



CASE STUDY



Essex County Council



## TAC's Zero Trust Access Helps UK County Council Improve Productivity, Gain Granular Access Control

The Essex County Council is a governmental body with over 8,000 employees serving some 1 million residents in the UK. As such, it is imperative that the Council's systems enable its employees to collaborate effectively with other organizations, including the National Health Service (NHS) in the U.K.

The Council relies on Total Access Control (TAC), a Zero Trust access solution from PortSys, to allow NHS staff and other companies in partnership with the ECC to securely gain access to Council resources in order to work more efficiently. Daniel Holbrook, a Senior IT Analyst for the Council, says a key benefit of TAC's zero trust approach is that it allows the ECC to control access not only on the user level, but also on the device level.

TAC's zero trust access control enables the Council's IT team to determine what criteria the NHS users must meet before getting access. There is not a direct connection to any resources – every user must pass inspection through TAC first and every connection is validated before allowing access.

### PORTSYS TAC MAKES SOUND SECURITY SIMPLE

The NHS example illustrates just how simple security can be. TAC is a reverse proxy gateway that provides secure access and Single Sign-On to any application from any device. Rather than log in directly to an application, all users log in to the TAC gateway, which applies predefined policies to determine whether the user should be allowed access to the requested application. TAC offers the Council the option of Single Sign-On or manual authentication.

By examining the users' context of access, TAC provides many factors of authentication to create a much stronger security posture that prevents or limits access from untrusted scenarios. It is also easier for end users, who only have to provide their log-on credentials and go through the multi-factor authentication. Once approved, users gain access only for the resources for which they are authorized, based on security policies set up by the Council's IT team and incorporated with the TAC policy engine.



“ TAC PROVED TO BE A COST-EFFECTIVE SOLUTION FOR OUR NEEDS. ”

DANIEL HOLBROOK, SENIOR IT ANALYST FOR ESSEX COUNTY COUNCIL

Holbrook said one of the strategic goals for the Council is to allow flexible working, which raises its own security concerns.

“TAC allows our users to easily access certain internal resources from their home machines or mobile devices, but it also bakes in the safeguards we need to prevent users from accessing sensitive data from home,” Holbrook said. Because the Council is deeply concerned about security, it has some experience with multi-factor authentication. For instance, with UAG, the Council’s IT team had to use a token-based multi-factor authentication system and another server license. That means getting a new user established, which required issuing a token and often took days to accomplish.

“Using TAC enabled us to decommission the physical tokens and move to a more secure, web-based two-factor solution,” said Holbrook. “That significantly reduced our overhead, since we didn’t have to purchase physical tokens and licenses anymore.”

TAC has multi-factor authentication built-in, with its SafeLogin feature that enables users to choose an alphanumeric keypad that becomes the second factor, in addition to a password. “Using SafeLogin, I’ve managed to get current users with credentials in Active Directory set up in five minutes, including multi-factor authentication,” Holbrook says, although implementations for other organizations may be dependent on the user’s set-up.

ECC uses Direct Access for employees who have Council-issued Windows-based laptops, which have the Direct Access VPN client built in. It uses TAC for IT contractors and others who don’t have Council-issued laptops, or who use non-Windows machines – which don’t support Direct Access. It also

provides the Council with business continuity if Direct Access has issues. TAC has proven useful to IT engineers – they no longer need to keep a separate laptop at home or carry one home, so they can access most of their systems from a personal device if the system has been approved to be used on home devices.

“As I work on out-of-hours support, I use TAC to respond to calls and only switch to a work laptop if I am going to be working for a few hours,” Holbrook said.

By examining the users’ context of access, TAC provides many factors of authentication to create a much stronger security posture that prevents or limits access from untrusted scenarios. It is also easier for end users, who only have to provide their log-on credentials and go through the multi-factor authentication. Once approved, users gain access only for the resources for which they are authorized, based on security policies set up by the Council’s IT team and incorporated with the TAC policy engine.

The Council found TAC upon searching for a replacement for UAG, for which Microsoft was ending support. Around the same time, the Council’s contract with its token vendor was expiring. TAC’s built-in multi-factor authentication meant tokens were no longer required. “TAC proved to be a cost-effective solution for our needs” Holbrook says.

