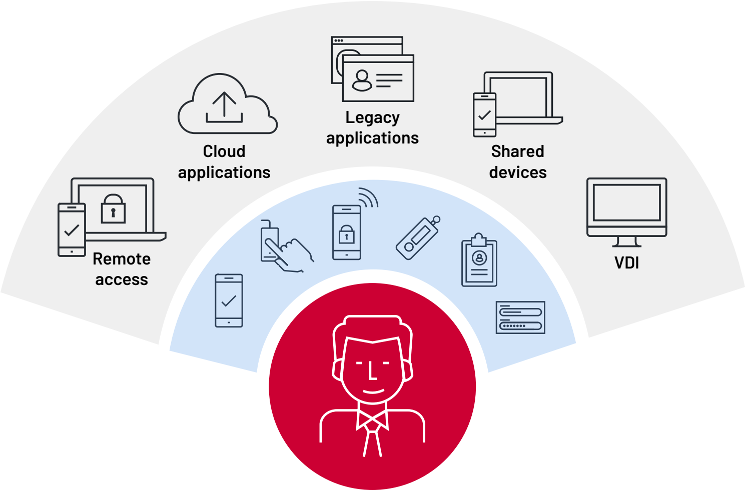
DATASHEET

Imprivata Enterprise Access Management with MFA (formerly Imprivata Confirm ID)

Multifactor authentication for remote access use cases

As organizations adopt cloud applications, enable remote work, and integrate IoT devices, while continuing to support many legacy applications, the digital attack surface continues to expand, increasing the risk of unauthorized access and data breaches. This makes enterprise-wide multifactor authentication (MFA) more critical than ever. However, businesses need flexible solutions allowing secure remote access that adapts seamlessly to diverse scenarios and evolving user needs.

Imprivata Enterprise Access Management with MFA (formerly Imprivata Confirm ID) is the comprehensive identity and MFA platform for fast, secure authentication, and provides the flexibility that organizations need. Imprivata Enterprise Access Management (EAM) combines security with convenience by offering a broad range of innovative and convenient authentication methods that make security invisible, such as proximity badges, tokens, biometrics, and more.



Whether looking for MFA for remote access, to meet compliance requirements, or for secure access to sensitive data, EAM delivers a single, robust solution.

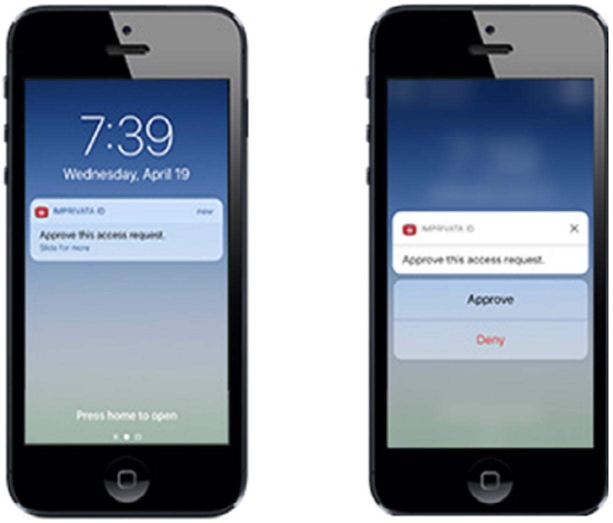
Remote access use cases

Enterprises in every industry continue to be victimized by large-scale, high-profile data breaches, and hackers are employing highly targeted, sophisticated, social engineering techniques to gain access to sensitive data.

EAM for remote access improves security by enabling multifactor authentication for remote network access, cloud applications, and other critical systems and needs. The solution also offers convenient authentication methods such as push token notifications that can be leveraged across workflows, allowing organizations to incorporate two-factor authentication for an added layer of security that's familiar, fast, and efficient for users.

Improve security across the enterprise

With remote access gateways, cloud applications, and Windows desktops, EAM for remote access improves security by delivering holistic, enterprise-wide multifactor authentication across critical business and IT use cases. Together with Microsoft 365, EAM integrates with Entra ID conditional access, which simplifies MFA for users without compromising security. This gives customers a single, phone-based token (Imprivata ID) to support numerous use cases, allowing customers to consolidate vendors and ensuring a consistent authentication experience for users.



Approve this access request.

Approve this access request.

Anywhere, anytime self-service device management

EAM for remote access allows users to self-enroll their mobile device from anywhere, anytime. Self-service device management delivers fast and frictionless enrollment, which improves the end user experience and reduces the administrative burden of helping users enroll new devices. This enables organizations to scale the enforcement of two-factor authentication quickly and efficiently for remote access to the entire enterprise.

Frontline use cases

In manufacturing, government, banking, retail environments and more, EAM improves security and regulatory compliance by enabling fast, secure authentication for critical use cases. Imprivata transforms authentication by replacing passwords with fast, convenient methods such as the tap of a proximity badge, swipe of a fingerprint, or Hands-Free Authentication. The solution also integrates with legacy and cloud apps via EAM with single sign-on integration to give frontline workers a seamless authentication experience, where they are only prompted for authentication methods that are available and allowed.

EAM offers detailed reporting capabilities to establish a secure, auditable chain of trust for critical authentication use cases. This gives organizations better visibility into how, when, and where employees interact with intellectual property (IP), personally identifiable information (PII), or other sensitive data that must be safeguarded while adhering to regulatory compliance requirements.

Integration with shared devices and virtual desktop access

EAM offers productized integration with shared kiosks and virtual desktop integration (VDI) with Citrix Virtual Desktop, Omnissa Horizon, and Azure Virtual Desktop applications. A single instance of EAM will work across the entire ecosystem regardless of how many shared devices and applications are used in the network, giving organizations a consistent experience while reducing the total cost of IT ownership.

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