

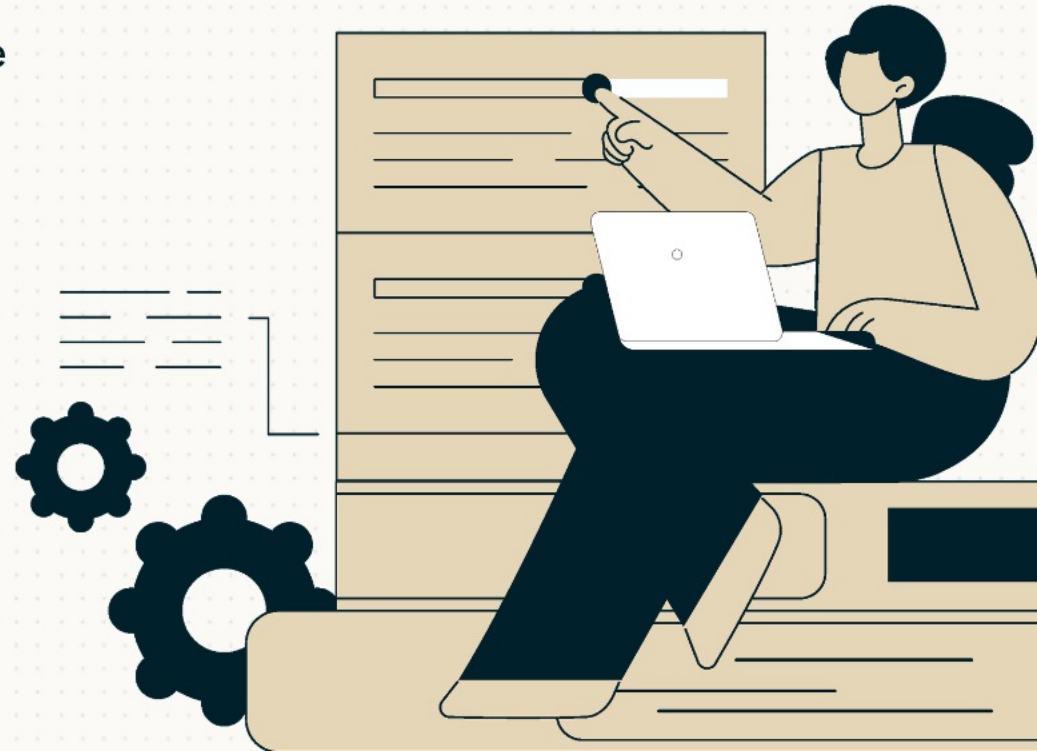
Boost your organization's security and centralize management with Identity360

A cloud-native identity platform for workforce IAM



Outline

- Identity360's vision
- Critical IAM challenges for enterprises
- Identity360 solutions
- Universal Directory
- Integrations
- Life cycle management
- Single sign-on (SSO)
- Multi-factor authentication (MFA)
- Access management
- Delegation
- Reports and identity analytics
- Identity360 architecture
- Identity360 licensing



Identity360's vision

Unify identity silos, streamline
identity management, and secure
resources with centralized access
management

Critical IAM challenges for enterprises



Identity fragmentation

Enterprises often struggle with managing multiple user identities across various platforms, leading to inefficiencies and security risks



Complex identity life cycle management

Managing the entire identity life cycle, from onboarding to offboarding, can be challenging and error-prone for enterprises.



Increased IT costs

The lack of scalability and flexibility in managing access requirements can result in higher infrastructure costs as organizations struggle to adapt to changing business needs

Identity360 solutions



Universal Directory



Life cycle management



Single sign-on (SSO)



Multi-factor authentication (MFA)



Access management



Delegation



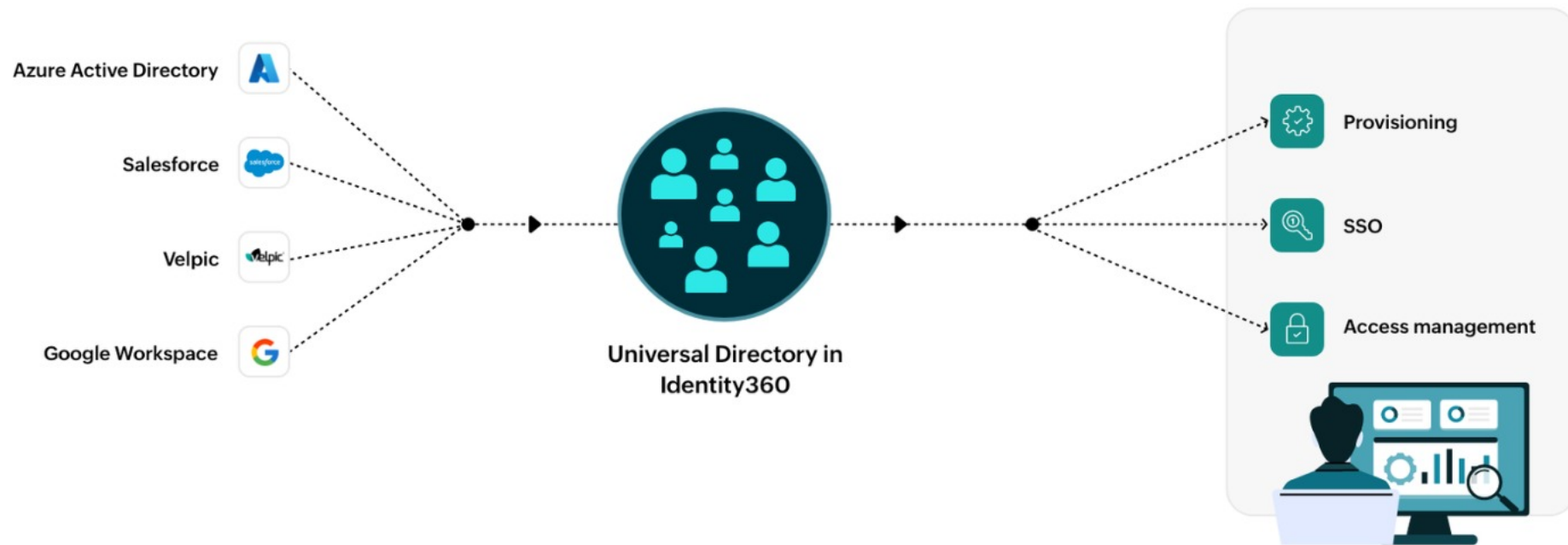
Reports and identity analytics

Identity360 solutions

Universal Directory

Consolidate identity silos into a single source of truth and enable centralized identity management with our cloud directory

How does Universal Directory work?



Unlock efficient directory services with Universal Directory



Unified solution

Leverage Universal Directory to consolidate identities from multiple platforms



Cost saving

Centralize identity management and streamline access control to achieve significant cost savings by reducing manual processes and errors



Efficiency gains

Effortlessly gather precise information from all your integrated directories with preconfigured reports

Unify users from multiple directories and applications, providing a single point of access management

The screenshot shows the 'Universal Directory' dashboard. At the top, there are two tabs: 'Dashboard' and 'Universal Directory'. On the left, a sidebar menu lists the following options: 'Universal Directory', 'All Users', 'All Groups', 'Orchestration', 'User Creation Templates', 'Directory Integration', 'Manage Directory', and 'Directory Sync Settings'. The main content area features two cards. The first card is for 'Azure Directory', featuring the Azure logo, a description of Azure Active Directory as Microsoft's cloud-based identity and access management service, and a 'Configure' button. The second card is for 'Salesforce', featuring the Salesforce logo, a description of Salesforce as a leading CRM platform, and a 'Configure' button.

