UDV Technologies One Identity Manager

Granular control and access management automation

OVERVIEW

Problem: A Conglomerate business needs to **optimize access management** for multiple IT systems, while retaining control over the infrastructure.

Project milestones: Design and implement access management process by developing the **algorithms** and building the **role-based model. Integrate with existing systems**. Implement SoD conflict detection mechanisms. Launch the **Self-Service Portal** for corporate end users.

Result: The implemented solution based on One Identity Manager (IDM) allows the Customer to **automate access management**. Additional benefits include granular control and usage analytics.

CUSTOMER PROFILE

The Customer is one of the world's largest steel producers and holds leading positions among steel companies. The Company's assets represent a large steelmaking complex with a full production cycle, from preproduction ore processing to iron, steel and rolled metal production. The Customer produces a wide range of steel products, predominant share of which are premium.

Customer facts:

- 35 companies
- Geographic dispersion – EMEA, USA, India
- 50 thousand employees plus 8 thousand external contractors
- Over 70 target IT systems and resources

PROJECT GOALS

Starting point

- The growth in the number of systems and end users has led to a significant increase in labor, required for access provisioning, including support and maintenance required by every related system.
- The service desk handles about 18 thousand of requests every month. YoY growth in request number can be estimated at 30%.
- Average time wasted by every manager on analysis and approval tasks amounts to approximately 300 hours every year.
- Typical access request processing takes 7 days, which leads to a noticeable decrease in user productivity.
- The growing number of the systems makes sufficient access control impossible, deepening the security risks, related to users having excessive or improper access privileges.

IMPLEMENTATION STEPS

Step 1: Perform strict algorithmization defining the procedural steps in various conditions and possible system responses for all processes related to access provisioning.

Step 2: Develop an RBAC (role-based access control) model to facilitate control over access provisioning process, including approvals.

Step 3: Design a customized workflow for managing external contractors including verification and storage of the authorizing documents provided by the contractor, using One Identity Manager.

Step 4: Implement privileged account lifecycle management in One Identity Manager.

Step 5: Integrate One Identity Manager with existing IT systems to interconnect SAP-based HR systems (HCM, SRM, SF), access management systems (SOAR, AD, ISM Ivanti) and target IT systems.

Step 6: Integrate the solution with SAP GRC to enable SoD conflict detection and resolution.

Step 7: Integrate the solution with SAP Solution Manager to detect IT and IT Security incidents related to access provisioning.

Step 8: Integrate the solution with SOAR to automate user credentials blocking and unblocking in case of a security incident.

Step 9: Deploy the self-service portal with a directory of Company's systems, resources and roles, streamlining both access request process for the end users and approval process for systems' owners and managers.

RESULTS

One Identity Manager has become a single point of control for all access management and provisioning processes.

Integration with existing IT systems and resources allowed to connect HR and access provisioning events as well as to automate the processes of granting, review and revocation of the access rights and credentials blocking and unblocking.

During the 24 months that One Identity Manager has been in use the following outcomes were achieved:

- Over 510 thousand of HR events processed
- 11306 domain credentials were provisioned, 81,8% of which were created automatically, the rest were created in automated mode
- Implementing One Identity Manager allowed to reduce the total labor required for supporting access provisioning by 81%
- Average access provisioning time reduced to 2 hours including approvals collection
- Average access provisioning using role-based model diminished to 3 minutes
- Automatic access group assignment implemented for new end users: 4 groups common for all employees and 822 custom groups based on Employer, Location, category, etc.
- All access approvals are handled via IDM.