### PROPER SECURITY IS CRUCIAL

Saving money can’t come at the expense of compromising on security, which is crucial to ECC. As the Council keeps critical and personal data on county residents, it is subject to the new EU General Data Protection Regulation (GDPR).

“Any breach of security may cost us up to €20 million in fines or 4% of our annual revenue,” Holbrook says. “Failure to have appropriate security in place to protect our information will also result in reputational damage to the Council, and damage to our customers who are the service users.” Because it is a public entity, any fines levied would ultimately be borne by county citizens, he notes.

In the face of such penalties, ECC was justifiably concerned about how it could safely open up its network to third-party contractors, such as the engineers who perform printer support, patching, upgrades and the like. TAC enables the Council to ensure such contractors can only access the resources they really need. TAC also does a security check on each client device, ensuring it is running a modern support operating system with up-to-date antivirus (AV) software, to comply with Council policy.

In fact, security is so important that the Council recently had a security company perform penetration tests on its environment to find any security holes.

“TAC performed well in the last round of penetration tests with no issues reported,” Holbrook says.

### MULTIPLE TAC USE CASES, GRANULAR CONTROL

TAC was a godsend for some 170 former ECC personnel who went to work for a third-party highway company the Council hired on an outsourced basis.

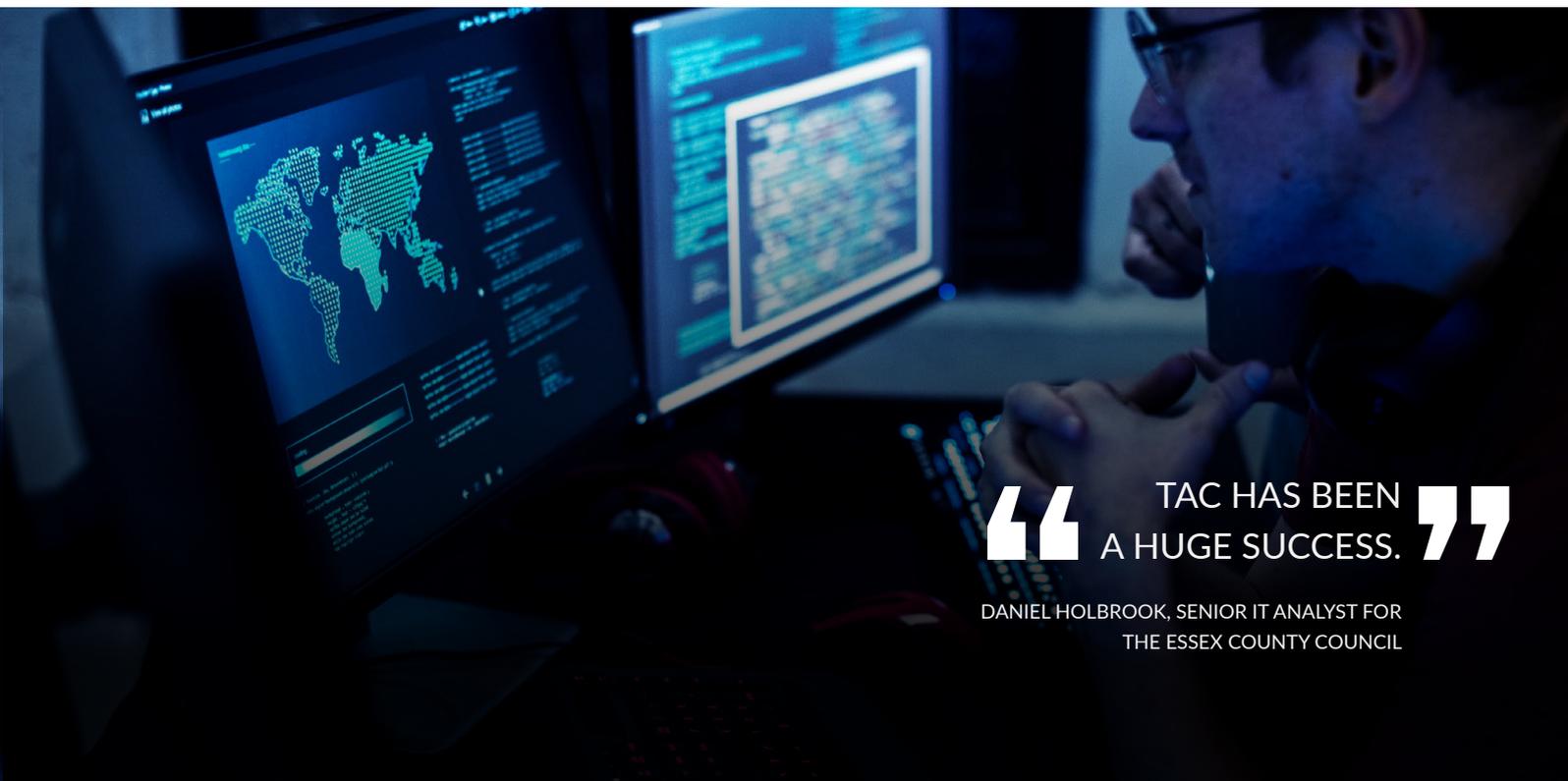
Although they are still paid by the Council, they are technically employees of the third party, and thus no longer have an ECC-issued computer with Direct Access.

