ManageEngine
Identity360

Proof of Concept

Overview

This document assesses the feasibility and success of implementing Identity360 in the organization's infrastructure. The primary goal is to analyze and measure the potential benefits Identity360 can bring to the organization in terms of security, operational efficiency, and digital user experience.

Scope

The proof of concept will focus on testing the various capabilities offered by Identity360, such as user authentication, provisioning, and access management. A select group of users and systems will be involved to demonstrate these features.

Goals and objectives

- Analyze user life cycle management, from provisioning to deprovisioning, and orchestrate the journey across various identity stores.
- Evaluate the seamless operation of user authentication and authorization processes.
- Assess the effectiveness of access management capabilities.
- Test the integration capabilities with cloud directories such as Microsoft Entra ID (formerly Azure AD), Salesforce, and other enterprise apps used by the client's organization.
- Measure Identity360's impact on user productivity and security.
- Determine the solution's scalability.

Methodology

- Determine the specific organizational scenarios that need to be tested.
- Configure and deploy Identity360 in the test environment.
- Set up the required test accounts and user roles for the testing scenario.
- Test the features of Identity360 and gather feedback on their functionality in the organization.
- Evaluate the results against the predefined success criteria.

Timeline

- The setup and configuration process for Identity360 is expected to be completed in at least two business days.

Note: The duration can vary based on the complexity of the implementation.

- It will take up to 30 days to test and evaluate the solution within the organization's infrastructure.
- The analysis and results will be presented within 2-10 days.

Testing scenarios

A comprehensive breakdown of the testing scenarios that highlight the practical uses of Identity360's capabilities.

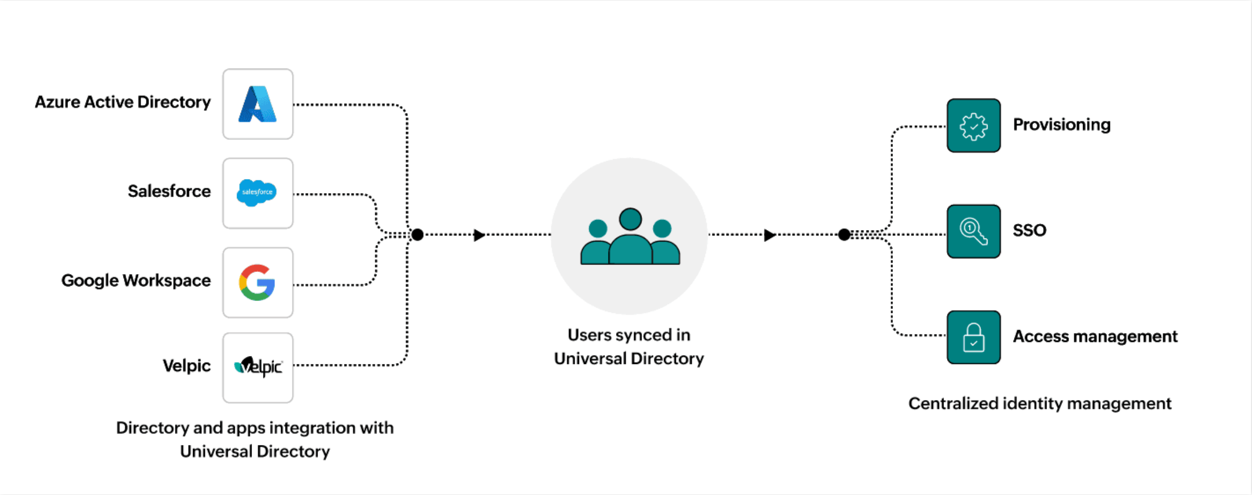
Scenario 1

Shifting the digital identities to Identity360's Universal Directory for centralized user administration

The security of the organization can be in jeopardy if the identities are scattered across various sources. Admins are frequently confronted with the challenge of user management, where they rely on manual procedures that are error-prone and time-consuming. Moreover, they don't have precise control over the user accounts across various identity stores, limiting the options for tailoring user-specific access.

Identity360's role in centralized user management

Identity360's Universal Directory is designed to seamlessly integrate with different directories and applications, simplifying the process of creating and managing user access across various sources based on organizational requirements. Admins can meticulously administer the identities and their access rights from a centralized console while automatically modifying roles and permissions as users transition within the organization.