Dashboard **Universal Directory**

Universal Directory

- All Users
- All Groups
- Orchestration
- User Creation Templates
- Directory Integration**
 - Manage Directory
 - Directory Sync Settings

Azure Directory

Azure Active Directory is Microsoft's cloud-based identity and access management service, allowing organizations to securely manage user identities and enable single sign-on to various applications and resources.

Configure

Salesforce

Salesforce is a leading customer relationship management (CRM) platform that helps businesses manage customer interactions, streamline processes, and drive growth through cloud-based applications and services.

Configure

Integrate with our roster of applications including Slack, Zendesk, Google Workspace, Jira, Zoho People, and more



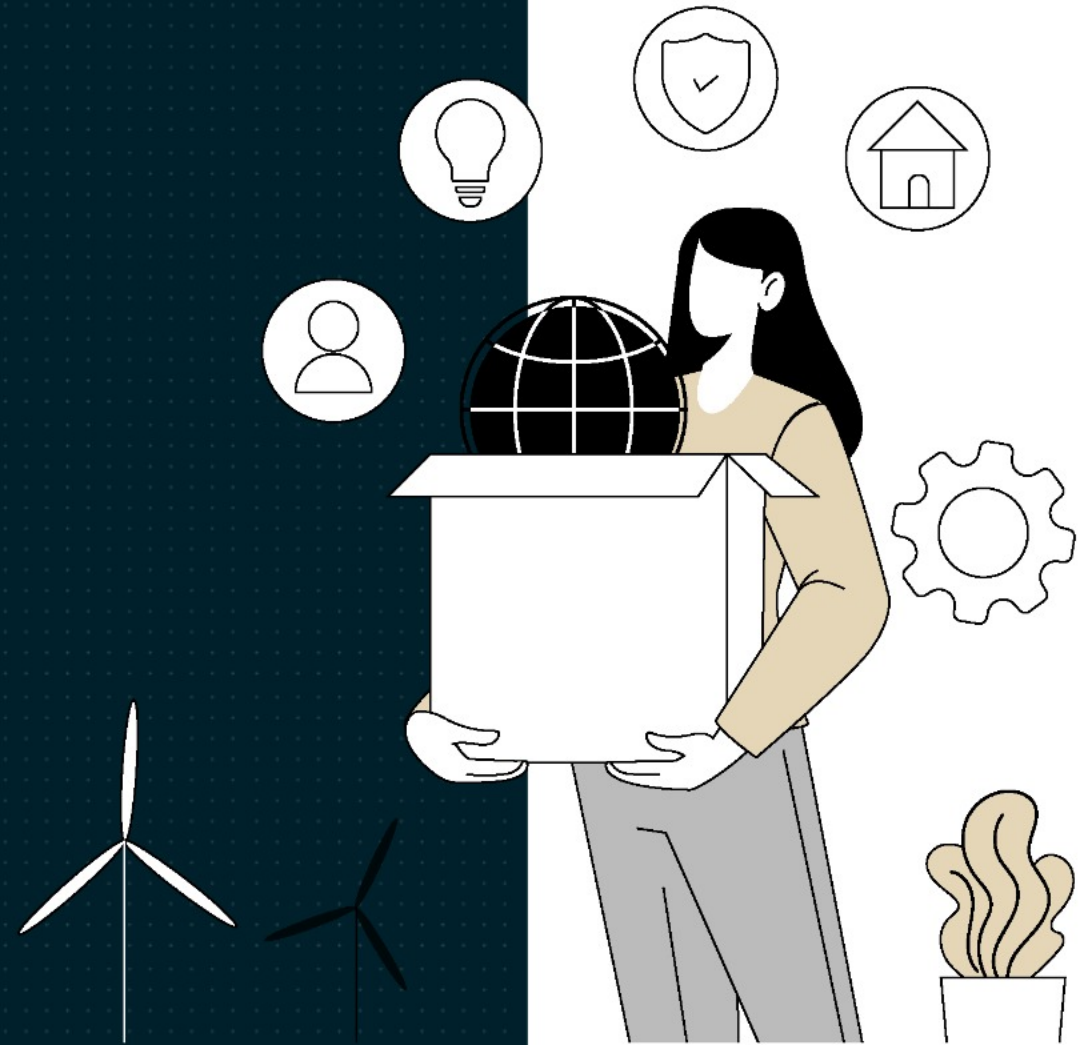
Universal Directory use case

Problem

Organization faces identity management challenges due to fragmented sources across directories and applications, causing operational inefficiencies.

Solution

Implement Universal Directory to centralize identity management and consolidate sources into a single, cloud-based directory. Gain a unified view of identities for streamlined access control.