With TAC, these employees can now once again access various resources they still need from the Council. “Through a single login to the TAC portal they can access Outlook email, newsletters, our intranet with HR, training and payroll systems,” Holbrook says. “TAC has been a huge success.”

TAC is also used by some internal IT personnel, enabling them to tap in from home when necessary, for example. In such cases, TAC’s ability to take connection context into account is crucial.

For example, TAC can consider the geographic location of a device that’s attempting access. The Council blocks access attempts from any IP address outside of the EU or United States, given the fact that legitimate users typically come only from these areas. In the rare case when a legitimate user does need access from some other area, Holbrook says it’s a simple matter to white-list the user.

The ability to consider context also gives the Council granular control over when users can access various resources. A user who is authorized to access financial applications, for example, may be denied access when trying to connect from an unsecure, public network, such as in a coffee shop or even a home Wi-Fi connection – a nod to the GDPR and its stiff fines.



“ TAC HAS BEEN A HUGE SUCCESS. ”

DANIEL HOLBROOK, SENIOR IT ANALYST FOR THE ESSEX COUNTY COUNCIL



### EASY IMPLEMENTATION, OUTSTANDING SUPPORT

While it provides thoroughly sound security, Holbrook reports TAC is nonetheless easy to implement. That's especially true for former UAG users, as it has a similar look and feel.

"The TAC deployment was extremely quick," he says. "It was pretty much plug and play. We turned it on and it was very straightforward." The only aspect that took any significant time was configuring access policy and settling on what images to use for two-factor authentication. Some users had a hard time remembering what pictures they chose, so Holbrook switched to images of words and numbers, which solved the problem.

Through it all, Holbrook said his experience with the support team from PortSys has been positive.

"Most of the calls I make to request support are immediately dealt with by a small

group of dedicated engineers, who make the whole process feel just a little more personal."

### TAC IMPROVES PRODUCTIVITY, PROVIDES PEACE OF MIND

TAC has also enabled ECC employees and contractors to be more productive. The 170 outsourced workers, for example, now have a much easier time with things like purchasing. Without access to Council procurement systems, they'd have to email someone who did have access in order to purchase anything. "TAC's allowing them to carry on with their jobs," Holbrook says.

Similarly, support engineers and internal IT folks now have an alternative way to access the resources they need, from wherever they may be. Going forward, they will have more capability to work at home, save on travel time and get work done after hours.

Through it all, the Council can rest assured that TAC is keeping them secure.



Learn more about how PortSys and TAC can secure access to all of your applications, from any device.  
Visit: [www.portsys.com](http://www.portsys.com).

+ 1 781 996 4900 (North America)

+ 44 208 196 2420 (International)

[sales@portsys.com](mailto:sales@portsys.com) / [www.portsys.com](http://www.portsys.com)