SailPoint

CUSTOMER SUCCESS

# Sacramento Municipal Utility District Extends Identity to Manage Sensitive Files

## UTILITIES

### OVERVIEW

Sacramento Municipal Utility District (SMUD) is the sixth largest community-owned power company in the United States, servicing more than 1.5 million customers in and around Sacramento, California. The company has been recognized as an industry leader and award winner for their innovative energy efficiency programs, renewable power technologies and sustainable solutions for a healthier environment.

### CHALLENGE

SMUD's immediate need called for a solution that could automatically enable and disable employee access, as well as eliminate the paper processes involved with onboarding employees and requesting access to applications. Unstructured data was a growing concern, and after an audit finding, it became more pressing to find a comprehensive governance solution.

### SOLUTION

Leveraging SailPoint IdentityIQ™, SMUD has automated its identity processes and now monitors employee access to applications and systems. The company also has visibility into where sensitive files reside and which employees are accessing this data.

Sacramento Municipal Utility District (SMUD) is dedicated to staying at the forefront of green initiatives and is California's first utility to receive over 20% of their energy from renewable resources. The organization breeds a culture committed to innovation and efficiency, so it's no surprise their identity governance program is focused on just that.

While SMUD received recognition for their innovative business approach, their identity management lagged. User access and onboarding was managed manually, which was time-consuming and left room for error. With efficiency and innovation at the core of SMUD's IT strategy, they knew investing in an identity program – one that offered visibility into their unstructured data – was necessary for the overall health of the company.

SMUD made the decision to invest in SailPoint IdentityIQ and set initial goals that included automating the management of roles, password management, access certifications and access requests. After implementation, the IT team saw an immediate improvement with the time it took to onboard and offboard employees, including visibility of who has access to applications used across the company.

John Peters, Senior Enterprise Infrastructure Specialist at SMUD who spearheaded the program, reflected on the ease of using the tool saying, "The flexibility of IdentityIQ is what makes it such a powerful tool, and something we haven't had access to before."

SMUD's identity program has had several achievements over the past few years, and is crucial to mitigating overall risk and remaining compliant under strict regulatory requirements in the industry. Under John's guidance and with the help of SailPoint, SMUD has automated identity processes, reduced call center tickets with password self-service and increased adherence to regulatory standards.

But SMUD was just getting started with the power of identity.

After implementing IdentityIQ, an audit revealed overexposed file shares that included sensitive information such as Social Security numbers, addresses, credit card information, etc. SMUD extended their identity governance program with IdentityIQ File Access Manager to address the concerns with unstructured data.

> **IdentityIQ File Access Manager is an incredibly powerful tool, and SMUD has seen a dramatic reduction in IT risk by securing our unstructured data and having visibility into where it resides.**

**JOHN PETERS**
Senior Enterprise Infrastructure Specialist

SMUD uses IdentityIQ File Access Manager's permissions reporting to identify employees who have access to unstructured data files. IdentityIQ File Access Manager automatically collects and analyzes permissions across on-premises and cloud data repositories. IT departments can then easily visualize, manage and control how employees are granted access to data.

Moreover, IdentityIQ File Access Manager classifies sensitive data and puts effective controls in place to manage and protect it, which is extremely helpful for validating compliance with PCI and looking for credit card information.

SMUD falls under North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) compliance requires SMUD to ensure no one is added to certain security groups without approval. If someone is added natively, IdentityIQ File Access Manager alerts the IAM team and automatically reverses the native change.

"IdentityIQ File Access Manager enforces and monitors the policies set up within IdentityIQ," John said. "We monitor access to applications very strictly, and using a tool that quickly reacts in a short amount of time and removes access given through an improper channel helps us sleep better at night."

## Featured SailPoint Capabilities

| FEATURE | FUNCTION |
|---|---|
| **Data Classification** | Identify where sensitive data resides by crawling files across the organizations, and classify data based on content or behavior. |
| **Permission Analysis** | Model who has access to what files and how it is granted, and proactively address access issues. |
| **Activity Monitoring** | Monitor who is accessing data in real-time, and maintain visibility with actionable dashboards. |
| **Complete Data Coverage** | Discover and provide access controls across Active Directory, Exchange, Windows File Shares, NetApp and SharePoint. |

**SAILPOINT: THE POWER OF IDENTITY™**

**sailpoint.com**

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.



CU1220-1903