Omada Identity

Do more with identity

Govern identities and manage access to resources across your on-premises and cloud-based IT environments. Control risk, ensure compliance with regulatory requirements, and enable efficient collaboration between employees, customers, and business partners.

Digital transformation is imperative for businesses of all sizes to leverage the opportunities and impact of digital technologies. As more and more businesses utilize hybrid IT environments on their digital transformation journey, many are faced with the challenges that emerge when managing identities and access across multiple applications, clouds, networks, and servers.

Delivering an agile, user friendly, and efficient digital business experience with easy access to a multitude of systems and applications to customers, employees, and business partners requires the use of next generation identity management and access governance solutions.

Omada Identity is the leading end-to-end identity governance solution built on Microsoft technology, delivered on-premise or as-a-service, that empowers your organization to speed up its digital transformation journey.

Omada

Omada Identity

Manage Risk, Maintain Security, and Ensure Business Efficiency across Hybrid IT Environments

The access governance challenges of hybrid IT environments

As more and more businesses utilize hybrid IT environments (cloud and on-premises combined), many are faced with the challenges related to managing identities and access across multiple applications, clouds, networks, and servers.

Hybrid IT environments make it challenging to ensure that the right people, and only the right people, have access to the right resources and information at the right time across both cloud and on-premises resources.

Equally important, is the ability to govern your organization's identities and access to resources, and document compliance with legislative regulations such as the GDPR as consequences of non-compliance can be significant and costly.

Identity and access governance is key to security

Identity and access governance (IGA) processes are key to secure your digital journey, by efficiently and securely managing identity and access to resources across hybrid IT environments.
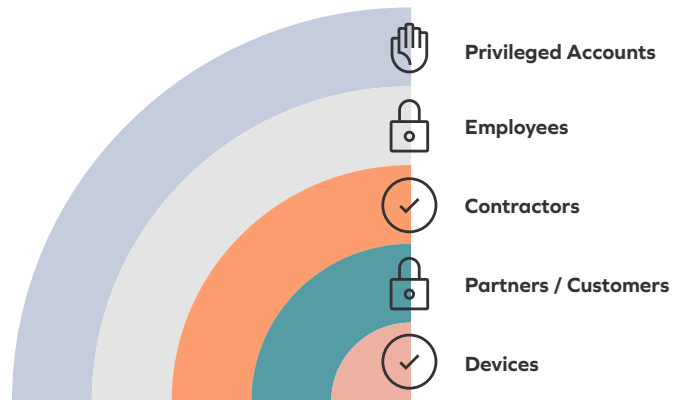
IGA processes include:

- A structured approach to 'on-boarding' applications and managing access to applications on a granular level, in compliance with company policies and external regulations

- Automation of access assignment policies and provisioning to save costs, ensure compliance, and minimize the risk of data theft by insiders or hackers

- Centralized audit and compliance reporting to ensure continuous risk overview and general visibility for the business

- Automated access reviews and certifications across all cloud and on-premises applications

End-to-end IGA solution

Omada Identity enables the digital enterprise to be secure, compliant, and work efficiently.

The end-to-end solution allows organizations to manage and govern all identity types (privileged users, employees, contractors, business partners, customers, devices, and machine identities) and manage access to all resources across systems, applications, and cloud resources.

In addition, Omada provides a clear and consistent path for organizations that migrate users and their access from on-premises to hybrid to multi-cloud solutions.

Identity types covered by the solution

- Privileged Accounts
- Employees
- Contractors
- Partners / Customers
- Devices

Best practice IGA processes

With almost two decades of experience helping organizations implement IGA, Omada has pioneered many of the best practices in use today.

To support a quality implementation, Omada Identity provides a range of built-in processes for best-practice identity management and access governance.

Key capabilities include:

- Identity lifecycle management

- Access management

- Reviews and certifications

- Self-service access requests and approvals

- Segregation of duty policies

- Role lifecycle management

- Audit reporting

All these capabilities are essential for enabling organizations to continuously meet security, risk of insider threat, regulatory access compliance, and efficiency needs in the management of users and their access to ensure regulatory compliance.

Built on Microsoft technology, supporting heterogeneous environments including SAP, the Omada Identity is an ideal and future-proof choice. The adoption investment is very low, as the solution uses standard interfaces, technologies and concepts already familiar to organizations using Microsoft technology.

IGA Reference Architecture

Import - Capture - Compare - Reconcile

Complete access overview

Delivered on-premises or as-a-Service, Omada's solution empowers enterprises to manage identities across hybrid IT systems. The flexibility of the solution allows a high degree of configurability, enabling organizations to meet business specific requirements. This approach reduces the need for custom development, decreasing deployment time, so ROI is achieved quickly.

