Server Admin Web-Applikation stellt einen Überblick sowohl über den Zustand der Java- und C++-basierten Server als auch der Message Broker zur Verfügung und ermöglicht die Verlagerung von Aufgaben zwischen diesen Servern. DirX Identity unterstützt sowohl den administrativ gesteuerten Failover und automatischen Failover. Im Falle von administrativem Failover können die Administratoren folgende Aufgaben verschieben:

- einen Java JMS-Adapter und damit die zugehörigen Workflows zu einem anderen Java-basierten Identity Server
- die Verarbeitung von Antrags-Workflows zu einem anderen Java-basierten Identity Server
- den Scheduler Service zu einem anderen Java-basierten Identity Server
- die Tcl-basierten Workflows zu einem anderen C++-basierten Identity Server.

DirX Identity unterstützt automatischen Failover mittels ringförmigem Monitoring: Jeder Java-basierte Identity Server überwacht den Zustand eines anderen; zusammen bilden sie einen Ring. Wenn der überwachte Server nicht mehr verfügbar ist, übernimmt der überwachende Server dessen Funktionen. Einer der Java-basierten Identity Server überwacht die C++-basierten Server. Wenn einer der Server nicht mehr verfügbar ist, werden die Workflows zu einem anderen C++-basierten Identity Server verschoben.

Die automatische Failover-Lösung wird von einem Groovy-Skript gesteuert, das an Projekt-spezifische Anforderungen anpassbar ist.

DirX Identity stellt Backup- und Restore-Funktionen zur Verfügung, um die Verfügbarkeit und Ausfallsicherheit der Daten zu gewährleisten. Dies beinhaltet ein synchronisiertes, gemeinsames Backup und Restore des Java-basierten Identity Servers und des DirX Directory Servers.

Nagios-Unterstützung

DirX Identity stellt eine Reihe spezialisierter Nagios-Plugins sowie Kommandos für die Nagios-Zusatzkomponente JNRPE zur Verfügung, die in einer existierenden Nagios-Umgebung genutzt werden können, um den Status von DirX Identity Service-Ressourcen und -Operationen zu überwachen und Statistiken dazu für spätere Auswertungen zu sammeln.

Die DirX Identity Nagios-Plugins ermöglichen die Überwachung

- aller Informationen, die über JMX zur Verfügung gestellt werden, speziell vom Java-basierten Identity Server und von anderen JMX-fähigen Programmen wie Apache ActiveMQ oder Tomcat
- des C++-basierten Server mittels der internen DirX Identity Schnittstellen.

Die DirX Identity Nagios-Plugins stellen Eingabeparameter zur Festlegung von Schwellwerten für Warnmeldungen und für Hinweise auf kritische Werte für die überwachten Operationen bereit. Damit wird den Administratoren die Gelegenheit gegeben, auf Probleme, die von den Nagios-Plugins über die Nagios-Oberfläche angezeigt werden, zu reagieren, bevor diese kritisch werden, und deren Lösung zu überwachen.

DirX Identity stellt Kommandos für die Nagios-Zusatzkomponente JNRPE zur Verfügung, mit denen die folgenden Komponenten überwacht werden können:

- Der Status des Java-basierten Identity Servers
- Die ausstehenden Antworten eines spezifizierten JMS-Adapters
- Ein Statistik-Attribut eines spezifizierten Workflows
- JVM Speichernutzung
- Der Status des C++-basierten Servers

Kundenspezifische Anpassungen

DirX Identity ist in höchstem Maße kundenspezifisch anpassbar in Bezug auf seine Funktionen, Objekte und die Darstellung der Objekte an der Benutzerschnittstelle. Zu den Anpassungsmöglichkeiten gehören die

- Konfiguration über LDAP, XML, Flags, Parameter, etc.
- Erweiterbarkeit mittels JavaScript, Java, C++ oder durch die Integration anderer Prozesse

Lizenz-Optionen

DirX Identity ist mit zwei Optionen für die Basis-Lizenz verfügbar: **Business Suite** und **Pro Suite**. Die **Pro Upgrade** Option ermöglicht einem Kunden, seine Lizenz von der Business Suite Lizenz zur Pro Suite Lizenz zu erweitern. Die Basis-Lizenzen können durch folgende Zusatz-Lizenz-Optionen erweitert werden: **Connectivity Packages, Password Management Option** und **High-Availability Option.**

Die Tabellen 1 und 2 am Ende dieses Dokuments geben einen Überblick über die wesentlichen Funktionen der Business Suite, der Pro Suite und der Password Management Option.

