Microsoft

OMADA AND MICROSOFT SHARED SALES GUIDANCE

HOW TO DISCOVER WHAT SOLUTIONS ARE RIGHT FOR YOUR CUSTOMERS

08 May 2018

Contents

Preface

Who is this document for?

This document is meant to provide solutions-based guidance for sellers working with organizations that are looking to deploy modern Identity Access and Management (IAM) and Identity and Access Governance (IAG) solutions, which leverages capabilities from both the Omada and Microsoft solutions. Particularly organizations in regulated industries such as financial services, or government agencies, where there are mandates for how the organization must store and manage access to sensitive information.

Assumptions

These are the pre-supposed assumptions regarding the conversations that have occurred up to this point:

- Customer/prospect has high-level knowledge of IAM and IAG capabilities
- 2nd – 3rd conversation with technical personnel (i.e. initial discovery on opportunity has occurred)

Document goal

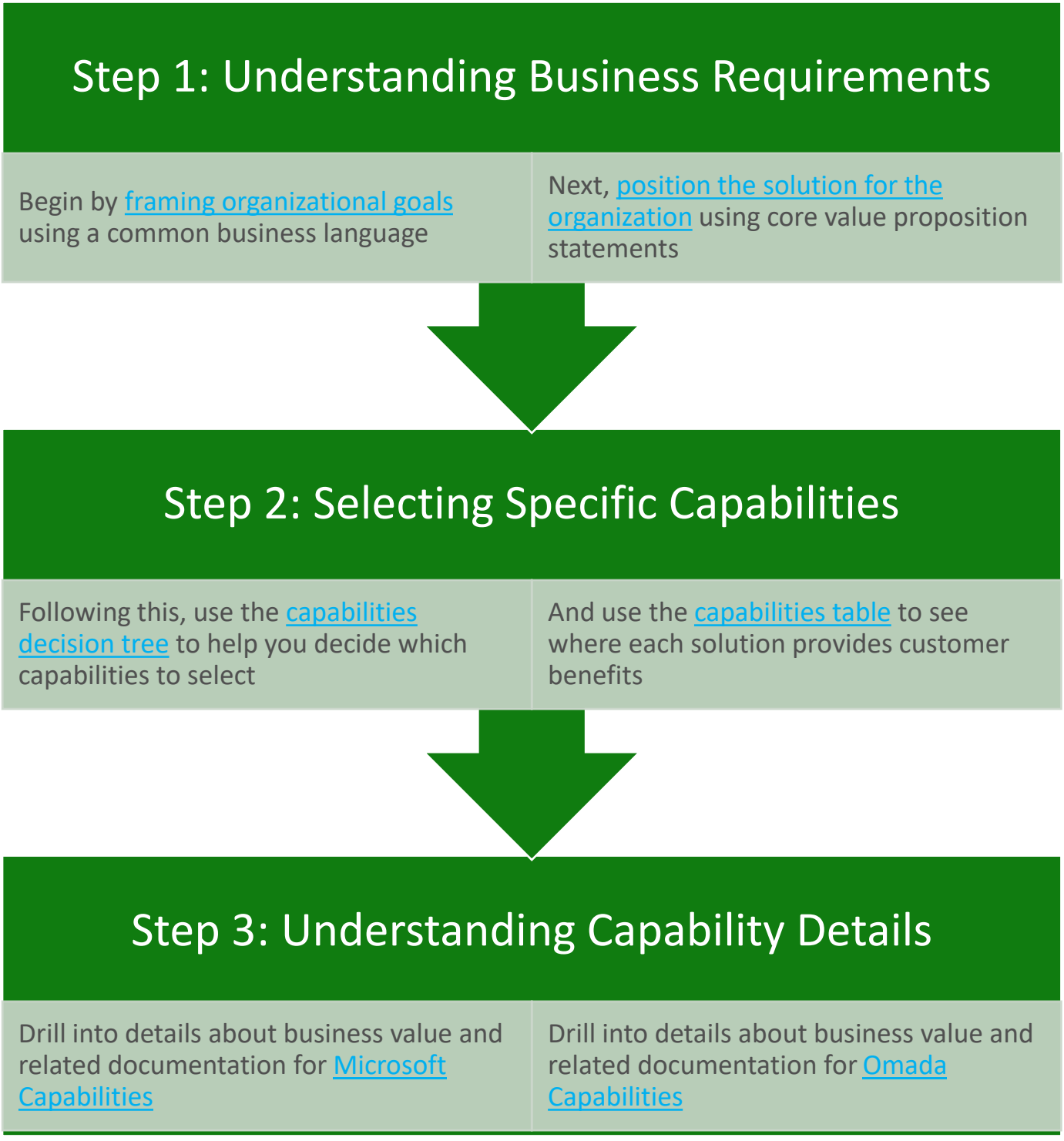
The goal of this document is to provide clarity around which technologies are applicable in which scenarios in a shared Omada and Microsoft deployment, and provide a logical mapping between common customer business requirements and scenarios, and the specific capabilities that Omada and Microsoft provide that enable these requirements.

How to use this document

This document is split up into three main sections to help you:

- Step 1 helps you to understand the specific business requirements in scope for an organization
- Step 2 then allows you to select the specific capabilities in scope based off those requirements
- Step 3 then enables you understand the specific details of the capabilities selected to facilitate future deployment motions

The below diagram contains links to deeper sections of this document to help guide you through this process.



Understanding Business Requirements

Framing the Conversation

Manage costs

Business Intention Description

Due to regulated industries, today's businesses often need advanced access governance controls across on-premises and cloud-based resources to meet their security, compliance, and efficiency requirements. A strategic alliance between Microsoft and Omada enables customers to deploy a richer 'better together' approach by enabling Microsoft Azure Active Directory Premium with Omada's Identity Governance solution, to provide full provisioning and lifecycle governance capabilities across more enterprise systems both on-premises and in the cloud, in a seamlessly integrated solution, delivered on the Azure cloud and in Microsoft Online Services.

To assist in driving down IT management and supports costs, self-service features within the joint solution allow end users the ability to request and gain access to the necessary groups and applications at the right time, through an approval process managed by the relevant business owner.

As users are granted the self-service access to groups and applications, an organization will need to ensure that they also implement cost-effective credential lifecycle management, for consistent authentication and seamless sign-on, the joint deployment offerings from Microsoft and Omada that will ensure strong authentication methods can be used, not only across 1st and 3rd party connected systems, but also across systems deployed in a hybrid cloud environment.

With the dynamic access to systems, organizations need to ensure that they can classify unstructured data correctly and accordingly, track access to this data, all whilst providing the business owners with a view and control to act on any access risks or compliance violations.

With digital transformation organizations are moving to the cloud, IT departments and business owners are under cost pressures to ensure that through any migrations or system consolidations they can reduce the user impact of accessing systems and data across a hybrid cloud deployment. The features and functionality that Microsoft provide will ensure that migrations can happen in not only a staged manner, but also in a simple and governed manner through automatic provisioning and single sign-on access to the necessary business applications. Omada build on this through their Identity Governance and Administration (IGA) best practice process framework allowing the business to not only establish control over their business-critical applications, but also maintain control to avoid costs increases as they migrate to the cloud.

Related Value Propositions

1. Business Automation of Access Governance
2. Truly Global Password Management
3. Compliance Monitoring, Rich Data Classification and Change Auditing
4. Simple & Staged Migration to the Cloud (e.g. during Mergers and Acquisitions)
5. Governance to a World of Users, Apps, and Devices

Manage Risk

Business Intention Description

As cloud migration projects are encountered, the fine line that an organization needs to navigate, is that of trying to reduce migration costs through reduction of expensive infrastructure and increase process efficiency, all while still managing business risk. One of the risks associated with a business migrating to the cloud, is the quality of user validity and data that needs to be synced into Azure Active Directory.

Customers can address that risk with the user lifecycle management features of Azure Active Directory Premium. Organizations with a Human Capital Management (HCM) system such as SAP, Workday, Oracle PeopleSoft or Oracle e-Business suite, can ensure that their users in Active Directory and other directories correspond with employees in their HCM system. When employees join an organization, accounts for them are automatically created in corporate systems, and furthermore, they can ensure that when employees leave, accounts are managed properly automatically disabled or removed from corporate systems.

For customers who have additional systems which are not integrated with a directory service, or do not have an HCM system for their users, Omada data cleansing and mapping features can mitigate this risk, thus not only ensuring the quality of user information and data migrated to Azure Active Directory, but also ensuring that a high quality is maintained through a continuous

governance process. Through Omada's governance process, organizations can also create and implement complete end-to-end user and Identity lifecycle scenarios, scenarios such as when organizations are acquired or merged through business consolidation, thus minimizing the risk associated to application and business resource access, provisioning, and while ensuring segregation of duties requirements continue to be addressed.

With the dynamic access to systems, organizations need to ensure that they can classify unstructured data correctly and accordingly, track access to this data, all whilst providing the business owners with a view and control to act on any access risks or compliance violations.

Through the linked Microsoft and Omada solution, an organization can provide their business owners and external identities with real-time access control, allowing for the implementation of continuous identity risk protection through conditional access, backed by a Cross-System Access Suspension workflow to disable a user's access depending on the event severity. This dynamic approach will ensure that an organization is able to rely on the business implemented policies to allow them to comply to their relevant industry standards and compliance authorities, whilst still providing the correct access, to the correct user, at the correct time.

Related Value Propositions

1. Active Directory to Azure Active Directory migration, including Actual versus Desired State Analysis
2. Business Automation of Access Governance
3. Simple & Staged Migration to the Cloud (e.g. during Mergers and Acquisitions) Experiences
4. Governance to a World of Users, Apps, and Devices
5. Real-Time Access Control
6. Governance of Azure B2B and Azure B2C User Access

Increase Employee Productivity

Business Intention Description

As organizations navigate the process of managing costs and mitigating risks though digital transformation, they need to ensure that they are still able to provide effective identity services and compliance to their business owners though the correct solutions that enable their users to be as productive as possible, whether these are internal users, or external users such as vendors or customers.

Implementing a shared Microsoft and Omada solution will ensure that customers can increase employee productivity through automation of lifecycle management processes such as on-boarding, off-boarding and departmental change processes for employees, external business partners, and customers across hybrid cloud infrastructures. The combined solution can also provide significant time savings by eliminating manual work associated with recertification surveys across a multitude of systems in the hybrid enterprise.

As employees, partners, and contractors join the organization, the combination of Azure Active Directory Premium and Omada's Identity Governance solution ensures they have easy access to the initial resources and applications they need even before day one in the company. This increases productivity as no workhours are wasted on getting access to the systems and applications they need. Ensuring users will be up and running from day one without compromising compliance.

With the deployment of the necessary shared solution components, an organization can provide the necessary self-service user experience in the front-end UI delivered via end user's familiar Windows, Office and mobile experiences, thus boosting productivity by ensuring employees, partners, customers, and contractors have the access they need when they need it, all the while leveraging the hybrid cloud automated processes and functionality in the back-end.

Related Value Propositions

1. Business Automation of Access Governance
2. Governance to a World of Users, Apps, and Devices
3. Governance of B2B and B2C User Access

Address Governance and Compliance

Business Intention Description

By implementing access governance organizations ensure that employees and external identities always have access to what they need, and only what they need. This core principle leads to regulatory compliance, significant savings, increased productivity, and reduced helpdesk requirements.

With a deployment of a joint Microsoft and Omada solution, customers obtain an enterprise grade end-to-end complete identity & access solution across hybrid heterogeneous platforms.