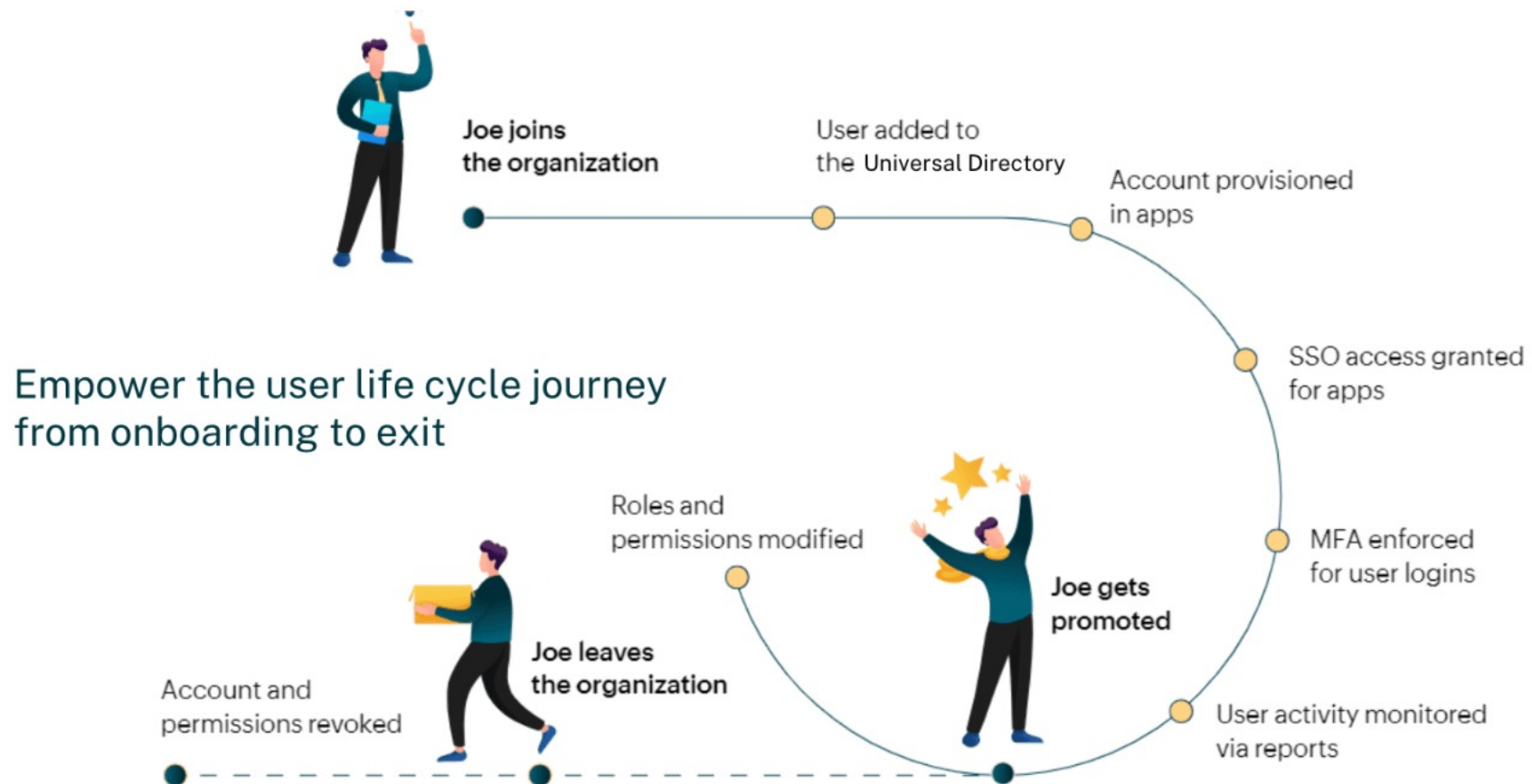


Identity360 solutions

Life cycle management

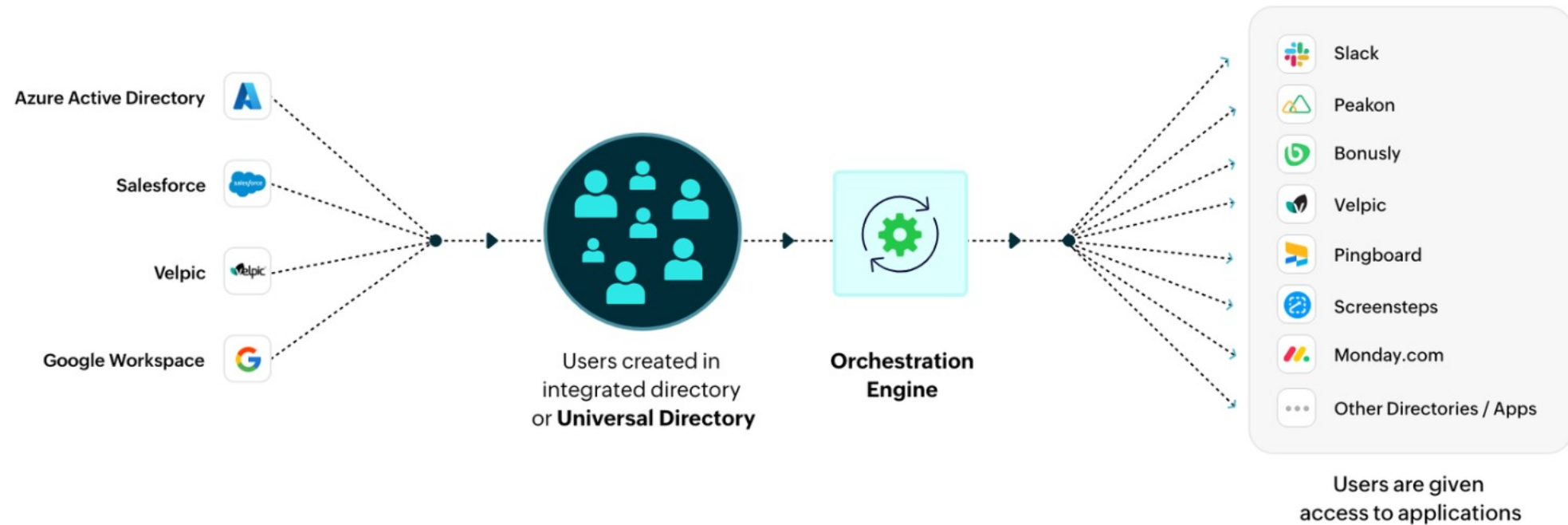
Enhance workforce productivity by seamlessly managing the complete life cycle of digital identities

Identity life cycle management breakdown



Orchestration

Streamline IAM processes with centralized cloud orchestration



Universal Directory

All Users
All Groups

Orchestration

User Creation Templates

Directory Integration

Manage Directory
Directory Sync Settings

Create New Profiles

Profile Name * User Onboarding Profile Description

Action executed/synced in Universal Directory

Choose Action User Created

Profile Criteria

1. Member Of In User Onboarding Group
 2. AND Office Is not Empty
 3. Created Date On 2024/01/01 12:00:00 AM
 4. AND Is Active Is True
 5. AND Title Contains Employee
- Criteria Pattern : (1 & 2) | (3 & 4 & 5)

Add conditions based on which tasks should be executed

Orchestrate events across external applications from a single interface

Action to be performed in other directories/applications

Choose Action Create User

Action will be performed in the below selected directories/applications

- GSuite Google User Creation Template
- id360.onmicrosoft.com AAD Onboarding Template
- Salesforce Salesforce Onboarding Template
- Velpic Velpic User Creation Template

Receive notifications when the orchestration occurs

Enable Notification

Select Template Employee Onboarding Notification

Smart templates

Speed up your onboarding process with smart templates



Generate common
templates



Automate
management with
Orchestration



Utilize customized
templates in orchestration
profiles



Successful user

☒ Active Directory
admanagerplus.com
 ☒ Microsoft 365
adselfservice.onm...
 ☒ Azure Active Directory
gcp.google.com
 ☒ Ultipro
ultipro.com
 [10 more](#)
[+ Add More](#)
[Copy User Attributes](#)
[Disable Drag-n-Drop](#)
[Creation Rules](#)

Active Directory

General

General

First name

Last Name

Email

Role

Profile

Alias

Date Of Birth

Phone

Mobile

Website

Fax

Account

Contact

Exchange

Custom Attributes

Microsoft 365

Applications

General

Account

Contact

Exchange

Remote Mailbox

Microsoft 365

Google Workspace

General

First Name

Initials

Logon Name*

Logon Name*
(Pre-Windows 2000)

Full Name*

Display Name

Employee ID

Description

Telephone number

Email

Web page

Select container

First Name + Last Name

@

admanagerplus.com

eg. johnsmith@admanagerplus.com

admanagerplus\

Same as Logon Name

eg. johnsmith@admanagerplus.com

Same as Logon Name

1

G

+3

OU=ZOH0,OU=Users, OU=All...

Set up rules that assign values to fields when they match a specified criteria

Effortlessly craft customizable templates tailored to various departments using the drag-and-drop interface

Reap the benefits of managing your identities throughout their entire life cycle with life cycle management

Operational efficiency

Automate the entire identity life cycle process by streamlining administrative tasks, thereby reducing the burden on IT administrators, minimizing the risk of errors, and improving overall operational efficiency



Reduced risk of errors

Reduce the likelihood of manual errors that can occur during user onboarding, offboarding, and role changes, ensuring data accuracy and consistency across all integrated platforms.



