Government healthcare agency ensures security and compliance

Region Halland gains deep visibility into its hybrid Active Directory and slashes troubleshooting time by more than 80% with Quest® Change Auditor.

> “Previously, investigating an issue could easily take an hour. Change Auditor cuts that time to just 5–10 minutes.”
>
> *Dennis Persson,*
> *IT Systems Technician,*
> *Region Halland*

CUSTOMER PROFILE

BÄSTA LIVSPLATSEN
Region Halland

Company	Region Halland
Industry	Healthcare
Country	Sweden
Employees	8,000
Website	**regionhalland.se**

BUSINESS NEED

To deliver quality healthcare and development initiatives while ensuring regulatory compliance, Region Halland needed deep, unified visibility into its Active Directory and Azure AD.

SOLUTION

With Quest Change Auditor for Active Directory, Region Halland now has a single, correlated view of activity across its hybrid deployment. Instead of manually collecting and poring through cryptic native logs from multiple servers, the IT team can review actionable intelligence in real time to quickly troubleshoot incidents. Moreover, detailed alerts about critical changes enable them to slash response time, and they can even proactively prevent changes to the most critical AD objects to maximize both security and system availability.

BENEFITS

- Enhances security by delivering a single, correlated view of activity across the hybrid deployment
- Slashes the time for incident investigations from an hour or more to just 5–10 minutes
- Makes monitoring of critical changes as easy as checking an email folder
- Ensures individual accountability and regulatory compliance

SOLUTIONS AT A GLANCE

- Microsoft Platform Management

Region Halland has set itself a lofty goal: to make Halland County in Sweden the "best place to live." To that end, the organization works hard to ensure high-quality healthcare services for the county's 327,248 inhabitants and to promote strong and responsible development across the region. Naturally, these efforts require a wide range of IT systems and data, both on premises and in the cloud, which the IT team must keep secure as mandated by ISO 27001, GDPR and other regulations. For the deep insight into Active Directory and Azure AD required to maintain and prove compliance, the IT team relies on Quest® Change Auditor for Active Directory.

> "Before, I had no control over changes to administrative groups whatsoever. With Change Auditor, I can easily monitor those critical changes just by looking at a folder in my mail."
>
> *Dennis Persson,*
> *IT Systems Technician,*
> *Region Halland*

LACK OF INSIGHT INTO ACTIVE DIRECTORY PUTS SECURITY AND COMPLIANCE AT RISK.

Region Halland delivers a broad range of services for the county: It operates three hospitals and several health centers and public health services, and it also develops and implements strategies for advancing the area's infrastructure, public transportation, employment, education, environmental policy, arts and culture, and more. To support those initiatives, the IT team has built a rather sophisticated hybrid IT environment. On premises, there are two data centers, five domain controllers running Windows Server 2016, and numerous legacy applications. The cloud environment is also Microsoft-based, with Azure Active Directory at the center. Because the services that Region Halland provides are so critical, the IT team must keep all these systems both highly secure and highly available. Moreover, they must ensure and demonstrate compliance with several regulations, including ISO 27001, GDPR and the NIS directive.

However, the IT team lacked the visibility into Active Directory and Azure AD that they needed to effectively understand and manage user permissions, troubleshoot issues, and quickly spot and respond to critical events such as privilege escalation. "Investigating incidents was difficult and time-consuming," explains Dennis Persson, IT systems technician for Region Halland. "For example, to see whether Group Policy had been changed, we had to manually collect the native audit logs from five different domain controllers and look for relevant events. The native auditing logs are hard to read and incomplete, so we were not able to find answers as quickly as we needed to. It was stressful and put us at risk of downtime, security incidents and compliance violations."

CHANGE AUDITOR BLOWS AWAY THE COMPETITION.

When an external audit confirmed that Region Halland's lack of visibility into Active Directory posed a clear security risk, Persson was able to convince management of the wisdom of allocating budget for a third-party product that would provide deep visibility into AD and Azure AD. The team began evaluating solutions from several vendors, but once they saw the features and functionality of Quest Change Auditor for Active Directory, they quickly dropped the other options.

"I didn't dive as deeply into the other products because I saw what Change Auditor could do and how easy it was," recalls Persson. "Also, it uses SQL Server, and I saw that Quest is focused on Microsoft products and following Microsoft lifecycle plans. I was particularly impressed by the many best-practices searches, alerts and reports that it offers out of the box." For example, Change Auditor includes over 150 predefined reports for GDPR alone to simplify the work of establishing, maintaining and demonstrating GDPR compliance.

PRODUCTS & SERVICES

SOFTWARE

Change Auditor for Active Directory

Region Halland was very pleased with the quick time to value for the Quest solution and the quality of the support they have received. "I don't think it took us more than an hour or so to get Change Auditor up and running in our environment," Persson notes. "Everything went really smoothly and we had all help we needed from Quest to get it in place very quickly. Plus, Quest Support has been really helpful. They are technically really good and they respond very quickly. I couldn't ask for anything more."

DEEP INSIGHT ACROSS THE HYBRID ENTERPRISE

With Change Auditor auditing both its on-premises AD and its Azure AD environment, Region Halland now has a single, correlated view of activity across its hybrid deployment. With that visibility, the IT team can clearly understand who has access to what and how they got that access, so they can rigorously enforce the least-privilege principle and strictly control membership in privileged groups.

INVESTIGATIONS THAT USED TO TAKE AN HOUR NOW TAKE MINUTES

When something goes wrong, troubleshooting is simple because all the data is easily accessible from a central console. The team can review changes to users, groups, permissions, Group Policy and more in real time from intuitive dashboards and reports, instead of having to manually pull native logs from multiple separate servers and spend hours trying to decipher them in search of relevant information. As a result, they can investigate issues faster and ensure individual accountability. "Previously, investigating an issue could easily take an hour," reports Persson. "Change Auditor cuts that time to just 5–10 minutes."

For example, now the team can see right away if someone changes the permissions for an AD account or provisions a new guest user in Azure AD, so they can quickly investigate and revert any improper changes to avoid a data leak. In fact, the team can restore the previous values directly from the Change Auditor console with the click of a button.

ALERTS AND CHANGE PROTECTION, TOO

Change Auditor also alerts the IT team about critical changes, such as the addition of a user to a highly privileged group, enabling them to respond quickly and minimize the damage from malicious or otherwise improper modifications. "At first, I thought that the product would only show me what happens in real time, but then I learned it could also send me alerts on potentially malicious activity," says Persson. "Without alerts, I would not see malicious activity unless I'm actually looking into what happened, so that's a huge plus. For example, before, I had no control over changes to administrative groups whatsoever. With Change Auditor, I can easily monitor those critical changes just by looking at a folder in my mail, which I do each day and sometimes even a few times a day."

Moreover, Change Auditor can also prevent changes to the most critical Active Directory objects, such as the accidental deletion of an OU or the modification of GPO settings. This feature enables Persson and his team to proactively avoid changes that could lead to service disruptions, downtime or a security incident.

THE ULTIMATE TEST: SATISFYING AUDITORS

It's not just the IT team who are pleased with the results that they've achieved using Change Auditor for Active Directory: Region Halland's auditors also say they are now satisfied with the level and quality of auditing for Active Directory.

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.

> "I don't think it took us more than an hour or so to get Change Auditor up and running in our environment."
>
> *Dennis Persson,*
> *IT Systems Technician,*
> *Region Halland*

View more case studies at Quest.com/Customer-Stories