

DATASHEET

Imprivata Mobile Access Management (formerly Imprivata GroundControl) and Bretford SmartHub with Display: A powerful combination for frontline mobile workflows

In life- and mission-critical environments, every second matters. Frontline workers need mobile solutions that enhance productivity, security, and user experience. Imprivata Mobile Access Management (formerly Imprivata GroundControl) and Bretford PowerSync Pro SmartHub with Display provide a robust and efficient check-out solution.

We make the efficient use of shared devices a reality with Imprivata Mobile Access Management (MAM). This end-to-end mobile solution empowers organizations with a fast, efficient end user workflow. It also enhances security and supports IT and mobile teams in managing their fleets.

When used together, MAM and Bretford PowerSync Pro SmartHub with Display offer a comprehensive solution that boosts both security and user experience in modern workspaces.

How Imprivata creates a better checkout experience

The intuitive Imprivata interface ensures that users can quickly and easily access the mobile tools they need. This saves time, promotes faster adoption, and increases productivity.

- Easy, badge-tap check out
- Near-immediate device assignment
- Intuitive access to fully charged, ready-to-go devices
- Clear communication of status and next steps

Key features:

- **Integrated Technology**
Combines a high-quality display with built-in power and connectivity options.
- **USB Connectivity**
Provides up to 20 USB ports for easy and fast data transfer and charging.
- **Durable Design**
Built to withstand the rigors of daily use in busy environments.



Intelligent charging and more, powered by Bretford

The Bretford SmartHub with Display offers a best-in-class experience for simplifying the management of shared devices.

- Full-time, full-rate charging to reliably maintain devices
- Built-in display delivers easy-to-follow instructions for checking out and returning devices
- Built-in badge reader makes device check-out simple and fast
- Sleek base houses Launchpad computer and wiring to minimize footprint

Team up with Imprivata and Bretford for seamless security and effortless collaboration

MAM and Bretford PowerSync Pro SmartHub with Display offer a powerful and integrated solution that enhances security, improves user experience, and promotes collaboration in modern workspaces. The result: organizations can experience a comprehensive and cost-effective approach to managing shared mobile access. This powerful combination is the ideal choice for organizations looking to stay safer and more efficient while enabling better outcomes for their teams.



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:

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

Copyright © 2025 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.

2981-2025_MAM-DS-bretford-smarthub



DATASHEET

Imprivata Mobile Device Access



Shared device management, simplified

Healthcare organizations are implementing mobile solutions to improve care quality and increase operational efficiency; however, the introduction of new mobile technologies creates challenges around security, inventory management, and clinical efficiency.

Ensuring the proper balance of security and efficiency, both from technology and user management standpoints, is critical for the successful adoption of mobility initiatives in healthcare.

With Imprivata Mobile Device Access, organizations can be confident in knowing that devices are left in the proper state, every time. The comprehensive solution enables secure assignment of devices between users to ensure patient privacy, data integrity, and clinical productivity.

Improved security for shared-use devices

With Imprivata, organizations can lock down devices between use, ensuring that only trusted identities have access to sensitive tools and information.

Additionally, users are fully logged out between each use to ensure a clean state, every time.

Effortless access to devices and applications

Users experience streamlined access to secured devices with either the simple tap of a proximity badge, or utilizing facial biometrics for passwordless device checkout and unlocking. Additionally, with Imprivata single sign-on (SSO) technology, the need for manual authentication into individual applications is removed, saving time and reducing frustration.

Benefits

- Fast, badge-tap access to devices and seamless SSO into mobile applications
- Increased security for shared-use environments
- Auditable visibility into user interactions with devices
- Simplified inventory management and loss prevention
- Facial biometric functionality for passwordless device check out and unlocking

Inventory management and loss prevention

Comprehensive reporting and audit logs bring visibility into user interactions with devices and applications. Accessing and understanding information such as which users accessed devices last, as well as the last known location of a device, not only expedites investigations into lost devices but also leads to increased user accountability.

Shared mobile, simplified

Imprivata Mobile Device Access is healthcare's only authentication solution that enables fast, secure access to Android devices and applications. Users can access shared mobile devices with the simple tap of a proximity badge, and can then SSO into their applications. Imprivata Mobile Device Access helps organizations unlock the full potential of shared mobile devices by ensuring a fast, efficient workflow while improving security and auditability.



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. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables 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

Copyright © 2025 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.

3629-2025_MDA-DS-overview

Unlock the power of mobile workflows



Organizations are looking to mobile tools to improve freedom and flexibility of workflows, especially in the face of constrained budgets and personnel resources. However, it isn't easy to achieve an efficient workflow experience on mobile devices without compromising security, privacy, and compliance. Additional security requirements can create barriers that hinder usability and threaten adoption, leaving organizations unable to optimize their investment in mobile technology.

Imprivata delivers mobile device security and privacy without compromising on workflow efficiency, solving challenges for both BYOD and enterprise-owned device environments. By leveraging digital identity to support security and compliance directly within mobile workflows, Imprivata eliminates friction that can impact usability while also reducing points of exposure. Imprivata removes barriers to use and supports care delivery with secure, real-time access to critical tools and information, from anywhere at any time.