The Microsoft and Omada solution provides the full range of required capabilities for the modern enterprise while transitioning to leverage more of cloud while operating in a hybrid reality. The solution includes Microsoft's Identity and access management with advanced protection for users and privileged identities, single sign-on, Privileged Identity Management (PIM), Multi-Factor Authentication (MFA), Conditional Access and advanced security reporting, combined with Omada's Identity & Access Governance & Administration capabilities - delivered on the Microsoft Azure cloud.

Related Value Propositions

1. Cross System Separation of Duty Rules
2. Business Automation of Access Governance
3. GDPR and ISO 27001 Compliance Enablement
4. One Identity, Multiple Accounts
5. Governance to a World of Users, Apps, and Devices

Positioning the Solution

The below will help you to take the framing concepts above and understand how to position the breadth of capabilities delivered through a combined solution. Once you come to an understanding of this combined solution, you can then select the specific capabilities required for the customer by using the decision tree which follows.

Governance to a World of Users, Apps, and Devices

Value Proposition Statement

Microsoft provides automatic provisioning and single sign on to many cloud and on-premises application through the Azure Active Directory Application Gallery and Azure Active Directory Application Proxy, synchronization and provisioning experiences. Once these applications are integrated, Microsoft then offers integrated single sign-on experiences to B2E, B2B, and B2C users from the Microsoft application access panel, Office end user portal, Mobile Devices through the Intune Company Portal, and Windows 10 devices.

Omada extends these capabilities with its Identity Governance and Administration best practice process framework. Omada provides out of the box configurable integrated identity lifecycle processes, simple to understand business delegation workflows, in process Separation-of-Duties (SoD) policies, fine grained access control policies and provisioning, hybrid attestation, governance, and compliance overview - all in a way that IT administrators and Business Decision Makers can understand and action. Upon implementation of Omada's IGA process framework, an organization can establish and maintain control over business-critical access control requirements in complex hybrid environments.

Enabled Business Scenarios

- Integrate business resources into governance and access review procedures
- Ensure and verify that the right people are accessing the right resources
- Increase employee collaboration and process efficiency through new digital tools and processes
- Provide employees secure remote access to email and file sharing
- Provide secure access to apps from anywhere at low cost
- Provide secure remote access to on-premise applications
- Provide single sign on for both cloud and on-premise applications
- Rapidly onboard new Software-as-a-Service Applications to enable the business to move more quickly

Compliance Monitoring, Rich Data Classification and Change Auditing

Value Proposition Statement

Microsoft provides an audit and sign-in log that captures activity occurring against Azure Active Directory, as well as changes to on-premises passwords and group memberships. Microsoft also provides Azure Information Protection that provides classification of unstructured data.

Omada extends these capabilities through the Omada Compliance Dashboard, as the business gets a real time 360-degree overview of the access status vs. business policy and changes occurring against each connected and unconnected system, on- premise and in the cloud. This overview is displayed to business decision makers in a way that highlights business risk, potential compliance

violations, and issue severity so that they can then make an effective and accurate access control decision and remediate it instantly by launching mitigating activities directly within the Omada Compliance Dashboard. This includes the business context in which a user has been granted access, and the underlying data classification applied to the resource being requested.

Enabled Business Scenarios

- Ensure and verify that the right people are accessing the right resources
- Share data usage metrics to inform decisions and encourage responsible behaviors
- Minimize security threats with automated monitoring & reporting
- Meet global and local data compliance standards
- Rapidly address auditors' requests for who accessed what, and when

Truly Global Password Management

Value Proposition Statement

Microsoft provides a globally-available password management experience that can be extended to on-premises Active Directory using the Password Writeback capability, as well as to directories, databases and applications that use Active Directory for Authentication (for example those based on users stored in relational databases leveraging Active directory accounts). Omada extends this capability with further reach to additional systems connected via the Omada connectivity framework.

Enabled Business Scenarios

- Reduce helpdesk call volume by empowering your users to manage their passwords

Simple & Staged Migration to the Cloud (E.g. during Mergers and Acquisitions)

Value Proposition Statement

Microsoft provides single-sign on to a world of SaaS and Office business applications. A common scenario as companies move to the cloud are requirements to migrate from legacy software implementations (whether they are on-premises or in the cloud), or to absorb new technologies and systems as part of mergers and acquisitions where multiple Active Directories are merged.

Omada provides experiences allowing migration to the cloud to happen with a simple and staged approach to absorb new technologies such as cloud applications with available Azure Active Directory connector.

This is done by establishing hybrid governance of access across both legacy software and cloud apps, including managing synchronization for all target cloud and on-premises applications with an available Azure Active Directory connector and managing all connectivity with on-premises systems and cloud applications with an Omada Connector.

Secondly, a range of on-premises applications can be decommissioned in stages while the business continues to remain in control. From the end user perspective, while this migration is occurring, access is provided seamlessly through the various Microsoft application launching experiences.

Enabled Business Scenarios

- Migrate workloads and data to the cloud to increase uptime and availability
- Reduce equipment costs and increase efficiency with cloud services
- Upgrade outdated solutions

Business Automation of Access Governance

Value Proposition Statement

Microsoft provides end-to-end user identity lifecycle scenarios, tied to HCM systems such as SAP, Oracle eBusiness, Workday, and Oracle Peoplesoft, as well as self-service user management for users with no corresponding HR representation.

Omada extends this story significantly by automating complete end-to-end user and Identity lifecycle scenarios, access assignment policies, fine grained provisioning, and Separation of Duties (SOD) policies across all additional hybrid systems within the enterprise, reducing the need for a business decision maker to get involved and understand the underlying implementation of access control rules (e.g., what groups secure what access) through mapping this access to easy-to-understand logical entitlements, and bridging it to the organization’s organizational structure.

Omada's Connectivity Framework provides automated processes and functionalities for managing synchronization for all target cloud and on-premises applications with available Azure Active Directory connectivity as well as managing connections with all additional on-premises systems and cloud applications though the Omada Connectivity Framework.

Using Omada's out of the box comprehensive reporting, dashboard experiences and SoD Policy Lifecycle Management, a business decision maker can then be empowered to make the appropriate access control decisions in alignment with organizational policies. In addition to this, Omada supports human workflows to be triggered as part of these experiences (like managing a legacy mainframe system, provisioning a FIDO 2.0 security key, or providing a physical laptop to a user as part of an onboarding experience), as well as the ability to trigger these workflows based on multiple sources of authority for end users (such as different HR systems for someone transitioning from a contractor to full time employee role).

Enabled Business Scenarios

- Automatically assign or prevent access based on job role
- Empower business units to manage access to their resources
- Empower employees to securely self-service manage their own access
- Enable end users to securely manage their own access to increase employee agility
- Minimize security threats with automated monitoring & reporting

Governance of B2B and B2C User Access

Value Proposition Statement

Microsoft provides B2B and B2C integration scenarios for access to resources secured by Azure Active Directory, on-premises Active Directory -integrated applications, or custom-developed B2C applications.

Omada provides an out of box end user access portal that can be extended to B2B, and B2C users to enable those users to self-register and manage their accounts and request access to additional resources. Omada also enables governance and compliance solutions for Azure B2C Identity repositories to ensure proper audit and compliance requirements are achieved. For Azure B2C Omada can report on who has B2C collaboration enabled.

Enabled Business Scenarios

- Provide internal and external partners secure access to appropriate business resources
- Seamlessly bring business partners into your company's business systems
- Ensure authorized identities have access to Azure B2C Identity provider
- Report on Azure B2B collaboration to ensure governance and compliance

One Identity, Multiple Accounts

Value Proposition Statement

Microsoft can provide a one-to-one mapping between a HCM representation of an employee, a logical identity and one or more a connected user account(s) in multiple Active Directory forests, multiple directories, databases and applications such as SAP. Microsoft also provides the ability to step up access to more privileged accounts in real time with the PIM and Privileged Access Management (PAM) features, and also to manage access to shared accounts in specific SaaS applications such as Twitter.

Omada's IGA Solution provides the additional capabilities to handle users with different credentials for different systems, to manage multiple user stores, and to manage the fact that users underrepresented in multiple Azure Active Directory subscriptions tenants who have, or multiple Active Directory forests have multiple accounts. These Omada IGA capabilities are available across employee contract type, role, and affiliation, and between separate user accounts with different levels of privilege in Active Directory or a variety of connected systems such as SAP. To ensure that a holistic mapping of a user's identity is maintained, these mappings can be defined based on hard or soft matching rules to ensure that a single view of a real user's access is maintained over time.

Enabled Business Scenarios

- Assure the right people have access to the right resources at the right time
- Empower business units to manage access to their resources
- Empower employees to securely self-service manage their own access
- Enable end users to securely manage their own access to increase employee agility

AD to Azure Active Directory migration, incl. Actual versus Desired State Analysis

Value Proposition Statement

Microsoft provides an access control platform that encompasses the full range of single sign-on and user provisioning standards available in the world today. These are based on directory data stored in Active Directory and Azure Active Directory, and so requires high-quality user lifecycle management and attributes.

Organizations with a Human Capital Management (HCM) system such as SAP, Workday, Oracle PeopleSoft or Oracle e-Business suite, can ensure that their users in Active Directory and other directories correspond with employees in their HCM system. When employees join, accounts for them are automatically created, and furthermore, they can ensure that when employees leave, accounts are automatically disabled or removed. In addition to synchronization between Active Directory and Azure Active Directory, Microsoft can also provide user provisioning to other directories both on-premises and the cloud.

Omada provides the capability to significantly ease Active Directory and Azure Active Directory migrations for organizations with complex data quality issues. As part of migrating key on-premises workloads to the cloud, organizations must often first perform a full Active Directory clean-up, remediation, and potential consolidation of their Active Directory environments. Through data cleansing features and data mapping features, Omada can reduce the time it takes to migrate and/or synchronize users and data from Active Directory and Azure Active Directory, and to ensure that data quality in Active Directory and Azure Active Directory is continuously governed. Through the definition of desired state and inspection of a users' actual state in Active Directory, Omada can determine what the appropriate level of access is and can the trigger automated remediation activities. Once this has been completed, Omada can then perform ongoing analysis at any point in time to keep Active Directory clean based on human-driven access review workflows.

From the end user's perspective, while this lift and shift is occurring, access is available seamlessly through the various Microsoft application launching experiences.

Enabled Business Scenarios

- Use the power of the cloud to increase user and data security

GDPR and ISO 27001 Compliance Enablement

Value Proposition Statement

Microsoft Azure Active Directory and Microsoft Compliance manager supports native GDPR & ISO 27001 compliance experiences in terms of acting on incoming data subject requests, and supports the export, update, and delete operations necessary to fulfill these requests within the Microsoft Platforms. Microsoft also provides guidance for how customers can operate their Microsoft products and technologies, including Windows Server, Microsoft Identity Manager, and Azure Active Directory Connect.

To enable customers to identify potential compliance issues, Azure Information Protection and Microsoft Cloud App Security combine to provide data labeling, classification, and protection of unstructured data within in Office 365 and the customers file repositories and other SaaS apps.

Omada's IGA solution further extends these capabilities through its best practice process framework and data classification capabilities. A system and its underlying data can be classified as PII and in scope of GDPR. Once this step has been completed, a Business Decision Maker can then be empowered to make the correct access control decision based on the understanding that the access will be provided to sensitive data, allowing an organization to meet ISO 27001 standards.

Enabled Business Scenarios

- Meet global and local data compliance standards
- Rapidly address auditors' requests for who accessed what, and when

Cross System Separation of Duty Rules

Value Proposition Statement

Microsoft provides PIM and PAM experiences with identity lifecycle management, enforced through conditional access to mitigate common attack vectors, to enable customers to define policies on defined privilege user's access. For example, a user's ability to request a security group membership may be dependent or limited on their organizational position or may require additional approval workflows or reviews.