Customizable templates

Utilize predefined templates with intuitive creation rules for quick and easy user onboarding



Life cycle management use case

Problem

An organization is managing the identity life cycle for a diverse workforce. Traditional processes don't keep up with employee turnover and profile changes. These challenges result in time-consuming, error-prone onboarding and offboarding, leading to security gaps and compliance concerns

Solution

Implementing identity life cycle management enhances agility and security, ensuring regulatory compliance and aligning employee engagements with legal standards. This fosters sustainable growth in today's dynamic business landscape

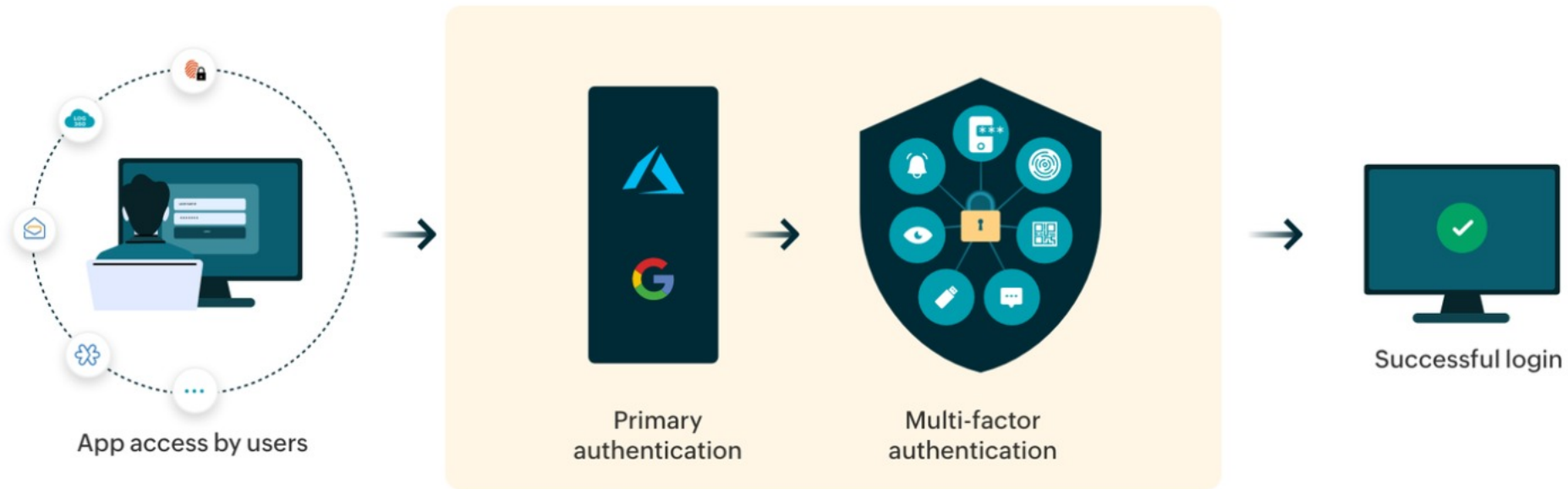


Identity360 solutions

Single sign-on (SSO)

Streamline access to enterprise resources with secure SSO

How does SSO work?



Elevate user experience with secure passwordless login and seamless SSO



Increase employee productivity

Provide one-click access to enterprise apps and reduce password fatigue by eliminating traditional passwords and time-consuming login processes.



Broad spectrum of supported apps

Enable SSO to over 450 pre-integrated enterprise applications, or any custom application that supports federation standards, in a few steps



Secure user access

Mitigate security threats by empowering IT teams to promptly disable access to accounts in the event of theft or unauthorized access

Application Integration

















SSO can be enabled easily for a myriad of pre-integrated applications

Easily integrate your own custom applications for end-user SSO

Search Application

1 - 25 of 401

25

 <p>Azure Active Directory Directory</p> <p>Import/Sync SSO Provisioning</p>	 <p>Slack Directory IT Management</p> <p>SSO</p>	 <p>Salesforce Directory</p> <p>Import/Sync SSO Access Management Provisioning</p>	 <p>Zendesk CRM</p> <p>SSO</p>
 <p>Google Workspace Messaging Apps</p> <p>Import/Sync SSO Access Management Provisioning</p>	 <p>Dropbox Messaging Apps</p> <p>SSO</p>	 <p>PagerDuty Messaging Apps</p> <p>SSO</p>	 <p>PlanMyleave Messaging Apps</p> <p>SSO</p>
 <p>Sumo Logic Code Analytical Tools</p> <p>SSO</p>	 <p>JitBit Collaboration</p> <p>SSO</p>	 <p>AppDynamics Messaging Apps</p> <p>SSO</p>	 <p>Panorama9 HR Management</p> <p>SSO</p>
 <p>Velpic Customer Support</p> <p>Import/Sync SSO Access Management Provisioning</p>	 <p>Egnyte Messaging Apps</p> <p>SSO</p>	 <p>Canvas LMS by Instructure Customer Support</p> <p>SSO</p>	 <p>Flutter Files Messaging Apps</p> <p>SSO</p>

+ Custom Application Application Connection < Back

SSO use case

Problem

A large enterprise faces challenges managing access to numerous applications. Employees waste time navigating multiple login screens, causing inefficiencies and frustration

Solution

Implementing SSO improves efficiency, granting employees one-click entry to multiple enterprise apps, cutting login friction, and enhancing productivity

