

## Advanced Authentication Integrated with MEDITECH

Hospitals are faced with the challenge of bridging security and user convenience. Furthermore, end users are more likely to secure workstations and adopt technology, like CPOE, if user authentication and e-signature requirements are streamlined.



# Authentication Manager

## The Solution

Authentication Manager is an application programming interface (API) designed specifically with, and for, MEDITECH. Authentication Manager provides a way for third-party authentication systems, such as single sign-on applications, to integrate with authentication devices to streamline clinician workflow and enhance security. Advanced authentication devices include fingerprint biometrics, smart cards, proximity cards, and more. To ensure that Authentication Manager works seamlessly with your MEDITECH system, the third-party authentication system's use of the API must be certified by Forward Advantage.

## Streamlined Clinician Workflow

Authentication Manager allows you to use the same authentication method within your MEDITECH applications that you use with your single sign-on deployment. For example, a clinician can log onto a workstation with a fingerprint scanner and then later uses the same method for bedside medication verification. Eliminating the need for a PIN provides additional convenience for the clinician, and security is increased with biometric authentication.

With Authentication Manager, virtually all MEDITECH authentications are streamlined this way, including signing on to MEDITECH, launching a suspended MEDITECH client session, and electronic signature verification.

## Positive Identification for CPOE

Authentication Manager identifies physicians for electronic order entry with the simple use of an authentication device, such as a fingerprint scanner. This same authentication method can be used consistently throughout the hospital. The security of electronic orders is enhanced with Authentication Manager, and patient safety is increased. Additionally, hospitals that use authentication devices for CPOE typically report a higher level of physician satisfaction and overall adoption.

## Key Features:

- Developed with MEDITECH for API connectivity
- Can use the same authentication method available with your single sign-on
- Improves physician and clinician workflow
- Increases overall security and patient safety
- Physicians and clinicians no longer need to remember passwords or PINs

## Requirements for Using Authentication Manager:

### MEDITECH MAGIC

- MEDITECH MAGIC v5.6.3 PP 3
- MEDITECH MSO service
- MEDITECH Network Authentication (Login) for all users (Compatibility Mode)
- ANP Service (running on Windows server with MSO and Authentication Manager)

### MEDITECH Client/Server

- MEDITECH Client/Server v5.5.6 PP 3
- MEDITECH Client/Server 5.6.5
- TCP connectivity deployed throughout
- MEDITECH MSO service
- MEDITECH Network Authentication (Login) for all users (Compatibility Mode)

Authentication Manager version 1.0.4.10 or higher (running on each MAGIC workstation). Certified third-party authentication system (please contact your Forward Advantage representative for information regarding certified solutions).

Note: MEDITECH 6.x support available in future release; PDA use not supported.

## For more information, please contact us at:

Forward Advantage  
7255 N. First Street, Suite 106  
Fresno, CA 93720 USA

1-877-636-7927 (t) 1-559-436-4217 (f)  
info@forwardadvantage.com - www.forwardadvantage.com