Omada's Governance solution provides additional capabilities to define cross system business defined SoD policies – e.g. what constitutes a duty within the organization and constraints around which duties can be performed by a single identity. These SOD

constraints can be mapped across multiple different system types (for example, Active Directory and SAP). Once those constraints are defined, violations to those constraints are surfaced to Business Decision Makers on their compliance dashboard for remediation efforts.

Enabled Business Scenarios

- Separate and scope the duties of server administrators to mitigate risk

Real-Time Access Control

Value Proposition Statement

Microsoft provides real-time identity protection and conditional access experiences against any Azure Active Directory connected applications. Upon Azure Active Directory detecting risky sign-in activity, a security analyst can then be notified of these events. Once notified, this analyst can use Omada's Cross-System Access Suspension workflow to disable all of a user's access based off of the type of the user and the severity of the event.

Enabled Business Scenarios

- Improve security without negatively impacting the end user's experience
- Increase security for accessing your applications
- Secure access to business-critical applications in alignment with risk-based access policies

Selecting Specific Capabilities

Capabilities Decision Tree

This decision tree will help you to map a specific customer's scenario requirements to a solution, as well as understand the breadth and depth covered by each of Microsoft and Omada separately and together.

ID	Value Proposition	Microsoft Capabilities	Omada Capabilities
1	Governance to a World of Users, Apps, and Devices	• Access Panel (MyApps) • Access Reviews • Application Proxy • Group-based access management • Microsoft Identity Manager (user and group provisioning) • Multi-Factor Authentication • RBAC for Azure Active Directory Administrators • Sign-in and Audit Reporting • Single Sign-On (SSO) • User and Group Provisioning • Windows, Office, and Intune Integration [*EMS*]	• Business Delegation Workflows • Business Context Management • Cross-System Separation of Duty Rules and Mitigating Controls • Current-State vs. Actual State Entitlements Reporting • Desired-state vs Actual-state Reconciliation • Entitlement catalogue • Fine Grained Provisioning • IGA Process Framework • Integrated Identity Lifecycle for hybrid environments • Logical Business Application Onboarding and Management • Policy Lifecycle Management • Provisioning Service with SDK • Role Lifecycle Management • System onboarding
2	Compliance Monitoring, Rich Data Classification and Change Auditing	• Data Access Governance [*Azure Information Protection*] • Identity Protection • Sign-in and Audit Reporting • Hybrid Reporting	• Compliance Dashboard • Cross-System Data and System Classification Surveys • Point-in-time Auditor Reporting • Provisioning Service with SDK

3	Truly Global Password Management	• Self-Service Password Reset/Change/Unlock with on-premises writeback to AD • Microsoft Identity Manager (User password provisioning)	• Cross-System Password Management
4	Simple & Staged Migration to the Cloud (e.g. during Mergers and Acquisitions)	• Application Development with Modern Authentication and Microsoft Graph • Application Proxy • Azure Active Directory Connect • Azure Active Directory Domain Services • Pass-Through Authentication • Self-Service Password Reset/Change/Unlock with on-premises writeback to Active D • Microsoft Identity Manager (User and group provisioning from on-premises directories and databases)	• Business Context Management • Desired-state vs Actual-state Reconciliation • Policy Lifecycle Management • Provisioning Service with SDK • Role Lifecycle Management • Self-Service Access Requests to hybrid environments
5	Business Automation of Access Governance	• Access Panel (MyApps) • Access Reviews • Administrative Units • Dynamic Groups • Group-based access management • Group-Based Licensing • Identity Protection • Microsoft Identity Manager (user lifecycle management) • Self-Service Application Access • Self-Service Group Management • Sign-in and Audit Reporting • User and Group Provisioning	• Access reviews across hybrid environments • Business Context Management • Cross-System Separation of Duty Rules and Mitigating Controls • Entitlement catalogue • Fine Grained Provisioning • Logical Business Application Onboarding and Management • Logical Identity Mapping from Multiple Sources of Authority • Policy Lifecycle Management • Provisioning Service with SDK • RBAC and ABAC for hybrid environments • Role Lifecycle Management • Self-Service Access Requests to hybrid environments
6	Governance of B2B and B2C User Access	• Access Reviews • Azure Active Directory B2C • B2B Collaboration • Microsoft Identity Manager (User provisioning)	• Access reviews across hybrid environments • Configurable out-of-box B2C and B2B user self-service portal
7	One Identity, Multiple Accounts	• Application Proxy • Conditional Access • Identity Protection • Microsoft Identity Manager (identity lifecycle management) • Multi-Factor Authentication • RBAC for Azure Active Directory Administrators • Single Sign-On (SSO) • User and Group Provisioning	• Business Delegation Workflows • Integrated Identity Lifecycle for hybrid environments • Logical Identity Mapping from Multiple Sources of Authority • Multi-affiliation support • Provisioning Service with SDK
8	AD to Azure Active Directory Migration including Actual versus Desired State Analysis	• Access Reviews • Azure AD Connect • Conditional Access • Identity Protection • Microsoft Identity Manager (user provisioning)	• Access reviews across hybrid environments • Business Context Management • Desired-state vs Actual-state Reconciliation • Policy Lifecycle Management • Role Lifecycle Management

		• Multi-Factor Authentication • User provisioning	
9	GDPR and ISO 270001 Compliance Enablement	• Access Reviews • Cloud App Security • Data Access Governance [*Azure Information Protection*] • Delete and Export (GDPR) • Sign-in and Audit Reporting • Windows, Office, and Intune Integration [*EMS*]	• Compliance Dashboard • Cross-System Data and System Classification Surveys • Cross-System Separation of Duty Rules and Mitigating Controls • Desired-state vs Actual-state Reconciliation • IGA Process Framework • Logical Business Application Onboarding and Management • Point-in-time Auditor Reporting
10	Cross System Separation of Duty Rules	• Access Reviews • Administrative Units • Microsoft Identity Manager (User and group provisioning) • Privileged Identity Management • RBAC for Azure Active Directory Administrators	• Access reviews across hybrid environments • Compliance Dashboard • Cross-System Separation of Duty Rules and Mitigating Controls • Desired-state vs Actual-state Reconciliation • Out-of-box connectors for 3rd party PAM solutions
11	Real-Time Access Control	• Advanced Threat Analytics • Advanced Threat Protection • Cloud App Security • Conditional Access • Data Access Governance [*Azure Information Protection*] • Identity Protection • Multi-Factor Authentication • RBAC for Azure Active Directory Administrators • Windows Hello • Windows, Office, and Intune Integration [*EMS*]	• Access reviews across hybrid environments • Cross-System Access Suspension • Cross-System Separation of Duty Rules and Mitigating Controls • • Integrated Identity Lifecycle to hybrid environments • Provisioning Service with SDK

Microsoft Capability Details

Access Panel (MyApps)

What is it?

The access panel is a web-based portal where users can launch all their Azure AD connected applications they have been granted access to by their Azure AD administrator. The portal also supports a variety of management capabilities that can be enabled for end-users through the Azure portal. These additional capabilities include:

- Change the password associated with a work or school account.
- Manage access to applications and get request access to applications.
- Edit password reset settings.
- Edit contact and preference settings related to multi-factor authentication (for accounts that have been required to use it by an administrator).
- View account details, such as user ID, alternate email, mobile and office phone numbers, organizations, and devices.
- Self-manage group memberships.
- Participate in access reviews for apps or groups.
- Allow guests to access company resources.

Why is it useful for your business?

- One stop portal for access to all apps a user has single-sign on enabled for
- Self-service capabilities that allow admins to delegate day to day access management responsibilities to end-users
- End users have a clear way to find access to their company's apps, groups and account management settings

Related documentation

- What is the access panel?
- Troubleshooting the access panel

Access Reviews

What is it?

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships and access to enterprise applications, with re-attestation/access recertification. It can also be used to review user's privileged administration rights in Azure AD or users who have administrative access to business-critical Azure subscriptions. Azure AD access reviews is part of Azure AD Premium P2.

Why is it useful for your business?

- You can recertify guest user access by using access reviews of their access to applications and memberships of groups. Reviewers can use the insights that are provided to efficiently decide whether guests should have continued access.
- You can recertify employee and guest user access by using access reviews of their access to applications and memberships of groups. Reviewers can use the insights that are provided to efficiently decide whether guests should have continued access.
- You can schedule recurring access reviews and have decisions automatically applied after the review completes
- You can collect access review controls into programs that are relevant for your organization to track reviews for compliance or risk-sensitive applications.

Related documentation

- Azure AD access reviews for groups and apps

Administrative Units

What is it?

Administrative units allow grouping users and groups into management containers, that can then be used for delegating administrative permissions. Administrative units enable central administrators to delegate permissions to manage users and groups to regional or departmental administrators.

Why is it useful for your business?

- Allows large organizations to better enforce least privilege administrative permissions
- Allows large organizations to free up central administrators' time by delegating basic management to local administrative teams

Related documentation

- Administrative units management in Azure AD

Azure Advanced Threat Protection

What is it?

Azure Advanced Threat Protection (Azure ATP) is a cloud-based security solution that helps you detect and investigate security incidents across your networks. It supports the most demanding workloads of security analytics for the modern enterprise. It monitors entity (user, device, resources) behavior to create a baseline and then detects anomalies with the adaptive built-in intelligence, giving you insights into your identity and network traffic so you can quickly respond. Working in tandem with Azure AD Identity Protection, Azure ATP provides a comprehensive solution to enable you to protect your identities.

Azure ATP is part of the EMS E5 suite.

Why is it useful for your business?

For security operators, analysts, and professionals who are struggling to detect advanced attacks in their environment, Azure ATP is a threat protection solution that helps:

- Detect and identify suspicious user and device activity with learning-based analytics

- Protect user identities and credentials stored in Active Directory
- Provide clear attack information on a simple timeline for fast triaging, providing a detailed timeline showing which users have been compromised, what techniques are being used, and on what devices.
- Monitor multiple entry points through integration with Windows Defender Advanced Threat Protection

Azure ATP can detect advanced malicious attacks leveraging network signals, reducing false positives, and providing an end-to-end investigation experience including across endpoint and identity with Windows Defender ATP integration.

Related documentation

- Azure Advanced Threat Protection Documentation
- Azure Advanced Threat Protection Announcement Blog
- Azure Advanced Threat Protection Marketing Page

Advanced Threat Analytics

What is it?

Advanced Threat Analytics (ATA) is an on-premises platform that helps protect your enterprise from multiple types of advanced targeted cyber attacks and insider threats. It uses information from multiple data-sources in your network to learn the behavior of users and other entities in the organization by building a behavioral profile about them and leveraging ATA's proprietary network parsing engine to capture and parse network traffic of multiple protocols. ATA is part of the EMS E3 suite.

Why is it useful for your business?

- Detect threats fast with behavioral analytics.
- Adapt as fast as your attackers - rely on continually updated learning that adapts to the changing nature of your users and business.
- Focus on only important events - review the attack timeline for a clear and convenient view of suspicious activity or persistent threats.
- Reduce false positive fatigue.

Related documentation

- Advanced Threat Analytics Documentation
- Advanced Threat Analytics Marketing Page

Application Proxy

What is it?

Azure AD Application Proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. These on-premises web applications are integrated with Azure AD, so you can leverage conditional access, multi-factor authentication, and all the security controls in AAD for your on-premises applications. End users can access your on-premises applications the same way they access O365 and other SaaS apps integrated with Azure AD, and you can configure this feature through the Application Proxy and Enterprise Applications menus in the Azure Portal. This feature is easy for you to deploy since you don't need to change the network infrastructure or require VPN to provide this solution for your users.

Why is it useful for your business?

