DATASHEET

Imprivata Confirm ID for Remote Access

Secure and convenient two-factor authentication for the healthcare enterprise

Key benefits

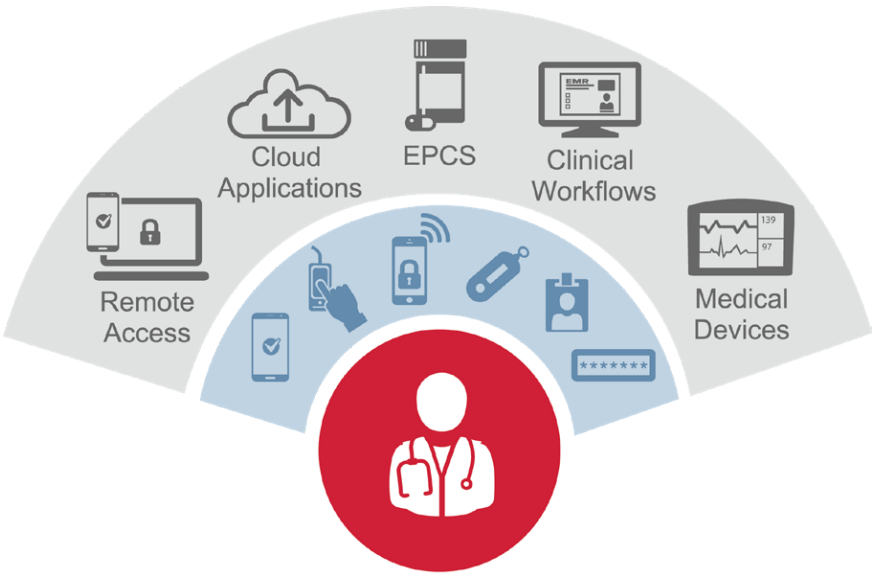
- Improve security by enabling enterprise-wide two-factor authentication for remote network access, cloud applications, and Windows servers and desktops
- Make security invisible to users with innovative and convenient authentication methods such as push token notification
- Streamline reporting and simplify authentication management with a single, centralized identity and authentication platform for all enterprise workflows

Imprivata Confirm ID® for Remote Access is a secure and convenient two-factor authentication solution purpose-built to meet the critical security and workflow challenges of today's healthcare enterprise.

Healthcare continues to be victimized by large-scale, high-profile data breaches, and hackers are employing highly targeted, sophisticated, social engineering techniques to gain access to patient records and other sensitive data.

Imprivata Confirm ID for Remote Access improves security by enabling two-factor authentication for remote network access, cloud applications, and other critical systems and workflows.

Imprivata Confirm ID also offers convenient authentication methods such as push token notification that can be leveraged across workflows, allowing organizations to add a layer of security that is familiar, fast, and efficient for users.



Improve security across the enterprise

Imprivata Confirm ID for Remote Access improves security by delivering holistic, enterprise-wide two-factor authentication across critical business, IT, and clinical workflows, including:

- **Remote access gateways —** Imprivata Confirm ID integrates seamlessly with VPNs and remote access gateways from Citrix, Cisco, VMware, and other leading providers to enable fast, secure two-factor authentication and safeguard against unauthorized network access
- **Cloud applications —** Imprivata Confirm ID integrates with Microsoft ADFS to enforce two-factor authentication when users access cloud applications. This improves security as hospitals move PHI, employee data, financial records, and other sensitive information into the cloud.
- **Windows servers and desktops —** Imprivata Confirm ID enables two-factor authentication for administrator access to ensure only authorized users can access Windows desktops and servers. This safeguards against attempts by hackers to access these critical systems using credentials obtained through phishing or other cyberattacks.

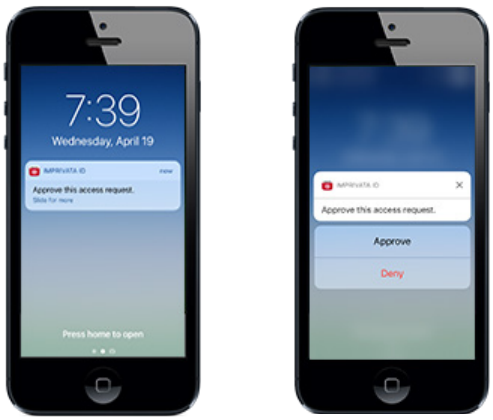
> **“Imprivata Confirm ID allows physicians to securely but conveniently access patient information from anywhere. The push token notification is quick and easy, so users can stay focused on the task at hand.”**
>
> **Dr. Anthony Carbone, CMIO at Genesis Health System**

Fast, convenient push token notification

Through convenient push token notification, Imprivata Confirm ID for Remote Access enables the enforcement of two-factor authentication with a workflow that is fast and efficient for users.

Employees enter their username and password as the first factor of authentication, and Imprivata Confirm ID will then send a notification to the user’s mobile phone, asking them to verify their identity. Users simply approve the notification from the lock screen of their device, and the second factor of authentication is complete. They are not required to unlock their phone or manually type a token code, and they don’t have to carry at hardware token fob (though these methods are supported if necessary).

In addition, Imprivata’s push token notification meets DEA requirements for two-factor authentication for electronic prescribing of controlled substances (EPCS), allowing physicians to access the hospital network and prescribing controlled substances remotely using the same convenient, secure, and compliant authentication method.



Alternatively, if users do not have the push token functionality available, Imprivata Confirm ID for Remote Access supports additional authentication methods such as conventional software tokens, SMS text, and temporary codes generated by IT administrators. This increases flexibility to meet the requirements of various user authentication workflow scenarios while maintaining security.

Frictionless security with skip second-factor

Imprivata Confirm ID for Remote Access allows organizations to establish grace periods during which users can skip the second factor of authentication. After using two-factor authentication for the initial login, users will only be prompted for a single factor upon subsequent logins from a trusted device. This improves usability and ease of implementation while ensuring security for remote network access and other workflows.

Anywhere, anytime self-service device management

Imprivata Confirm ID for Remote Access allows users to self-enroll their mobile device from any device, anywhere. Imprivata's cloud-based 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 allows organizations to more quickly and efficiently scale the enforcement of two-factor authentication for remote access to the entire enterprise.

For more information, visit www.imprivata.com/remote-access.

Imprivata Confirm ID combines security and convenience by enabling fast, secure authentication across enterprise workflows.

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

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

Copyright © 2021 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.

DS-RemoteAccess-0713