imprivata

DATASHEET

Imprivata Enterprise Access Management with self-service password reset

A fast, safe, and user-friendly password reset solution

The password reset problem

Clinicians face constant password challenges — complex rules and busy schedules make forgetting passwords inevitable. A few failed attempts lock them out, disrupting care and flooding IT with reset requests. This costly cycle wastes time and resources across the hospital.

Improve productivity, reduce frustration

Imprivata Enterprise Access Management (EAM) simplifies and automates authentication for healthcare by enabling clinicians to access shared and private workstations, and single sign-on into applications, with passwordless methods like badge tap, face or fingerprint biometrics, and hands-free access. However, clinicians still must enter passwords at the beginning of each shift and for certain workflows. As we move to environments where passwords are unknown to clinicians, there will be an increased need for fast self-service to regain access when passwords are needed. When passwords are forgotten, modern self-service reset options from Imprivata such as face authentication, an SMS OTP code sent to an authorized mobile device, or the Imprivata ID secure mobile app allow instant, user-driven recovery.

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

Boost efficiency and cut costs

Self-service password reset empowers clinicians to manage their own login credentials quickly and securely — without involving the help desk. By eliminating one of the most frequent support requests, this solution significantly reduces help desk call volume. Fewer calls translate to lower staffing needs and support costs, allowing IT teams to focus on higher-value initiatives, thus improving overall operational efficiency.

Reset passwords instantly with face authentication, SMS OTP, or mobile app — no help desk needed, no downtime for clinicians.

Improve security

EAM self-service password reset improves security in several ways. By giving clinicians an easy way to address forgotten passwords, it reduces the likelihood of clinicians using risky workarounds, such as "borrowing" a colleague's password. The solution also prevents IT staff from authenticating users over the phone, which minimizes opportunities for social engineering resulting in unauthorized access to the hospital's network resources and patient information.

Self-service password reset: A closer look

Clinicians enroll in self-service password reset with a comprehensive set of secure authentication options. These include advanced methods like face authentication, SMS one-time passwords (OTP), and Imprivata ID — a secure mobile app designed for fast, seamless verification. While personalized security questions remain available as an option, they are less emphasized due to the stronger security and smoother experience provided by the newer technologies.

Hospital administrators centrally manage these authentication methods and select the verification threshold that aligns with organizational security policies. Every self-service password reset event is logged to create a detailed audit trail, enhancing security and simplifying compliance reporting.

When clinicians forget their primary credentials, they can easily initiate the reset process via customizable links or buttons embedded on login screens, with clear prompts such as "Help me log in" or "Forgot my password." This functionality is also accessible through a branded web portal tailored to the hospital's look and feel, providing a familiar and trustworthy user experience. This web portal can be configured to be limited to the local network, or accessible from anywhere clinicians, or other users, may need to reset their primary credentials.

Beyond password resets, self-service helps clinicians regain access even if they forget or lose proximity cards, allowing them to authenticate via secure authentication methods to maintain workflow continuity. Regardless of their primary authentication method, clinicians can quickly resolve credential issues without IT help desk involvement, maximizing productivity and operational efficiency.

The EAM administrator centrally manages authentication methods and selects the verification threshold that aligns with organizational security policies.

Thin- and zero-client support

EAM self-service password reset 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.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. Imprivata's platform of innovative, interoperable access management and privileged access security solutions enable organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

3402-2025_EAM-DS-self-service-password-reset