- Simpler Remote Access for Increased Productivity
  - Empower your users to be productive from anywhere, on any device.
  - You don't need to change or update your applications to work with Application Proxy.
  - Your users get a consistent authentication experience. They can use the MyApps portal to get single sign-on to both SaaS apps in the cloud and your apps on-premises.
- Additional Security
  - When you publish your apps using Azure AD Application Proxy, you can take advantage of the rich authorization controls and security analytics in Azure. You get cloud-scale security and Azure security features like conditional access and two-step verification for your on-premises resources.
  - You don't have to open any inbound connections through your firewall to give your users remote access – Application Proxy works using **outbound** connections only.

- Cost-effective
    - Application Proxy works in the cloud, so you can save time and money. On-premises solutions typically require you to set up and maintain DMZs, edge servers, or other complex infrastructures.

Related documentation

- Application Proxy Overview
- Get Started with Application Proxy

Azure Active Directory B2C

What is it?

Azure AD B2C is a customer identity and access management service that allows you to create a seamless identity experience for your customers. You can configure sign up or sign in for your application with complete control over the layout and branding all while running on Microsoft's secure cloud platform.

Why is it useful for your business?

- Allow your customers to use their social identities with your app
- Customize the experience using your brand
- Tailor your experience to 36 languages supported natively, or provide translations to any language
- Protect your users by providing the option of using MFA

Related documentation

- Azure AD B2C Overview
- Quickstart: Test drive an Azure AD B2C enabled web app

Azure Active Directory Connect

What is it?

Azure Active Directory Connect enables the integration between an on premises Windows Server Active Directory and Azure Active Directory. The feature synchronizes identity information between the two directories, enabling several scenarios. Among those are single sign on of your on premises users into Office365, SaaS applications and Azure AD features such as the Access panel and Application Proxy applications.

Why is it useful for your business?

- Centrally manage users in a hybrid environment.
- Users sign in only once for many applications.
- Users only use on set of credentials for all applications.

Related documentation

- What is Azure Active Directory Connect?
- Azure Active Directory Connect frequently asked questions

Application Development with Modern Authentication and Microsoft Graph

What is it?

The Azure AD Developer Experience & Platform enables app developers (internal and external) to build secure, robust applications that sign in your work accounts, leverage productivity data through the Microsoft Graph, and integrate with other Azure AD features like Conditional Access. Apps can use modern protocols like OAuth2.0 and OpenID Connect with their choice of authentication libraries in several major platforms including .NET, Xamarin, JavaScript, Angular, Android, iOS, Python, Java, Node, and PHP. Microsoft apps including Office 365 and Azure, industry leading ISVs, and organizational developers all trust and rely on the Azure AD identity developer platform.

Why is it useful for your business?

- Develop smarter apps with data from the Microsoft Graph.
- Build line-of-business apps that achieve SSO with Office 365 and external apps.

- Build apps for customers that achieve SSO with Office 365 and the organization's internal apps.
- The Microsoft Graph allows your organization to automate internal processes, dev ops, and management of Azure AD (users, apps, directory), Azure infrastructure, Intune, and Office 365.

Related Documentation

- Azure AD Developer Platform
- Microsoft Graph API
- Authentication Basics
- Microsoft Graph Explorer

Azure Active Directory Domain Services

What is it?

Azure AD Domain Services enables you to login to Azure virtual machines using your corporate credentials and manage them securely using Group Policy. You can use the service for the identity needs of older applications that rely on Windows Server Active Directory, such as LDAP, Kerberos/NTLM authentication, Windows Directory Services APIs etc. These legacy apps can now be migrated from your on-premises network and deployed in Azure Infrastructure Services, relying on Azure AD Domain Services for the identity needs of these apps. This enables you to retire aging infrastructure on-premises.

Why is it useful for your business?

- Admins can migrate apps from on-premises server to Azure Infrastructure Services, without needing to re-write the app.
- Admins can publish Kerberos based apps deployed in an Azure virtual network and joined to AAD-DS domains through the Azure AD Application Proxy, thus enabling them to modernize and secure legacy applications.
- Users can sign-in to Azure application servers using their corporate credentials. Application servers can be managed & secured using Group Policy.

Related documentation

- Azure AD Domain Services Overview
- Scenarios – what can you use the service for?

Azure Active Directory Connect Health

What is it?

Azure AD Connect Health helps you monitor and gain insights into your on-premises identity infrastructure and the synchronization services. It enables you to maintain a reliable connection to Office 365 and Microsoft Online Services by providing monitoring capabilities for your key identity components such as Active Directory Federation Services (AD FS) servers, Azure AD Connect servers (also known as Sync Engine), Active Directory domain controllers, etc. It also makes the key data points about these components easily accessible so that you can get usage and other important insights to make informed decisions.

Why is it useful for your business?

- Admins can monitor the health of identity infrastructure deployed on-premises that is critical to their use of Office 365 and other SaaS applications.
- The Connect Health portal and associated email alert capabilities help administrators gain visibility into important issues impacting service health and take timely remedial actions.
- Azure AD Connect Health provides insights and analytics into the usage of on-premises identity infrastructure.

Related documentation

- Azure AD Connect Health - Overview
- Monitor Active Directory Federation Services
- Monitor Active Directory Domain Services
- Monitor Azure AD Connect Sync

Azure AD B2B Collaboration

What is it?

Almost every organization on the planet needs to work with other organizations to be successful. But there aren't many products out there that offer a secure and easy way to connect applications across organizational boundaries, across all platforms and devices, and across on-premises and cloud deployments. With Azure AD B2B collaboration, you can enable your organization to work with any other organization on the planet without having to manage your partners' identity in-house – while still advancing Azure AD's enterprise grade security to your partner relationships.

Why is it useful for your business?

- Admins can add partner using PowerShell or UX to groups, apps and directories
- Admins can delegate adding partner users to non-admin business owners in their organization who will use the Access Panel to work with guest users.
- You can enable bulk onboarding and policy-based, self-service sign-up for your partner orgs.
- You can enable your partners to access to most O365 apps, third party apps and OnPrem apps without having to manage local identities for your partner organizations.

Related documentation

- Azure AD B2B Overview
- Ignite 2017 presentation and demos

Cloud App Security

What is it?

Cloud App Security is a CASB (Cloud Access Security Broker) that provides deep visibility, real-time control and protection for cloud Apps.

Why is it useful for your business?

More and more organizations are adopting SaaS apps, not only to reduce costs but also to unlock competitive advantages such as faster time to market and improved collaboration. Cloud App Security can help extend the protection you have on-premises to cloud apps by providing comprehensive visibility, auditing and policies to help ensure your sensitive data stays safe.

- Discovery – Identify more than 16k apps and asses risk based on 60 customizable security parameters including compliance.
- Information Protection – Granular policies and remediation actions to control user activity and data sharing in cloud apps for both Microsoft and third-party apps such as Salesforce and Box. Scan & classify files in cloud and apply Azure information protection labels. Also integrate with existing SIEM or other DLP solutions.
- Conditional Access – Monitor and control access & user activity in cloud apps in real time using Azure AD conditional access policies. Ex. Block download of sensitive data from unmanaged device.
- Threat Detection – Identify high-risk usage and detect anomalous user activity with behavior analytics. Ex. mass download of data or brute force attack.

Related documentation

- What is Cloud App Security?
- Deploy Cloud App Security

Conditional Access

What is it?

Conditional access policies to satisfy organizations security and compliance requirements, by controlling access to applications. Access can be restricted on factors like user identity, location, session risk, device compliance or a multi-factor authentication requirement. These policies are being applied by Azure AD when a user signs into an application and integration with Microsoft offerings, to provide richer capabilities, such as Azure Identity Protection, Intune, Cloud App Security and Azure Information Protection.

Why is it useful for your business?

With a mobile workforce that access apps from anywhere, many of the traditional controls to protect organizational data, no longer apply. These traditional methods of access control relied on the network perimeter and related technology, like firewalls and VPNs. Conditional access policy provides a cloud-based approach to satisfy these requirements.

- Restrict access to managed devices – make sure devices are compliant with company policies so data is kept safe
- Risk based policies help keep attackers out – Azure Identity Protection provide session and user risk signals that conditional access policy can use to trigger multi-factor authentication of block access.
- Block access outside the corporate network for from regions of the word – block access based on IP Ranges or country/region
- Trigger session policies to limit access on unmanaged devices – working with Cloud App Security and SharePoint Online, policies can limit action a user can take within a session, like block download.

Related documentation

- Conditional access documentation

Data Access Governance [*Azure Information Protection]*

What is it?

Azure Information Protection is a cloud-based solution for protecting unstructured data (e.g. documents and email) in the enterprise environment. It is a component of the Enterprise Mobility Suite together with Azure Active Directory Premium, Intune and other products, and it is tightly integrated with many other solutions from Microsoft and third parties both in the cloud and on-premises, providing a natural, seamless user experience when working with protected information.

The solution can protect content regardless of its type, supporting Office documents, PDF and other types of documents. Its protection extends to any location in which the data may reside and travels with the data in a persistent way. It also enables sharing of protected data in a controlled way between different organizations, enhancing rather than restricting collaboration.

It does so by combining the elements of data classification and labeling, encryption, access controls, usage restrictions and content access monitoring and reporting. Sensitive content can be detected automatically or by indication of the end-user, which interactively drives labeling and protection based on configurable rules.

Azure Information Protection is a key element of the broader Microsoft Information Protection architecture, which extends this functionality thorough the enterprise by integrating AIP with compliance controls in Office 365, content detection and tagging by Microsoft Cloud Application Security, protection of data at rest in file servers and more for a comprehensive Information Protection approach across all workloads.

Why is it useful for your business?

Azure Information Protection enables organizations to establish a simple approach for securing unstructured data. By defining a classification taxonomy that applies to all data, establishing rules for its automatic or manual application and defining location-independent access controls and restrictions that will be automatically applied to each class of data an organization can ensure their information is properly protected from leakage and misuse from the moment it is generated and that it remains protected thorough its lifecycle including when it needs to be shared with others during regular business.

- Microsoft Azure Information Protection Premium P1 allows users to manually label data for protection and includes integration with cloud and on-premises workloads such as Exchange Server and Office 365.
- Microsoft Azure Information Protection Premium P2 builds on top of AIP P1 adding interactive automatic content detection and labeling to the solution.

Related documentation

- Azure Information Protection Feature Overview
- What is Azure Information Protection?
- Azure Information Protection Quickstart Tutorial

Delete and Export (GDPR)

What is it?

General Data Protection Regulation (GDPR) is regulation from the EU that goes into effect May, 2018 and requires that large segments of customers are able to view, export, or delete personally identifiable information about them. Microsoft has provided this capability for all tenants, managed through admins. For each feature that a tenant uses, the admin will be able to request to export or delete information about a given user. This will be largely facilitated through the Azure Portal, and exceptions are documented within the feature documentation. Please note that some features store data client side, and you should read through the documentation to ensure that you include those data when processing a request.

Why is it useful for your business?

GDPR is a requirement for any business operating in the EU, with EU citizen, or EU employees. We support GDPR compliance, so you can manage your business and be GDPR compliant while using AAD features.

Related documentation

- Licensing Terms and Documentation
- Azure Security Center

Dynamic Groups

What is it?

Azure Active Directory (Azure AD) groups allow customers the flexibility to manage users, resources and assets by enabling security, access control and collaboration. Organizations large and small are often challenged with managing membership of large number of groups being used. Dynamic groups are helpful as they are groups whose membership update automatically as people join, leave, or move within your organization, whenever the user's or device Azure Active Directory attributes are updated. Customers with Azure Premium license, can set up simple or advanced rules to enable attribute-based dynamic memberships of security groups or Office 365 groups including custom attributes within the tenant and Azure AD does the heavy lifting of evaluating the rules and calculating the memberships.