Azure Active Directory
Salesforce
Google Workspace
Velpic
Directory and apps integration with Universal Directory
Users synced in Universal Directory
Provisioning
SSO
Access management
Centralized identity management

Success criteria

- The **integration success rate** is determined by the completion of integrating the organization's existing directories and applications into the solution.
- The **synchronization success rate** involves evaluating the percentage of digital identities seamlessly synced from the integrated directories and applications to the Universal Directory without any technical errors or data loss.
- The **improved efficiency in user management** can be assessed with the successful user creation, modification, deletion, and other actions, in the integrated directories and applications via Identity360.

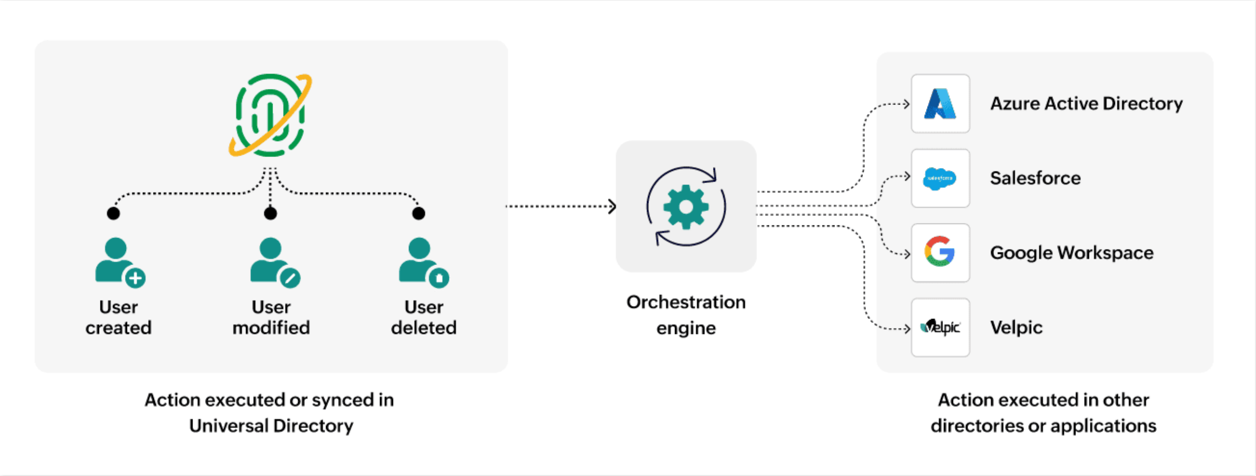
Scenario 2

Provisioning and deprovisioning the digital identities across various integrated platforms through Identity360's orchestration

Manual account provisioning and deprovisioning are tedious processes that are prone to inaccuracies and delays, especially in large organizations with a high turnover rate. This will impact user productivity, as new employees may not have timely access to the resources needed to perform their duties. Failing to promptly delete or deactivate user accounts after an employee leaves the organization can lead to unauthorized access and expose sensitive data.

Identity360's role in harmonious identity life cycle management

With Identity360, admins can create custom orchestration profiles based on their requirements to automatically manage user account creation, modification, and deletion in the integrated directories and applications while ensuring that user roles and permissions are consistently updated throughout the user's journey within the organization. By automating provisioning, deprovisioning, and access management, the organization can enhance security and improve overall efficiency by eliminating delays in the execution of user management tasks.



Success criteria

- The **success rate of provisioning and deprovisioning** can be assessed with successful user creation, modification, and deletion in the integrated directories and applications via Identity360.
- The **accuracy of modifying permissions** can be evaluated by ensuring user roles and permissions are promptly granted and revoked in alignment with organizational policies and regulatory requirements.
- The **boost in productivity** can be measured by the reduction in manual intervention and processing time of Identity360's orchestration capability in provisioning and deprovisioning identities across multiple integrated directories and applications.

