



CASE STUDY: METROPOLITAN POLICE SERVICE ADOPTS SINGLE SIGN ON

ActivIdentity® partners with Capgemini to deliver project for 50,000 staff, officers and temporary employees

- The Metropolitan Police Service (MPS) is using ActivIdentity SecureLogin® SSO to manage password security across six core applications for its staff of almost 50,000.
- Phased deployment of ActivIdentity SecureLogin SSO licences for all 50,000 MPS staff and officers completed in just six months.
- The new Single Sign On (SSO) infrastructure provides flexibility and scalability to support the MPS' future identity management and assurance initiatives.

Meeting demands of policing London in the 21st Century

Effective information, communications and technology (ICT) have an important role to play in supporting the MPS mission of working together for a safer London. As part of its modernisation programme, the MPS is working with Capgemini - its information, communications and technology outsourced contractor - and partners such as ActivIdentity to ensure it has a robust, flexible, resilient and cost effective ICT service to support front line policing in the 21st Century.

The password management challenge

The MPS has a world-wide reputation and has a unique place in the history of policing. Founded in 1829, the original establishment employed 1,000 officers and policed a seven-mile radius from Charing Cross and a population of less than 2 million. Today, MPS employs 31,141 officers, 13,661 police staff, 414 traffic wardens and 2,106 Police Community Support Officers (PCSOs) and, since the realignment of police boundaries in April 2000, it covers an area of 620 square miles and a population of 7.2million.

The extensive IT infrastructure at the MPS plays a central role in day-to-day policing. Therefore, ensuring that access to information is as secure and effective as technology allows is a key part of the ongoing drive to improve policing. However, the sensitive nature of police work means it is common practice for constabularies to

password protect applications. Furthermore, the sheer volume and complexity of log-on details can have knock on effect on efficiency due to re-keying and sometimes forgetting of passwords.

“Any technology decisions must reinforce the Service’s objective of making efficient and effective use of our resources,” explains Ailsa Beaton, Director of Information at the MPS. “SSO offers increased security while enhancing the productivity of our staff. Ultimately this benefits the people we serve.”

Reducing SSO-related risk

In April 2006, the MPS began an in-depth evaluation of SSO solutions to ascertain which one could provide the best fit for its requirements. The final decision was based on the technical competencies and management requirements of the solutions, the support infrastructure available for MPS’s project team throughout the implementation phase and the scalability and flexibility to support future developments in the Service’s IT infrastructure and business requirements. The favoured solution would have to score well in each of these areas to succeed, as Beaton outlines:

“Delivery against our basic criteria was fundamental and we have been rigorous in our assessment of the available options. We have evaluated the various solutions available to ensure that they could support both our short and long-term objectives. Not only does this protect our investment, it frees-up our resources in the future to focus on other parts of the IT estate.”

ActivIdentity SecureLogin® SSO, implemented by Capgemini and supported by the vendor’s professional services team, presented the most compelling solution for the MPS. The new SSO solution future proofs the MPS investment by offering the scalability to SSO-enable additional applications and the flexibility to integrate with smart card technologies should the Service decide to adopt them in the future.

On a technical level, the solution meets the MPS’s requirements through functionality such as: password randomisation, automated password expiry, to ensure consistent security both for applications with and without native expiry facilities; and a high level of compatibility with applications in the Service’s IT infrastructure.

The experience ActivIdentity had of supporting customers through large-scale deployments was another critical factor. “The support programme presented by ActivIdentity ensured that we could call on the professional services team’s expertise and proven methodology, and transfer that knowledge to our own people,” Beaton continues.”

Implementation support

Capgemini began the implementation with a 15 user pilot and then an 800 user, two borough test before the full scale deployment began, which involved a phased approach to delivery across all 32 of the Service’s boroughs. Initially, the MPS identified six applications to SSO enable which included a mixture of facilities to ensure that a wide range of password management issues were addressed.

ActivIdentity SecureLogin SSO works within the MPS Microsoft® Active Directory without the need for an additional data source or repository. Not only does this mean the IT team is able to use the system in the context of a familiar management console, it also streamlines the deployment process and associated costs by negating the need for additional server hardware to be implemented and managed at the back-end. As a result, ActivIdentity SecureLogin SSO licences for 50,000 users have now been delivered on budget and in just six months.

Capgemini and ActivIdentity have worked closely with the MPS to ensure its project team has been able to facilitate the transition to SSO as seamlessly as possible for its employees. Workshops have been held for the project team to demonstrate the process of SSO-enabling additional applications in the future. In addition, MPS requested support for its end users during the implementation phase, which ActivIdentity addressed by providing extensive, tailored documentation to give proactive responses to frequently asked questions.

Future plans

With frame works, such as the Unified Police Security Architecture (UPSA) and ISS4PS, on the horizon the SSO infrastructure will also be able to support the police service’s emerging identity assurance requirements. The aim of UPSA will be to create a national identification and authorisation system for the UK police service, criminal justice and public safety organisations and their agents. Once the details of the architecture have been confirmed, police forces will be required to integrate their own secure infrastructure with the centralised UPSA system. Because ActivIdentity

technology is based on open standards, MPS can future-proof its investment in SSO by integrating the new system with smart cards and other required components of UPSA.

“SSO is a key component of our long-term security and efficiency strategy, rather than a quick fix to the password management problem,” concludes Beaton. “The flexibility and scalability of the new infrastructure provides MPS with a solid and secure foundation for developing its systems and supporting staff working practices for the foreseeable future. The support we are continuing to receive from ActivIdentity and Capgemini ensures we’re well placed to gain the maximum benefit from the system to meet our business requirements.”

Circa 1,110 words