Why is it useful for your business?

Dynamic groups are useful and provide capabilities to organizations that desire flexibility because they:

- Allow group membership to automatically update group membership whenever group attributes are updated
- Work well for large organizations where people change teams, roles, and locations often.
- Enable the flexibility to be created for managing users or device objects based on a variety of simple or advanced attributes, including role, geography, department, device id and device model.
- Ability to be changed to static groups and vice versa, avoiding the need to create a new group while allowing you to keep the same group name and ID in the system.

Related documentation

- Create attribute-based rules for dynamic group membership in Azure Active Directory

Group-based access management

What is it?

Within Azure AD, one of the major features is the ability to manage access to resources. These resources can be part of the directory, as in the case of permissions to manage objects through roles in the directory, or resources that are external to the directory, such as SaaS applications, Azure services, and SharePoint sites or on-premises resources. There are four ways a user can be assigned access rights to a resource:

- **Direct assignment** - Users can be assigned directly to a resource by the owner of that resource.
- **Group membership** - A group can be assigned to a resource by the resource owner, and by doing so, granting the members of that group access to the resource. Membership of the group can then be managed by the owner of the group. Effectively, the resource owner delegates the permission to assign users to their resource to the owner of the group.
- **Rule-based** - The resource owner can use a rule to express which users should be assigned access to a resource. The outcome of the rule depends on the attributes used in that rule and their values for specific users, and by doing so, the resource owner effectively delegates the right to manage access to their resource to the authoritative source for the

attributes that are used in the rule. The resource owner still manages the rule itself and determines which attributes and values provide access to their resource.
- **External authority** - The access to a resource is derived from an external source; for example, a group that is synchronized from an authoritative source such as an on-premises directory or a SaaS app such as WorkDay. The resource owner assigns the group to provide access to the resource, and the external source manages the members of the group.

Why is it useful for your business?

- Allows you to automate and centralize access control based off the needs of your business
- Supports mapping access to cloud resources to on-premises group memberships through Azure Active Directory Connect tooling

Related documentation

- Manage access to resources with Azure Active Directory groups
- Azure Active Directory group management examples in PowerShell

Group-Based Licensing

What is it?

Using Microsoft paid cloud services, such as Office 365, Enterprise Mobility + Security, Dynamics CRM, and other similar products, requires licenses. These licenses are assigned to each user who needs access to these services. To manage licenses, administrators use one of the management portals (Office or Azure) and PowerShell cmdlets. Until now, licenses could only be assigned at the individual user level, which can make large-scale management difficult. For example, to add or remove user licenses based on organizational changes, such as users joining or leaving the organization or a department, an administrator often must write a complex PowerShell script. This script makes individual calls to the cloud service. To address those challenges, Azure AD now includes group-based licensing.

Why is it useful for your business?

Group Based Licensing allows organizations to assign one or more product licenses to a group. Azure AD ensures that the licenses are assigned to all members of the group. Any new members who join the group are assigned the appropriate licenses. When they leave the group, those licenses are removed. This eliminates the need for automating license management via PowerShell to reflect changes in the organization and departmental structure on a per-user basis.

Related documentation

- Group-based licensing basics in Azure Active Directory

Hybrid reporting

What is it?

Hybrid reporting enables customers to have a unified view of self-service password and group management operations, including on-premises password changes and AD security group join requests.

Why is it useful for your business?

Customers can more easily track who is requesting and approving access to resources, both on-premises and cloud-hosted.

Identity Protection

What is it?

Azure Active Directory Identity Protection is a feature of the Azure AD Premium P2 edition that can help detect and protect against identity-based attacks. Azure AD Identity Protection is built on Microsoft's experience protecting consumer identities and gains tremendous accuracy from the signal from over 14B logins a day.

Why is it useful for your business?

Azure AD Identity Protection can help your business in following ways:

- Provide visibility into accounts that might be compromised and sign-ins that might be suspicious
- Protect your organization in real-time using risk-based policies

Related documentation

- Get started with Azure AD Identity Protection
- Check out the Identity Protection playbook

Microsoft Identity Manager

What is it?

Microsoft Identity Manager provides comprehensive on-premises identity and access management, including

- HR-driven user provisioning
- Synchronization of identities between directories, databases, and applications
- Self-service password, group, and certificate management
- Increased Active Directory-based admin security with policies for privileged access, and just-in-time role assignment

Microsoft Identity Manager 2016 is licensed on a per-user basis. A Client Access License (CAL) is required for each user whose identity is managed. A Windows Server license is required to use Microsoft Identity Manager 2016's server software as a Windows Server add-on. Microsoft Identity Manager 2016 is also included with Azure Active Directory Premium P1 which is part of Enterprise Mobility + Security.

Why is it useful for your business?

- Provides a common identity for your business through automated workflows, business rules, and easy integration with heterogeneous platforms across the datacenter and cloud.
- Enables users to self-remediate identity issues, including group membership and smart card functions.
- Unify access through a reduction of the number of usernames and passwords needed to login. Ensure admin accounts are only going where they need to go and doing what they need to do

Related documentation

- Microsoft Identity Manager Overview
- Microsoft Identity Manager Documentation

Multi-Factor Authentication

What is it?

Azure Multi-Factor Authentication (MFA) is Microsoft's two-step verification solution. Azure MFA helps safeguard access to data and applications while providing a seamless sign-in process for users. This feature delivers strong authentication using a range of authentication methods including phone call, text message, mobile app notification, or mobile app verification code. When a user signs in to a resource that requires MFA, they will use a previously registered authentication method to provide additional verification of their identity. Thus, even if an attacker manages to learn the user's password, it is useless without also having possession of an additional authentication method.

Why is it useful for your business?

- Azure MFA ensures your organization is always protected using the highest industry standards of strong authentication.
- Azure MFA is simple to set up and use. It can be applied to SaaS apps, or on-premise apps through the NPS Extension or ADFS MFA adapter. Best of all, in many instances it can be set up with just a few simple clicks.
- End users have a clear registration and logon experience that is similar for all authentication methods. Users can manage their own authentication methods through a portal.

Related documentation

- What is Azure Multi-Factor Authentication?
- How Azure Multi-Factor Authentication works

Pass-Through Authentication

What is it?

Azure AD Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords. This feature provides your users a great sign-in experience - one less password to remember, and reduces IT helpdesk costs because users are less likely to forget how to sign in. And organizations get the benefits of Azure AD's cloud authentication - security, scale and reliability. This feature works by validating users' passwords directly against your on-premises Active Directory as part of the authentication process.

You can combine Pass-through Authentication with the Azure AD Seamless Single Sign-On feature. This way, when your users are accessing applications on their corporate machines inside your corporate network, they don't need to type in their passwords to sign in.

Why is it useful for your business?

Key benefits of using Pass-through Authentication:

- **Great user experience**
  - Users use the same passwords to sign into both on-premises and cloud-based applications.
  - Users spend less time talking to the IT helpdesk resolving password-related issues.
  - Users can complete self-service password management tasks in the cloud.
- **Easy to deploy & administer**
  - No need for complex on-premises deployments or network configuration.
  - Needs just lightweight agents to be installed on-premises.
  - No management overhead. The agent automatically receives improvements and bug fixes.
- **Secure**
  - On-premises passwords are never stored in the cloud in any form.
  - The agent only makes outbound connections from within your network. Therefore, there is no requirement to install the agent in a perimeter network, also known as a DMZ.
  - Protects your user accounts by working seamlessly with Azure AD Conditional Access policies, including Multi-Factor Authentication (MFA), and by filtering out brute force password attacks.
- **Highly available**
  - Additional agents can be installed on multiple on-premises servers to provide high availability of sign-in requests.

Related documentation

- Pass-through Authentication
- Seamless Single Sign-On

Privileged Identity Management

What is it?

Organizations want to minimize the number of people who have access to secure information or resources, because that reduces the chance of a malicious user getting that access, or an authorized user inadvertently impacting a sensitive resource. However, users still need to carry out privileged operations in Azure AD, Azure, Office 365, or SaaS apps. Organizations can give users privileged access to Azure resources like Subscriptions, and Azure AD. There is a need for oversight for what those users are doing with their admin privileges. Azure AD Privileged Identity Management helps to mitigate the risk of excessive, unnecessary or misused access rights.

Why is it useful for your business?

- See which users are assigned privileged roles to manage Azure resources, as well as which users are assigned administrative roles in Azure AD
- Enable on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune, and to Azure resources of subscriptions, resource groups, and resources such as Virtual Machines
- See a history of administrator activation, including what changes administrators made to Azure resources
- Get alerts about changes in administrator assignments
- Require approval to activate Azure AD privileged admin roles
- Review membership of administrative roles and require users to provide a justification for continued membership

Related documentation

- What is Azure AD Privileged Identity Management?
- Privileged Identity Management for Azure resources

RBAC for Azure Active Directory Administrators

What is it?

Using Azure Active Directory (Azure AD), you can designate separate administrators to serve distinct functions. Administrators have access to various features in the Azure portal and, depending on their role, can create or edit users, assign administrative roles to others, reset user passwords, manage user licenses, and manage domains, among other things.

Why is it useful for your business?

- Assigning non-Global Administrator roles allows organizations to better enforce the principle of least privilege when granting administrative permissions
- The principle of least privilege is important to preventing accidental or malicious misconfiguration of critical services, or the compromise of sensitive information.

Related documentation

- Assigning administrator roles in Azure Active Directory

Self-Service Application Access

What is it?

Self-service application access allows your users to self-discover applications and access application on demand, optionally allow the business group to approve access to those applications. You can allow the business group to manage the credentials assigned to those users for Password Single-sign on Applications right from their access panels. Enable Self-service application access to any applications that you wish to allow users to self-discover and request access to.

Why is it useful for your business?

- Save time and money for your IT group by delegating the access management to the user and your business group
- Improve user productivity by facilitating the access to key application in a secure manner

Related documentation

- How to use self-service application access
- Problem using self-service application access

Self-Service Group Management

What is it?

Managing access rights to resources and apps can be cumbersome for administrators. Azure Active Directory (Azure AD) provides the ability for these rights to be managed by groups which admins can then more easily control access of users. There are multiple ways for IT admins to manage these groups including delegation of group management operations to the trusted people who understand the business context for that group and its membership while still maintaining ultimate control. With Self-service group management features, users can create and manage their own security groups or Office 365 groups as well as approve or deny membership with Azure Premium licensing.

Self-service group management can be broken into two categories: delegated group management and self-service group membership management.

- **Delegated group management** - Admins can delegate group creation, and the ability to manage group membership by adding or removing users as necessary to one or more group owners. These group owners are fully empowered to manage the group properties and its membership and can in turn add additional group owners as required, without the need to wait for the admin. The admin can still access and control other elements of the group including group properties, membership, licensing and policies as usual.

- **Self-service group membership management** - With an Azure Premium license, admins can allow groups owners to manage group membership requests. With this feature, users can request to join a security group or Office 365 group from the Access Panel, and then the owner of the group can approve or deny the membership request. Admins control this feature along with other group settings from the Azure AD Admin center.

Why is it useful for your business?

Self-service group management is useful because it provides admins flexibility to:

- Delegate the day-to-day control of group membership to the people who understand the business context for that membership while efficiently managing access
- Provides more granular control over membership management for user looking to join groups to the trusted groups owners assigned by the admin
- Maintain ultimate control over all elements and aspects of the group including creation and owner assignment

Related documentation

- Set up self-service groups

Self-Service Password Reset/Change/Unlock with on-premises writeback to AD

What is it?

