

# Case Study

## UNIQUE CREDENTIALS (OIPS & SAPM)



### ABOUT THE CUSTOMER

Headquartered in California, the company referenced in this case study is a multinational biopharmaceutical company. Since its inception in 1980, the company has expanded and established itself as one of the world's largest independent biotechnology companies.

Beyond the enterprise headquarters, the company also has multiple manufacturing units in several regions across the globe. In the case of the 'Unique Credentials' project, the team from ISSQUARED™ serviced the enterprise domain and seven manufacturing sites.

### CHALLENGES

The company had unique passwords across eight different Active Directory domains for both the enterprise and manufacturing networks. Every end-user has an account with the enterprise domain where they login to the domain, check their emails, and access the SharePoint site. However, if an end-user is located at a manufacturing site, they also require an identity for their respective manufacturing site. This lead to a complex and time-consuming process for users and required the company to administer and maintain unique credentials for multiple Ids.

### OBJECTIVE

The company was seeking a mechanism to protect all of its Active Directory Accounts. The company also wanted to be sure that a user with multiple Ids had unique credentials for each. Ultimately, a solution that combines identity insights, administration, access control, and threat intelligence was required. The solution also needed to provide seamless and secure access to identities, resources, and information.

### TECHNOLOGY OVERVIEW

- ✓ Deployment of SAPM (Shared Account Password Manager)
- ✓ Testing and configuration of 'Unique Credentials' scripts
- ✓ Deployment of ORSUS (Operational Identity Provisioning System -OIPS)
- ✓ Consolidate 'Unique Credentials' scripts for all domains and start sending the notification to end-users
- ✓ Integrated with Active Directory to manage access policy to users and groups.

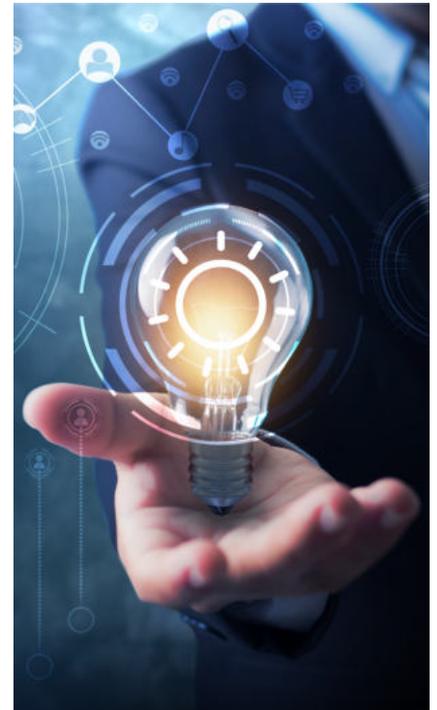
## SOLUTION

After a thorough discussion with the project manager of the company, ISSQUARED proposed to deploy two solutions to secure the company's accounts and tackle the challenges it was facing. For accounts associated with the manufacturing sites, ISSQUARED proposed to deploy ORSUS (Operational Identity Provisioning System - OIPS). To secure admin accounts, the team recommended SAPM (Share Account Password Manager- a Lieberman solution) for both the enterprise location as well as manufacturing sites.

Once the solution was confirmed with management, ISSQUARED's engineers had multiple meetings with the site leads in order to understand the challenges they were experiencing and educate them on the technology solution that would resolve those challenges. Based on their feedback, 'Unique Credentials' solutions were deployed site by site. The service owner of the project had also contributed to the discussion, suggesting how the script should run and how the project would work best if deployed in a phased manner.

Based on that feedback, the solution was implemented in a phased manner over 18 months. ISSQUARED deployed SAPM and OIPS at seven manufacturing sites as well as the enterprise domain. A script that compares the password hashes in all the domains and notifies the user if a password matches in any of his domains was ultimately created and implemented.

ISSQUARED held 30+ information sessions with the admins and end-users to educate them on the new technologies and how to retrieve their new passwords using these solutions.



## KEY BENEFITS

The solutions have enhanced the data security of the company and cut down on repetitive tasks. It ensures that the company employees have unique credentials for their multiple ids. A list of additional benefits listed below:

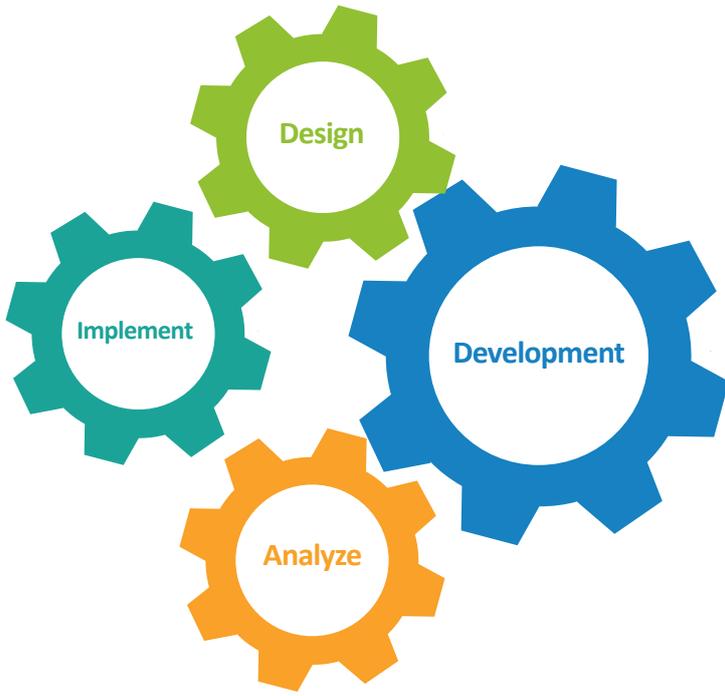
- ✔ Lieberman's comprehensive Shared Account Password Management (SAPM) solution enables the company to manage and audit passwords in a secure IT environment.
- ✔ These solutions have centralized and automated identity management with reduced risk, cost, and improved operational efficiency.
- ✔ Periodically re-validate end-user identities, groups, entitlements, memberships, roles, and access privileges across diverse systems.
- ✔ End-users can access their systems or credentials by signing into a web-portal. They could launch sessions directly into their systems through the browser or view unique credentials directly.
- ✔ The SAPM enforces time-based access, restricts certain actions, and enables monitoring, recording, and alerts to session activity.
- ✔ The solutions have enabled the company to automate setting and managing passwords of privileged accounts.
- ✔ The solutions have integrated with the Active Directory for managing access policy to users and groups.
- ✔ Enforce password security, least-privileged access, and policy configuration for all privileged sessions.
- ✔ ORSUS periodically re-validate identities, groups, entitlements, memberships, roles, and end-users' access privileges across systems, and audits requests from end-users for access. It also enables to create of groups or roles with defined access privileges and control group membership.
- ✔ ORSUS OIPS has provided simple administration and access control and safeguarded the company from security risks & threats. It has also provided flexibility by customizing workflow processes, list entries, window attributes, business scenarios, UIs, reports, etc.
- ✔ OIPS enables the end-user to establish connections with various resources and offers scalability on any platform, on-premise, or cloud.

**Future Plans:** 'Unique Credentials' is an offshoot of the ECR (Enterprise Cyber Resilience) project. The ECR Operation remains ongoing.

## TESTIMONIALS

"Congratulation to the entire team of ISSQUARED™ to drive this critical project to this important milestone" – Senior Manager

"Tremendous collaboration and accomplishment, reflecting great credit to the entire organization. Thanks to the entire DIAS (IT and Operations) team of ISSQUARED™." – Senior Manager



## ISSQUARED™

ISSQUARED™ is one of the leading providers of end-to-end IT technology solutions, delivering fine-tuned services across IT Security, Cloud, Infrastructure, Unified Communications, Industrial Operational Technologies and other solution areas. For many years, ISSQUARED™ has been helping several Fortune 500 organizations and delivered several multi-million-dollar projects. Our proven expertise takes our clients through a seamless digital and security transformation, resulting in rapid business benefits and positions them for future success.

ISSQUARED™ is headquartered in Westlake Village, California, with global delivery capabilities and presence across the UK, Ireland, India, Singapore, the Middle East, and the U.S.



 HQ: 2659 Townsgate Rd, Suite 227  
Westlake Village CA 91361 USA

 +1 805 371 0585  
+1 800 779 0587

 [sales@issquaredinc.com](mailto:sales@issquaredinc.com)  
[www.issquaredinc.com](http://www.issquaredinc.com)



Copyright © 2020 ISSQUARED™, Inc. All rights reserved. The information contained in this document is the property of ISSQUARED™, Inc. No part of this document may be disclosed, copied, communicated, distributed, edited, used or distributed, in whole or in part, in any purpose, in any form or by any means, without the prior written permission of ISSQUARED™, Inc.

Though ISSQUARED™, Inc. has used best efforts to ensure accuracy in this document, ISSQUARED™, Inc. cannot accept responsibility for the completeness of this document or warranties concerning the accuracy of the information contained herein and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, the information in this document is subject to change, at any time, without obligation to notify any person or entity of such changes. The contents or information furnished in this document is not warranted or guaranteed to produce any specific results, and methods, strategies, or advice contained here in may not be suitable for every user.