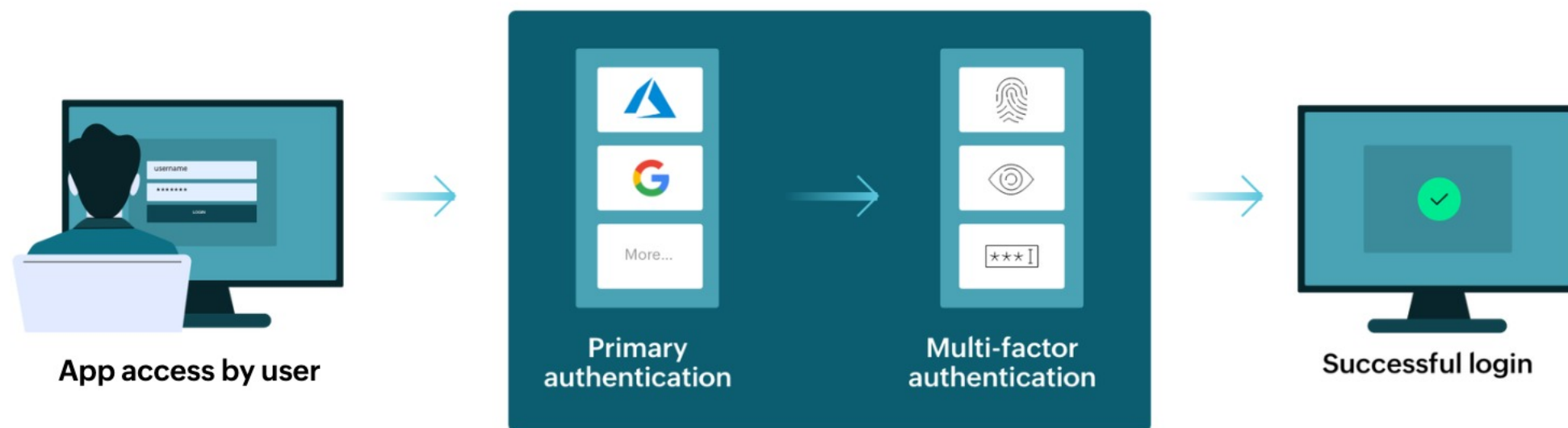


Identity360 solutions

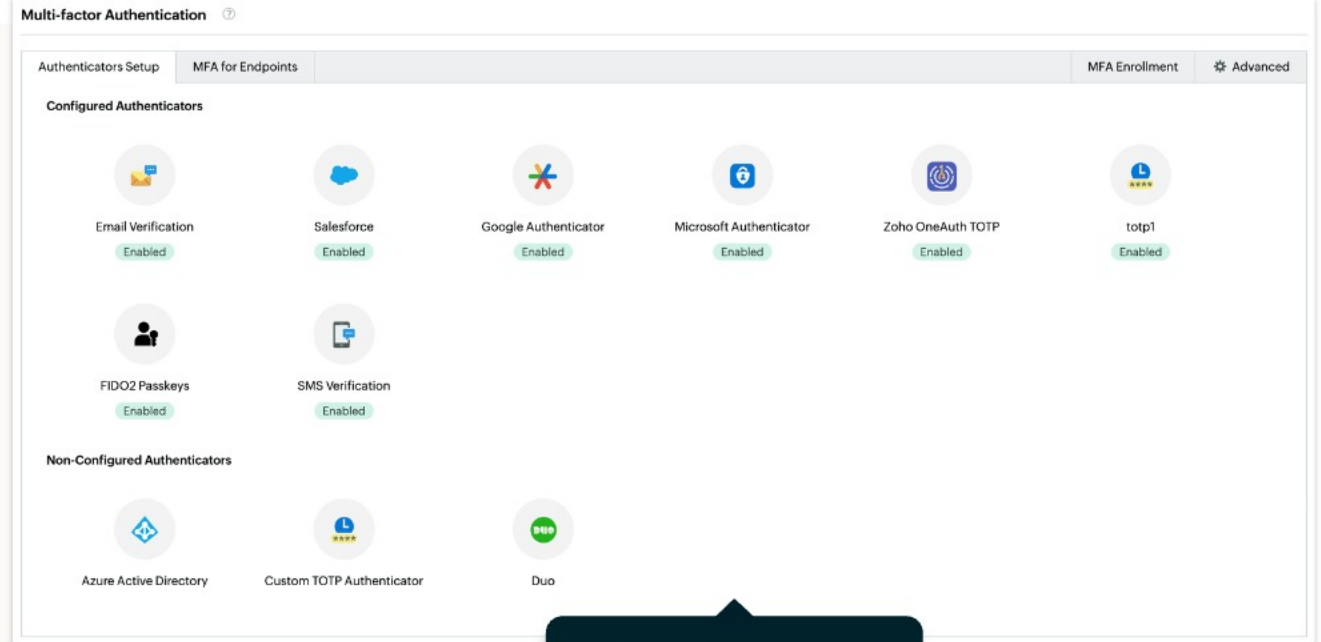
Multi-factor authentication

Secures access to enterprise applications with MFA

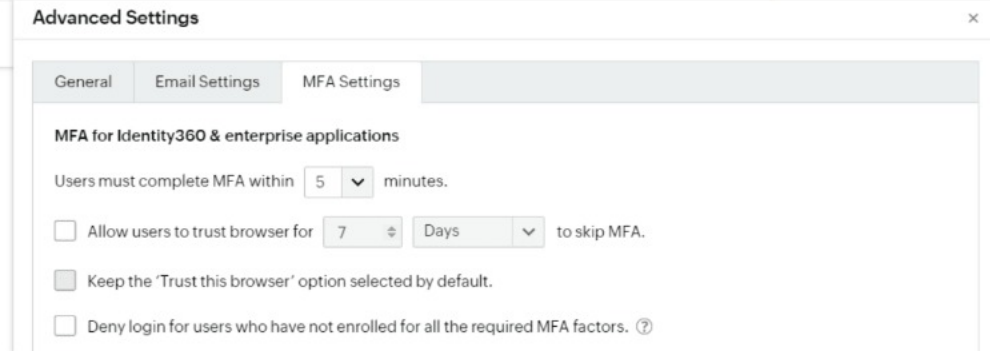
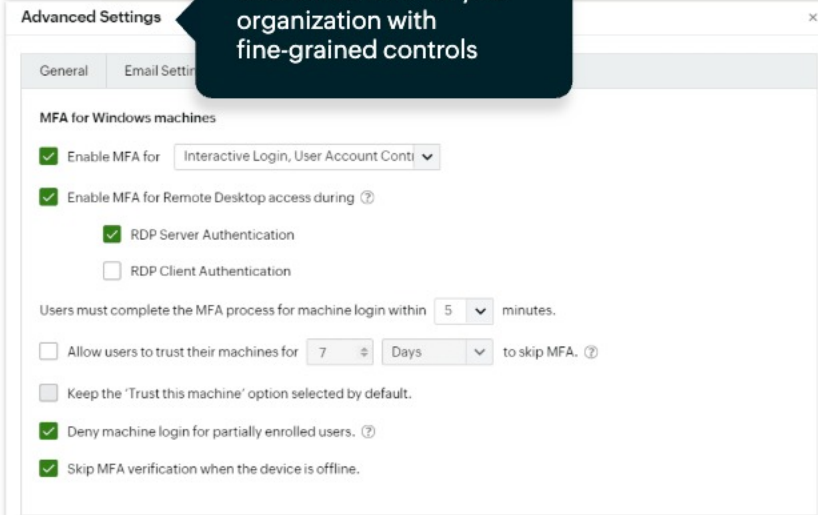
How MFA works



Customize MFA for your organization with fine-grained controls



Choose from a variety of MFA authenticators to verify users' identities



Secure identities with multi-factor authentication



Compatible with multiple directories

Choose your preferred directory for primary authentication—like Azure AD, Google, and Salesforce—which your users may already be a part of



An interactive, user-friendly UI

Makes MFA configuration and enrollment easy for admins and end users respectively, with a simple and easy-to-understand UI



Security against cyberthreats

Defend against various credential-based attacks, including those targeting UAC, Windows login, RDP, VPN and RADIUS-supporting endpoints while ensuring seamless application access to employees

MFA use case

Problem

A corporation in diverse sectors faces growing cybersecurity threats to sensitive data. Traditional password-based authentication methods used for Windows login are vulnerable to phishing and breaches, posing significant security risks

Solution

Implementing MFA for Windows login strengthens the organization's security by enhancing security during logins to Windows machines, RDP sessions, and UAC prompts. This multi-layered authentication adds robust protection against unauthorized access



Identity360 solutions

Access management

Secure and ensure that the right users have the right access consistently across resources

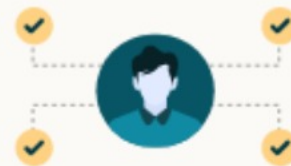
How does access management work?



User
creation



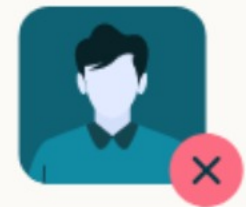
User
onboarding



SCIM-based resource
provisioning



User role
change



User
offboarding

Cross-platform access management capabilities



Improved compliance

Ensure compliance with regulatory requirements and industry standards related to data protection and privacy



Enhanced user experience

Users experience seamless and convenient access to the resources they need, leading to higher satisfaction and improved user experience



Security against cyberthreats

Safeguard against unauthorized access attempts and mitigate the risk of various cyberthreats, while also providing easy application access to employees

Within each app, you can fine-tune users' access rights by assigning them relevant roles and permissions in bulk

Application Access Management

Select Application: Salesforce

1 Add user details 2 Access Management 3 Status

Refine Search

	First Name	Last Name	Full Name	Username	Email
<input type="checkbox"/>	Regina	Peters	Regina Peters	reginapeters@testmail.com	reginapeters@testmail.com
<input type="checkbox"/>	Rocky	Arnold	Rocky Arnold	rockyarnold@testmail.com	rockyarnold@testmail.com
<input type="checkbox"/>	Juliet	Ford	Juliet Ford	julietfords@testmail.com	julietfords@testmail.com
<input type="checkbox"/>	Wilona	Nelson	Wilona Nelson	wilonanelson@testmail.com	wilonanelson@testmail.com

Application Access Management

Select Application: Salesforce

1 Add user details 2 Access Management 3 Status

Account

Account Permission

Profile: Salesforce API Only System Integrati...