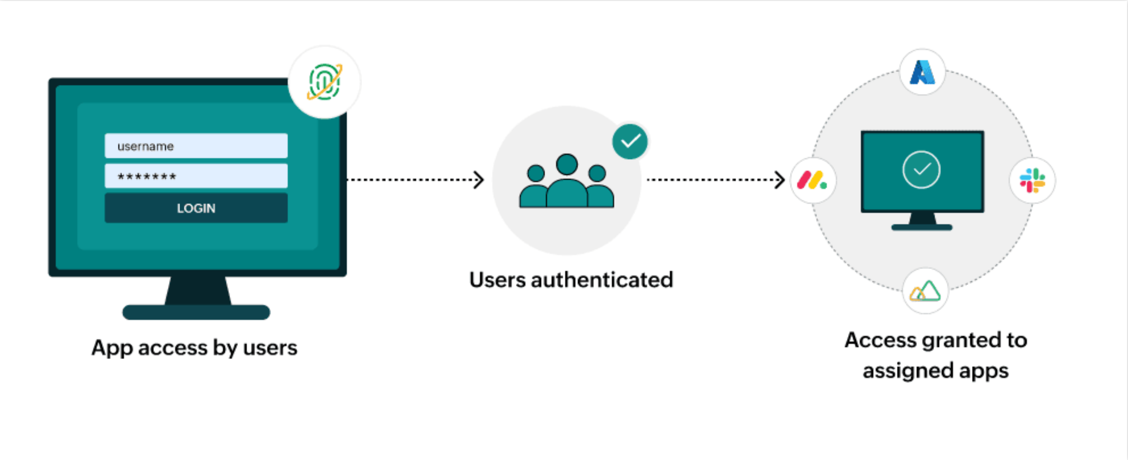
Scenario 3

Streamlining user authentication to multiple applications and providing swift access via Identity360's single sign-on (SSO) capability

Lack of seamless access to enterprise applications and constantly logging in and out of different applications can result in poor user experience, disrupting employees' workflow and impacting overall productivity. Employees may also resort to using weak passwords or reusing the same passwords for multiple accounts, increasing the organization's vulnerability to cyberattacks.

Identity360's role in simplified user authentication

Identity360's SSO capability helps users to seamlessly access multiple applications and resources with a single set of credentials, eliminating the need to remember multiple passwords. Implementing SSO will also minimize password reset requests and account lockouts, reducing the burden on admins. Users can work undisrupted with quick and effortless access to organizational resources, leading to enhanced productivity and workflow efficiency.



Success criteria

- The **ease of application configuration** can be determined based on the number of applications that are swiftly and successfully configured to provide users with easy access to resources.
- The **expedited application login time** can be measured when employees access multiple applications and resources effortlessly without the need to enter login credentials repeatedly.

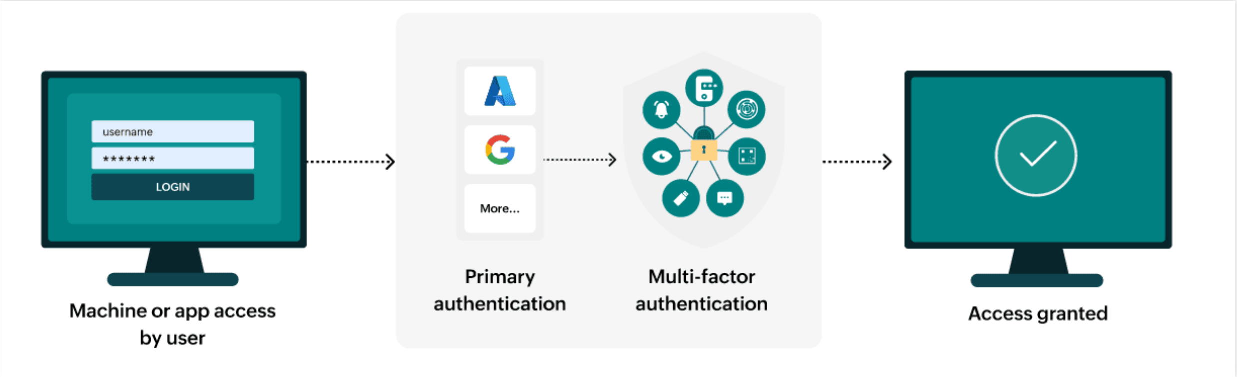
Scenario 4

Safeguarding applications and endpoints and ensuring secure access with Identity360's multi-factor authentication (MFA) capability

In the absence of MFA, stolen credentials can easily be used by threat actors to gain unauthorized access, posing security risks to organizations. Relying solely on passwords makes it easier for cyberattackers to compromise user accounts and gain access to sensitive information or systems. Without MFA, organizations may struggle to meet compliance standards that require MFA implementation.

Identity360's role in securing user authentication

Identity360 enables organizations to implement MFA, which requires users to authenticate with multiple factors, such as phishing-resistant FIDO2 passkeys, Duo, various TOTP authenticators, and email or SMS verification, to validate their identities before granting access to apps and endpoints. Identity360 helps the organization set up robust authentication procedures, making it harder for unauthorized users to gain access to crucial data. With MFA, strengthen the overall security posture of the organization and reduce the likelihood of data breaches and cyberthreats effectively.



