ManageEngine
Identity360

E-BOOK

ManageEngine Identity360 Use cases

www.manageengine.com/identity360

Table of Contents

About Identity360

ManageEngine Identity360 is a cloud-native identity platform that helps enterprises address workforce IAM challenges. Its powerful capabilities include a built-in Universal Directory, identity orchestration, SSO, MFA for enterprise apps and endpoints, role-based access control, detailed reports, and more. It empowers admins to manage identities across directories and their access to enterprise applications from a secure, centralized console. With Identity360, not only can enterprises scale their businesses effortlessly, but they can also ensure compliance and identity-first security.

USE CASE 1

Move your digital identities to the cloud and efficiently manage your hybrid environment through the Universal Directory

Without a centralized identity store, identities can be fragmented across many sources, compromising consistency and accuracy. Access management then becomes a challenge for admins, having to rely on manual processes that are time-consuming and error-prone. This often results in a lack of granular control over user profiles and access rights, leaving little to no room for customization of user-specific access. In addition, not being able to visualize data also complicates tracking user activities and poses difficulties in ensuring compliance and investigating security incidents.

How Identity360 helps

Leverage an identity store and centralize user management

Identity360's Universal Directory integrates with various directories and applications, helping admins easily assign and manage user access to a wide range of applications while adapting to changing organizational needs. It helps maintain granular control over identities and their access rights, automatically modifying roles as users move across an organization. Identity360 also enables users to enjoy a seamless login experience to multiple resources using SSO, while ensuring that their logon activities are tracked through detailed reports.

USE CASE 2

Integrate and centralize administration of various applications and directories

Employees within organizations utilize numerous enterprise applications for their daily tasks. Managing identities across multiple platforms becomes scattered, leading to increased complexity and security risks. Admins also lack visibility into user activities across diverse apps, making it challenging to monitor them. Many organizations may already have a repository containing user information and access permissions. It is essential to have a centralized control panel for efficiently managing integrations between multiple applications and directories to maintain uniformity across all platforms and effortlessly handle user lifecycle management.

How Identity360 helps

Manage user identities and permissions centrally across all apps and directories

Centralizing user information and access privileges across integrated systems enables administrators to manage and provision users efficiently, as well as control user access from a single console through identity lifecycle management features such as orchestration and smart templates. Simplify user experience by implementing SSO, allowing users to effortlessly access all their applications through a unified dashboard using a single set of credentials.

USE CASE 3

Eliminate complexities and simplify user onboarding with user creation templates

In any organization, it's common to have multiple departments, such as IT, HR, Sales, and certain specialized departments specific to each company. While it's possible to create individual user profiles in directories and assign applications and permissions manually based on each user's role and responsibilities, this approach is impractical. Admins would need to repeat this process every time different groups of employees are brought on board, not to mention the tedious task of entering repetitive information for users who share common attribute values. This can be overwhelming due to the huge volume of data. This complexity makes user onboarding a time-consuming and error-prone procedure. This is where Identity 360's user creation templates come into play.

How Identity360 helps

Streamlining user provisioning

Utilize smart templates containing a plethora of attributes to centrally populate data and provision users across multiple applications and directories effortlessly.

Accurate role-based access

Create custom templates with account configurations and access permissions for individual roles and responsibilities within the company, simplifying and expediting the onboarding process.

Seamless user creation

Simplify the user creation process by automatically populating attribute values based on predefined conditions or creation rules.

Enhancing user experience

Make use of template layouts with drag-and-drop functionality for a seamless user experience.

Safeguard crucial information with field customization

Customize attribute fields, making them either read-only to ensure the information remains unaltered or silently active to conceal values from all technicians accessing the product (except for the super admin).

Prevent duplication of attributes

Prevent duplication errors by applying unique naming formats or by appending numbers to the duplicate values. This relieves a common challenge faced by admins during employee onboarding, where users share common identifying attribute values.

USE CASE 4

Enhance efficiency and unify management of identities with automated actions across platforms with orchestration

Numerous organizations employ a diverse range of systems, applications, and directories to handle identity and access management tasks. These tasks encompass onboarding users, provisioning them across various applications, granting essential permissions, and executing other administrative actions in various applications and directories. This makes orchestration tools necessary to integrate these disparate systems and create a unified identity management ecosystem. This approach streamlines the management of user identities and access privileges throughout the entire organization.