Role: APAC role

Permission set: X00ex00000018ozh_128_09_04_12_1

Application Access Management

Select Application: Salesforce

1 Add user details 2 Access Management 3 Status

Refresh

First Name	Last Name	Full Name	Username	Email	Provisioning Status
Regina	Peters	Regina Peters	reginapeters@testmail.com	reginapeters@testmail.com	Assignment is pending
Wilona	Nelson	Wilona Nelson	wilonanelson@testmail.com	wilonanelson@testmail.com	Assignment is pending

Provides enhanced tracking capabilities for admins using consolidated tables showing users' access assignment statuses for each application

Access management use case

Problem

An organization handles extensive customer data, including personal information and payment details. With rising cyberthreats, securing access to this sensitive data is vital to preserving customer privacy and trust in the brand

Solution

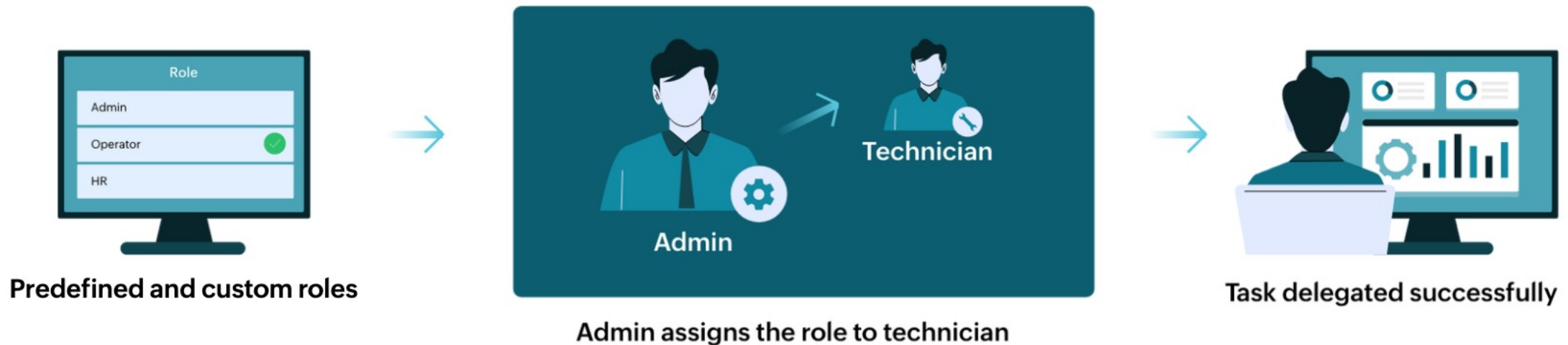
Implementing access management provides robust control over data access while adhering to regulatory requirements such as the GDPR and the PCI DSS. This is achieved through tailored access controls that align with the organization's structure and operational needs



Delegation

Entrust routine tasks to non-admin users without altering their inherit permissions, allowing admins to focus on critical tasks

How does help desk delegation work?



Adopt **delegation** to transform your IT support environment



Reduced workload

Decrease the workload for IT admins by delegating management tasks to technicians, mitigating burnout and boosting job satisfaction



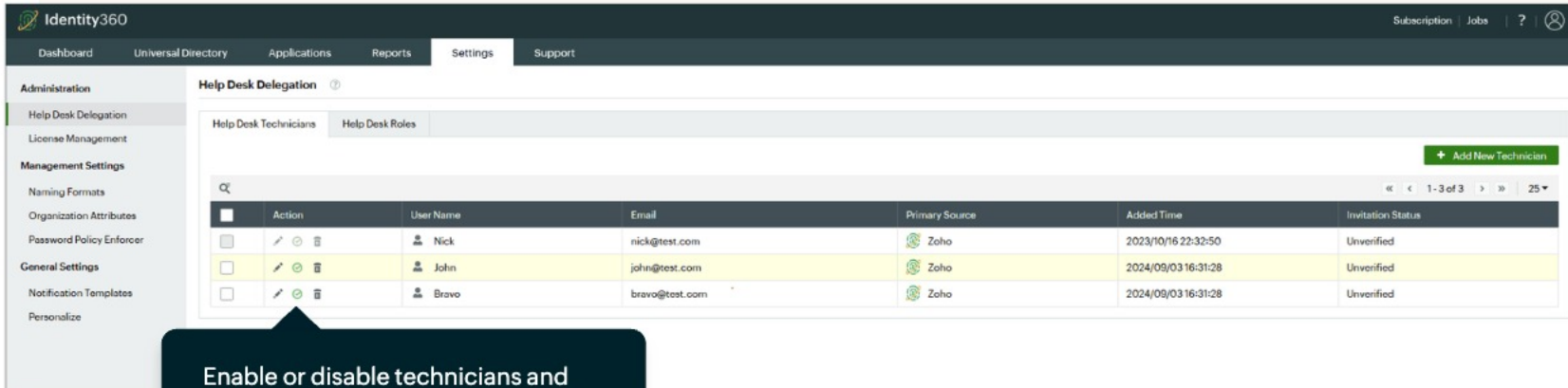
Improved responsiveness

Enable quicker response times to user inquiries and technical issues by assigning specific tasks to designated team members



Scalability and flexibility

Adapt to changing workload demands and scale operations as needed, ensuring continued efficiency and effectiveness in providing support services

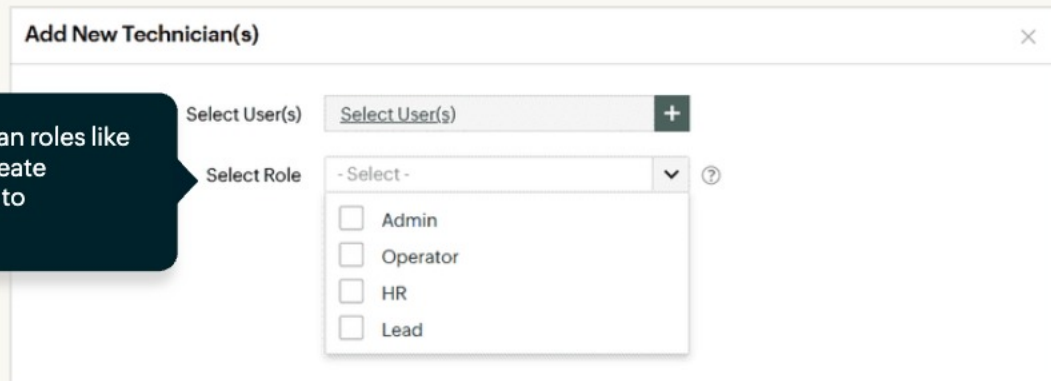


The screenshot shows the Identity360 web interface. The top navigation bar includes 'Dashboard', 'Universal Directory', 'Applications', 'Reports', 'Settings', and 'Support'. The left sidebar lists 'Administration' (Help Desk Delegation, License Management), 'Management Settings' (Naming Formats, Organization Attributes, Password Policy Enforcer), 'General Settings' (Notification Templates, Personalize), and 'Personalize'. The main content area is titled 'Help Desk Delegation' and has tabs for 'Help Desk Technicians' and 'Help Desk Roles'. A green '+ Add New Technician' button is in the top right. Below it is a table with columns: Action, User Name, Email, Primary Source, Added Time, and Invitation Status. The table contains three rows of technicians.

Action	User Name	Email	Primary Source	Added Time	Invitation Status
<input type="checkbox"/>	Nick	nick@test.com	Zoho	2023/10/16 22:32:50	Unverified
<input type="checkbox"/>	John	john@test.com	Zoho	2024/09/03 16:31:28	Unverified
<input type="checkbox"/>	Bravo	bravo@test.com	Zoho	2024/09/03 16:31:28	Unverified

Enable or disable technicians and modify the delegated roles from the central console

Choose predefined technician roles like the Admin or Operator, or create custom roles to be assigned to non-admin users



The 'Add New Technician(s)' dialog box contains two main fields: 'Select User(s)' with a 'Select User(s)' button and a '+' icon, and 'Select Role' with a dropdown menu. The dropdown menu is open, showing a list of roles with checkboxes: Admin, Operator, HR, and Lead.

