

# NHS Trust separates AD domains with zero impact on clinicians and patient care

Quest®

Worcestershire Health and Care NHS Trust used Quest® tools to separate from their shared IT infrastructure and create their own Active Directory domain.

## NHS Trust

Country: **United Kingdom**

Employees: **4,700**

Industry: **Healthcare**

Website: [hacw.nhs.uk](https://www.hacw.nhs.uk)

**If NHS Trust users can't log in, then clinics are cancelled, patients aren't seen and doctors can't access medical records. So Active Directory migration has to go right the first time.**

Worcestershire Health and Care NHS Trust is a community-based trust with 4,700 staff members in community hospitals and community nursing, plus mental health facilities.

For years, the Trust had shared IT infrastructure, including an AD domain, with two neighbouring acute services hospitals. The shared domain was essential for enabling physicians and staff to move freely among clinics, hospitals and offices, accessing medical records and running workloads from any computer. All of the shared infrastructure had been supported and maintained by an outside provider. The level of IT service was high, but the Trust was concerned about security.

### About this case study

When a security accreditation prompted a re-examination of security in its shared infrastructure, The Trust's IT team decided to migrate their users to a new, separate Active Directory (AD) domain. But it was imperative that healthcare and day-to-day operations not be affected by the migration.

### Solution

Instead of using native tools, The Trust chose AD migration tools from Quest, which allowed them to create a domain separate from the other entities for security purposes. The Quest tools kept passwords in sync between domains so users could log in and work across organisations and buildings, as smoothly as they had done before the migration.

### Benefits

- Separated AD domain from shared infrastructure with no impact on users or clinical operations
- Set up security boundary while allowing thousands of clinicians and staff members to continue logging in to domains of affiliated entities
- Enabled AD migration of thousands of local and remote endpoints without the need to touch or reconfigure them
- Improved security posture to pass audit and earn Cyber Essentials Plus accreditation

## Aiming for Cyber Essentials Plus, with easy access for users

“When we were in the shared environment, potential security risks were outside of our control,” says David Brown, chief information officer for the Trust. “If you’re sharing infrastructure and logging into the same domain as an entity with a lax password policy, that has a critical impact on your security posture. So our primary goal was to ensure that we became absolutely self-sufficient in IT.”

The Trust was keen for IT independence because they sought Cyber Essentials Plus accreditation. Cyber Essentials is a set of technical controls produced by the UK Government and the security industry to strengthen cybersecurity defences, and the Plus accreditation includes an audit of the organisation’s networks and devices.

“We had several security audits, with high-critical alerts on items that we couldn’t change,” says Richard Danson, enterprise architect for the Trust. “That meant that we could either live with the security risks or separate from the shared service and create a security boundary with our own Active Directory domain.”

The latter path could get the Trust to the Cyber Essentials Plus accreditation they desired. But there’s nothing easy about separating AD domains. The users usually bear the brunt of the process, and the Trust had to avoid the danger of breaking clinical processes or the normal workflow of day-to-day patient care.

## Choosing Quest for the migration tool

“Too many administrators would rather go through and re-image every PC than perform an AD migration,” observes Danson. “They don’t think of the impact on users, who could be anywhere — on premises, remote or working from home. It’s a lot of work to organise and a lot of unnecessary bother for users. Fortunately, we knew that seamless AD migration is possible without re-imaging everybody’s PC.”

While AD migrations are not uncommon, few IT departments budget for them. Most admins resort to the in-house Active Directory Migration Tool (ADMT) from Microsoft.

The Trust, however, was already a Quest customer, having opted for and used KACE Systems Deployment Appliance and KACE Systems Management Appliance instead of Microsoft System Center Configuration Manager. Their confidence in value for money with KACE helped them choose Quest when the separation project arose. After a training session on the tools with Quest’s Professional Services group and a couple of follow-up support calls, Brown and Danson’s team undertook the migration on their own.

“Because the Quest tool works so well and keeps the passwords in sync between the two domains, our staff still use it to log on to the hospitals. We can use other tools to do that, but Quest tools do it so well.”

*Richard Danson, Enterprise Architect,  
Worcestershire Health and Care NHS Trust*

## Separating AD domains with Quest tools: Three advantages

For AD migration, the Quest tool had three important advantages over Microsoft’s tools: coexistence, user experience and support for remote users.

“Our clinicians depend on services hosted by the acute hospitals,” says Brown. “We needed to be in a separate domain yet maintain trust and synchronisation of users between our domain and the hospitals. It was important that our clinicians have a consistent experience, without logging into a different system with a different account and password. Quest kept passwords synchronised across domains so our users could continue logging on to the other

systems under their existing accounts. They can log in normally to our domain yet still access systems and run workloads in the hospitals' domain that are AD-aware for the hospitals only. With Microsoft tools we couldn't rely on keeping the passwords synchronised across both domains."