DirX Identity Business Suite

Die DirX Identity Business Suite stellt die Verwaltung des Lebenszyklus von Benutzern, regelbasiertes Provsioning von Accounts und Gruppen in Zielsysteme, Validierung und Abgleich mit Zielsystemen, Metadirectory-Funktionalität, Web-basierten User-Self-Service zur Verwaltung der eigenen Daten, die Verwaltung von Business-Objekten, Domänen-Verwaltung, und Default Connectivity zur Verfügung. Ebenfalls bietet es Report-Funktionalität für Accounts, Gruppen, Zielsysteme und Access Policies.

DirX Identity Pro Suite

Die DirX Identity Pro Suite basiert auf der Business Suite und stellt zusätzlich zu dessen Funktionalität Identity und Access Governance Funktionalität wie Rollenverwaltung mit zugehöriger Policy-Verwaltung und Report-Funktionalität, Unterstützung von Funktionstrennungen (Segregation of Duties), Antrags-Workflows, Genehmigungen und Wiedergenehmigung, Berechtigungsprüfung, regelbasierte und manuelle Zuweisungen von Rollen an Benutzer, Passwortmanagement-Funktionalität und Auditmöglichkeiten für administrative Änderungen und für Passwort-Änderungen in DirX Identity zur Verfügung.

DirX Identity Password Management Option

Zusätzlich zur grundlegenden Passwortmanagement-Funktionalität, die mit der Pro Suite zur Verfügung gestellt wird, bietet die Password Management Option ein spezielles Web Center für Passwortmanagement, das Passwortänderungen durch Benutzer für eine Untermenge ihrer Accounts ermöglicht, sowie die Anzeige des Passwort-Änderungsstatus und das Challenge-/Response-Verfahren zum Rücksetzen vergessener Passwörter durch Administratoren oder den Help Desk. Diese Option schließt den Password Reset Client für Windows ein.

DirX Identity High Availability Option

Die High Availability Option unterstützt den kontinuierlichen Betrieb durch automatisches und administratives Failover. Der Supervisor überwacht die Server und ermöglicht automatisches Failover. Die Server Admin Web-Anwendung ermöglicht administratives Failover durch manuelles Verlagern von Aufgaben zwischen Servern.

DirX Identity Connectivity Packages

DirX Identity stellt die Konnektivität zu den unterstützten Zielsystemen mittels seiner Connectivity Packages zur Verfügung.

Default Connectivity

DirX Identity stellt standardmäßig Konnektivität zu DirX Access, zu SPML-fähigen Anwendungen, zu LDAP-Directories, zu DirX Identity Domänen und zu Unix-Systemen (Linux) basierend auf PAM als Teil seines Basissystems zur Verfügung.

DirX Access

- Konnektivität zu DirX Access V8.4 oder neuer
- Nahtlose Integration durch gemeinsam genutzte LDAP-Benutzerdatenhaltung
- Provisioning und Passwort-Synchronisation in Echtzeit
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

SPML-fähige Anwendungen

- Unterstützt SPML V1.0 und V2.0
- Unterstützt Add, Modify, Delete, Search und getSchema Operationen
- Provisioning und Passwort-Synchronisation in Echtzeit
- Agenten- und agentenloser Betrieb möglich (in diesem Fall läuft der Konnektor im Java-Server)
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

LDAP Directories

- Konnektivität zu LDAPv2- und LDAPv3-konformen Systemen
- Voll- und Delta-Import und -Export aller Objektklassen und Attribute
- Provisioning und Passwort-Synchronisation in Echtzeit
- Unterstützt LDAP-Filter und Attribute mit mehreren Werten
- Agenten und agentenloser Betrieb möglich (in diesem Fall läuft der Konnektor im Java-Server)
- Kundenspezifische Anpassung / Erweiterung möglich
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

DirX Identity Domäne

Ein spezialisierter Real-Time-Konnektor unterstützt das Provisioning einer DirX Identity Domäne. Er nutzt direkt die Funktionen des Service Layers wie die Regeln von Objektbeschreibungen, Zuweisung von Rollen, auch mit Rollenparametern, und die direkte Rollenauflösung. Dieser Konnektor vereinfacht das Importieren von Benutzern durch die Berechnung von Defaultwerten von Attributen, durch Anwendung von Provisioning-Regeln zur automatischen Rollenzuweisung und das Anfordern von Genehmigungen, wo nötig:

- Konnektivität zu einer DirX Identity Domäne
- Unterstützung aller Typen von Einträgen, von Benutzern zu Business-Objekten, Rollen, Gruppen und Accounts
- Wertet Objektbeschreibungen aus und verarbeitet ihre Regeln, um Defaultwerte und Werte von abhängigen Attributen zu berechnen
- Zuweisen von Privilegien mit Start- und Endedatum und von Rollen mit Parametern
- Passwortänderungen für Benutzer und Accounts
- Suchen, auch seitenweise
- Anwendung von Provisioning- und Konsistenz-Regeln nach Änderungen
- Durchführen von Rollenauflösungen sofort nach relevanten Änderungen