Success criteria

- The **success rate of MFA verification for apps** can be assessed by the successful validation of identities using the configured authenticators before granting access to the Identity360 portal and applications.
- The **success rate of MFA verification for endpoints** can be determined by the successful validation of identities using the configured authenticators before granting access to their Windows machines and privileged actions.
- The **time taken for authentication** can be measured by calculating the average time taken to complete MFA verification, ensuring that security measures do not impact user productivity.

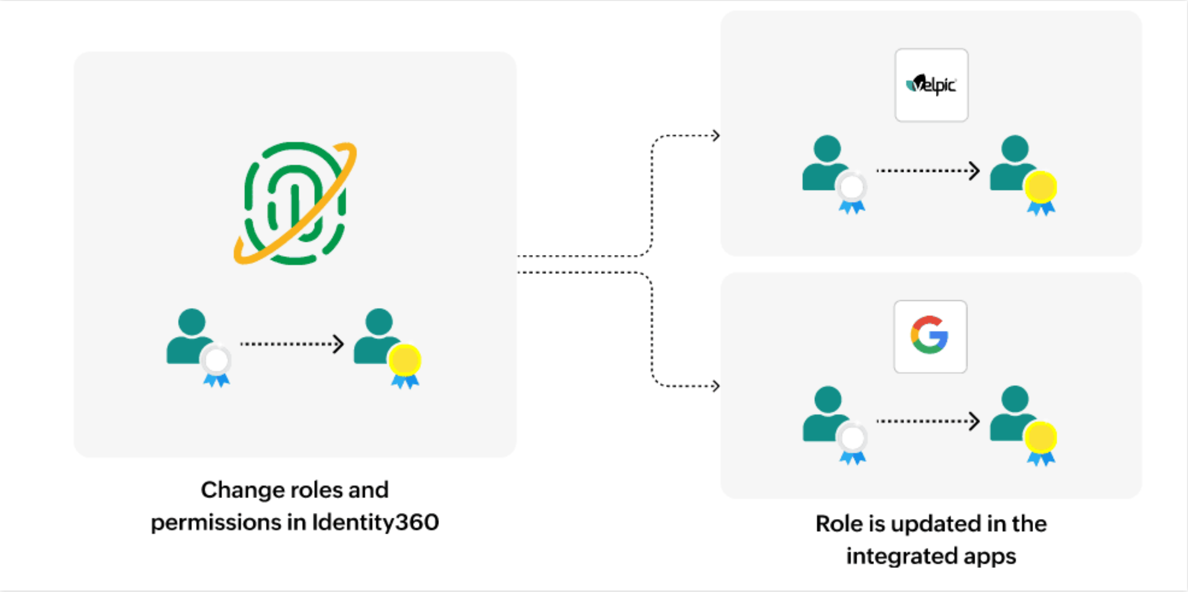
Scenario 5

Managing user roles and permissions centrally through Identity360's access management capability

Inefficient access management practices could result in operational disruptions, unauthorized access, and sensitive information being accessed or shared inappropriately. Organizations may struggle with the timely provisioning of user roles and permissions, which can also affect employee productivity.

Identity360's role in effective user roles and permissions management

Identity360 assists in modifying and maintaining uniform roles and permissions across all the integrated apps, streamlining access control protocols. This helps to enforce the principle of least privilege and ensure that users only have the necessary access permissions to perform their duties. With Identity360's access management, identify and mitigate access risks while ensuring compliance and maintaining a secure access environment.


Zelpic
Change roles and permissions in Identity360
Role is updated in the integrated apps

Success criteria

- The **success rate of updating roles and permissions** can be measured by confirming that changes made in Identity360 are reflected in the desired application.

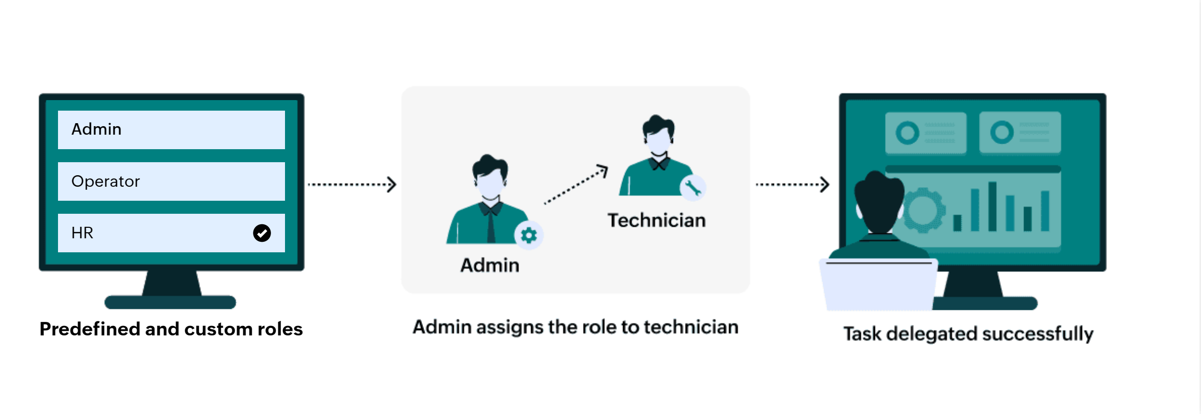
Scenario 6

Empowering non-admin users to handle identity management tasks with Identity360's help desk delegation

