

Port management company strengthens security and accountability

Abu Dhabi Ports enhances security with comprehensive auditing and reporting, slashes onboarding time by up to 90 percent, and eliminates password reset tickets with Microsoft platform management solutions from Quest.



“With InTrust and Change Auditor, we have confidence that all changes and other actions are properly audited and tracked, and all the data is automatically consolidated and stored in an encrypted repository.”

Zaid Al-Ali, Infrastructure & Service Delivery Manager, Abu Dhabi Ports

CUSTOMER PROFILE



Company Abu Dhabi Ports
Industry Transportation
Country United Arab Emirates
Employees 1,200
Website www.adports.ae

BUSINESS NEED

To effectively manage and secure its complex and growing IT infrastructure, Abu Dhabi Ports needed comprehensive auditing, proactive alerting about changes, automated provisioning and self-service password resets.

SOLUTION

By implementing Quest® Change Auditor and InTrust®, along with One Identity Active Roles and Password Manager, Abu Dhabi Ports now has the comprehensive Microsoft platform management it needs. All actions are now properly audited, automatically consolidated and securely stored, so reporting on an incident takes seconds, rather than days or weeks of digging through cryptic logs. Real-time alerts about critical changes further enhance security. Automated provisioning slashes onboarding time by up to 90 percent, and self-service password resets reduce service desk workload while improving user productivity.

BENEFITS

- Ensures that all actions are properly audited, automatically consolidated and securely stored, so reporting on an incident takes seconds rather than days or weeks
- Improves security with real-time alerts about critical changes
- Streamlines provisioning and deprovisioning, including slashing onboarding time by up to 90 percent
- Improves security and productivity with a secure self-service portal that eliminates service desk calls for password resets

SOLUTIONS AT A GLANCE

- [Microsoft Platform Management](#)

Abu Dhabi Ports understands firsthand how technology can enable a rapidly growing business. Established in 2006, the organization now manages eleven ports in the United Arab Emirates, including the state-of-the-art Khalifa Port, where software and wireless technologies enable integrated movement of containers, and loading and tracking information are fully integrated with customs to increase throughput. The company is also developing a world-class industrial zone designed to reduce the emirate's dependence on oil revenue. To help its IT team effectively manage and secure the critical IT infrastructure supporting these ambitious projects, Abu Dhabi Ports chose Microsoft Platform Management solutions from Quest.

“When we need to investigate an issue, we can create detailed reports with a single click, instead of digging through multiple event logs for hours or days.”

Zaid Al-Ali, Infrastructure & Service Delivery Manager, Abu Dhabi Ports

NATIVE TOOLS LEAVE DANGEROUS VISIBILITY GAPS

Like many organizations, when Abu Dhabi Ports began building its IT systems, it relied on the native Microsoft tools. However, the IT team soon recognized that managing a complex and growing IT infrastructure and user base with those tools was difficult, if not impossible. Most important, the IT team found it challenging to effectively track and audit changes to Active Directory, Exchange, file servers and other key infrastructure components, which put both security and system availability at risk.

“To investigate an action or incident, the IT engineer had to go through the tedious process of digging through multiple event logs. Since the logs are not centralized, this process had to be repeated for each server, which could take anywhere from a few hours to a couple of days,” explains Zaid Al-Ali, infrastructure & service delivery manager at Abu Dhabi Ports. “Moreover, the logs get overwritten regularly, so important data could be lost.”

This lack of visibility into IT system activity meant a lack of accountability for both users and administrators. “The logs simply do not capture critical information, such as changes to share or folder permissions and the modification or deletion of files,” notes Al-Ali. “We were unable to determine what changes were made, who made them, and whether they were legitimate changes, unintentional mistakes or intentional abuse of privileges. And

since we were unaware of what changes had been made, rollback was impossible, which put system performance and availability at risk.”

MANUAL USER PROVISIONING AND PASSWORD RESETS SAP PRODUCTIVITY

User provisioning was also a tedious and error-prone process. “The onboarding process for a user would take one to two weeks, which both delayed new employees from becoming productive and bogged down IT staff,” explains Sara Al Najjar, vice president of IT at Abu Dhabi Ports. “And since provisioning was a manual process, it was prone to errors that could result in users having more or less access than they needed, which could impact both their productivity and system security.” Similarly, manual deprovisioning

PRODUCTS & SERVICES

SOFTWARE

Active Roles

Change Auditor for Active Directory

Change Auditor for Exchange

Change Auditor for Windows File Servers

InTrust®

Password Manager

processes failed to ensure that users did not retain access to systems or data once they left the company.

Password resets represented another significant drain on both IT and user productivity. “Users were requesting 300–400 password resets a year,” says Al Najjar. “In addition to the burden that put the service desk, users could not be as productive while they were waiting for their passwords to be reset.”

SOLUTIONS THAT MEET EVERY REQUIREMENT AND ARE UP AND RUNNING IN AN HOUR

Abu Dhabi Ports knew that it needed to strengthen and automate its Microsoft platform management processes. “We needed comprehensive auditing and tracking of configuration changes and user activity, along with real-time alerts about critical changes and advanced reporting capabilities,” explains Al-Ali. “We also wanted a simple, intuitive and customizable interface.”

