SailPoint

WHITE PAPER

SailPoint + Microsoft: A Collaborative Integration

Extending the Value of Microsoft Azure Active Directory with SailPoint Identity Governance

To date, Microsoft has brought Azure Active Directory (Azure AD) to thousands of enterprise organizations across the globe; providing the market leading access management solution to millions of current and active user accounts. For these users, Azure AD serves as an entry point to identity management with services such as:

- A streamlined single sign-on experience to thousands of applications
- Simple provisioning for Azure AD, Active Directory and many key cloud applications
- Self-service password reset for Azure AD and connected on-premises Active Directory

Utilizing Azure AD, thousands of enterprises are solving the access management portion of their identity management needs. To create a complete identity and access solution, SailPoint has partnered with Microsoft to deliver identity governance to these organizations. SailPoint is the industry leader in identity governance and brings over a decade of successful identity governance experience to Azure AD customers.

Addressing Enterprise Identity Governance Needs

In addition to enabling and controlling access, enterprises need to govern users' access to all their systems and applications throughout the lifecycle of each user. Accomplishing this requires the strong identity governance platform from SailPoint.

SailPoint adds identity governance to Azure AD in these fundamental ways:

- Securely connect to all systems, both on-premises and in the cloud, that are in use by the enterprise with the ability to read and write to users' accounts and entitlements.
- Create flexible policies that define who should have access to which systems or applications, and ensure those policies are enforced through automated provisioning.
- Enable users to request access to applications or resources and provide workflows so access can be given with appropriate oversight.

- Define segregation-of-duty (SoD) policies that are automatically enforced and alert admins when SoD policies are found in violation.
- Provide traceable access certifications to allow users' access to be reviewed and remediated if necessary, and provide audit reports to satisfy compliance needs.

Enterprise Connectivity

To govern access across the entire range of enterprise applications and systems, an advanced connector fabric must be provided. SailPoint enhances the connectivity of Azure AD by employing a governance platform that includes connectors to virtually all enterprise systems, both on-premises and in the cloud. This enables governance of users' access on these system through provisioning, access certification, password management, and detective and preventive controls for separation of duties.

Databases	Microsoft SQL Server, Oracle DB, Sybase DB, JDBC, IBM DB2 for Windows, SAP, HANA
Directories	Microsoft Azure Active Directory, Microsoft Active Directory, OpenLDAP, IBM Domino, Oracle Internet Directory, Sun Java Directory, IBM Security Directory Server, LDAP, Novell eDirectory, Red Hat Directory Server
Mainframes	Top Secret, RACF, ACF2, RACF LDAP, Generic Mainframe
ERP & HR Applications	SAP Solutions, SAP CUA, SAP HR, SAP Enterprise Portal, Siebel, Oracle E-Business, PeopleTools, PeopleSoft Financials, Remedy AR System, PeopleSoft HRMS, Salesforce, NetSuite, Oracle HRMS, Workday
Healthcare	Epic, Cerner, GE Centricity
Communications & Productivity Tools	WebEx, GoToMeeting, Exchange, Google Apps
Collaboration	Box, Jive, Microsoft SharePoint, Yammer, Dropbox
Operating Systems	AIX, Solaris, SUSE Linux Enterprise, Windows Server, IBM I, Red Hat Enterprise Server, UNIX
Other Systems & Special	Microsoft Exchange, Microsoft Lync Server, RSA Authentication Manager, BMC ITSM, IBM Security Access Manager, Microsoft SharePoint, Microsoft Project Server, SCIM, Web services (REST), ServiceNow, RemedyForce, Amazon Web Services IAM, Duo

SailPoint's advanced connector fabric enables full connectivity to a growing range of enterprise applications and systems. In addition to the extensive out-of-the-box connectors, SailPoint's governance platform can be extended through custom connectors, web services (REST) and a plugin framework.

Lifecycle Management & Provisioning

Effective identity governance begins when a new user is added to the organization, such as when they are onboarded through a human resources system. Automatically provisioning the accounts and access they need according to attributes such as their role, geography or user population not only increases productivity, but also increases security and avoids shadow IT by ensuring they have access to what they need. Then, as the user moves through various stages of their lifecycle within the organization, their access is automatically adjusted, ensuring continued productivity while no unauthorized or inappropriate access remains.

The tight integration between SailPoint and Azure AD allows users to have accounts and access automatically provisioned for every resource they need from day one. Access is provided according to their business role and customizable business logic to ensure their access is enabled in concert with the company's policies. Access to provisioned resources and applications are added to the users' Microsoft Access Panel automatically, while the appropriate access level and entitlements are granted through SailPoint's advanced connector fabric.

SailPoint ensures Azure AD users have the appropriate level of access by fine-grained, entitlement-level provisioning and de-provisioning of accounts onto the whole range of on-premises and cloud applications used by most enterprises.

The SailPoint and Microsoft Azure AD alliance ensures the productivity and agency of the workforce by giving them automated and appropriate access to resources.

As a user moves through their lifecycle, for instance, when an employee goes on leave of absence, a contractor becomes inactive, or a staff member retires, their access is automatically adjusted according to policies set by the company administrator. This access is then reflected in the Microsoft Access Panel; when new applications are needed, they are automatically added, and those no longer needed are removed from the user's access panel.

