DATASHEET

Enterprise Access Management (formerly OneSign) self- service password management

Put an end to password reset calls

Problems with passwords

Password reset calls are a persistent and costly nuisance for clinicians and hospital IT teams. Clinicians need to create, use, and frequently change their passwords to improve health data security and protect patient information. However, given healthcare's complex password requirements and the fast-paced nature of clinical work, it is easy for clinicians to forget their passwords. When that happens, it only takes a few failed login attempts for them to get locked out of their accounts.

Improve productivity, reduce frustration

Imprivata Enterprise Access Management (formerly OneSign) self-service password management enables hospitals and other healthcare organizations to eliminate password reset problems with more effective password management. Enterprise Access Management (EAM) authentication management and single sign-on (SSO) capabilities eliminate many password-related barriers to productivity by simplifying and automating password processes. With No Click Access™, users can simply sign in once and gain instant access to their desktops and applications, with just the tap of their badge or swipe of their fingerprint, for the rest of their shift. When clinicians forget their passwords, EAM self-service password management empowers clinicians to address the problem on their own, by resetting their primary credential quickly and easily. This process results in sustained productivity for clinicians and fewer help desk calls for IT.

Benefits

- Avoid productivity loss, relieve frustration, and increase convenience for clinicians
- Reduce password-related help desk calls, freeing up IT staff
- Lower IT costs and password-related administrative burden
- Improve security and compliance with better password management

Simplify self-service, reduce reset calls

EAM self-service password management enables clinicians to reset their own primary login credential, view what their current, application-specific single sign-on credentials are, and log in via a set of personalized questions. EAM clears a productivity roadblock for clinicians, enabling a quick, convenient, and secure process that requires no help desk involvement. By eliminating one of the most common reasons for help desk calls, EAM self-service password management takes all those calls “off the board.” Lower call volume reduces help desk staffing requirements and costs, freeing valuable IT resources to work on more strategic projects.

The EAM Administrator sets verification thresholds for the identities of users or groups of users in accordance with the hospital’s security policies.

Improve security

EAM self-service password management improves security in several ways. By giving clinicians an easy way to address forgotten passwords, it reduces the likelihood of clinicians using insecure workarounds, such as “borrowing” a colleague’s password. The solution also prevents IT from having to get involved with authenticating users over the phone, which minimizes opportunities for unauthorized access to the hospital’s network resources and patient information.

Self-Service Password Management: A closer look

Clinicians enroll by providing “shared secret” information in the form of a personalized question-and-answer list. The hospital’s EAM Administrator compiles these questions and manages them in a centralized EAM repository. The EAM Administrator sets verification thresholds for the identities of users or groups of users in accordance with the hospital’s security policies. In addition, all user-driven primary password reset events are logged, enabling EAM to create an audit trail which enhances security and makes compliance reporting easier.

When clinicians forget their primary credential, they simply click on the dialogue screen link or button and are automatically prompted through the Q&A and password reset process.

Users access the password-reset functionality by clicking on links or buttons that are added to the hospital’s login dialogue screens. These customizable links or buttons typically contain simple statements, such as “Help me log in” or “Forgot my password.” Clinicians and administrators can also access this functionality from a web-based portal that can be fully customized to their hospital’s functional and branding requirements. Branded portals provide users with a familiar and trustworthy password reset experience.

This EAM module also helps avoid help desk involvement, when clinicians lose or forget their proximity cards. EAM can be configured so that caregivers who have left their proximity card at home can access their workstations directly by answering their identifying questions. No matter what their primary authentication modality may be, clinicians maintain productivity by being able to access their hospital’s system while they resolve their credential issues.

Thin and zero client support

EAM self-service password management supports a wide range of thin and zero client devices from major vendors, including Dell Wyse, HP, and Samsung. With their smaller footprints, thin and zero client devices enable hospitals to make better use of their patient care spaces. Thin and zero clients also lower hospitals' power consumption, reduce support costs, and minimize IT management requirements.

EAM self-service password management supports a wide range of thin and zero client devices from major vendors, including Dell Wyse, HP, and Samsung.

Enterprise Access Management

EAM is the industry-leading SSO solution for healthcare. As a central pillar of the Imprivata healthcare security and authentication platform, EAM enables providers to access, communicate, and transact patients' protected health information (PHI) securely and conveniently. EAM empowers clinicians to spend more time focusing on patient care and less time dealing with authentication technology. With EAM, clinicians can improve the security and efficiency of clinical workflows by using the same identification and authentication credentials to access PHI from multiple locations and environments, including virtualized desktops. EAM integrates seamlessly with other Imprivata solutions, including Enterprise Access Management with MFA (formerly Confirm ID), the comprehensive identity and two-factor authentication platform for remote access, electronic prescribing of controlled substances (EPCS), medical device access, and other critical clinical authentication workflows.

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

Copyright © 2024 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.