Central to the Omada implementation approach and the Omada reference architecture is to enable enterprises to get in control of users' entitlements across a wide range of systems, and at the same time enable them to scale and stay in control for the future.

The fundamental principle of the architecture is to import and capture all identity and access related data from target systems. Combined and matched up with HR and entitlement data this import determines the actual state of identities, entitlements, and access rights.

Ongoing access control

The access overview delivers the foundation for advanced reporting and analytics to determine access compliance.

Automated processes for recertification and approval surveys rules and policies determine whether access rights are compliant and if policies like segregation of duties (SoDs) are adhered to.

When the actual state has been verified, processed and enriched, it becomes the desired state. Based on the generated overview of the desired state, policies and workflows are applied to make the required changes. Once changes have been made in the target system, the data is once again compared and reconciled to the actual state, ensuring that all changes are applied, and that the target systems are in sync.

The circular model of the reference architecture illustrates that the cycle runs continuously, making incremental changes and ensuring ongoing access compliance.
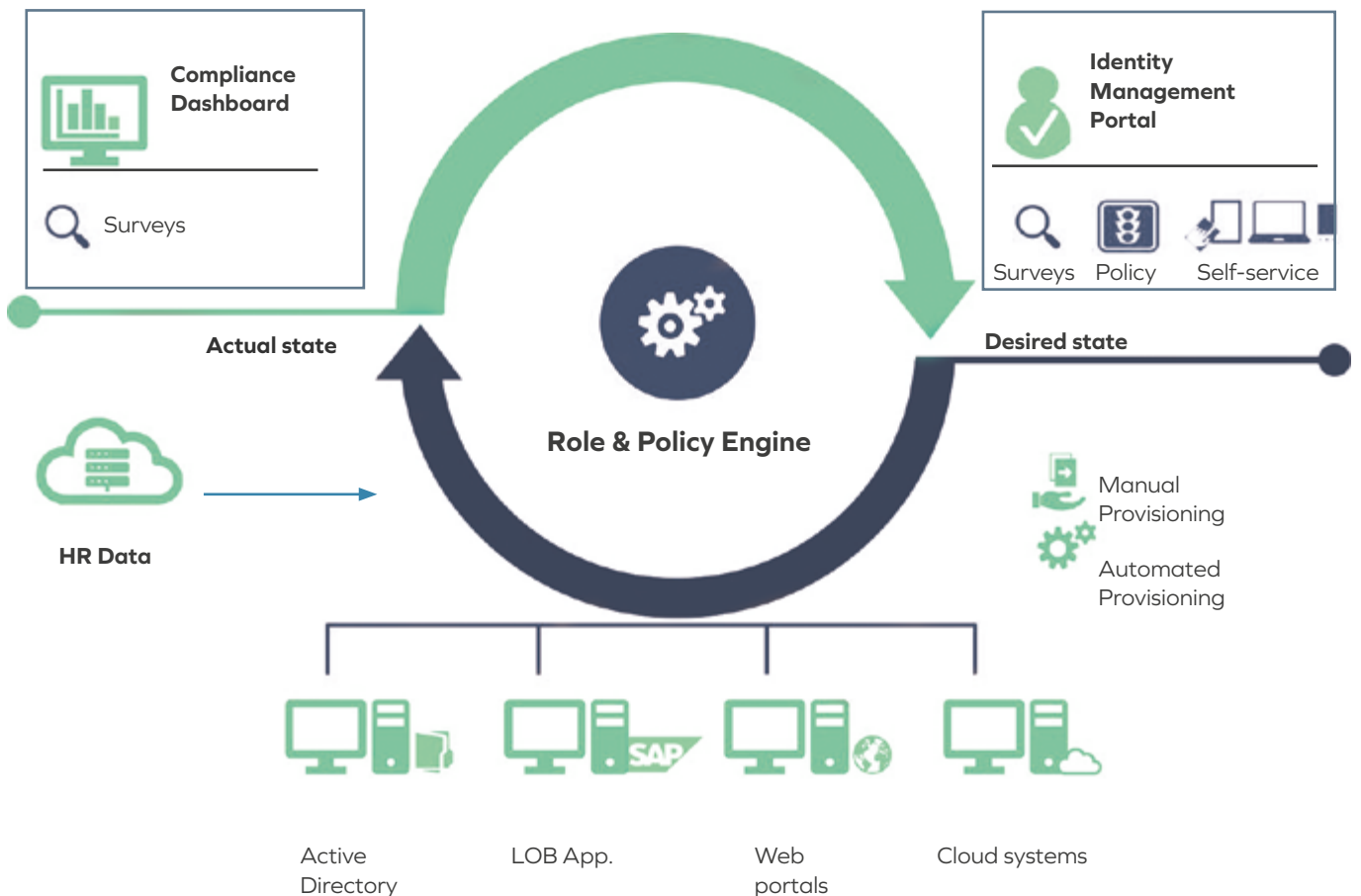
IdentityPROCESS+
Best-Practice IGA Process Framework