Improve access security on personal devices

When organizations allow employees to expand their workflows beyond the walls of the organization, it's critical that privacy and security measures expand in kind, offering protection regardless of where or how employees access sensitive information. To maximize the benefits of mobile technology, organizations must enforce strong authentication in convenient, familiar ways that usability and adoption. Imprivata Digital Identity plays a key role in supporting this dynamic.

Enforce stronger, practical security on mobile devices

- Enforce strong authentication methods and complex passwords without disrupting users
- Require multifactor authentication to access sensitive information
- Establish trust to leverage mobile-based authentication modalities

Create a seamless user experience

- Leverage familiar authentication workflows on your mobile device, such as facial recognition, soft tokens, and biometric identification
- Turn mobile devices into a trusted, second factor of authentication for a hands-free authentication experience
- Support secure access to critical tools from anywhere, at any time, including EPCS-compliant devices that meet FDA requirements for prescribing controlled substances

Enable privacy in shared-use environments

Organizations are leveraging shared-device models to help reduce the investment needed to support untethered workflows. As with any workplace technology, usability and efficiency are equally important, and staff need to access all critical tools and information regardless of which device they use. But when resources are shared between users, this balance is more difficult to achieve. Imprivata is the only solution that supports both privacy and personalization in enterprise-owned, shared device environments.

Ensure only trusted access to devices and applications

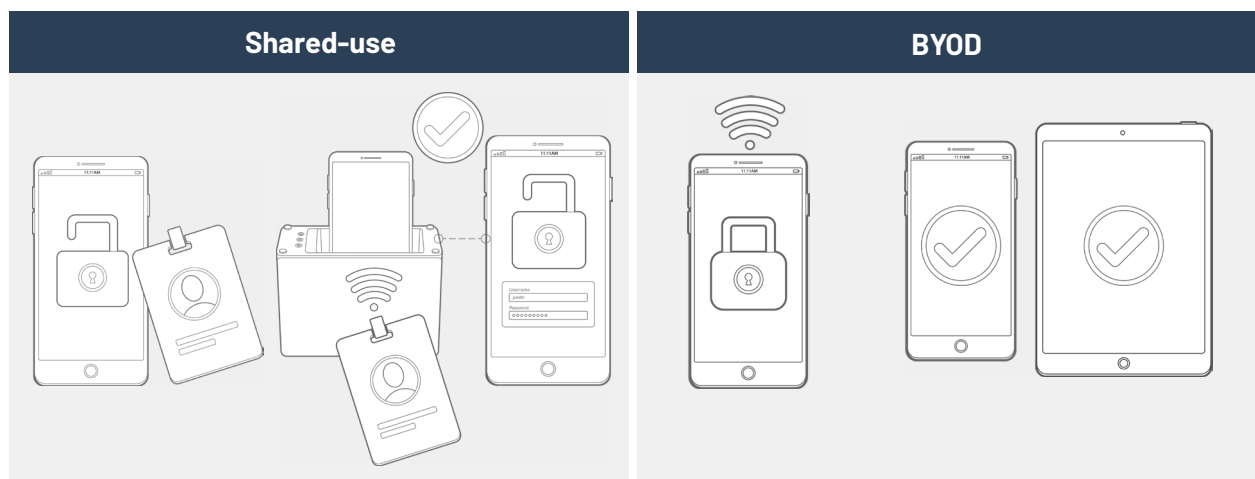
- Leverage trusted digital identity with badge-tap assignment of mobile devices
- Lock down shared devices between users to prevent unauthorized access
- Enforce authentication after device lock to control access to sensitive information

Streamline access and device management

- Leverage familiar authentication workflows on your mobile device, such as facial recognition, soft tokens, and biometric identification
- Turn mobile devices into a trusted, second factor of authentication for a hands-free authentication experience
- Create audit trails for who used which device when, where, and for how long, to reduce device loss
- Depersonalize devices between users by removing user credentials and controlling access to information as devices are exchanged between users

Enabling secure access without barriers

By leveraging digital identity to enforce authentication at the device and application level, Imprivata delivers frictionless security for both shared-use and BYOD environments. We support adoption by extending familiar digital identity driven access and authentication to mobile workflows.



Imprivata Mobile Device Access:

Imprivata Mobile Device Access is healthcare's only mobile authentication solution that enables fast, secure access to clinical mobile devices and applications. Users can access shared clinical mobile devices with the simple tap of a proximity badge and can then single sign-on (SSO) to their applications.

Imprivata Mobile Access Management (formerly GroundControl):

Enable a hands-on device management experience from the cloud – maintaining and updating from anywhere at any time. Employees and IT teams benefit from simple, personalized device checkout, effortless application access, and cloud-based management of assets and workflows.

Imprivata Enterprise Access Management (formerly OneSign and Confirm ID) for remote access:

Improve security by enabling enterprise-wide two-factor authentication for remote network access, cloud applications, and Windows servers and desktops.

Imprivata Enterprise Access Management for EPCS:

Providing the broadest range of DEA-compliant two-factor authentication modalities, including Hands Free Authentication, push token notification, and fingerprint biometrics, to make EPCS fast and convenient for providers.



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 © 2023 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.

