



National Cyber
Security Centre

a part of GCHQ



Renfrewshire
Council



Improving authentication at Renfrewshire Council

Case study: How innovative, low-cost changes to authentication at Renfrewshire council has improved the user experience for staff

At a glance:

- Surveys and user observation used to identify the more painful aspects of authentication
- Single-sign on (SSO) was a key enabler for making authentication seamless and transparent
- Improvements to remote access authentication delivers improved reliability and speed
- Pull print is made significantly quicker and easier with NFC authentication
- Improved password management and policy drastically reduces the number of weak passwords

With end users at Renfrewshire Council becoming accustomed the nuances of 'legacy' authentication, the IT staff set about removing some of the more irritating pain points. By surveying users and finding out particularly troublesome instances of unnecessary authentication, the IT team's innovative solutions made significant improvements to the end-user experience, without great expenditure.

Innovating authentication

Renfrewshire Council is a local authority in the west of Scotland, delivering a range of services to citizens and the community. Like many other public sector organisations, we face the challenge of delivering secure but usable IT in the face of tightening budgets and increased demand. In 2017, we agreed a 3-year strategy for improving the council's IT, which included commitments to adopt 'innovative authentication and identity management'.

When the NCSC's 'Secure by Default Partnership Programme' was announced for 2017 - focusing on improving authentication - we were naturally delighted to be part of it. In an initial meeting with the NCSC, we discussed some of the challenges around login that our staff face, and we agreed a set of activities to pursue which would improve IT for our users.

Changing perceptions

Right from the start, we had a strong desire to change perceptions and encourage investment to modernise end user security practices. We found that just **discussing** the challenges that staff face in certain areas quickly led to suggestions for where to make improvements first.

To make sure we were targeting the right areas, our Cyber Security Architect developed a short questionnaire asking users to record each time they logged into a system during the day, and to pass the results back to the IT team. This gave us some tangible data to act upon, and highlighted some problems we weren't previously aware of.

Quick wins from single sign-on

We are increasingly moving to online services, and staff traditionally have separate credentials for logging into each service they use. We soon identified several 'quick wins' that would make using online services much easier.

1. We enabled ADFS in our Office 365 instance to provide single sign-on to internal services and, where possible, our external hosted services.
2. We configured Windows Hello for Business to enable password-less single sign-on to our ADFS service, which supports both face recognition and fingerprint authentication.
3. Around half our staff are fixed desktop users, so we purchased external USB fingerprint readers to allow them to use Windows Hello. Staff who preferred not to use biometrics, or couldn't (some of our desktop PCs are kept under the desk and others have no USB ports) can use a PIN code instead.
4. In our IT SyOps, we made it clear that staff can use the 'remember me' function on websites if the site content is not highly sensitive. There was no technical reason to not allow this, but users weren't sure if they could.

We also sped up our replacement to remote access via Citrix. Before, logging on could take over 10 minutes and require multiple authentication steps. As our estate was migrating to Windows10, we deployed Direct Access and saw big improvements to user authentication. Users now only log into the device once, as it provides onward authentication and immediate access to enterprise services.

Password quality and management

Using NCSC tools, we audited user passwords, looking for ones that were weak. We discovered that 50% of them were either easy to guess, or were on compromised password lists. Consequently we:

- adopted the NCSC's new password guidance (<https://www.ncsc.gov.uk/guidance/password-collection>)
- configured our domain controller to accept the new recommendations
- looked at password enforcement tools to help people make good choices in the first place
- started a regular audit program so we can measure compliance with the new guidance

We expect these measures to improve password standards over time.

Previously we stored passwords for shared accounts in a spreadsheet. This was cumbersome, insecure, and lacking the features of modern password managers. We replaced this with RoboForm, a multi-platform password manager, which includes secure password generation and autofill. It's now much easier to use strong, unique passwords.

"I love the fingerprint authentication. I can use one finger for standard user access and another for my administrator account access, making it quick and easy to swap between the two."

Data Centre Manager, Renfrewshire Council

"We recognise the importance of linking technology innovation with improved experience for staff. It's not all about spending a lot of money; what this project showed was that sometimes it's the smallest and simplest of changes that make the biggest difference."

Head of ICT Services, Renfrewshire Council

Pull print

Improvements to our pull print service have proven very popular. Previously, staff had to enter their full domain username and password using the printer's tiny touch screen, which meant login mistakes were inevitable. It could also take over a minute to authenticate. Staff will soon be able to authenticate automatically (and instantly) using NFC (near-field communication) via their staff passes.

Changing security culture

Organisations can be reluctant to invest in technology. When investment is approved, it's not always welcomed by everyone. In addition, austerity over the last decade has had a significant impact on the public sector ability to invest and modernise. I'm delighted to report that our changes delivered **real benefits** to customers, staff and the council services. By **simplifying** authentication to services we've streamlined staff logins, and reduced the number password resets, allowing IT staff more time to deal with customers.

We also realised that we would need to contact compliance agencies (such as PSN, PCI and our security colleagues in Partner agencies) as some of them raised concerns about practicality and security. We are doing this by writing a Cyber Security Risk Report which shows how **risk has in fact reduced**. Our PSN assessor had no concerns that our changes would affect our PSN compliance.

Our experience of this programme just goes to show that change can happen when staff are committed and the benefits, for the entire organisation, are visible.

Find out more

- For more information about the NCSC's Secure by Default Partnership Programme, please visit: <https://www.ncsc.gov.uk/sbd>.