Omada IdentityPROCESS+ is a comprehensive, best practice process framework, which includes the most important processes needed to ensure a successful IGA deployment. The framework has been developed with the goal of supporting successful IGA projects for organizations worldwide and to help organizations implement well-proven best practice processes, reducing the need to 'reinvent the wheel'.

Identity Lifecycle Management

Controls the entire lifecycle of employees, customers, and partners. Manages employees' or contractors access rights as they join the company, move roles within the company, and leave the company. Identity Lifecycle Management processes enable the granting of access rights according to defined roles, rules, and policies.

Access Management

Supports automated provisioning and de-provisioning of users' access. Target system provisioning can be automated from policy-driven access rules and defined roles. Automated provisioning and assignment of access rights via rules and policies enables quick roll out of access to new business applications.

Business Alignment

Automated processes for on-boarding of new applications as a virtual resource, including providing meaningful business descriptions and setting default access rights based on the existing policies. Policies, roles, and contexts can be designed to accurately model and reflect the business structure.

Identity Security Breach

Enables the administrator to perform an emergency lockout to suspend all accounts associated with a compromised identity. Once the situation is under control and any access violation has been mitigated the administrator can reactivate the access.
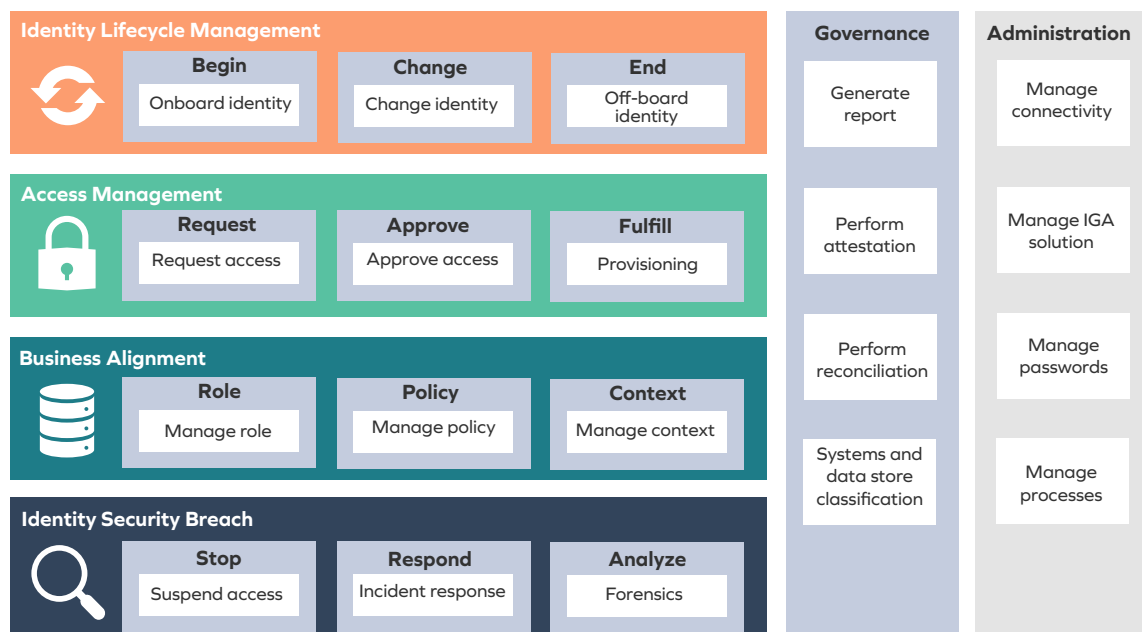
Governance

Enables easy access review, cross system reporting and analysis. Secures validation and approval of the current state of identities, account ownerships, and resource assignments. The recertification process allows definition of scheduled or event-based certifications as well as on-going periodical certifications.