Self-service password management offers a simple means for IT administrators to empower users to change or reset their password and unlock their accounts. The feature includes password writeback which leverages Azure AD Connect to update passwords in your on-premises AD. The three components of self-service password management are as follows:

- **Self-service password change:** The user knows their password but wants to change it to something new.
- **Self-service password reset:** The user is unable to sign in and wants to reset their password by using one or more authentication methods
- **Self-service account unlock:** The user is unable to sign in with their password and has been locked out. The user wants to unlock their account without administrator intervention by using one or more authentication methods.

With self-service password management, users no longer need to call a helpdesk when they need to change their password or unlock their account. Instead, they will verify their identity with previously registered authentication methods and change their password or unlock their account themselves. This reduces helpdesk volume and costs, improves the end-user experience, and allows admins to maintain control of their security policies.

Why is it useful for your business?

Azure AD self-service password management helps you to:

- Reduce costs as help desk assisted password reset typically account for 20% of an IT organization's support calls
- Improve end-user experience and reduce help desk volume by giving end users the power to resolve their own password problems
- Drive mobility as users can reset or change their passwords or unlock their accounts from wherever they are
  Maintain control of your security policy through granular controls and settings

Related documentation

- Azure AD self-service password reset for the IT professional
- Password writeback overview
- Reset your work or school password

Sign-in and Audit Reporting

What is it?

Azure Active Directory Activity logs comprise of "Audit" and "Sign-in" logs.

- **Audit Logs:** All Management activities done on Azure Active Directory is tracked using Audit logs. Examples of Audit logs include "user management", "group management", "role management", "app management" etc. With these logs, you can trace the changes made to your directory or tenant
- **Sign-in logs:** Sign-in logs track all the user sign-ins done to resources in your tenant. The sign-in logs include app sign-ins from various sources like your federated, managed or hybrid scenarios.

How is it useful for your business?

- Helps you meet your compliance and regulatory requirements
- Provides an exhaustive list of logs that can help you troubleshoot issues in your environment (e.g. includes issues with access, security breach, access reviews, access control etc.)

- Provides a way for you to get all the Azure Active Directory logs into your SIEM tool using our rich Graph APIs.

Related documentation

- Intro to Azure Active Directory Activity logs in Azure Portal
- Context based Search on Azure Active Directory Activity logs
- Programmatic Access to Azure Active Directory Activity Logs API
- Azure Active Directory Activity logs in Power BI

Single Sign-On (SSO)

What is it?

Azure Active Directory supports several different methods to configure connections to public SaaS apps, which vary depending on the protocols and integration capabilities supported by the app. These can be broken into three categories:

- **ISV-Integrated Apps** - These include applications who have registered their apps with Azure Active Directory and have done work to deeply integrate with it. These apps typically support Open ID Connect as the authentication method (but can support other methods), and support "one-click" setup and configuration with customers Azure Active Directory tenants via an OAuth-based "consent" work flow. There are hundreds of apps that support this level of integration, some examples of which include Smartsheet and Collabco MyDay.
- **Microsoft-Integrated Apps** – These include applications that support a standard method of authentication (SAML 2.0, WS-Federation, or forms-based login) for which Microsoft has validated as working with Azure Active Directory, and published configuration tools and guidance to make it easy for customers to connect them to their Azure Active Directory tenants. For some of these apps, such as Google Apps and ServiceNow, Microsoft provides a "one-click" set up experience whereby a customer enters their app admin credentials in the Azure management portal, and Azure Active Directory automates setup and configuration through a management web API provided by those apps. For other apps, the Azure management portal provides step-by-step instructions for setting up the integration on the app side. Azure Active Directory provides a pre-integrated Application Gallery containing thousands of apps that support this level of integration, some additional examples of which include Salesforce, Workday, Box, Dropbox, Concur, Workplace by Facebook, and Zendesk.
- **Self-Integrated Apps** – Using our "bring your own apps" feature, an organization can also manually configure any non-Microsoft-or-ISV-integrated SaaS apps that support SAML 2.0, WS-Federation, or forms-based authentication to perform SSO with their Azure Active Directory tenant. An organization can also integrate third-party apps that use OpenID Connect and OAuth 2.0 through the Azure Active Directory developer experience.

Why is it useful for your business?

Azure Active Directory's single sign-on capabilities allow an organization to extend their access control and governance boundaries to a world of connected SaaS and other custom-developed applications.

- Enables users to access any SaaS application based on their organizational account in Azure Active Directory from any device, anywhere in the world.
- Provides centralized application access management in the Azure portal enables single point of SaaS application access and management, with the ability to delegate application access decision making and approvals to anyone in the organization.
- Enables a unified layer of reporting and monitoring of end user activity.

Related documentation

- Azure Active Directory Application Marketplace
- What is application access and single sign-on with Azure Active Directory?

User and Group Provisioning

What is it?

The Azure Active Directory (Azure AD) User Provisioning Service allows you to automate the creation, maintenance, and removal of user identities in cloud Software-as-a-Service (SaaS) applications such as Dropbox, Salesforce, ServiceNow, and more. Below are some examples of what this feature allows you to do.

- Automatically create new accounts in the right systems for new people when they join your team or organization.
- Automatically deactivate accounts in the right systems when people leave the team or organization.

- Ensure that the identities in your apps and systems are kept up-to-date based on changes in the directory, or your human resources system.
- Provision non-user objects, such as groups, to applications that support them.

Automated user provisioning also includes the following functionality:

- The ability to match existing identities between source and target systems.
- Customizable attribute mappings that define what user data should flow from the source system to the target system.
- Optional email alerts for provisioning errors
- Reporting and activity logs to help with monitoring and troubleshooting.

Why is it useful for your business?

Some common motivations for using this feature include:

- Avoiding the costs, inefficiencies, and human error associated with manual provisioning processes.
- Avoiding the costs associated with hosting and maintaining custom-developed provisioning solutions and scripts
- To secure your organization by instantly removing users' identities from key SaaS apps when they leave the organization.
- To easily import large numbers of users into a particular SaaS application or system.
- To enjoy having a single set of policies to determine who is provisioned and who can sign in to an app.

Related documentation

- Automate user provisioning and deprovisioning to SaaS applications with Azure Active Directory

Windows Hello

What is it?

Windows Hello for Business replaces passwords with strong two-factor authentication on Windows PCs. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN. Windows Hello can be used to sign in or unlock the PC and then get single sign on to all the cloud resources as well as on-premises resources.

Why is it useful for your business?

The primary goal for Windows Hello is to provide fast, secure sign in without a password. Reducing the reliance on passwords helps accomplish the following:

- Reduce costs as resetting passwords typically account for 20% of an IT organization's support calls
- Improve end-user experience and increase productivity since employees don't spend time trying to remember or type in their password
- Set customizable security policies (I.e. PIN complexity, MFA unlock, etc.)

Related documentation

- Windows Hello for Business Information
- Windows Hello for Business Deployment Guide

Windows, Office, and Intune Integration *[EMS]*

What is it?

Beyond the value that Azure AD Premium P1 and P2 provides, with the full Enterprise Mobility + Security Suite (EMS), you can enable additional scenarios, such as mobile device and application management with Intune, information and content protection with Azure Information Protection, and full virtualization support with Remote Desktop Services. With EMS, you get deep, out of the box, integration across the Office and Windows suites, which enables your users to get access to important organizational resources securely, no matter what device they are using. And with the rich security tools provided in the Azure AD Premium P1 and P2 suites, you can be confident that your user's access is protected no matter where they are or what they are doing.

Why is it useful for your business?

- Give your organization the freedom to work from any device and enable full user self-service with Intune's Mobile Device Management and Mobile Application Management platform.
- Reduce cost and get anywhere access to windows apps and services through Remote Desktop Virtualization
- Classify, encrypt, and track access to your business-critical data and assets with Azure Information Protection

- Protect your organization through a unified identity-driven security story that spans on-premises the cloud alike with Azure Active Directory
- Stay productive by providing seamless access to organization resources from any device anywhere on the planet with Azure Active Directory

Related documentation

- Enterprise Mobility and Security Suite Overview
- Intune Overview
- Remote Desktop Services Overview
- Azure Information Protection Overview
- Azure Active Directory Overview

Omada Capability Details

Omada Identity Governance solution, running on Azure, in combination with Microsoft Azure Active Directory Premium provides a comprehensive next-generation identity governance solution, enabling you to utilize your existing Microsoft resources.

Omada Identity Governance solution is the only comprehensive identity and access governance platform built on the Microsoft stack, provided as a service on Azure. The open platform architecture enables organizations to rapidly adopt to future functionality.

The Omada solution connects directly with Microsoft AD, Azure Active Directory, Azure Active Directory Premium, Azure Active Directory Access Panel, Azure Management API, the Azure Graph API, MIM and supports OpenID Connect via Azure and a long list of other systems enabling businesses to implement full identity and resource lifecycle governance across all enterprise systems both on-premises and in the cloud.

The Omada solution also provides an extended experience by supporting SQL Server Integration Services, Power BI, and the .Net framework, which means existing skilled resources in the organization can be used.

In addition, the solution integrates with a range of applications such as SAP and RACF/Mainframe-based banking systems and other on-premises applications. The solution centrally handles multiple Active Directory forests, and multiple Azure and Office 365 subscriptions.

Access Reviews across Hybrid Environments

What is it?

Omada's Automated Access Review & certification of access across hybrid environments verifies that users still only have the access they need, when they need it – eliminating excess access, supporting compliance, and enhancing the overall security position of the enterprise.

Access Reviews across hybrid environments allow managers and business system owners to verify on a regular or ad hoc basis that business system users have appropriate levels of access to all on-premises and cloud-based applications. The information provides decision support in a way that is meaningful for the business.

If an employee no longer need access to a resource in e.g. a SAP system, for example, if they have moved to a different project or left the company, their access can be automatically de-provisioned. When Access Reviews are conducted the system validates for e.g. cross system SoD policy violations.

The access certification and access review process is supported by data classification features to disclose high-risk entitlements. Access review changes are automatically propagated to the Azure Active Directory Premium.

Why is it useful for your business?

Conducting Access reviews across all critical on-premises and cloud-based applications ensures:

- The business remains compliant with internal access policies as well as any external government data protection regulations as defined in SoX, HIPAA, CoBIT, EU GDPR, ISO27001, BaFin and other regulatory requirements
- Users only have access to the information they need when they need it
- Compliance with SoD policies, role-based policies, and other policies

Related documentation

- Risk Assessment
- Hybrid Access Governance – Microsoft Azure – Seamless Integration Across Hybrid Platforms
- Identity and Access Management
- Automated Workflows

Business Context Management

What is it?

Omada Business Context Management allow organizations to model and govern advanced organizational structures such as matrix management structures or organizations where employees have multiple organizational affiliations.

Omada Business Context Management allows for the fact that that people can be part of project teams or assigned to temporary assignments in addition to their normal job role. Specific entitlements can be associated with the context. Examples of business context include a department, project, cost center, or building. Omada Business Context Management supports the governance of organizational contexts throughout their lifespan.

Why is it useful for your business?

- Organizations can automate access governance that fits with their (complex) organizational setup
- Organizations significantly reduce the number of user-entitlement settings that need to be configured by the administrator
- Enables governance of business centric policies such as separation of duty (SoD) policies.

Related documentation

- Hybrid Access Governance – Microsoft Azure – Seamless Integration Across Hybrid Platforms

Business Delegation Workflows

What is it?

The Business Delegation Workflows capabilities provides a delegated experience of a multitude of governance processes for business users e.g. Line Managers. This enables the business to take ownership of the processes without involving the IT department.

Business managers can further delegate their governance responsibilities to others within the business, such as conducting approvals, to ensure e.g. the process of granting access to business systems is not delayed.