Danson believes that it's possible to apply Microsoft tools with roughly the same technical outcome, but it places a greater burden on users. Plus, Quest held additional advantages for users.

**“It was important that our clinicians have a consistent experience, without logging into a different system with a different account and password. Quest kept passwords synchronised across domains so our users could continue logging on to the other systems under their existing accounts... With Microsoft tools we couldn't rely on keeping the passwords synchronised across both domains.”**

*David Brown, Chief Information Officer,  
Worcestershire Health and Care NHS Trust*

“If you're working from the data centre outwards, it seems easy to use the Microsoft tools,” he says. “But when you start with the users and understand what their requirements are, you always find more complexity that you weren't expecting. With Quest, whenever users connected, they received user-friendly messages informing them of the migration. That user engagement piece made the migration much easier, for them and for us. With traditional Microsoft tools, admins have no control over

messages or timing. I've used those tools and I've never had a problem with them before, but I know the disadvantages. The users' journey is much better with Quest.”

As for supporting remote users, a traditional migration would require that users take their PCs onsite at a specific time for configuration or imaging. But in the world of working from home and remote work, IT administrators can't count on that — far better to work from the centre outward.

“ADMT will deal with offsite users,” says Brown, “but not very elegantly. It doesn't take kindly to losing connectivity, which often happens when users are off site. The advantage with Quest is we could preload the system with what we wanted, then wait for users to connect. Quest tools have coped with all our users working from home. ADMT wouldn't have allowed it in the same way, but the Quest tool is brilliant for that, especially if your primary goal is not to break any users.”

### **More than they bargained for**

For organisational reasons, the coexistence feature of the Quest tool has proved more useful than Brown and Danson — or anybody in the Trust — anticipated.

Through the entire AD migration project, plans had been evolving for the Worcestershire Trust to merge with the NHS Trust in Herefordshire. The problem was that the migration project had to proceed even as the merging entities were still sorting out the definitive name of the merged organisation. The name of the new AD domain would need to match it.

“Part of the reason we chose Quest is that there was a slim chance of needing to do another AD migration once the new domain name was settled,” says Danson. “With Quest tools we could have done back-to-back migrations painlessly for users; with ADMT it wouldn't have been painless.”

Another unexpected benefit is the durability and robustness of the Quest tool, which has kept the domains synchronised longer than anticipated.

“Because the Quest tool works so well and keeps the passwords in sync between the two domains,” says Danson, “our staff still use it to log on to the hospitals. We can use other tools to do that, but Quest tools do it so well.”

“The advantage with Quest is we could preload the system with what we wanted, then wait for users to connect. Quest tools have coped with all our users working from home. ADMT wouldn’t have allowed it in the same way, but the Quest tool is brilliant for that, especially if your primary goal is not to break any users.”

*David Brown, Chief Information Officer,  
Worcestershire Health and Care NHS Trust*

## An AD migration tool for all NHS Trusts

The Trust has achieved their main goals for the migration:

- **IT independence** — By separating, the Trust has separated their services into a new domain that they alone operate on their own infrastructure.
- **Security boundary** — With the new domain, the Trust has addressed the high-critical alerts, passed the audit and received Cyber Essentials Plus accreditation.
- **Coexistence** — The Trust’s users can still interact freely with the hospitals, and domain trust is in place so that each set of users can still work in the other’s buildings.
- **Zero impact** — After migration, the health professionals worked as they always had done, unaware that the IT departments had separated.

Danson sees more AD migrations in the NHS’s future. “I’ve been through this five times now,” he says. “Within the NHS things are always changing and organisations merge and split up often. That means Active Directories merge and split up often. Timelines are short — we had one month to migrate this AD — because the changes at the organisation level occur so often. The security boundaries matter because you’re expected to earn these accreditations, but your users need to work normally with other NHS Trusts. With the Quest tool it was easy for a user to go between buildings and not realize they had been migrated. We couldn’t have users unable to use certain machines within the Trust. They had to have the same experience wherever they went.”

Brown concurs: “I would recommend Quest tools to anybody considering an AD migration of this complexity in an NHS environment, with constraints around connectivity or ease of migration. Some organisations would not be as meticulous as we’ve been, and if your primary goal is not to break any users, then this tool is fantastic.”

## SOLUTIONS AT A GLANCE

### Software

- Migration Manager for Active Directory
- KACE Systems Management Appliance
- KACE Systems Deployment Appliance

## About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.