Identity Manager – Data Governance Edition

Data governance that puts you in control of sensitive data access

Overview

Many businesses today are at risk due to inadequate data protection. Security and compliance officers are facing increased difficulties in securing sensitive data because they do not have an appropriate access system in place. As a result, compliance falls short, which puts companies in jeopardy. While IT managers have permission to grant access to specific data, they often do so without understanding the repercussions, which often leads to unauthorized access to individuals within the company, potentially exposing additional accounts to outside threats. Increasing your internal controls ensures that access to unstructured data remains in appropriate hands so that security is not breached and regulations are not violated. Identity Manager - Data Governance Edition secures and enables your organization by putting a data access governance tool into hands of the business owner rather than the IT staff. Identity Manager - Data Governance Edition provides a self-service portal to manage access to data using an approval, attestation and fulfillment engine, and enables the business owner to grant access to sensitive data. The power to analyze, approve and fulfill unstructured data access requests is granted to files, folders and shares across NTFS, NAS devices and SharePoint. Identity Manager - Data Governance Edition ensures that sensitive, unstructured data is only accessible to approved users, increases security and reduces the burden on IT staff.

Benefits

- Analyze unstructured data access request to files, folders, NAS and SharePoint
- Power to approve unstructured data access requests
- Protect high risk areas
- Empower data owners to control access
- Automate request and approval workflow
- Detect and remediate policy violations
- Audit user or group rights to ensure the correct data access

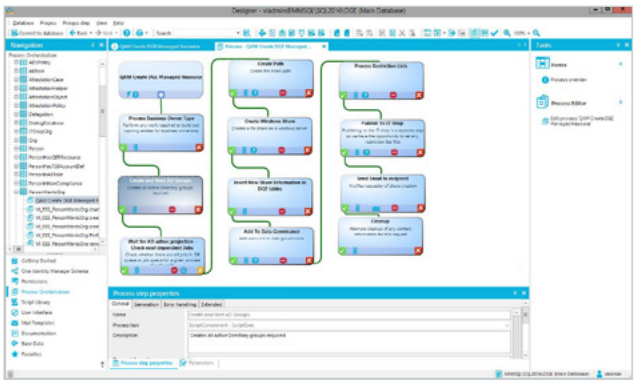

Figure 1. Employees submit requests for a new resource and managers are responsible for approving or denying the request for a new resource

Features

Cloud Governance

Govern the cloud and perform access reporting with support for Microsoft SharePoint Online and OneDrive.

Classification of Data

Classify governed data manually. Business owners can set classification in the web portal. Provide out-of-box policies and risk calculation based on the assignment of the classification level.

Restricted access

Define access policies for your organization to ensure that sensitive unstructured data is only accessible to approved users. Identity Manager – Data Governance Edition locks down sensitive data such as files, folders and shares across NTFS, NAS devices and SharePoint.

Data owner assignment

Determine and assign the appropriate owner of data for all future access requests by evaluating usage patterns and read and write access.

Simplified auditing

Identify user access to enterprise resources (such as files, folders and shares) across NTFS, NAS devices and SharePoint to provide key information during audit preparations.

Automated access requests

Use built-in workflows to automatically direct access requests from the request portal to the appropriate data owner. Approved requests are automatically and correctly fulfilled, with no burden on IT.

Access verification

Ensure that only approved users have access to specific resources, including those who have left the organization or department or whose roles have changed. Identity Manager – Data Governance Edition enables you to monitor user and resource activity, and configure and schedule a recertification process for data owners to verify and attest to employee access.

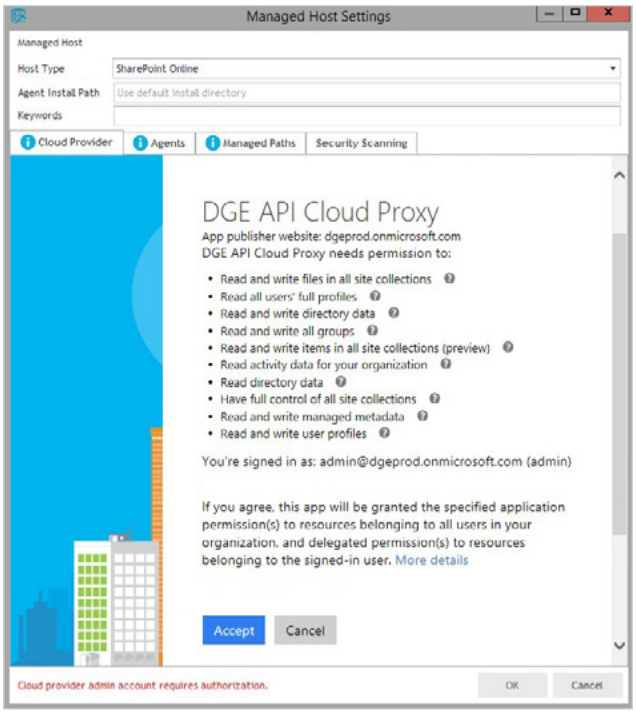

Figure 2. Manage cloud unstructured data storage

Personalized dashboard

View trends, historic and current data access activity and attestation status on a personalized dashboard with reports that can be used to prove compliance to auditors.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit www.oneidentity.com.

System Requirements For a complete list of system requirements, visit Identity Manager - Data Governance Edition

ONE IDENTITY by Quest