Defines and manages segregation of duties (SoD) policies incl. toxic combinations of access rights. Detect and evaluate violations, to determine if the combination of access rights should be allowed or blocked, and handle mitigating actions.

Classification of data types improves management of and reporting on systems that contain business sensitive or GDPR critical data. The data classification features improve general management and oversight of data assets and enable fact-based conclusions and decision making.

Administration

Management of target systems, applications, and passwords ensure the smooth onboarding of business systems, so they can be brought under the management in the IGA system. Enables easy password reset without helpdesk contact, with synchronization of passwords across all connected applications, so users only have one password to remember.

Identity Lifecycle Management			
	Begin	**Change**	**End**
	Onboard identity	Change identity	Off-board identity

Access Management			
	Request	**Approve**	**Fulfill**
	Request access	Approve access	Provisioning

Business Alignment			
	Role	**Policy**	**Context**
	Manage role	Manage policy	Manage context

Identity Security Breach			
	Stop	**Respond**	**Analyze**
	Suspend access	Incident response	Forensics

Governance	Administration
Generate report	Manage connectivity
Perform attestation	Manage IGA solution
Perform reconciliation	Manage passwords
Systems and data store classification	Manage processes

Next-Generation IGA

## End-To-End Identity Management and Access Governance as-a-Service

Omada IdentityPROCESS+ is a comprehensive, best practice process framework, which includes the most important processes needed to ensure a successful IGA deployment. The framework has been developed with the goal of supporting successful IGA projects for organizations worldwide and to help organizations implement well-proven best practice processes, reducing the need to 'reinvent the wheel'.

✓ Automated setup of the service

✓ 24/7/365 operations

✓ High performance, high availability, capacity monitoring

✓ Dedicated service delivery manager

✓ Geo-redundancy

✓ Disaster recovery

✓ Proactive monitoring of service and data storage performance

✓ Dedicated support

✓ Patching and maintenance

✓ Diagnostics and troubleshooting

✓ Automatic scaling of database to demands in minutes

✓ Application monitoring and health check reporting

Intelligent Compliance
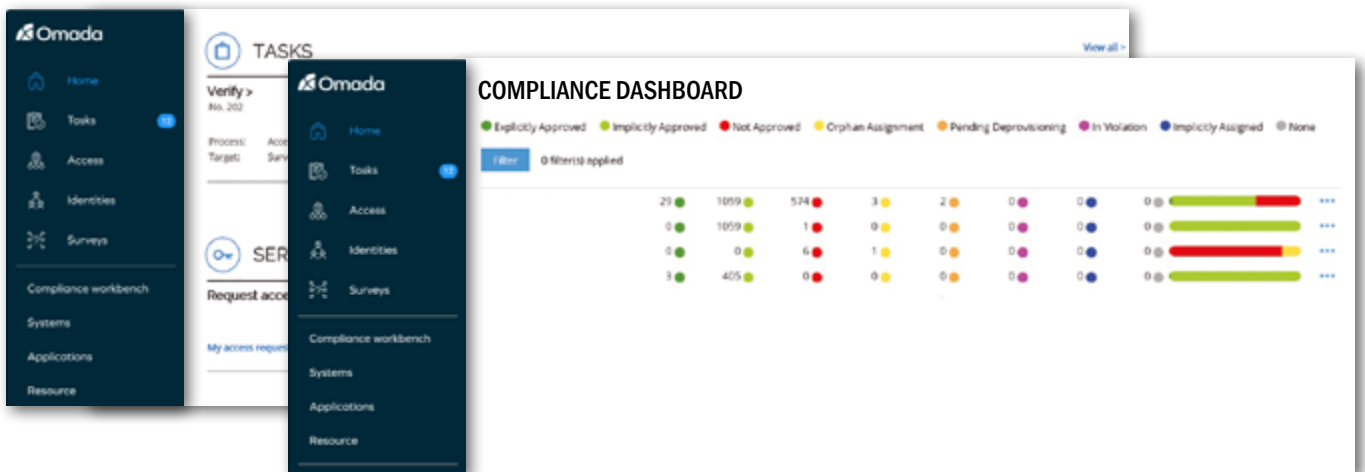
Identity intelligence through the compliance dashboard

At the heart of the solution is an interactive Compliance Dashboard, which provides a complete overview of all systems that contain critical data, with actionable workflow-based remediation functions. Built-in analysis and reporting features deliver identity intelligence and provide an overview of 'who has access to what', and 'who approved that access'.

