



## An Executive Briefing with Tom Cleveland, Information Security Analyst, University of North Carolina Hospitals

In 2007, UNC Healthcare deployed Passlogix v-GO Single Sign-On (v-GO SSO) as the first step in a broad identity management initiative designed to simplify application access for the nearly 6,000 users at the system's seven hospitals as well as ensure the security of patient information. UNC is now preparing to add strong authentication to the identity infrastructure, leveraging the ability of the v-GO Sign-On Access Accelerator Suite to extend single sign-on to any kind of two-factor authenticator. Here UNC's Tom Cleveland explains his organization's identity and access management strategy.

Q: What was the catalyst for adopting enterprise single sign-on technology?

A: We have almost 6,000 users, including more than 1,500 UNC-Chapel Hill faculty physicians and physicians in training. Each person uses 8 or 12 of our 96 applications on a regular basis. Each system has different password rules and standards. There's a lot of user frustration in managing so many passwords and a lot of time spent in getting forgotten passwords reset. Single sign-on was the logical solution because users only have to remember their Windows password. ESSO handles the rest.

Q: What about strong authentication? What was the driver behind that?

A: Security in general and HIPAA in particular. ESSO helps with security issues because it eliminates the need for users to choose easy passwords that can be easily hacked or keep a written password list that can be stolen, but strong authentication adds an extra layer of security that we believe is important for HIPAA compliance. This is especially true in our kiosk environment, where you run the risk of exposing patient information to anyone who walks up to a shared workstation. The more protection, the better.

Q: Why did you start with ESSO rather than strong authentication?

A: We were investigating both technologies at the same time, and we realized that we could deploy ESSO while we were still evaluating strong authentication devices if we selected a solution like Passlogix's v-GO Sign-On Access Accelerator Suite that supports all different forms of two-factor authentication. ESSO would solve our immediate password manageability problem fairly quickly so we could eliminate some of our users' pain, and we would still have the flexibility to adopt any kind of strong authentication without being locked into any specific device type or brand.

Q: What form of strong authentication have you selected?

A: We evaluated everything, including at least three different fingerprint solutions, face recognition systems, smart cards, and SecurID and CRYPTOCARD tokens. The Hospital Police are deploying HID proximity readers to shore up physical security, so it would make sense to use the same badge for application access. We haven't determined the exact solution, but it should have both physical and logical access. We are exploring the idea of adding other authentication methods that would be used in conjunction with prox cards for added security, but no decisions have been made.



Q: How will the proximity badges work with single sign-on?

A: For the user, this will be transparent. The proximity card will identify the user as he or she approaches the workstation. Then the user will enter his or her Windows password to get authenticated to the machine as well as to the single sign-on system. Behind the scenes, the interaction between the prox card and the single sign-on system will be handled by the v-GO Authentication Manager (v-GO AM) module of the v-GO Access Accelerator Suite. v-GO AM maps the prox badge ID to the user ID for the primary logon, authenticates the user to v-GO SSO, regulates the applications that a given user can access, and so on.

Q: Why did you select the Passlogix sign-on Access Accelerator Suite?

A: One of the biggest reasons was that v-GO would allow us to ESSO-enable most of our applications out of the box without writing scripts. Obviously this reduces deployment time and expense. Also, as I mentioned earlier, the fact that v-GO can support any form of strong authentication was very important. It allowed us to roll out single sign-on without having our two-factor authentication plan in place and still have the freedom to choose any authenticator we wanted at any time.

Q: What strategy did you use to roll out ESSO to your users?

A: We started with 10 applications, primarily clinical information systems and other clinical objects, and a beta group of about 200 selected users. We sent out notices that v-GO was available for them to download and use. We didn't provide any training because we didn't think it was necessary. Instead we supplied simple documentation that included instructions for adding single sign-on to Web-based applications related to the user's own area of specialization. v-GO will automatically try to handle the credentials for any application, so we decided to let people do this themselves. It's working well.

Q: Are you planning to add identity provisioning?

A: We have been working with one of the major IdM providers for a year to explore this, and it's something we really need. We have about 25,000 moves, adds and changes every year. Some of these are because of the per diem nurse concept, where nurses work for 30 days and then go away for a while. Others are because we're in an environment where people work for the hospital one day and the university the next. Identity management will allow us to automate system setup and quickly adjust to all of these changes.

Q: How will your ESSO installation affect your IdM initiative?

A: IdM projects take four or five years. We couldn't wait that long to solve our immediate password problem or implement strong authentication. Instead, we're using single sign-on as the foundation for the entire identity infrastructure. With v-GO we have a choice of IdM systems, just as we had a choice of strong authenticators, so we were able to leave our IdM options open. v-GO can also give us the documentation to show which applications are used most frequently to help us with our IdM deployment. And once our IdM system is in place, newly assigned user credentials could be automatically populated into v-GO through the v-GO Provisioning Manager (v-GO PM). You have to start somewhere, and single sign-on was the easiest and fastest point of entry.

**passlogix**<sup>®</sup>

75 Broad Street, Suite 815

New York, NY 10004

Tel: 212.825.9100 x 2 or

866.727.7564 x 2

EMEA: +44 0 20 7917 2754

APAC: +65 6725 6295

Email: sales@passlogix.com