Sample options to further delegate:

- Permanent delegation – appointing a manager's personal assistant as fulltime approver
- Temporary delegation – short term delegation to another employee while approver is away
- In-process delegation – reassigning an incorrectly forwarded access request to a more appropriate approver such as a business system owner

Enforcement policies can be put in place to allow delegation for certain resources but not for others depending on their level of risk or sensitivity. So, for example, controls ensure that domain admin access requests cannot be granted or optionally require additional levels of approval before they are granted.

Why is it useful for your business?

- Empowers the business to get in control and reduces the burden on IT
- The processing of approving various tasks is not delayed due to business system owners not being available
- Employees gain access to required resources quicker, so they can become productive sooner

Related documentation

- Automated Workflows
- Hybrid Access Governance – Microsoft Azure – Seamless Integration Across Hybrid Platforms

Compliance Dashboard

What is it?

The Omada Compliance Dashboard (Compliance Dashboard) is a graphical dashboard showing the compliance levels of all entitlements across all target business systems across the hybrid enterprise.

The Compliance Dashboard provides a 360-degree view of all access rights in the organization and provides comprehensive access control with the capability to drill down into the details of a system and launch mitigating activities directly within the Compliance Dashboard.

The Compliance Dashboard show a business-level overview of compliance levels across all on-premises and cloud-based systems. Any accounts or entitlements highlighted as non-compliant can be drilled into so that mitigating action can be taken.

The Compliance Dashboard provides automated detection of non-compliant access across identities, user contexts, accounts, and entitlements from all application sources.

Any entitlement and/or accounts that are non-compliant because of, say, not being approved or not being assigned to an actual employee can be investigated by drilling down into the details. This provides the administrator with information that allows them to determine the actions that need to be taken to bring the system back into compliance.

The Compliance Dashboard is used on an on-going basis by the identity administrator to ensure that all systems remain compliant as changes are made to each business system.

For example, Active Directory accounts can automatically be compared to an HR database (often referred to as the "authoritative source" as it is usually the most reliable record of current employees), the Compliance Dashboard will show how many of them could not be matched with an HR record. The administrator can then drill down to determine whether this is, for example, because the employee has left the company but still has an active account resulting in an orphan account, there is a mismatch between the names in AD and the HR system, or the account is an administrator account without an owner assigned to it. Using this information, the administrator can take corrective actions to delete/disable the account, correct the details in AD or in the HR system, or assign the administrator account to an individual.

Why is it useful for your business?

The Compliance Dashboard provides the organization a continuous view of whether all their business systems are access compliant:

- Provides means for quick remediation of any non-compliance and enables organizations to meet global and local data compliance standards
- Provides an overview of showing that corporate policies are enforced across all applications and systems, and establishes full access overview and documentation

Related documentation

- Risk Assessment
- Prepare for EU GDPR
- Omada E-Book EU GDPR
- Audit Reporting
- Segregation of Duties (SoD) Management
- Reconciliation – Automated processes for comparison and evaluation of identity and access data

Configurable out-of-box B2C and B2B user self-service portal

What is it?

Omada's Configurable out-of-box B2C and B2B user self-service portal (the portal) allows business partners to enroll themselves, so they can access relevant business systems made available to them via a service catalog. Business partners can be granted access to systems across hybrid environments, including systems that are not managed via AD groups, with or without workflow-based approvals based on defined policy. In addition, the portal provides self-registration via multiple identity providers such as LinkedIn and Facebook. The portal provides additional services available for the end user such as maintaining their own user profile and associated data.

Why is it useful for your business?

- The user self-service portal reduces the need for IT to be involved in processes that do not require their intervention.
- Having business partners perform self-service functions means that they remain efficient as they are able to enroll themselves into systems quickly.

Related documentation

- Configurable out-of-the-box B2C and B2B user self-service portal

Cross-System Access Suspension

What is it?

In the event of a security breach, it is necessary to lock out one or more identities from accessing business systems. Omada Cross-System Access Suspension provides an emergency lockout feature which enables an administrator to disable a user's access to all on-premises and cloud-based systems the user has access to.

Why is it useful for your business?

This cross-system access suspension limits a company's exposure to further breaches while an investigation is carried out and the user's passwords are reset.

Cross-System Data and System Classification Surveys

What is it?

Omada's Cross-System Data and System Classification Surveys enable resources to be classified according to the company classification system. For example, if a company is considering GDPR compliance then they need to establish where all the personal data is stored. By conducting classification surveys, managers as well as system and resource owners can specify whether a system holds personal data or not. Once classification is complete, access reviews can be performed on systems that meet certain criteria – for example, all those resources that hold data relevant to GDPR compliance or resources that are a high risk.

Why is it useful for your business?

Classifying systems based on the data they hold or the level of business risk they present is a key step to managing risk and compliance. Once these systems have been identified, access surveys can be carried out against them to verify that only appropriate users have the access to them. This increases the overall compliance and security posture of the company.

Related documentation

- Prepare for EU GDPR
- Omada E-Book EU GDPR
- Risk Assessment

Cross-System Password Management

What is it?

Omada cross-system Password Management makes the task of password management simpler by taking control of the resetting and synchronization of passwords across all systems regardless of whether they are on-premises or cloud-based applications.

Omada cross system password synchronization covers all connected systems including AD, automatically propagating a password change through Azure Active Directory and AD SSPR extension.

Cross-System Password Management makes password management simpler by taking control of resetting and synchronizing passwords across all systems. It also supports password policies and specific policies based on account types. So, for example, for an administrator account of a highly sensitive system, a highly complex password would be required whereas an ordinary user of a low risk system would only require a basic password.

Why is it useful for your business?

The management of passwords across systems ensures greater levels of security while also reducing the administrative burdens of password management by the IT department.

Cross-System Separation of Duty Rules and Mitigating Controls

What is it?

Omada's Cross-system Separation of Duties (SoD) and mitigating controls allow the creation and enforcement of policies spanning multiple business systems. This ensures that SoD rules are not being violated due to access levels being granted across multiple platforms.

As an example, a SoD policy can be established to prevent a toxic combination of two entitlements, e.g. a person in a bank cannot have access to both front office and back office entitlements.

Enforcement of policies for segregation of duties happens continuously throughout a user's lifecycle within an organization. Policies can be defined and enforced during access reviews or access request processes for additional control.

These SoD policies and rules are verified in a variety of processes, such as access requests, to ensure that provisioning actions do not violate specific rules. If the administrator decides to manually override the control due to a valid business reason, they can input the justification which can be used for future auditing purposes.

Why is it useful for your business?

Cross-system separation of duty rules and mitigating controls make it easier for the business to prevent global SoD rule violations and to prove that they remain compliant.

Related documentation

- Segregation of Duties (SoD) Management

- Risk Assessment

Current-State Entitlements Reporting

What is it?

Omada's Current State Entitlements Reporting provides automated audit and compliance reporting with predefined reports that demonstrate the effectiveness of the identity controls across the organization, reducing the burden on IT and improving visibility for the business. The current/actual state of user account entitlements in the target business systems is continuously compared to the organization's desired state. Any differences are visible in the Compliance Dashboard, so they can be instantly resolved.

Why is it useful for your business?

Understanding the current-state of entitlements across all target business systems means that the administrator can continually assess the level of risk that the company is exposed to due to non-compliant identities. The business-level overview makes this risk assessment easier as the actual systems are represented rather than the underlying security architectures that support them.

Related documentation

- Reporting and Analysis
- Risk Assessment

Desired and Actual State Reconciliation

What is it?

Omada provides a unique reconciliation feature-set for comparison of the actual state of data versus the desired state to disclose out of band entitlements, resources, or applications. This is automated by a role and policy engine that performs continuous reconciliation between the desired state which is based on the defined policies and the actual state of user access rights to business systems. Any inconsistencies which need to be resolved are flagged in the Compliance Dashboard and different types of mitigation activities can be launched automatically or manually.

Why is it useful for your business?

The continuous reconciliation ensures the Compliance Dashboard always displays the most up-to-date compliance status for all business systems governed/monitored. This means that the business is constantly aware of any risks that they need to take into consideration.

Related documentation

- Reconciliation – Automated processes for comparison and evaluation of identity and access data
- Risk Assessment

Entitlement Catalog

What is it?

The Omada Entitlement catalog contains a repository that provides a means to capture, organize and assign ownership of accounts and entitlements that determine the access users have from various account repositories throughout their environments. An entitlement is an abstract data structure that can represent the many forms of permissions that users have in a broad range of infrastructure systems and business applications.

The Omada Entitlement Catalog can capture entitlements from a variety of source systems, using standard connectors or Omada SDK, or by importing entitlements from flat-file extracts which is, for example, useful in the early stages of IGA deployment. The Omada entitlements catalog is kept up-to-date with the actual data in target systems through Omada's reconciliation processes.

The Omada Entitlement Catalog can handle administrative entitlements, such as roles or resources that are used for day-to-day user administration in the target systems. It also handles business systems that have complex, multilevel authorization models that and have their own role-based administration frameworks. The Omada Entitlement catalog can consume and understand the different types of entitlements from multiple levels of complex authorization models for specific applications from vendors such as SAP. As entitlements are often defined using IT-oriented cryptic names and lack descriptive metadata on source systems, the Omada Entitlement Catalog can contain enriched entitlements such as associating them with friendly names, descriptions, tags, additional metadata and synthetic entitlements that are more meaningful to business users. The Entitlements catalog provides a schema that is extensible through configuration.

Why is it useful for your business?

The Omada Entitlement Catalog enables governance of entitlements across all systems in a hybrid environment, ranging from simple cloud systems to complex business systems such as SAP that have complex, multilevel authorization models and provide their own role-based administration frameworks. The Omada Entitlement Catalog enables entitlement data governance for connected systems as well as for systems that are manually reconciled by importing entitlements from flat-file extracts.

Fine-Grained Provisioning

What is it?

Omada Fine-Grained Provisioning includes capabilities to handle granular control across complex target systems, including fine grained provisioning and de-provisioning operations. Fine grained provisioning is supported out of box to a range of applications such as a range of SAP applications.

Why is it useful for your business?

Automates access governance with the required level of detail

IGA Process Framework

What is it?

The Omada Process Framework is a comprehensive set of best practice out-of-the-box processes that are pre-configured in the solution. Created during two decades in close collaboration with leading international organizations, the Omada Process Framework provides a great input for any organization helping them to implement high quality compliant governance processes successfully.

Why is it useful for your business?

The best practices provided within the Omada Process Framework accelerates the implementation process and thus enables companies to get results quickly from their IGA implementation. It also helps companies achieve international standards such as ISO 27001.

Related documentation

- Omada Process Framework – Accelerate your IAM Projects
- Step-Wise Implementation Approach

Integrated Identity Lifecycle Management for hybrid environments

What is it?

Integrated Identity Lifecycle Management manages the on-boarding, changes and off-boarding of employees and contractors – the joiner-mover-leaver processes – across all business systems regardless of whether they are on-premises or cloud-based.

As employees, partners, and contractors join the organization, the combination of Azure Active Directory Premium and Omada's identity governance solution ensures they have easy access to the initial resources and applications they need even before day one in the company. The capability generates all necessary content in the Azure Active Directory Access Panel to defined birth rights and user role(s) when onboarding a new employee or contractor.

This increases productivity as no workhours are wasted on getting access to the systems and applications they need. They will be up and running from day one.

Automated access changes based on identity lifecycle events such as join, move, or leave across all applications (cloud or on-premise) ensure access is granted and enforced in line with business policies or roles.