Unix PAM

- Unterstützt Unix PAM LDAP-Strukturen gemäß RFC2307 auf den unterstützten Linux-Plattformen
- Voll- und Delta-Import und -Export von Accounts, Gruppen und Gruppenmitgliedschaften
- Provisioning und Passwort-Synchronisation in Echtzeit
- Agenten und agentenloser Betrieb möglich (in diesem Fall läuft der Konnektor im Java-Server)
- Kundenspezifische Anpassung / Erweiterung möglich
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Hinweis: Das Provisioning von Unix-Accounts kann auch mit dem OpenICF Connector Bundle für Unix durchgeführt werden, das mit dem OpenICF Proxy Connectivity Package verfügbar ist.

CSV Import/Export

- Voller Import und Export von CSV-Dateien

Connectivity Package für Microsoft AD

Active Directory / Exchange / Lync

- Unterstützt Microsoft Active Directory für Windows Server 2008 R2, Windows Server 2012/ 2012 R2 und Windows Server 2016 (LTSC) als Agent über den Microsoft ADSI LDAP Provider bzw. als Konnektor über die LDAP Schnittstelle.
- Integrierte Behandlung von Microsoft Exchange 2000/2003/2007/2010/2013/2016 Mailboxen
- Integrierte Behandlung von Microsoft Lync 2013
- Integrierte Nachbearbeitung möglich, zum Beispiel das Anlegen von Shares
- Voll- und Delta-Import und -Export aller ADS Objektklassen, zum Beispiel Benutzer und Gruppen
- Provisioning und Passwort-Synchronisation in Echtzeit (Konnektor)
- Unterstützung von Serverless Binding, Paging bei Export (für große Mengen von Einträgen), Attributen mit mehreren Werten und Verschieben von Objekten zwischen verschiedenen Bäumen
- Behandlung von gelöschten Einträgen
- Verwaltung von Home-Verzeichnissen für Microsoft Active Directory Accounts oder die sofortige Aktivierung von Mailboxen in Microsoft Exchange mit den Mitteln von Windows PowerShell
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows Plattformen (Agent) sowie allen unterstützten Plattformen (Konnektor).

Hinweis: Das Provisioning von lokalen Windows Accounts kann mit dem OpenICF Bundle für Windows Local Accounts durchgeführt werden, das mit dem OpenICF Proxy Connectivity Package verfügbar ist.

SharePoint

- Unterstützt Microsoft Office SharePoint Server 2007, 2010 und 2013
- Die Lösung nutzt die Windows Active Directory Accounts
- Provisioning von Gruppen und Gruppenmitgliedschaften in SharePoint
- Import von Gruppen und Gruppenmitgliedschaften aus SharePoint Sites zum initialen Laden der Daten und zur Validierung der Zielsystemdaten
- Bearbeitet SharePoint Sites und Gruppen, d.h. jede SharePoint Site hat eine eigene Menge von Gruppen mit unterschiedlichen Zugriffsrechten (als Rollen in SharePoint bezeichnet)
- Provisioning in Echtzeit
- Fehlerberichte und Tracing
- Läuft auf Microsoft Windows und allen unterstützten Linux-Plattformen

Windows Password Listener

Der Windows Password Listener erkennt die Änderungen von Benutzerpasswörtern in einer Windows Domäne, verschlüsselt die Information und erzeugt Passwortänderungs-Events. Diese Events steuern den Event Manager und die zugehörigen Passwortänderungs-Workflows.

Der Windows Password Listener ist geeignet für Microsoft Windows Server 2012 R2 und Windows Server 2016. Er wird als separate Installationseinheit bereitgestellt.

Connectivity Package für Datenbanksysteme

ODBC

- Unterstützt ODBC (ohne Cursor) und greift auf beliebige Quell- und Zieldatenbanken zu, auf die mittels ODBC zugegriffen werden kann
- Installation und Nutzung des zugehörigen ODBC-Treibers ist Voraussetzung
- DataDirect ODBC 4.0 oder höher ist Voraussetzung für Linux Plattformen
- Voll- und Delta-Export selektierter Zeilen einer Tabelle oder einer Verknüpfung (join) von Tabellen
- Voll- und Delta-Import in eine einzige Tabelle (begrenzte Importmöglichkeiten für Verknüpfung (join) von Tabellen). Relationen von Tabellen können verfolgt werden (referentielle Integrität)
- Unterstützung von Stored Procedures für Import-Operationen
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

