

Cross Identity Case Study

Global Wireless Telecommunications Company

The Client: World's leading mobile services and technology solutions company managing devices and mobile accessories across the wireless ecosystem



Introduction

World's leading mobile services and technology solutions company that manages devices and mobile accessories across the wireless ecosystem. They serve over 50,000 carriers, retail and enterprise customers across 100 countries, touching over 100,000 points of sale. They participate in every stage of a device's lifecycle from when it is manufactured to when it is time to trade it in and re-market it.

Challenges

The company was facing significant challenges related to inefficient end-user experiences. With extensive use of SAP modules in their daily operations, they had to deal with having to login to web apps and thick client apps, individually. End users were tasked with remembering multiple credentials to login to approximately 10 applications. They were also tasked with mandatory quick response time to cater to their external customers. All applications required individual login time which prevented applications from launching quickly and affected end user response time.

Remembering numerous complex credentials often resulted in forgotten passwords and subsequent account lockouts. Users had no way to quickly resolve these incidents on their own causing delays in response time to internal and external customers. Resolving access issues required significant IT assistance. Leadership noticed that costs related to Helpdesk dependency were increasing and administrative efficiency was declining. End user frustration due to delays affected daily productivity.

The company incurred a huge cost to maintain a dedicated Helpdesk team for such requests. With a high-performance environment where end users need immediate access to applications to cater to customer questions, a Single Sign-On solution was a must. However, they could not find a solution that could handle all types of applications.

Desired Solution

- Provide quick and easy end user login experiences for all types of applications with a SAP focus.
- Remove Helpdesk dependency for forgot password and account unlock scenarios.
- Find a solution that could grow with the company.

Solution Offering

Cross Identity was chosen as the best fit for this customer. Cross Identity was able to provide a single solution for both Single Sign-On and Password Management. As the company grows, this solution would be IGA (Identity Governance & Administration) ready for automating user provisioning, de-provisioning and access governance in the future without the need for another product.



Industry
Wireless
Telecommunications

Solution Implemented
Cross Identity

Employees
9,000+

Engagement Year
2018

Why Cross Identity

- With about two decades of expertise in IAM solutions, we have the right product with right features needed for telecom companies.
- One solution for both Password Management and Single Sign-On to SAP modules.
- Unique approach for our business size to be IGA-ready.
- Rapid implementation approach and cost-efficient licensing models.

Business Outcomes

- The **Cross Identity Single Sign-On** module was a very visible and quick success. End users got to work faster when they used this module – especially with their SAP modules. Now, upon login, their applications launch automatically and are ready for immediate use. End users, managers, other employees and customers no longer need to wait for an employee to go through the lengthy login process to get the information they need.
- The **Cross Identity Password Management** module provided end users the ability to reset passwords on their own without the Helpdesk. With the ability to be self-reliant, forgotten passwords and account lockouts were hardly noticeable anymore. Not only was the Helpdesk team relieved, their productivity improved and costs went down as they no longer needed to manage these transactions.
- Leadership noticed **Cross Identity's** impact on the organization. The administrative burden was immediately reduced with zero hardware to purchase, deploy and maintain. Auto updates no longer required internal effort to upgrade and the IT budget that was pulled back in line as the automation from the solution practically removed constant Helpdesk involvement.