As their role within the organization changes, their access rights might also change along with them, so they only have access to what they need to fulfill their new role. Each change not only affects accounts and entitlements within the enterprise, but is also synchronized with the Microsoft Access Panel, ensuring that users can easily see available applications.

These processes are typically triggered via changes in the HR system which results in updates to identities and their relationships within the company. Roles and assignment policies are then used to determine which access rights should be granted and revoked.

Access rights for terminated employees or contractors, can be closed down from one central location, thereby automatically disabling access to all on-premise and cloud-based systems minimizing the risk of unauthorized access.

Why is it useful for your business?

Automating the process of identity lifecycle management reduces the amount of IT administrative tasks while ensuring that all users' access rights are kept compliant with internal and external regulations. This includes ensuring that employees do not accumulate more access rights over time than they need to perform their current jobs. As employees, partners, and contractors join the organization, the combination of Azure Active Directory Premium and Omada's identity governance solution ensures they have easy access to the initial resources and applications they need even before day one in the company. This increases productivity as no workhours are wasted on getting access to the systems and applications they need. They will be up and running from day one.

Related documentation

- Hybrid Access Governance – Microsoft Azure – Seamless Integration Across Hybrid Platforms
- Identity Lifecycle Management

Logical Business Application Onboarding and Management

What is it?

Logical Business Application Onboarding and Management enables the business to govern its Applications. The business can translate technical objects and systems into language and provides experiences that are understandable for the business. For example, resources are translated into business language rather than being at a technical level.

This makes it easier for non-IT employees to choose the resources they need access to without understanding the underlying technical details. The seamless application onboarding process unifies onboarding of new applications, and applies appropriate governance policies, dependent on the sensitivity of the application.

Why is it useful for your business?

Non-IT employees can choose the resources they need access to without understanding the underlying technical details. This secures adoption, saves time, increases security as rubber stamping is avoided.

Logical Identity Mapping from Multiple Sources of Authority

What is it?

When verifying the validity and justification of AD user accounts, multiple sources of authority containing employee and contractor records must often be correlated and validated, as most organizations have multiple sets of employee records stored across different HR systems/authoritative sources. This could, for example, be due to a separation between permanent employees and contractors, or due to a history of company mergers and acquisitions.

Omada handles the mapping, combining and correlation of logical data from multiple authoritative sources and uses the built-in feature-set to clean up data and to run lifecycle processes in scenarios where such multiple sources of authority are maintained.

Why is it useful for your business?

- Cleans up directory data to accelerate the journey to the cloud
- Secures complaint data across multiple sources of authority
- Enables organizations to govern access under such circumstances

Multi-affiliation support

What is it?

Multi-affiliation support allows employees to be associated with several different functions with different types of access rights within the organization, supported by various concepts such as the fact that an identity can have multiple accounts and Omada's unique context concept. This gives the employees access to different sets of applications to perform their various duties while simplifying the administration of identities overall as each affiliation can still be managed separately.

Why is it useful for your business?

Unlike most organizations where employees have a single defined role, in some organizations such as government agencies or educational institutions, employees perform several different job functions. Multi-affiliation allows for the modelling of this type of environment but keeps the overall management of the identities simple.

Out-of-box connectors for 3rd party PAM solutions

What is it?

The out-of-the-box connectors collect information from a range of Privileged Access Management solutions so that information about access rights to both privileged accounts and normal accounts can be combined to determine overall compliance.

Why is it useful for your business?

Gives companies a complete overview of who has access to what, who authorized the access, and whether the access is appropriate and is being used appropriately.

Related documentation

- Privileged Access Management – One Central Platform for all Identities and Accounts
- Privileged Access Management – Control, Log, and Monitor Privileged Accounts

Point-in-time Auditor Reporting

What is it?

Point-in-time auditor reporting allows organizations to demonstrate who had what level of access to individual systems at any time in history. It also explains why they were given access which could be important information during any security incident investigations.

Why is it useful for your business?

- Eases preparation for an audit
- Eases investigations in connection with a potential security breach, providing internal or external investigators insight into which accounts had which level of access to the compromised systems at a given point in time.

Related documentation

- Audit Reporting – Meet On-Going Compliance Requirements
- Risk Assessment

Policy Lifecycle Management

What is it?

Omada Policy Lifecycle Management supports the full lifecycle of managing policies such as SoD policies, assignment policies and data classification policies throughout their lifespan including creation, management and attestation of policies. A policy can be assigned to an individual user, a context or a role.

Why is it useful for your business?

- Enforces corporate policies across all applications and systems
- Required to automate compliant access policy handling as defined in SoX, HIPAA, CoBIT, EU GDPR, ISO27001, BaFin and other regulatory requirements

Related documentation

- Policy Lifecycle Management

Provisioning Service with SDK

What is it?

Omada Provisioning Service enables creation of user accounts and their associated access rights in different business systems and applications. The provisioning process considers policies such as SoD to ensure there are no violations.

Omada Provisioning Service supports automated provisioning of access changes to the Azure Active Directory Access Panel and provisioning of applications on mobile devices via Intune.

Built-in provisioning and access governance of Azure infrastructure resources ensuring cloud resources stay in control throughout their entire lifecycle.

Omada Provisioning Service manages synchronization for all target cloud applications with available Azure Active Directory connector

Why is it useful for your business?

The provisioning service automates the creation or modification of user accounts and their access rights which reduces the workload for the helpdesk and minimizes the introduction of compliance-related issues as it considers all of the existing access rules that have been created.

RBAC and ABAC to hybrid environments

What is it?

Role-Based Access Control (RBAC) allows organizations to create advanced role models which can map to complex organizational structures. In addition, Omada's Attribute-Based Access Control (ABAC) provides additional dimensions to traditional RBAC implementations by allowing more advanced contexts to be created. For example, a context can be time-limited so that a user can only gain access to a resource for a defined period. It is also possible to have multiple assignments for the same context.

Why is it useful for your business?

- Provides a high degree of automation of access governance and reduces administrative time spent

Role Lifecycle Management

What is it?

Omada Role Lifecycle Management supports the full lifecycle of managing roles throughout their lifespan. A role describes users who have the same or very similar jobs. Examples of roles include a sales rep, accountant, programmer, and product manager. Users are typically assigned to a role based on their job description when they join the company.

Why is it useful for your business?

- Reduces the burden of administering individual users and policies associated with them

Related documentation

- Role Lifecycle Management

Self-Service Access Requests for hybrid environments

What is it?

Omada provides a user-friendly self-service portal for access requests with integrated approval workflows that supports request access across hybrid applications including for Microsoft applications including Office 365, cloud resources, and non-Microsoft applications with seamless integration to Azure Active Directory Access Panel.

Employees are for instance empowered to request temporary or privileged access to resources, if needed, by utilizing a self-service access request portal. Such requests are channeled through the appropriate approval workflows and preventive policy checks are automatically conducted. Entitlements on the applicable systems are subsequently provisioned while constantly ensuring compliance with security policies.

Using the Omada Self-Service experience, employees can:

- Request access to business systems listed in a service catalog, and follow the progress of their request
- Directly access information about their direct reports
- Request resources on behalf of others – for example a manager creating requests for a member of their team.

Why is it useful for your business?

The self-service experience reduces labor-intensive and removes inefficient manual activities by empowering the business user. This saves the helpdesk time and creates organizational efficiency.

Related documentation

- Self-Service Portal - Release helpdesk resources and enable business with easy and secure access

System Onboarding

What is it?

System onboarding allows administrators to quickly and easily connect and onboard systems from one central location. The wizard-driven user experience provides a checklist and guides the administrator through all the necessary and recommended configuration steps to add new systems.

Why is it useful for your business?

System onboarding ensures an easy, structured and error-free introduction of new enterprise cloud and on-premises systems and applications needing to be governed. This ensures that governance and control are established across all used systems whether governance is full automatic or manual.

Capabilities Overlap

Omada partially provides features provided by the following Microsoft Capabilities, and this table will help you to determine and discuss with your customers how those capabilities should be best used in their organization.

Omada's capabilities are always required if organizations have:

- Users with multiple credentials across various systems
- Separate admin accounts or users with multiple affiliations
- Multiple User Stores
- Users under multiple Azure AD subscriptions or have multiple AD forests
- A matrix organization where users get their access from multiple contexts
- Several user roles and require defining rich set of access policies
- Strict SoD requirements and require compliance reporting

Microsoft Capabilities	Related Omada Capabilities	Best Practices / Recommendations
Access Reviews	Access Reviews across Hybrid Environments	Organizations who need to review group memberships within Azure AD should select *Access Reviews*. However, organizations that need an enterprise wide Access Review solution to automate recertification across the hybrid enterprise should use Omada's *Access Reviews across Hybrid Environments*. In addition to handling Azure AD group access reviews, Omada's *Access Reviews across Hybrid Environments* handles Access Reviews of AD (on-premises) groups and systems such as SAP (on-premises and cloud) and systems that are not connected to Azure AD. Organizations wanting to evaluate business decision information such as SoD policy violations during access reviews should use Omada's *Access Reviews across Hybrid Environments*.
Dynamic Groups	RBAC and ABAC to Hybrid Environments	Organizations needing to manage users, resources and assets with Azure AD can take advantage of *Dynamic Groups*. However, organizations that need to manage resources across Azure AD and other systems and directories should take advantage of Omada's *RBAC and ABAC to Hybrid Environments* to assign entitlements across systems with full auditability and transparency. Omada *RBAC and ABAC to Hybrid Environments* allows organizations to create advanced role models across applications which can map to complex organizational structures.

		Omada's Attribute-Based Access Control (ABAC) provides additional dimensions to traditional RBAC implementations by allowing more advanced contexts (such as project membership) to be created.
Self-Service Application Access	Self-Service Access Requests for Hybrid Environments	*Self-service Application Access* allows your users to self-discover applications and access application on demand, optionally allow the business group to approve access to those applications. Omada *Self-Service Access Requests for Hybrid Environments* is required for organizations with the following characteristics: • Need to request fine grained access to hybrid environments that contain e.g. SAP • Need to request access on behalf of others • Need to request access for admin accounts or users with multiple affiliations • Need to handle strict SoD requirements with in-process checks Omada *Self-Service Access Requests for Hybrid Environments* provides: • A user-friendly self-service portal for access requests with integrated approval workflows that supports request access across applications in hybrid environments including Microsoft applications such as Office 365, cloud resources, and non-Microsoft applications. • A seamless integration to Azure Active Directory Access Panel.
User and Group Provisioning	Provisioning Service with SDK	The Azure AD *User Provisioning Service* allows you to automate the creation, maintenance, and removal of user identities in cloud SaaS applications such as Dropbox, Salesforce, ServiceNow, and more. Omada's overarching provisioning concept can embrace User and Group Provisioning utilizing Omada's *Provisioning Service with SDK* to provide provisioning that spans across hybrid environments. For customers who have an existing Microsoft Identity Manager installation, Omada provide a seamless bolt-on strategy to leverage customer's existing investments.
Self-Service Password Reset/Change/Unlock with on-premises writeback to AD	Cross-System Password Management	For Azure AD and on-premises AD self-service password management, Microsoft's *Self-Service Password management* can be used. For organizations with the following characteristics: • Users have multiple credentials across various systems • Separate admin accounts or users with multiple affiliations • Multiple User Stores • Users under multiple Azure AD subscriptions or have multiple AD forests • Require cross-system Password Management Omada provides *Cross-System Password Management* to make the task of password management simpler by taking control of the resetting and synchronization of passwords across all systems regardless of whether they are on-premises or cloud-based applications.

Have an opportunity or feedback?

Send an email to microsoft@omada.dk with:

- any feedback on this document
- cool customer stories or quotes you'd like to share
- possible customer case studies
- opportunity details and what you need help with

...and we'll be happy to connect with you!