Select User(s) +

Select Role ?

- ☐ Admin
- ☐ Operator
- ☐ HR
- ☐ Lead

Create custom technician roles to suit your organization's needs and manage the permissions required to carry out specific tasks

Untitled Role Description Create Role Cancel

☒ Universal Directory Applications Reports Settings

User Management Deselect All

- ☒ All Users
- ☒ Single User management
- ☒ Create User
- ☒ Modify User +
- ☒ Bulk User Management
- ☒ Delete Users
- ☒ Enable/Disable Users
- ☒ Modify UD Group Members
- ☒ Change Primary Source
- ☒ Create Users In Apps

Group Management Deselect All

- ☒ All Groups
- ☒ Single Group Management
- ☒ Create Group
- ☒ Modify Group
- ☒ Bulk Group Management
- ☒ Delete Groups

Directory Management Deselect All

- ☒ Directory Integration
- ☒ Manage Directory
- ☒ Directory Sync Settings

Others Deselect All

- ☒ Orchestration Profile
- ☒ Templates
- ☒ User Creation Templates

Identity360 Subscription Jobs ?

Dashboard Universal Directory Applications Reports Settings Support

Administration

- Help Desk Delegation
- License Management
- Management Settings
 - Naming Formats
 - Organization Attributes
 - Password Policy Enforcer
- General Settings
 - Notification Templates
 - Personalize

Help Desk Delegation ?

Help Desk Technicians Help Desk Roles

+ Create New Role

<input type="checkbox"/>	Action	Role Name	Role Description	Associated Technicians
<input type="checkbox"/>		Super Admin	Default Organization's Super Admin	Nick
<input type="checkbox"/>		Operator	Is capable of auditing the operations within the application.	John
<input type="checkbox"/>		Admin	Holds full control, except for the ability to modify the product's subscription.	Bravo
<input type="checkbox"/>		Lead	-	-
<input type="checkbox"/>		HR	-	-

1-5 of 5 25

Help desk delegation use case

Problem

A large corporation heavily relies on its IT support team for user inquiries, technical issues, and service requests. However, a surge in support tickets and limited resources strain the IT department's efficiency and responsiveness

Solution

Implementing a help desk delegation system streamlines operations and boosts service delivery. Technicians are assigned specific tasks, with access easily managed and revocable ensuring efficient handling for timely issue resolution

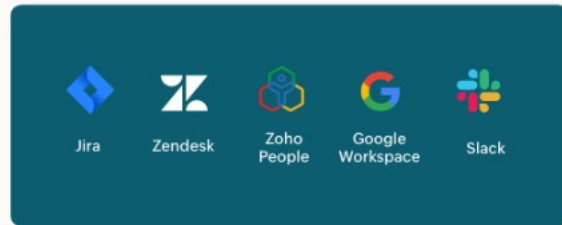


Identity360 solutions

Reports and identity analytics

Gain insights into application access, user activities, account status, and more to make informed decisions

How do reports and identity analytics work?



Administrators assign specific applications to user based on their roles and responsibilities within the organization



Users gain access to assigned applications.



Unlock superior access insights to boost your organization's security and efficiency



Enhanced visibility

Gain enhanced visibility into user activities and behaviors through comprehensive reports



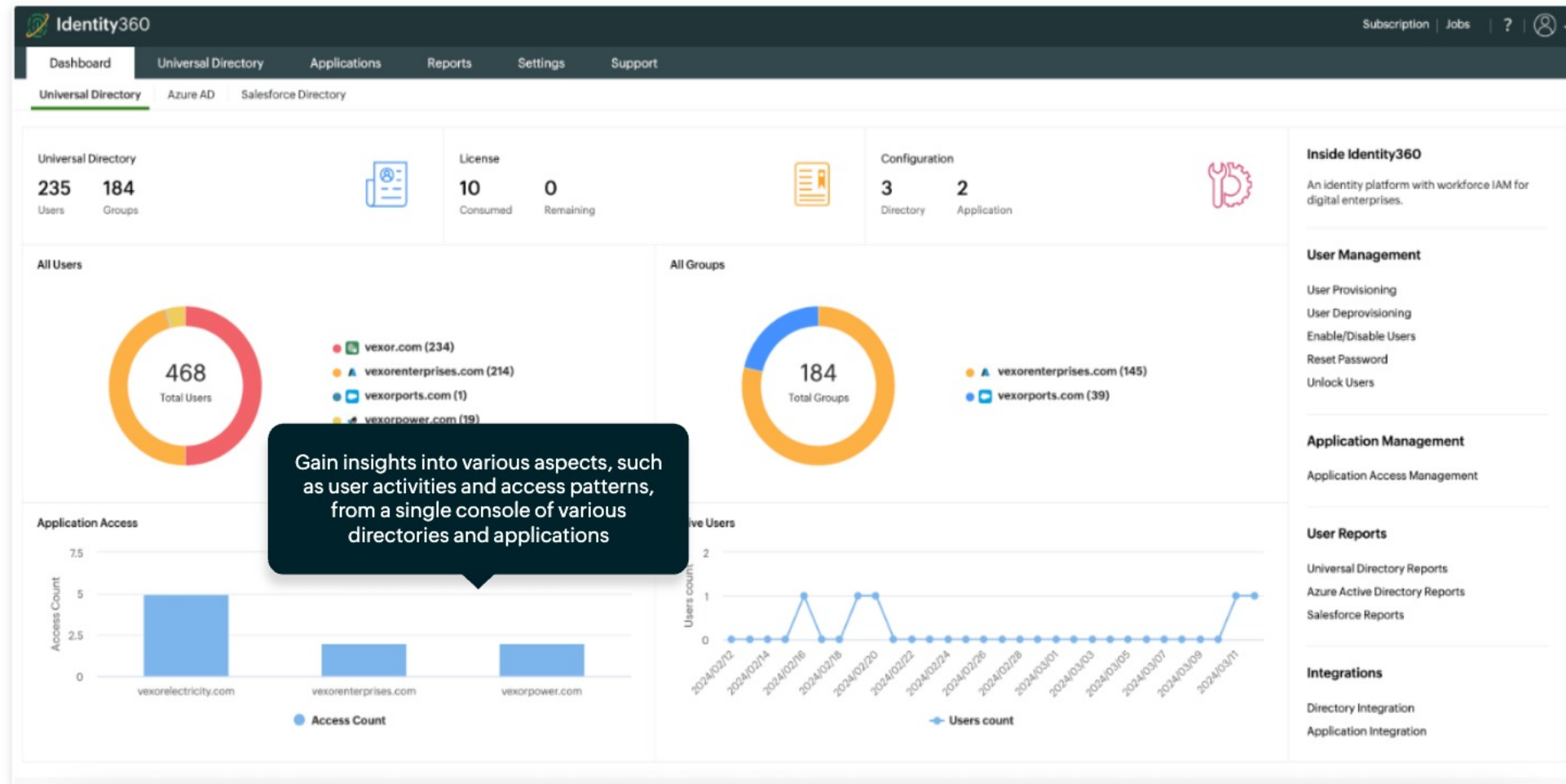
Informed decisions

Enable admins to make informed decisions based on real-time data and user interactions



Prebuilt reports

Access prebuilt reports to help admins identify security risks and understand end-user application and service consumption patterns