The IT team researched the solutions available on the market and found everything they needed with Quest® Change Auditor for Active Directory, Change Auditor for Exchange, Change Auditor for Windows File Servers and InTrust®, along with One Identity Active Roles and Password Manager. “We discovered that Quest was the clear market leader; in fact, their tools were the only ones that could provide the comprehensive Windows management functionality we needed,” Al-Ali recalls. “In addition, Active Roles scored very well on Gartner’s Magic Quadrant, and when we reached out to Active Roles customers, they gave us extremely positive feedback about both product performance and vendor support.”

After this initial research, Abu Dhabi Ports took the time to conduct thorough testing. “During the POC, we noticed that installation, configuration and reporting were pretty straightforward — in fact, all the products were up and running in an hour,” says Al Najjar. “We were surprised to find that the products met all of the success criteria we had laid out.”

EFFICIENT, COMPREHENSIVE WINDOWS MANAGEMENT

InTrust enables organizations to securely collect, store, search and analyze massive amounts of IT data from numerous data sources, systems and devices in one place. With one view, you can know what resources users have access to, how that access was obtained and how it was used.

Change Auditor proactively protects your IT systems by tracking all changes without the need for native audit logs. Real-time alerts enable prompt response to threats. And the solution can even prevent changes to your most critical Active Directory objects, such as the deletion of OUs or the modification of GPO settings.

Active Roles automates and streamlines provisioning and re-provisioning in AD and AD-joined systems, such as Unix, Linux and Mac OS X. Your organization can easily generate and strictly enforce access rules based on defined administrative policies and permissions, eliminating the errors and inconsistencies common with native tools.

Password Manager is a simple, self-service solution that enables users to securely reset forgotten passwords and unlock their accounts. Because users no longer need to write down their passwords, your organization can implement stronger password policies while still reducing helpdesk workload.

COMPREHENSIVE AUDITING AND REAL-TIME ALERTS ENHANCE SECURITY AND ACCOUNTABILITY

With the Quest and One Identity solutions implemented, Abu Dhabi Ports now has the comprehensive auditing, tracking, reporting and alerting it needs to effectively manage and secure its complex and growing IT infrastructure. “We no longer have to spend days manually collecting and sorting through multiple logs from all our different servers or worry about logs being overwritten or tampered with,” explains Al-Ali. “With InTrust and Change Auditor, we have confidence that all changes and other actions are properly audited and tracked, and all the data is automatically consolidated and stored in an encrypted repository. We get instant real-time alerts on all critical activities, so

“Active Roles has drastically simplified user provisioning and deprovisioning. In one click, we are able to complete a task that used to take two hours, and the onboarding process now takes a day instead of one to two weeks.”

*Sara Al Najjar, Vice President of IT,
Abu Dhabi Ports*

“Previously, the service desk had to perform 300–400 password reset a year. Password Manager has completely eliminated those calls.”

*Sara Al Najjar, Vice President,
Abu Dhabi Ports*

we can prevent damage before it happens. And when we need to investigate an issue, we can create detailed reports with a single click, instead of digging through multiple event logs for hours or days.”

Knowing that every action is being audited is also a powerful deterrent to inappropriate or malicious behavior. “With the Quest solutions in place, we now know about every change, so anyone who might consider playing around or misusing their access will think twice. Even well-intentioned admins are more careful to make sure the changes they make are properly authorized and documented,” notes Al-Ali. “Plus, rollbacks are easy if there is a problem, so we can maintain system performance and availability.”

AUTOMATED PROVISIONING SLASHES ONBOARDING TIME BY UP TO 90 PERCENT

By automating the provisioning, re-provisioning and de-provisioning of user identities, Active Roles has enabled Abu Dhabi Ports to slash onboarding time by up to 90 percent and reduce IT workload. “Active Roles has drastically simplified user provisioning and deprovisioning. In one click, we are able to complete a task that used to take two hours, and the onboarding process now takes a day instead of one to two weeks,” reports Al Najjar. “And delegating provisioning completely to the Human Resources department gives IT staff more time to focus on more strategic projects.”

The Quest and One Identity solutions have also improved the accuracy of employee information and access rights. “The combination of InTrust and Active Roles has enabled us to delegate responsibility for

updating employee records, job descriptions and other information to the HR employees who have that data, instead of having layers of communication between HR and IT. The tools also validate their entries, which further reduces inconsistencies and errors,” Al Najjar says. “The tools are easy to use, and they were also easy to customize with the specific fields and menus our organization needed.”

SELF-SERVICE PASSWORD RESETS REDUCE SERVICE DESK WORKLOAD WHILE ENHANCING SECURITY

With Password Manager, users across the organization are able to reset their own passwords at any time — securely and without help from the IT service desk. “Previously, the service desk had to perform 300–400 password resets a year. Password Manager has completely eliminated those calls. Everyone is more productive: Users no longer have to wait for someone else to reset their passwords, and service desk staff have more time for other tasks,” reports Al Najjar. “In fact, we’ve implemented a company policy requiring all password changes to be made through Password Manager — something we’ve needed and wanted from a security point of view.”

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

[View more case studies at Quest.com/Case-Studies](https://www.quest.com/Case-Studies)