JDBC

- Unterstützt JDBC und den Zugriff auf jede mit JDBC erreichbare Quell-/Ziel-Datenbank
- Installation und Nutzung des zugehörigen JDBC-Treibers ist Voraussetzung
- Vollständiger Export selektierter Zeilen einer Tabelle
- Voll- und Delta-Import in eine einzige Tabelle. Relationen von Tabellen können verfolgt werden (referentielle Integrität)
- Unterstützung von Stored Procedures für Import- und Export-Operationen
- Provisioning und Passwort-Synchronisation in Echtzeit
- Fehlerbericht und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Connectivity Package für HiPath

HiPath 4000 Manager / Hicom DMS

- Unterstützt HiPath 4000 Manager 3.0 und V3.1 und Hicom DMS V3.1 und 3.6 durch Nutzung der XIE Schnittstelle (Request / Response Dateien)
- Voll- und Delta-Import und –Export der PERS Tabelle mit Einfügen, Ändern und Löschen
- Unterstützt "join" mit eindeutiger ID oder mit bestmöglicher Übereinstimmung und Delta-Export mit SELECT_UPDATES Query
- Unterstützt referentielle Integrität mit COMPIMP, ORGIMP, LOCIMP und BUILDIMP Tabellen
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Connectivity Package für Gesundheitswesen

Health Enterprise Dashboard

- Unterstützt Health Enterprise Dashboard mit implementierter BatchXML API (Version 1.0)
- Nutzt Standard http-Verbindung zur URL des Dashboard Servlets
- Baut auf dem SPML-basierten Connector Integraton Framework von DirX Identity auf
- Voll- und Delta-Import von Benutzern und Accounts für externe Anwendungen mit Erzeugen, Ändern und Löschen
- Passwort-Synchronisation in Echtzeit
- Erzeugen von Backchannel-Informationen zur Unterstützung der automatischen Statusbehandlung von DirX Identity
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

medico//s

- Unterstützt medico//s Release 16 mit entsprechendem Service Pack/Patch
- Nutzt den Standard DirX Identity SPML Konnektor
- Voll- und Delta-Import von loginIds und Personen mit Operationen zum Erzeugen, Ändern und Löschen
- Voll- und Delta-Import von Gruppen, Profilen und Rollen mit Operationen zum Erzeugen, Ändern und Löschen
- Behandlung von Mitgliedschaften von loginIds in Gruppen, Profilen und Rollen
- Provisioning in Echtzeit
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Connectivity Package für Physical Security Systeme

SiPass

- Unterstützt SiPass 2.4, 2.5 und 2.6 und nutzt die SiPass Human Resources Interface (COM Technologie)
- Voll-Export von Karteninhabern und Workgroups eines SiPass Systems
- Delta-Import von Benutzern mit Erzeugen, Ändern und Löschen inklusive Zuweisung zu Workgroups
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows
- Setzt korrekte .NET Framework Installation auf dem System voraus

Connectivity Package für SAP-Systeme

SAP ERP HR und OM

- Konform zu SAP ECC 6.0 bzw. SAP ERP 6.0 und höher
- Implementiert als ERP Applikation mit GUI-Komponenten (SAPgui)
- Integrierte Nutzung von ERP Batch Jobs zur Ad-hoc- und zeitgesteuerten Ausführung
- Voll- und Delta-Export von Daten aus SAP HR und SAPoffice Komponenten
- Voll- und Delta-Export von Daten aus SAP OM (Organizational Management), die entweder mit HR-Daten integriert oder separat vorliegen
- Unterstützt Unicode
- Unterstützt mehrere Selektionskriterien zur Auswahl der Datensätze und –felder (Infotypes) und Attribute mit mehreren Werten
- Kundenspezifische Konfiguration und Ausführung
- Konfigurierbare Datenschutzmechanismen
- Fehlerberichte und Tracing
- Ablauf auf allen NetWeaver (ABAP Stack) Plattformen

SAP ECC User Management

- Konform zu SAP ECC bzw. SAP ERP 6.0 und höher
- Eine Installation von SAP Java Connector (SAP JCo 3.0.10 oder höher für Windows-/LinuxSysteme) wird zur Nutzung vorausgesetzt
- Baut auf dem SPML-basierten Connector Integraton Framework von DirX Identity auf
- Unterstützt Stand-Alone-Systeme und Zentrale Benutzerverwaltung (ZBV)
- Voll- und Delta-Synchronisation von Benutzern, Profilen (nur lesend) und SAP-Rollen (nur lesend) mit dem SAP ECC User Management
- Unterstützung von User Hooks, um ABAP-Erweiterungen auszuführen
- Provisioning und Passwort-Synchronisation in Echtzeit
- Fehlerberichte und Tracing
- Ablauf auf allen Plattformen, die sowohl von SAP JCo als auch von DirX Identity unterstützt werden