How Identity360 helps

Synchronized management through orchestration

Manage identities across multiple platforms through orchestrated actions that respond to specific triggers, facilitated by the utilization of the criteria builder to establish patterns and conditions. For instance, while onboarding a new employee, the orchestration process creates a user account, syncs data, assigns roles, and configures access in the required resources. This grants the new employee seamless access to Identity360 and all necessary enterprise applications, ensuring a swift and secure onboarding experience.

Enable notifications

Notify the concerned stakeholders upon the completion of orchestrated tasks. For example, if user information was modified, notifications will be sent to the user to whom the action was performed, that user's manager, and the administrator responsible for overseeing the task.

USE CASE 5

Protect and simplify access to resources with MFA-secured SSO

Users typically struggle with managing multiple passwords, leading to password fatigue and potential security vulnerabilities. Operational inefficiencies can also occur due to time-consuming login processes and increased support costs stemming from password reset requests. If an organization lacks robust authentication measures and fails to meet compliance standards, it becomes vulnerable to various risks. Administrators need good visibility over user access across systems and must protect identities from credential theft. With the rise of remote work environments, a strong authentication front is mandatory in the face of evolving digital identity challenges. Implementing SSO and MFA proves essential to mitigate these challenges, promoting both security and positive user experience within the organization.

How Identity360 helps

Secure SSO with MFA

Implement secure SSO with robust MFA, including email verification, Google Authenticator, and custom TOTP. Users can configure up to three authenticators with granular controls.

Improved user experience

Enable SSO effortlessly for pre-integrated and custom applications that support SAML, OAuth, and OIDC, and easily access them all from a single dashboard. The user-friendly UI enhances the SSO experience for both admins and end users.

Efficient tracking and visibility

Track SSO activity with prebuilt reports, including users assigned to each app, logon activity, failed logon attempts, and inactive users. Generate detailed MFA reports to track user MFA status and attempts effectively.

USE CASE 6

Enhance endpoint security against cyberattacks using MFA

Cybersecurity threats lurk around every corner, targeting critical endpoints such as networks, workstations, and servers. These threats, which include data breaches, privilege escalation, and insider attacks, can disrupt an organization's security posture. To combat these threats, endpoint MFA requires users to provide multiple forms of identification during Windows login and for various activities, such as UAC and RDP. This approach reduces the risk of unauthorized access even if a password is compromised. Relying solely on passwords for security is akin to having doors without locks. The lack of proper security measures makes it easy for attackers to gain entry. By adding layers of MFA, you build a robust fortress around your endpoints, significantly reducing the risk of breaches and unauthorized access.

How Identity360 helps

Prevents account takeovers

Reduces the risk of account takeovers and enhances overall security for users and their machines. With weak passwords causing many problems, an extra layer of security makes it difficult to achieve unauthorized access to exploit a data breach.

Secures elevation of administrative privileges

Protects critical system activities with MFA for UAC, preventing exploitation and unauthorized access, even if an administrator's credentials are compromised. This security measure adds an additional layer of protection, requiring multiple verification steps before anyone can access sensitive admin functions.

Enhances remote logon attempts

For employees logging into the company network through RDP from various locations and devices, implement MFA to enhance security for RDP-based logins to Windows machines. This helps reduce the risk of unauthorized access, particularly in remote work scenarios.

Unlocks insightful reports

Access detailed insights on the users' MFA enrollment status and track all MFA activities, including timestamps and the outcome of each attempt. You can customize reports to gain specific and relevant data.

USE CASE 7

Empower admins to delegate daily tasks and prioritize critical responsibilities

IT admins play a critical role in managing various aspects of an organization's technology infrastructure. They need to maintain crucial security configurations, ensure adherence to regulatory and compliance standards, and enhance the organization's cybersecurity. However, admins are constantly swamped with routine tasks such as user management, application assignments, report generation, and configuration adjustments. Therefore, administrators should be able to delegate these tasks to their team or non-administrative staff to focus on more critical responsibilities.

How Identity360 helps

Efficient workload management with delegation

Ease the administrators' workload by enabling them to delegate their daily routine tasks to their team or non-admin personnel without any privilege escalation, thereby enabling them to concentrate on their primary responsibilities.

Structured delegation with predefined technician roles

Use various predefined technician roles with access to role-specific management tasks, including user management, orchestration, report generation, application assignment, and security functions like MFA and SSO.

ManageEngine
Identity360

SAFEGUARD YOUR CLOUD

resources with our cutting-edge IAM solution

Get Quote | Sign Up

CONTACT US

www.manageengine.com/identity-360/

identity360-support@manageengine.com

Toll-free: +1-844-245-1104