

Inside Perspective

Helping you unleash the full power of MEDITECH

Electronic newsletter published every 8 weeks

Simplified Sign-On: MEDITECH and third party enhancements (Part 2 of 3) Scott Blanchette, Principal Consultant

In the [last issue of Inside Perspective](#) we talked about Simplified Sign-On (SSO) and covered the various components that make up a comprehensive SSO solution. In this second article, we will review the inherent capabilities of the MEDITECH HCIS for supporting SSO, and touch on a number of approaches to achieve additional functionality via third party solutions.

As customers continue to deploy advanced clinical applications, particularly those at or near the point of care, the importance of Simplified Sign-On continues to grow. And recognizing that providing secure and convenient access to clinicians is necessary for broad adoption, Simplified Sign-On has been high on MEDITECH's agenda for several years now.

MEDITECH has developed two significant functional enhancements to their MAGIC and Client/Server platforms to ensure that they can integrate effectively with the systems and technologies that make up an enterprise-wide, secure, Simplified Sign-On environment.

Integration with Windows Authentication

The first enhancement is the ability to integrate with Microsoft® Windows Authentication services. Beginning with MAGIC version 4.9 SR 6 (DTS 6481) and Client/Server version 5.3 SR 6 (DTS 3811), MEDITECH added an NT Logon Enhancement that allows hospitals to link MEDITECH application authentication with Windows Network Authentication. The result is that users can log into a workstation using their network password, and then they are prompted only for a PIN number when accessing MEDITECH. The MEDITECH system determines the correct user based on the original NT logon. This eliminates the need for a user to have two separate user IDs and passwords when accessing MEDITECH applications from secure desktops.

MEDITECH has also created functionality that allows organizations to easily convert their users into the new login, providing the capability to have users self-link their MEDITECH ID to the NT Logon using a one-time, "next login" screen that walks the user through the process.

Hospitals that choose to use this functionality will need to install a new service Mlogon.exe on multiple servers, set up several Network Authentication parameters, educate the user community, and then monitor the conversion process to ensure that users are creating the linkages as they log in. The processes are similar in both MAGIC and Client/Server.

For many organizations this functionality may be a relatively easy quick win, particularly those with a well-maintained Active Directory and those who do not make heavy use of "generic" network logins.

This integration with Windows authentication can alleviate the need for users to remember (and for IT departments to maintain) separate user IDs and passwords in MEDITECH and Windows, but does not address some of the broader needs of identity management, session management, or Single Sign-On. Organizations may also be looking for the ability to integrate other non-MEDITECH applications into the same authentication system, or they might want to use technologies such as proximity devices to automate both logon and safe logoff when a user

walks up to and away from a workstation. This brings us to the second *MEDITECH* enhancement.

MEDITECH and Forward Advantage

Several years ago MEDITECH began to work with our mutual partner, Forward Advantage, to develop a set of APIs (Application Programming Interfaces) that improve identity management integration across the MEDITECH applications. The “im-one” product line from Forward Advantage brings a broad selection of tested and supported biometric, proximity, and other Simplified Sign-on applications and technologies to the MEDITECH market along with professional services to assist in the planning, selection and deployment at MEDITECH facilities.

The technologies and systems that Forward Advantage works with are all from established vendors in the healthcare marketplace, supporting many departmental and non-MEDITECH applications—but with the added benefit of improved communications with the MEDITECH applications via the “im-one” APIs. The APIs allow for additional session and identity management functionality such as the ability to notify MEDITECH when a user leaves a device, which the basic Network Authentication functionality does not provide.

Novell, Sentillion, and other third parties

In addition, MEDITECH hospitals have successfully deployed other third party Simplified Sign-On solutions from vendors such as Sentillion or Novell. These other solutions generally rely on “scripting” style integration to provide the additional functionality beyond the basic Single Sign-On functionality provided by the NT Logon enhancement and to “mimic” the functionality that the “im-one” APIs would otherwise provide. In some cases, the scripting approach may offer additional custom functionality, but it can be less reliable and more troublesome to troubleshoot and maintain.

What does the SSO future hold?

Single Sign-On systems have been successfully deployed in the MEDITECH market, particularly over the past 12-18 months, with Forward Advantage, Sentillion, and Novell appearing to be the most referenced vendors. Vendor products will continue to mature with additional off-the-shelf integration into secondary applications.

The least developed SSO capabilities are those surrounding session management, context management, and proximity detection. The technologies themselves are fairly mature, such as thin client technologies, which often form the basis of session management, but there are still issues that need to be worked out with how applications should respond to roaming type usage. A couple of specific technical and workflow issues that need to be addressed are automatically and safely terminating applications, and “parking” sessions without locking portions of a patient record.

There has been some recent broader technology interest and development around creating open source and ubiquitous user identities for Internet use. Several companies, such as OpenID, are developing solutions that are similar to the Microsoft® Passport service, but without the proprietary (and vendor-controlled) aspect. These developments may affect the healthcare marketplace eventually—although due to the sensitive nature of patient data, such open initiatives may not have the same level of success in the healthcare market as in other industries.

In the next and final installment of this series of articles about Simplified Sign-On, we will focus on approaches that you may want to consider in planning for, deploying, and ultimately supporting an SSO environment at your organization. Meanwhile, we welcome any thoughts or experiences you might like to share. Contact editor@jjwild.com.

Scott Blanchette has over twenty-five years experience in the healthcare industry in which he spent more than ten years as a CIO, managing information system departments for a number of MEDITECH hospitals. Email him at editor@jjwild.com.

Next Issue: SSO Part 3—Implementation and operational considerations