The absence of help desk delegation can slow down the execution of management tasks and impact efficiency. Admins may find it challenging to focus on handling more complex issues if they are burdened with routine user management tasks. They are also prone to making mistakes as they are overworked, leading to security vulnerabilities within the organization.

Identity360's role in reducing the burden of IT admins

Identity360 enables the assignment of predefined technician roles or custom roles to non-admin users, allowing them to perform identity management activities based on their designated roles and responsibilities without increasing their native privileges. Through delegation, reduce the workload on IT admins, enabling them to concentrate on addressing more challenging issues for increased productivity and streamlined identity management.


Admin
Operator
HR
Predefined and custom roles
Admin
Technician
Admin assigns the role to technician
Task delegated successfully

Success criteria

- The **total number of tasks handled** by the technicians can be calculated to determine how promptly and effectively identity management tasks are executed and issues are resolved.

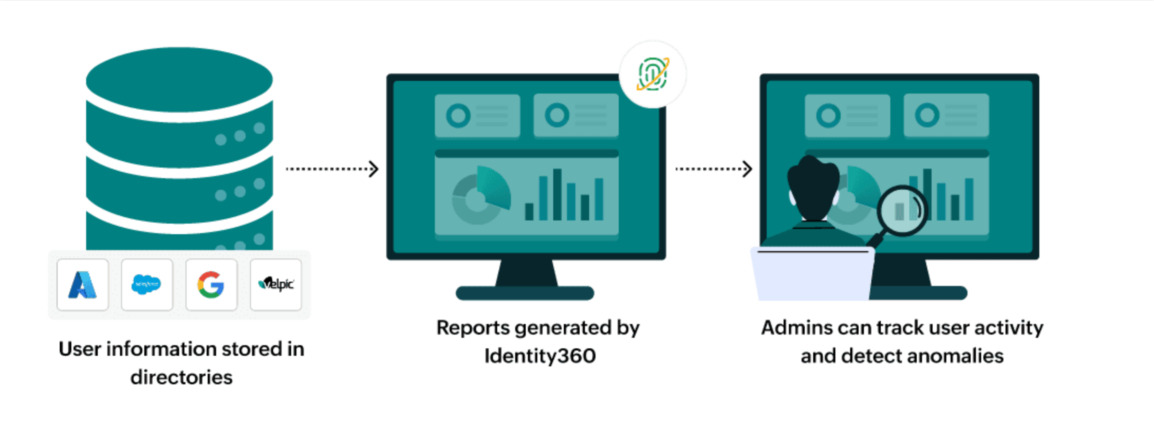
Scenario 7

Deriving user insights and meeting compliance requirements using Identity360's built-in reports

Without reports, organizations may struggle to have visibility into user management processes, making it challenging to proactively address user-related issues. It can also restrict the ability to gain valuable insights into user behaviors and patterns that could help track and detect potential threats. There may be gaps in compliance monitoring, making it difficult to ensure that the organization is meeting regulatory standards accurately.

Identity360's role in meeting compliance standards

Identity360 enables generating user activity reports, directory-specific reports, and authentication reports, providing the organization with a detailed overview of identity management processes. Through its advanced reporting capabilities, Identity360 empowers organizations to gain valuable insights into user activities and maintain compliance.


User information stored in directories
Reports generated by Identity360
Admins can track user activity and detect anomalies

Success criteria

- The **time taken to generate and export reports** can be determined by the duration required by Identity360 to process data and convert it into comprehensible reports.
- The **data accuracy of reports** can be measured by verifying whether the data presented is correct, up-to-date, and free from errors or inconsistencies by comparing reported data with actual data sources.

Stakeholders

The list of key stakeholders involved in the proof of concept of Identity360:

- Technical experts from Identity360's support team or pre-sales team.
- System admins, network engineers, database admins, or security analysts from the client's organization.

ManageEngine
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.

Resources

Sign Up ▶