In the case of termination, user access is automatically disabled without any manual IT intervention, ensuring no unauthorized access remains and nothing falls through the cracks.

It is not uncommon to have users change job roles or positions within the company, requiring access to be changed accordingly to meet the demands of their new role and avoiding potential entitlement creep. Administrators can define policies that enable SailPoint to automate the access changes that are required when a role change is made; removing access that is no longer required and adding access or applications that are needed for the new role. These changes are immediately reflected and available on the user's Microsoft Access Panel.

When a user requires new access to an application, Azure AD admins can permit applications available via Azure AD provisioning to be automatically added to the user's Microsoft Access Panel. SailPoint extends this capability by adding the ability for users to request access to any connected system from among the whole array of on-premises and cloud applications supported by SailPoint, while enabling administrators to define the approval workflow that can then be audited to ensure compliance.

Detective and Preventive Controls

SailPoint enforces identity governance throughout the lifecycle of the user via the creation and enforcement of security policies. These policies ensure that roles or entitlements are assigned in a coherent way: preventing users from holding conflicting entitlements at the same time (such as Accounts Payable and Accounts Receivable), preventing specific groups of users from having specialized access (such as restricting contractors from accessing sensitive data), or they may express some other enterprise-specific rule.

Policies are verified against the access afforded existing users (detective controls) as well as against new requests for access (preventive controls). The environment is thus brought into compliance with new policies as violations are discovered, and compliance is assured as the environment changes.

Detective controls identify violations of security policy. Supervisors are notified of these violations, and are prompted to either correct them (by removing inappropriate access) or document reasons why such violations should be allowed for a window of time. After those weeks or months have passed, the supervisor is prompted again to verify that this exception to policy is still required. This reduces the effort needed to satisfy auditors by providing a full audit trail for all compliance issues.

Preventive controls notify requesters of access when the application they have requested is not in compliance with existing policy and may present a security risk to the organization. They are required to modify the request or provide a reason why the exception should be made. As in detective controls, these exceptions are time-limited, and are presented to responsible parties for periodic review.

Detective and preventive controls, established through security policies, provide a mechanism for enterprises to define their security policy in a business-friendly construct. This allows these policies to be constructed easily and quickly by the business user – the person best suited to understand what access, applications, and data are sensitive, what combinations may be toxic, and thus what security controls must be put in place to reduce risk for the organization.

Access Review and Certification

Microsoft Azure AD provides access management to thousands of enterprises, enabling auto-population of apps onto users' access panels for thousands of applications. To effectively govern access to these systems necessitates ensuring that access is appropriate for the user's role, conforms to the company's policy, and meets audit and compliance requirements. SailPoint addresses these requirements by enhancing the Azure AD access management capabilities through access certifications. In this way, organizations can govern access to applications and systems that are under management of Azure AD.

SailPoint's proven identity governance extends Microsoft Azure AD to provide full, fine-grained controls across enterprise systems both on-premises and in the cloud.

SailPoint's flexible access certifications allow access reviews that are tailored to the business or compliance needs. This begins with visibility: providing business users with the information they need to effectively make decisions about users' access. It's important for users to know what they are certifying in a business-friendly way, and for the access to be reviewed by the right people in the organization to make the decisions. This business-friendly approach enhances security by avoiding the tendency for users to rubber-stamp access certifications. Business-friendly access certifications are not only compliant, but also secure.

SailPoint provides great flexibility to show granular, entitlement-level access in certification campaigns with customizable business-friendly entitlement names, along with logical grouping of access according to business roles. Access certifications are

not limited to only compliance needs, but satisfy business needs as well. It's critical to know who has access to what, and ensure that the right access is provided and inappropriate access is revoked. SailPoint remediates users' access in response to access reviewers' actions automatically, and provides audit reports to satisfy any compliance requirements.

Password Management

Azure AD offers single sign-on to thousands of applications, all controlled by the user's Azure AD password. Azure AD has password policy controls and multi-factor authentication options so organizations can effectively secure access to these connected systems. Through Azure AD Connect, on-premises Active Directory passwords are synchronized with the Azure AD password when a user resets or updates their password using the Azure AD self-service password reset.

SailPoint extends this functionality by further synchronizing passwords across the whole range of connected systems, either on-premises or in the cloud. This means Azure AD users can manage passwords on systems such as mainframes (RACF), Linux, SAP, ServiceNow, Oracle, Workday, databases such as MySQL, or any of the other types of systems that can be connected to SailPoint. This effectively extends the Azure AD self-service password reset and all password policy controls to the entire enterprise, beyond Azure AD and Active Directory alone.

Conclusion

The collaborative integration between Microsoft Azure AD and SailPoint provides enterprise organizations a complete and robust identity and access management solution. This gives the ability to effectively govern access throughout the users' lifecycle to thousands of enterprises who already rely on Azure AD to meet their access management needs, as well as those who are migrating their infrastructure to the cloud and embracing Azure AD as a foundational element in tomorrow's secure IT.

WP1126-1705