SAP NetWeaver User Management

- Konform zu SAP NetWeaver und Enterprise Portal 6
- Baut auf dem SPML-basierten Connector Integration Framework von DirX Identity auf
- Voll- und Delta-Synchronisation von Benutzer- und Rolleninformationen (nur lesend) zum SAP NetWeaver und Enterprise Portal User Management
- Passwort-Synchronisation in Echtzeit
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und auf allen unterstützten Linux-Plattformen

Connectivity Package für IBM-Systeme

Lotus Notes / Domino

- Unterstützt V8.5 und V9.0 durch Nutzung von Notes C++ und C APIs
- Zugriff auf entfernte Lotus Notes Directory Server
- Voraussetzung ist ein Lotus Notes Client auf dem gleichen System
- Voll- und Delta-Export von Adressen, Gruppen oder anderer Formulare mit Spezifikation von Suchfiltern und Auswahl der Attribute
- Voll- und Delta-Import von Adressen, Gruppen oder anderer Formulare inklusive Anlegen von Mailboxen (optional mit Replikas) und Benutzer-Registrierung in Notes
- Unterstützt AdminP Funktionalität
- Provisioning und Passwort-Synchronisation für das Internet-Passwort in Echtzeit
- Unterstützt Attribute mit mehreren Werten
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows Plattformen

IBM RACF

- Unterstützt z/OS und OS/390 V2R8 durch Nutzung der LDAP-Schnittstelle von IBM's LDAP Server, um auf RACF zuzugreifen
- Voll- und Delta-Export aller RACF-Objektklassen
- Voll- und Delta-Import von RACF Benutzern und Gruppen
- Passwort-Synchronisation in Echtzeit
- Unterstützt LDAP-Filter und Attribute mit mehreren Werten
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Connectivity Package für Enterprise Single Sign-On Systeme

Evidian Enterprise SSO

- Unterstützt Evidian Enterprise SSO 9.01b5901 oder neuer
- Evidian Enterprise SSO Benutzerdaten können entweder in Microsoft Active Directory oder in einem LDAP-Directory gespeichert sein
- Evidian Enterprise SSO wird über den Evidian User Access Web Service provisioniert
- Behandelt Evidian Enterprise SSO Account-Objekte, d.h. Applikation / Login Name / Passwort-Tupel
- Hinzufügen, Ändern und Löschen werden als Operationen unterstützt
- Voll-Export von Accounts von DirX Identity nach Evidian Enterprise SSO wird unterstützt
- Provisioning von Account-Objekten in Echtzeit
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows Plattformen

Imprivata OneSign

- Unterstützt Imprivata OneSign 4.1 SP1 oder neuer
- Imprivata OneSign wird mittels SPMLv1 Messages provisioniert, die an einen entsprechenden Provisioning System Adapter in der Imprivata OneSign Appliance gesendet werden
- Behandelt Subscriber und Application Account Objekte
- Hinzufügen und Löschen werden als Operationen unterstützt, Änderungsoperationen sind durch die Fähigkeiten des Imprivata SPMLv1 API beschränkt
- Unterstützt die eins-zu-eins Beziehung zwischen einem Subscriber-Objekt und einem Application-Account-Objekt in einer Applikation
- Voll- und Delta-Export von Subscriber- und Account-Objekten von DirX Identity nach Imprivata OneSign werden unterstützt
- Provisioning und Passwort-Synchronisation in Echtzeit für Subscriber- und Account-Objekte
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Connectivity Package für Cloud Systeme

Google Apps

- Der Konnektor nutzt die Google Directory API
- Konnektivität basiert auf dem HTTP Protokoll
- Voll-Import von Accounts, Gruppen und Gruppenmitgliedschaften
- Provisioning von Accounts, Gruppen, Gruppenmitgliedschaften in Echtzeit
- Passwort-Synchronisation in Echtzeit
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Citrix ShareFile

- Der Konnektor nutzt die Citrix ShareFile API
- Konnektivität basiert auf dem HTTP Protokoll
- Voll-Import von Accounts, Gruppen und Gruppenmitgliedschaften
- Provisioning von Accounts, Gruppen, Gruppenmitgliedschaften in Echtzeit
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Microsoft Office 365

- Der Konnektor nutzt die Microsoft Graph API Version 2013-11-08 von der URL https://graph.windows.net
- Konnektivität basiert auf dem HTTP Protokoll
- Voll-Import von Benutzern, Gruppen, Rollen, Service-Plänen mit Zuweisungen
- Provisioning von Benutzern, Gruppen, Rollen mit Zuweisungen in Echtzeit
- Zuweisung von Benutzern zu Plänen: dies ermöglicht Benutzern, ihre lizensierten Office 365 Funktionen wie Office-Applikationen, Exchange, Skype for Business, etc. nutzen zu können
- Passwort-Synchronisation in Echtzeit
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Salesforce