Soon To Expire Passwords

Azure AD Tenant: tester1695outlook.onmicrosoft.com

Filter By: -Select Domain(s)-

Account expiry within: 2024/03/08 12:00:00 AM - 2024/04/01

Display Name	User Principal Name	Days Since Last Password Change
John	john.titor@tester1695outlook.onmicrosoft.com	63
Jack	jack.daniels@tester1695outlook.onmicrosoft.com	84
Patricia	patricia.corner@tester1695outlook.onmicrosoft.com	84
Jade	jade.smith@tester1695outlook.onmicrosoft.com	84
Kumar	kokki.kumar@tester1695outlook.onmicrosoft.com	64
Samuel	samuel.ngaa@tester1695outlook.onmicrosoft.com	63
Jerry	samuel.jack@tester1695outlook.onmicrosoft.com	85
Mathew	mathew.thompson@tester1695outlook.onmicrosoft.com	85
Lucy	lucy.pesch@tester1695outlook.onmicrosoft.com	85
Luna	luna.prince@tester1695outlook.onmicrosoft.com	63

Explore various export options for your reports to further analyze identity data and gain insights

Explore built-in reports that offer insights into user-related data across various directories like Universal Directory, Azure AD, and Salesforce

Inactive Users/Technicians

Select the desired time period: Last 30 Days

Email Address	Display Name	Directory Type	Directory Name	Days Since Last Logon	Created Time	Last Activity
chesterpink@chatter.sale...	Chester	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
hankmint@gmail.com	HM	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
daniel@prod.com	Daniel	Universal Directory	Hozo	79	20/12/23 15:05:21	-
diana@hacker.com	Diana	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
ilena@tester1695outlook...	ilena	Azure Active Directory	tester1695outlook.onmic...	113	16/11/23 00:54:04	16/11/23 00:54:04
cleopatra@slajs.com	Cleopatra	Universal Directory	Hozo	115	14/11/23 13:19:29	-
penguin@kind.com	Penguin	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
lunapesch@kind.com	Luna	Salesforce	salesforce	160	29/09/23 17:57:42	29/09/23 17:57:42
lucypink@thangaraj1998...	Lucy	Universal Directory	Hozo	158	02/10/23 15:06:03	-
tonysmith@thangaraj199...	Tony	Azure Active Directory	thangaraj1998.onmicroso...	159	01/10/23 00:02:28	01/10/23 00:02:28
samuelthompsonking@z...	Samuel	Salesforce	ChanSales	77	21/12/23 17:47:43	21/12/23 17:47:43

Reports and identity analytics use case

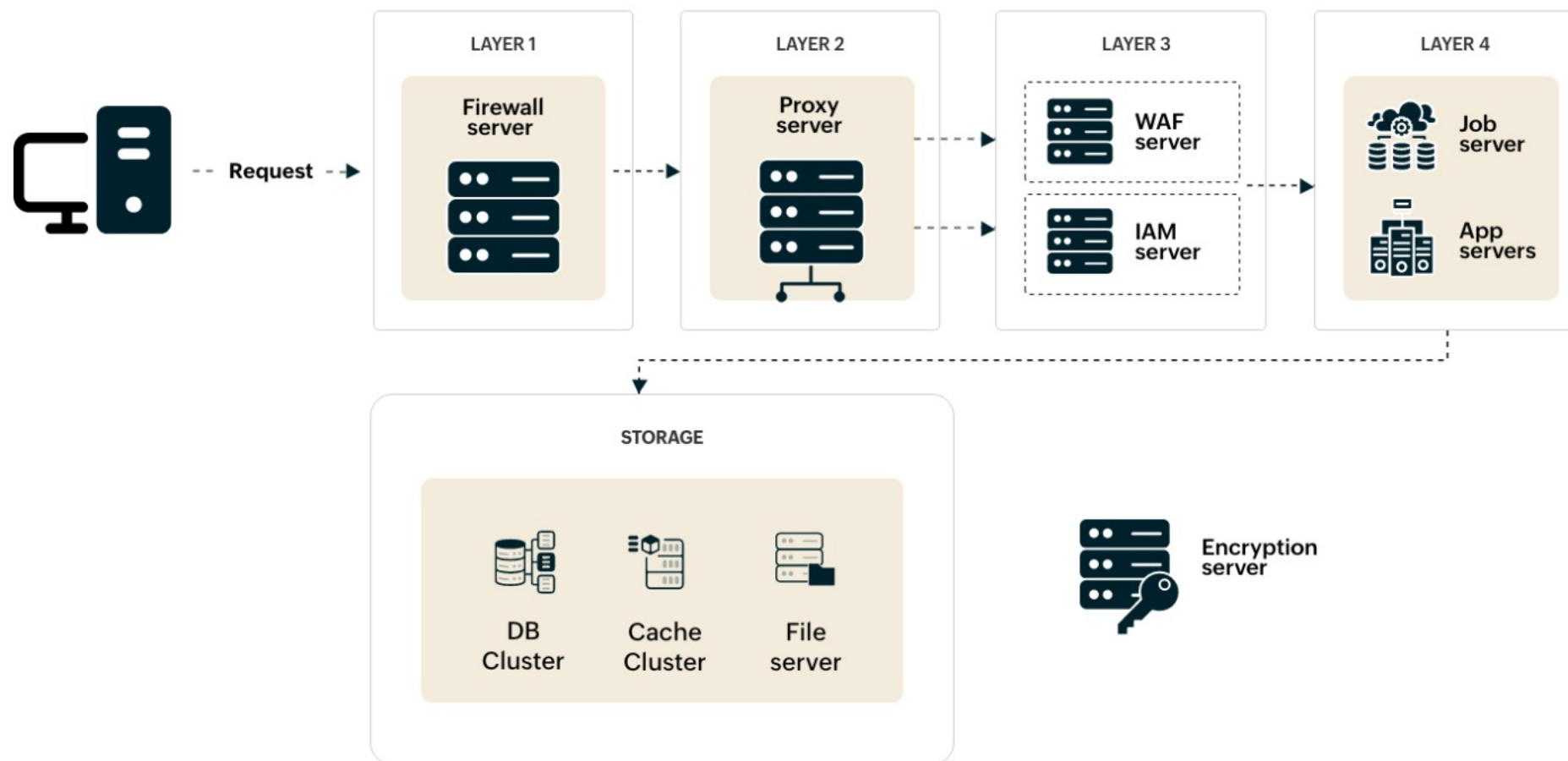
Problem

In an organization with a diverse workforce and extensive system access, ensuring security and compliance is paramount. With rising cybersecurity threats and regulatory standards like the GDPR and SOC 2, the challenge lies in effectively monitoring and managing user identities and access

Solution

Identity360 enables the organization to extract actionable insights from user access patterns and behavior, swiftly identifying anomalies, unauthorized access, and compliance issues





Security and compliance

Identity360 showcases its dedication to maintaining a secure and compliant environment by adhering to various industry-standard certifications:

- ISO/IEC 27001
- ISO/IEC 27701
- ISO/IEC 27017
- ISO/IEC 27018
- SOC 2 Type II
- Cyber Essentials
- ESQUEMA NACIONAL DE SEGURIDAD (ENS) - Spain
- CSA STAR Self-Assessment
- GDPR
- CCPA
- Signal spam

Identity360 licensing

Life cycle
management

Starts at **\$295** per
100 users,
per year

MFA and SSO

Starts at **\$195** per
100 users,
per year

All inclusive (life cycle
management with
MFA and SSO)

Starts at **\$415** per
100 users,
per year

ManageEngine
Identity360

Thank you!

www.manageengine.com/identity-360

identity360-support@manageengine.com

START FREE TRIAL →

