Imprivata Virtual Desktop Access for VMware Horizon View

**Benefits**

- No Click Access to virtualized desktops
- Thin and Zero clients integration
- Strengthened compliance, including password policy enforcement, workstation security and application access audit
- Support for flexible authentication technologies, including fingerprint biometrics and proximity cards

**Simple Secure Access to Virtual Desktops**

Organizations are implementing desktop virtualization to simplify user access to their desktop and applications.

Imprivata Virtual Desktop Access extends the benefits of desktop virtualization by streamlining access to follow-me desktops, providing:

- No Click Access® to virtual desktops with the tap of a badge or the swipe of a fingerprint
- Single sign-on to all applications for fast, secure access to data
- Strengthened compliance to meet international, federal and state compliance regulations

**No Click Access to Virtual Desktops**

VMware Horizon View desktops follow users, maintaining the state of their desktops and applications as they change locations and switch workstations. But repeated logins slow down the process taking users away from their goals. Mistyped or even forgotten passwords further slow the process leading to frustration and increased helpdesk calls. With Imprivata Virtual Desktop Access, the need to manually login is replaced by the tap of a badge or the swipe of a fingerprint. Able to integrate with the majority of proximity cards that you may already be using for building access, desktop roaming is quick and secure saving time and eliminating helpdesk calls.

From the virtual desktop, single sign-on gives users access to all other authorized applications. With no typing or passwords necessary, users can focus on their work.

**Zero and Thin Client Support**

With their smaller footprints, lower power requirements and simplified management, thin and zero client devices provide multiple opportunities to simplify IT management and create cost savings. Imprivata partners with every major thin and zero client vendor including Dell Wyse, HP, Igel, LG, NComputing, Praim and Samsung. By partnering with chip manufacturers Teradici and Texas Instruments, Imprivata is the only authentication provider able to support zero client devices providing flexibility for customers in their
Using Imprivata OneSign with VMware Horizon View strengthens the security and privacy of organizational assets.

endpoint strategies. API level integration with VMware Horizon View and the Teradici PC-over-IP protocol enables full roaming across to zero and thin client devices without any double-hop scenario simplifying access for users and management for IT.

**Strengthen Compliance**
Using Imprivata OneSign with VMware Horizon View strengthens the security and privacy of organizational assets.

**Automate password changes:** Password policies typically have passwords changing every 90-120 days. Imprivata OneSign removes this burden from the user, automating the process in the background, ensuring compliance while removing unnecessary workflow interruptions and inevitable forgotten passwords.

**Enforcing password policies:** Imprivata OneSign automatically enforces password strength policies, enabling organizations to stipulate password length and strength requirements, which are adhered to during the automated change process.

**Workstation security:** With desktop virtualization, no data is stored on the workstation itself.

**Transaction-level strong authentication:** Applications can leverage Imprivata OneSign strong authentication to re-authenticate a user at any point in the transactional workflow—enforcing their positive identity.

**Access control and audit:** All application access is tracked and audited by user.

**Easy to Implement, Deploy and Manage**
A certified component of VMware's AlwaysOn Point of Care reference architecture, organizations can be assured that Imprivata OneSign is tried and tested in high availability mission critical scenarios.

Imprivata Virtual Desktop Access is available as a physical or virtual appliance, simplifying deployment and maintenance. It requires no changes to applications or user directories, such as Active Directory. Centralized management of authentication, access control and audit reduces administrative overhead and eliminates password-related helpdesk calls.

For organizations in the early stages of their move to virtual desktops, or are executing a phased roll out, Imprivata Virtual Desktop Access eases the physical-to-virtual transition by creating a consistent user experience every time they log in whether it be into a physical or virtual environment.
Key Technology Differentiators
Following are some of the technological characteristics of Imprivata Virtual Desktop Access that make it the authentication management solution of choice for VMware AlwaysOn Point of Care Desktop customers.

- **API Level integration with the VMware Horizon View Connection Broker**
  - Allows policy decisions to be made at runtime to streamline and tailor the connection process, e.g. VMware Horizon View users can be signed in to their virtual desktop while other users are signed in to the local desktop
  - Policy-driven end user workflow optimization delivers the ability to tailor workflows for a clinician’s specific needs or for different groups of users
  - Automatically secures the previous endpoint when the session roams to a different workstation or device
  - By integrating at the API level, the need to produce scripts is removed. This helps reduce the burden on IT and ensures a smooth upgrade process across new versions of VMware Horizon View

- **Native firmware level integration with Teradici PC-over-IP zero client devices**
  - Strong authentication support for proximity card workflows, including transaction-level re-authentication and second factors
  - Out of the box configuration for Imprivata OneSign workflows across all Teradici-based zero client devices from vendors including Dell Wyse, HP, Igel and Samsung

Imprivata Virtual Desktop Access is available as a physical or virtual appliance, simplifying deployment and maintenance.
About Imprivata

Imprivata is a leading provider of authentication and access management solutions for the healthcare industry. Imprivata's single sign-on, authentication management and secure communications solutions enable fast, secure and more efficient access to healthcare information technology systems to address multiple security challenges and improve provider productivity for better focus on patient care.

Over 2 million care providers in more than 1,000 healthcare organizations worldwide rely on Imprivata solutions. Imprivata is the category leader in the 2012 and 2013 Best in KLAS Software & Services Report for SSO, and SSO market share leader according to HIMSS Analytics.

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

Offices in:
Lexington, MA USA
Santa Cruz, CA USA
Uxbridge, UK
Paris, France
Nuremberg, Germany
Den Haag, Netherlands