- Der Konnektor nutzt das Force.com REST API
- Konnektivität basiert auf dem HTTP Protokoll
- Voll-Import von Benutzern und Profilen
- Provisioning von Benutzern inklusive der zugewiesenen Profileld in Echtzeit
- Passwort-Synchronisation in Echtzeit
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

Proxy Connectivity Package

Remote Upload Connector

- Unterstützt Szenarien, in denen DirX Identity als Teil einer Cloud Service Infrastruktur wie zum Beispiel IDMaaS (Identity Management as a Service) bei einem Cloud Provider und Active Directory entfernt bei einem Kunden betrieben wird
- Konnektivität basiert auf dem HTTP Protokoll
- Der Konnektor nutzt Standard LDAP-Funktionalität, um auf das Active Directory von Microsoft Windows Server 2008 R2, Windows Server 2012 R2 und Windows Server 2016 oder jedes andere LDAP-Directory zuzugreifen
- Erfordert Java Runtime Environment 8 oder neuer und Apache Tomcat 8 oder neuer auf der Service-Seite
- Erfordert Java Runtime Environment 8 oder neuer auf der entfernten Kunden-Seite
- Voll-Import von Accounts
- Fehlerberichte und Tracing
- Ablauf auf Microsoft Windows und allen unterstützten Linux-Plattformen

OpenICF Proxy Connector

- Der Java-basierte OpenICF Proxy Connector läuft im Identity Java Connector Integration Framework
- Zur Kommunikation mit einem OpenICF Connector Server (Java- oder .NET-basiert) nutzt er ein internes OpenICF Protokoll
- Der Konnektor kann dynamisch Informationen über die benötigten Konfigurationsparameter und Datenschemata von diesem Connector Server erhalten
- Der Konnektor konvertiert Provisioning-Operationen und -Daten zwischen DirX Identity und OpenICF Formaten
- Der Konnektor ist Voraussetzung, um die OpenICF Connector Bundles mit DirX Identity zu integrieren.

Hinweis: Zusätzlich zum Provisioning mit den mitgelieferten OpenICF-basierten Workflows wird das Provisioning von anderen Zielsystemen unterstützt, die von OpenICF Connector Bundles unterstützt werden. Dies erfordert eine kundenspezifische Anpassung der mitgelieferten Workflows.

OpenICF Connector Bundle für Unix

- Provisioning von Unix-Accounts, Gruppen und Gruppenmitgliedschaften in Echtzeit
- Passwort-Synchronisation in Echtzeit
- Voll-Import von Unix-Accounts, Gruppen und Gruppenmitgliedschaften
- Fehlerberichte und Tracing
- Das Connector Bundle wird im Java-basierten OpenICF Connector Server eingesetzt
- Ablauf auf allen Microsoft Windows und allen unterstützten Linux-Plattformen, die vom OpenICF Connector Server unterstützt werden.

OpenICF Connector Bundle für Windows Local Accounts

- Provisioning von Accounts, Gruppen und Gruppenmitgliedschaften, die in einer lokalen SAM-Datenbank eines Microsoft Windows Computers gehalten werden, in Echtzeit
- Passwort-Synchronisation in Echtzeit
- Voll-Import von Accounts, Gruppen und Gruppenmitgliedschaften
- Arbeitet mit Microsoft Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 und Windows 7 (64-Bit) und Windows 10
- Fehlerberichte und Tracing
- Das Konnektor Bundle wird in einem .NET-basierten OpenICF Connector Server eingesetzt, der auf einem beliebigen Windows Server läuft
- Läuft auf allen Microsoft Windows Plattformen, die vom OpenICF Connector Server unterstützt werden.

Weitere DirX-Produkte

Die DirX-Produktfamilie bietet die Basis für ein vollständig integriertes Identity- und Access-Management; zur DirX-Produktfamilie gehören auch folgende Produkte, die separat bestellt werden können:

- DirX Directory stellt einen standardkonformen, leistungsstarken, hochverfügbaren, sehr zuverlässigen und sicheren LDAP und X.500 Directory Server und LDAP Proxy mit sehr hoher linearer Skalierbarkeit zur Verfügung. DirX Directory kann als Identity-Datenhaltung für Informationen über Mitarbeiter, Kunden, Geschäftspartner, Abonnenten von Diensten sowie über andere Teilnehmer von eBusiness-Verfahren dienen.
- DirX Access ist eine umfassende, Cloud-fähige, skalierbare und hochverfügbare Access Management Lösung, die Policy-basierte Authentifizierung, Autorisierung und Federation für Web-Applikationen und -Services bietet. DirX Access bietet Single Sign-On, vielfältige Authentisierungsmöglichkeiten, Identity Federation basierend auf SAML, OAuth und OpenID Connect, Just-in-Time Provisioning, Entitlement Management und die Durchsetzung von Sicherheits-Policies für Anwendungen und Dienste in der Cloud oder intern.
- DirX Audit DirX Audit bietet Auditoren, Sicherheitsbeauftragten und Administratoren analytischen Einblick und Transparenz in Identity und Access Management Prozesse. Mit historischen Identitätsdaten und aufgezeichneten Aktivitäten aus den Identity und Access Management Prozessen ermöglicht DirX Audit die Beantwortung der „Was, Wann, Wo, Wer und Warum"-Fragen bei Benutzerzugriffen und -berechtigungen. DirX Audit bietet historische Ansichten und Reports auf Identitätsdaten, ein grafisches Dashboard, einen Monitor für Identitäts-bezogene Aktivitäten und die Verwaltung von Jobs für die Reporterstellung. Mit seinen Analyse-Funktionen unterstützt DirX Audit Unternehmen und Organisationen bei der nachhaltigen Einhaltung von Compliance-Anforderungen und stellt Business Intelligence für die Identity und Access Management Prozesse bereit.

Tabelle 1 - DirX Identity Business Suite, Pro Suite, Password Management Option Überblick

	Pro Suite	Business Suite	Password Management Option
Web-basierter User Self-Service via Web Center	**Ja**	**Ja**	**-**
- Verwalten eigener Daten	Ja	Ja	-
- Verwalten eigener Passwörter	Ja	1)	-
- Verwalten von Delegationen	Ja	-	-
- Anfordern von Rollen	Ja	3)	-
Delegierte Administration via Web Center	**Ja**	**-**	
Passwort-Management	**Ja**	**Ja**	**Ja**
- Passwort Policies	Ja	-	Ja
- Passwort-Änderung durch Endbenutzer via Web Center	Ja	-	Ja
- Passwort-Änderung durch Endbenutzer für Untermenge ihrer Accounts	-	-	Ja
- Anzeigen des Passwort-Änderungsstatus	-	-	Ja
- Challenge/Response-Verfahren zum Rücksetzen vergessener Passwörter (Self-Service)	Ja	-	Ja
- Challenge/Response-Verfahren zum Rücksetzen vergessener Passwörter (über Administrator oder Service-Desk)	-	-	Ja
- Administratives Rücksetzen von Passwörtern	Ja	-	Ja
- Windows Password Listener	2)	2)	2)
- Passwort-Synchronisation in Echtzeit	Ja	Ja	Ja
- Passwort Reset Client für Windows	-	-	Ja
Benutzerverwaltung	**Ja**	**Ja**	**-**
- Verwalten von Benutzern	Ja	Ja	-
- Verwalten von Personas	Ja	-	-
- Verwalten von User Facets	Ja	-	-
- Verwalten von Funktionsbenutzern	Ja	-	-
Rollen-Verwaltung	**Ja**	**Ja**	**-**
- Verwalten von Accounts	Ja	Ja	-
- Verwalten von Gruppen	Ja	Ja	-
- Verwalten von Berechtigungen und Berechtigungsparametern	Ja	-	-
- Verwalten von Rollen und Rollenparametern	Ja	-	-
- Funktionstrennung (Segregation of Duties)	Ja	-	-
Business-Objekt-Verwaltung	**Ja**	**Ja**	**-**
Antrags-Workflows, Genehmigung und Wiedergenehmigung	**Ja**	**-**	**-**
Risikomanagement	**Ja**	**-**	**-**
Berechtigungsprüfung	**Ja**	**-**	**-**
Unterstützung von Outsourcing-Einsatzszenarien	**Ja**	**Ja**	**-**
- Verwaltung privilegierter Accounts	Ja	Ja	-
- Workflows für Gruppen von Zielsystemen	Ja	Ja	-
Policy-Verwaltung	**Ja**	**Ja**	**-**
- Access-Policies	Ja	Ja	-
- Audit-Policies	Ja	-	-
- Provisioning-Policies für Gruppen	Ja	Ja	-
- Provisioning-Policies für Rollen und Berechtigungen	Ja	-	-
- Validierungs-Policies	Ja	Ja	-
- Konsistenz-Policies	Ja	Ja	-
Provisioning	**Ja**	**Ja**	**-**
- Policy-/Regel-basierte Zuweisung von Gruppen zu Benutzern	Ja	Ja	-
- Policy-/Regel-basierte Zuweisung von Berechtigungen/Rollen zu Benutzern	Ja	-	-
- Manuelle Zuweisung von Gruppen zu Benutzern	Ja	Ja	-
- Manuelle Zuweisung von Berechtigungen/Rollen zu Benutzern	Ja	-	-
- Vererbung von Gruppen von Business-Objekten an Benutzer	Ja	Ja	-
- Vererbung von Berechtigungen/Rollen von Business-Objekten an Benutzer	Ja	-	-
- Real-Time Provisioning von Accounts und Gruppen in Zielsystemen	Ja	Ja	-

