Omada

BMW Group

Cross Platform Management for 400,000 Identities

Country: Germany

Industry: Auto manufacturer

Profile:
BMW Group is the world's leading provider of premium products and premium services for individual mobility, and focuses on the premium segments of the international automobile markets. BMW Group AG is headquartered in Munich and has activities in more than 150 countries.

Solution:
Role and access management with connectivity to SAP.

Omada has implemented a central role management solution at BMW Group AG to further extend the organization's comprehensive identity management platform.

The role management solution at BMW supports a world of employees, contractors, and business partners and is the key tool for overview and management of business roles and applications.

The implemented solution provided by Omada manages role assignments and changes to more than 400,000 identities within group directories, Microsoft AD, and SAP. The role management solution manages business roles and applications across 150 locations worldwide and ensures that access provisioning is compliant with regulatory requirements and that business policies are automatically adhered to.

Straightforward role management

In a system landscape, covering more than 3,000 applications and 70 million assigned roles, role and access management is an essential function.

BMW required a comprehensive role and access management solution that would standardize the core processes for authorization management, granting and approval of access rights, and recertification management. Equally important the solution should enable the business units to become responsible for authorization decisions, with business roles structured by processes instead of by IT-systems.

The role management solution provided by Omada covers both monitoring, management, access provisioning, reporting, and recertification in addition to the automation and optimization of processes. The implemented solution is easy to configure and includes core role management functionality as standard built-in processes.

Complex technical descriptions of which access rights are allocated to a job function, has been replaced with clear, intuitive processes, so the procedures to request and authorize roles are self-explanatory, based on business roles with parameters that require business knowledge only.

Business enabler

One of the aims with the role management project was that the functions should not just be available to a few highly specialized administrators. To enable the business, it was a prerequisite that the management and overview of applications and roles could be performed by role-owners in the business units and that access request processes would be available for end users.

Omada's role management solution places the reponsibility where it belongs enabling the business to take the responsibility for the role management. Responsibility for decisions on individual access and business role structure is part of the business processes, whereas the IT department has the responsibility for providing adequate tools and connecting applications.

The self-service portal enables users to request or change the access rights and applications they need to perform their job duties. To reduce risk Omada Identity automatically ensures that no critical access rights combinations will be assigned, and that access rights are compliant with business policies and SOD regulations. Clear rules and policies for access management are valid group wide, so no individual negotiation with, IT-security, internal audit, or information protection is necessary.

Increased transparency

The detailed graphical display of application and role status assignments provides managers, auditors, and IT administrators with transparent overview of current and historical access rights. Regular recertification cycles of accounts, access rights, and role attributes of IT users improves data quality and maintains compliant access. Recertification surveys can be launched to run automatically in defined intervals, assigned to the appropriate role or application owner.

Omada Identity controls and runs the attestation surveys, providing a detailed cross platform overview of roles, applications, and the accumulated access rights. The result is that far fewer resources, time and effort is spent on recertification processes and compliance analysis.

Omada Identity

Omada Identity is a Microsoft based solution for identity and access management and identity governance and administration. The solution integrates seamlessly with various systems including Windows Server IIS, Active Directory (AD), Azure IaaS, Forefront Identity Manager, and SAP to deliver a complete solution for identity and access management:

- Advanced role based access control
- Compliance reporting and attestation
- Workflows with approval
- Self-service
- Segregation of duties
- Delegated administration

These features provide immediate and significant business benefits including:

- Fulfilled regulatory compliance requirements
- Increased enterprise productivity
- Reduced user management cost
- Heightened data security

Omada