

End to End Identity Management

Bridging Identity Access Management and Identity Lifecycle Administration & Governance

The alliance between Omada and Optimal IdM combines Omada's best of breed Identity Governance and Administration (IGA) capabilities and Optimal IdM's cloud-based Identity and Access Management (IAM) solution to provide the most complete end to end identity management solution.

The OptimalCloud™ is a fully featured Identity as-a-Service (IDaaS) platform. It features single sign-on (SSO), federation, adaptive authentication, MFA, user/delegated administration, and auditing to provide a seamless end user experience. The OptimalCloud runs on top of Optimal IdM's Virtual Identity Server (VIS) to enable unique solution scenarios across disparate repositories.

Omada's identity governance platform provides a holistic approach to access control, this specialized suite facilitates the security, compliance and efficiency benefits customers need to run their business effectively, managing identities throughout their entire lifecycle.

Both solutions are deployed in B2E, B2B, and CIAM scenarios, used by some of the most recognizable companies on the globe and run in some of the most secure environments in the world.

End To End Identity Management



Highlights

- Address Compliance and Governance
- Manage Risk with Increased Security
- Manage Administration Costs
- Increase User Security
- Both solutions are deployed in B2E, B2B, and CIAM scenarios
- Both companies are very customer-centric
- The Optimal IdM and Omada partnership is a key differentiator in the industry



Address Compliance and Governance

With a complete access governance solution, organizations ensure that employees and external identities will always have access to what they need, and only what they need to perform their jobs. This core principle leads to achievable regulatory compliance, significant cost savings, increased employee productivity, and reduced helpdesk and IT support requirements.

The combined Omada and Optimal IdM solution provides a full range of capabilities for the modern enterprise as it digitally transforms without compromising governance, compliance, or security.

Topics to Consider

- Would the automation of your identities lifecycle management including the enforcement of security and compliance policies benefit your company? How much time is spent on handling this manually?
- How can you be sure that you have classified all your sensitive data correctly so that it can be managed appropriately to meet industry specific or legislative regulations (ISO 27001, GDPR, SOX, CoBIT, HIPPA, PCI, NIST, etc)?
- How confident are you that policies governing privileged accounts and segregation of duties are being followed across the entire enterprise?



Manage Administration Costs

Self-registration, self-service, and delegated administration features in the combined solution give end users the ability to register, request, and gain access to the system, necessary groups, and applications as requested through an automated approval process managed by the relevant business owner or delegated administrator.

Points to Consider

- Are business managers spending too much time making decisions on whether to grant access rights to employees?
- Does your helpdesk deal with a high volume of calls requesting access, group memberships, application access?
- Do you have a multi-cloud vendor strategy?



Manage Risk with Increased Security

With dynamic access control to applications and systems, organizations strive to ensure that they can provide secure access, all while providing the business owners with the views and controls to act on access risks and compliance violations.

Questions to Ask

- Can you ensure that your environments remain secure and compliant as your users' access on-premises and cloud-based applications?
- How do you provide business managers with the right level of information to determine the right levels of access their employees should be granted?
- Would you like to have control over external identities, B2C as well as B2B accounts and understand the level of access granted to external users?
- What systems do you have in place to protect against risky sign-in activity? Do your sensitive applications require increased levels of authentication?
- Do you have mechanisms to quickly lock out a user's account from all applications in the event of a potential breach being discovered?



Increase User Productivity

As employees, partners, or customers need access to the resources and applications, the joint solution ensures they have approved easy access, so no time is wasted.

Would Your Users Benefit?

- Would your organization benefit from self-registration to on-premises and cloud-based applications?
- Would federated single sign-on across your hybrid environment with full control and overview of business-critical access benefit your organization?
- How much time is spent handling provisioning manually?
- How are you using policy management automation for handling segregation of duties and other business policies to ensure compliance while minimizing human intervention?



Omada



OPTIMAL IdM