

DATASHEET

Imprivata Enterprise Access Management for virtual desktop access (formerly Imprivata Virtual Desktop Access)

Microsoft Remote Desktop Services

Harnessing the value of virtual desktops in healthcare

Hospitals are adopting virtual desktops to give their care providers faster, easier, and more flexible ways to access patient information and clinical applications. For hospitals using Microsoft Remote Desktop Services to deliver these capabilities, Imprivata Enterprise Access Management for virtual desktop access (formerly Imprivata Virtual Desktop Access) provides an easy and proven way to ensure success by streamlining clinicians' virtualized workflows.

Using advanced authentication and single sign-on capabilities, Imprivata Enterprise Access Management (EAM) for virtual desktop access enables clinicians to eliminate repetitive manual logins from their daily routines. EAM for virtual desktop access simplifies the clinical authentication process by automatically signing clinicians into their virtual desktops and clinical applications, increasing clinical productivity and enhancing care delivery.

No Click Access to roaming desktops

Microsoft Remote Desktop Services sessions follow users, maintaining the state of their desktops and applications as users change locations or switch workstations. EAM for virtual desktop access streamlines Microsoft Remote Desktop Services roaming capabilities by eliminating the need for manual logins. With Imprivata, clinicians just perform a quick badge tap or fingerprint swipe to access their roamed desktop on any device.

Benefits

- No Click Access™ to Microsoft Remote Desktop Services (MRDS) virtual environments
- Streamlined clinical workflows with faster, easier access to desktops and applications
- Industry-leading support for zero and thin client devices
- Flexible authentication options, including proximity cards and fingerprint biometrics



EAM for virtual desktop access delivers No Click Access™ to Microsoft Remote Desktop Services virtual desktops. No Click Access enables clinicians to access patient information quickly, without having to repeatedly type usernames or passwords. With faster and easier access, clinicians can spend more time focusing on patients and less time dealing with technology.

Thin and zero client support

EAM for virtual desktop access is the only solution that enables true desktop roaming between thin and zero client devices. EAM for virtual desktop access offers industry-leading support for zero and thin client devices, giving customers maximum endpoint device flexibility. 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, improve support costs, and reduce IT management requirements. Imprivata partners with the leading thin and zero client vendors, including Dell, HP, IGEL, 10Zig, Stratodesk, and LG.

Key technology differentiators

Some of the technological characteristics of EAM for virtual desktop access that make it the authentication management solution of choice for Microsoft Remote Desktop Services customers include:

- API-level integration streamlines the authentication process and ensures forward compatibility, as new versions of Microsoft Remote Desktop Services become available.
 - Allows policy decisions to be made at runtime, streamlining and tailoring the connection process. For example, Microsoft Remote Desktop Services users can be signed into their virtual desktops or applications while other users are signed into the local desktop.
 - Uses policy-driven end user workflow optimization to tailor workflows to clinician- or group-specific needs.
 - Automatically secures the previous end point when the session roams to a different workstation or device.
 - Integrates at the API level to eliminate the need to produce scripts, reducing the burden on IT and ensuring a smooth upgrade process across new versions of Microsoft Remote Desktop Services.
- Automated Microsoft Remote Desktop Services application launching from within a MRDS delivered desktop.
- Native firmware-level integration with thin and zero client devices.
 - Strong authentication support for proximity card workflows, including transaction-level re-authentication and second factors.
 - Out-of-the-box configuration for for Imprivata Enterprise Access Management workflows across devices from vendors, including Dell, HP, IGEL, 10Zig, and Stratodesk.

Strengthen compliance

Imprivata enables hospitals to more effectively safeguard patients' PHI in Microsoft Remote Desktop Services virtual desktop environments. The solution also tracks and audits all application access events by user, easing compliance with HIPAA reporting requirements.



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 © 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.