1) statt über Web Center mit Windows Password Listener über die Tools/Schnittstellen von Microsoft Windows
2) Erfordert DirX Identity Microsoft Connectivity Package
3) Gruppen stattdessen

Tabelle 2 - DirX Identity Business Suite, Pro Suite, Password Management Option Überblick - Fortsetzung

	Pro Suite	Business Suite	Password Management Option
Service Management Unterstützung	Ja	Ja	-
Metadirectory	Ja	Ja	-
- Default Applications	Ja	Ja	-
- Bidirektionale Synchronisation von strukturierten. Files (XML, LDIF, DSML, CSV)	Ja	Ja	-
Audit-Services	Ja	Ja	-
- Reports über Benutzer, Accounts, Gruppen	Ja	Ja	-
- Reports über Zielsysteme, Delegationen, Access Policies, Regeln	Ja	Ja	-
- Reports über Rollen und Berechtigungen	Ja	-	-
- Audit Trail von administrativen Änderungen in DirX Identity	Ja	-	-
- Audit Trail von Passwortänderungen und Passwortabfragen	Ja	-	-
- Audit Trail von Web Center Login/Logout	Ja	-	-
- Validierung und Abgleich von Zielsystemen	Ja	Ja	-
Domänen-Verwaltung	Ja	Ja	-
Konnektivität	Ja	Ja	-
Identity Manager	Ja	Ja	-
Business User Interface	Ja	Ja	
Web Center	Ja	Ja	4)
Java- and C++-basierter Identity Server	Ja	Ja	-
Web Services	Ja	Ja	-
Identity Integration Framework	Ja	Ja	-

4) Nur mit Password Management Funktionalität

Technische Voraussetzungen für DirX Identity V8.7

Hardware

- Intel Server-Plattform für Microsoft Windows Server 2012 R2/2016 (LTSC), Red Hat Enterprise Linux, SUSE Linux Enterprise Server

Speicherbedarf:

Hauptspeicher:	mindestens 8 GB
Plattenspeicher:	mindestens 4 GB plus Plattenspeicher für Daten

Software

DirX Identity wird auf folgenden Plattformen unterstützt, wobei für die gewählte Plattform die aktuellsten Patches/Service Packs erforderlich sind:

- Microsoft Windows Server 2012 R2 (x86-64 Intel-Architektur)
- Microsoft Windows Server 2016 LTSC (x86-64 Intel-Architektur)
- Red Hat Enterprise Linux 7 (x86-64)
- SUSE Linux Enterprise Server 12 (x86-64)
- Microsoft Windows 7 (x86-64), nur Client-komponenten Identity Manager, Client Signature.

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

Unterstützung virtueller Maschinen:

- VMWare ESXi 6.0, in Kombination mit den oben genannten Gast-Betriebssystemen, die für VMWare ESXi 6.0 freigegeben sind

Hinweis: Die C++-basierten Komponenten von DirX Identity laufen als 32-Bit Anwendung auf 64-Bit Plattformen, Die Java-basierten Komponenten von DirX Identity laufen als 64-Bit Anwendung auf 64-Bit Plattformen.

Für den DirX Identity Store

- DirX Directory V8.5/V8.6

Für DirX Identity Web Center/Web Admin

- Microsoft Internet Explorer 11
- Mozilla Firefox 52 oder neuer
- Google Chrome 62 oder neuer (Request Signing via Java Applet ist nicht unterstützt)
- Microsoft Edge 40 oder neuer (Request Signing via Java Applet ist nicht unterstützt)

Für DirX Identity Approvals App

- iOS 9/10/11

Für DirX Identity Business User Interface

- Mozilla Firefox 52 oder neuer
- Google Chrome 62 oder neuer
- Microsoft Edge 40 oder neuer

Für DirX Identity Manager

- Für die Smartcard-Unterstützung: Atos CardOS API V5.3 in Kombination mit Smartcards, die von Atos CardOS API V5.3 unterstützt werden.

Für OpenICF Connector Bundles

- Für Unix: Eine OpenICF Java Connector Server Installation, Version 1.1.1.0 oder neuer
- Für Windows Local Accounts. Eine OpenICF .NET Connector Server Installation, Version 1.4.0.0 oder neuer

Für Nagios-Unterstützung

- Nagios Core Version 4.0.8
- JNRPE Server Version 2.0.5
- JNRPE Plugins Version 2.0.3

Benutzeroberfläche

Englisch

Web Center: Englisch / Deutsch / kundenspezifisch anpassbar

Dokumentation

Manuale und Use Case Dokumente werden in Englisch bereitgestellt.

Manuale:

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

Use Case Dokumente

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

www.evidian.com

Atos