The Compliance Dashboard renders compelling insights about systems and protected data, visualizing the compliance level for each application and system. It provides a high-level overview with traffic light indicators and the ability to drill down into detailed access data. With a single click it is possible to instantly execute remediation activities for critical findings.

Accelerate Your IGA Project
Achieve Business Value Within a Short Timeframe

The unique accelerated implementation methodology Omada Essentials uses the IdentityPROCESS+ framework to enable organizations to quickly establish a governance foundation and derive great value in a short timeframe. We start with a well-defined scope, which includes cleaning and mapping data from Active Directory and the HR database as this tends to be the most up to date system across the business. The Omada solution imports the HR data, making it visible in the Compliance Dashboard. This provides a fast overview of the actual-state of employee identities and their access across the business, immediately highlighting access risks, and providing reports for auditing and stakeholder purposes. HR data is automatically matched with access data from multiple systems and directories, account ownerships are determined, and orphan accounts are surfaced for remediation.

Omada Essentials provides the foundation for any IGA project. From here, you can deploy additional solutions and standard features, giving you the business benefits your organization needs to stay ahead.
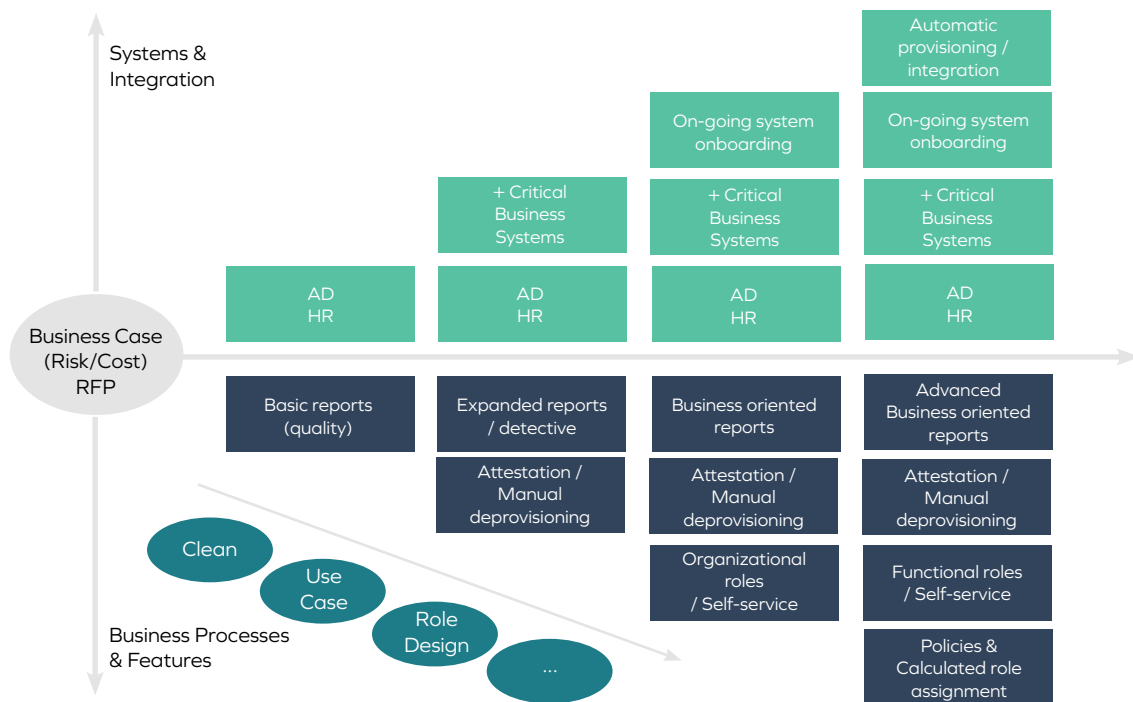
A future-proof technology platform

The Omada solution provides built-in best-practice processes derived from nearly two decades of working with some of the most successful enterprises in the world. Built on Microsoft technology the solution supports a wide set of applications through its extendable framework of connectors, including the most commonly used cloud services such as Salesforce, ServiceNow, Workday, and dozens of others, as well as various versions of SAP.

The solution runs on-premises and as-a-service on Azure and centrally handles multiple Active Directory forests, and multiple Azure and Office 365 subscriptions. Two-factor log-on experience is provided utilizing Azure AD/Federation services. We carefully follow the progress and roadmaps of our partners to ensure long-term compatibility across our connectors and core capabilities. We know our customers count on consistent performance and we are committed to ensuring that in the long-haul.

Microsoft Partner
Gold Cloud Platform
Gold Application Development
Microsoft

Omada