



# Fast, Secure Access to VDI Applications

*The Role of Automated Access in Accelerating Virtual Desktop Adoption*

*By: David Ting, CTO, Imprivata, Inc.*

*This whitepaper looks at ways that organizations can increase virtual desktop adoption and security simultaneously using automated access for VMware View™ 4.5 and Oracle's Sun Ray™. It demonstrates how automated access can reduce the number of steps to logon and logoff virtual workstations from 7 to 3. It also explains how Imprivata's automated access solution, Imprivata OneSign Virtual Desktop Access™ :*

- o Improves virtual desktop user productivity and workflow*
- o Embeds transparent security*
- o Integrates location awareness into roaming and security policies*

## TABLE OF CONTENTS

---

<b>Desktop Virtualization Gains Ground .....</b>	<b>2</b>
<b>User Access: The Potential Productivity Bottleneck .....</b>	<b>2</b>
<b>Automated VDI Access = Faster Access.....</b>	<b>4</b>
<b>Streamlined, Secure Access with Imprivata OneSign VDA .....</b>	<b>5</b>
<b>OneSign VDA = Improved VDI User Productivity and Workflow .....</b>	<b>5</b>
<b>OneSign VDA = Productivity Gains and Transparent Security Across the Workflow</b>	<b>6</b>
<b>OneSign VDA = Roaming with Location Awareness .....</b>	<b>8</b>
<b>Considerations for Successful VDI Adoption .....</b>	<b>9</b>
<b>Conclusion .....</b>	<b>9</b>

## DESKTOP VIRTUALIZATION GAINS GROUND

Virtualization technology is transforming the user desktop, replacing the need for fully loaded PCs on every user's desk with virtual desktops delivered to static and mobile workers. Virtual Desktop Infrastructure (VDI) solutions like VMware View™ 4.5 and Oracle's Sun Ray™ offer centralized management and control of the desktop environment, while providing the user with a consistent experience, regardless of the specific endpoint they are using.

A VDI environment allows administrators fine-grained control over access to applications and data, reducing risks of data leakage. These attributes are particularly valued in environments like healthcare and government, where employees are mobile and controlling access to information is essential.

However, as with any new technology, there is a danger that the technology can get in the way of productivity rather than enhance it. Particularly with security measures, the more roadblocks you put in the way of the business users, the more resistant they are to embracing new technology. In deploying VDI, you have an opportunity to improve the user experience and workflow while providing greater security.

As you deploy a VDI environment, you must ensure that security measures do not interfere with productivity. Automated access solutions for VDI can help you increase productivity, reduce user resistance and lead to faster and greater adoption.

## USER ACCESS: THE POTENTIAL PRODUCTIVITY BOTTLENECK

A VDI implementation offers the chance to improve and enhance the user experience—delivering a seamless workflow for application access on any device. You can now allow users to move throughout their work environment, with their virtual desktop “following” them throughout the day. Keeping the context of the user desktop from location to location makes it easier for a user to complete their jobs by removing the interruptions associated with constantly logging off, logging on and restarting applications.

To achieve these benefits, however, you must simultaneously address the challenges associated with desktop and application access. The access point is where you enforce security controls to ensure that only authorized individuals can access sensitive applications. Each additional login or security measure imposes another obstacle between the user and the completion of their task.

The chart below shows the steps a user needs to take to traverse the security layers within a VDI system in order to use an application.

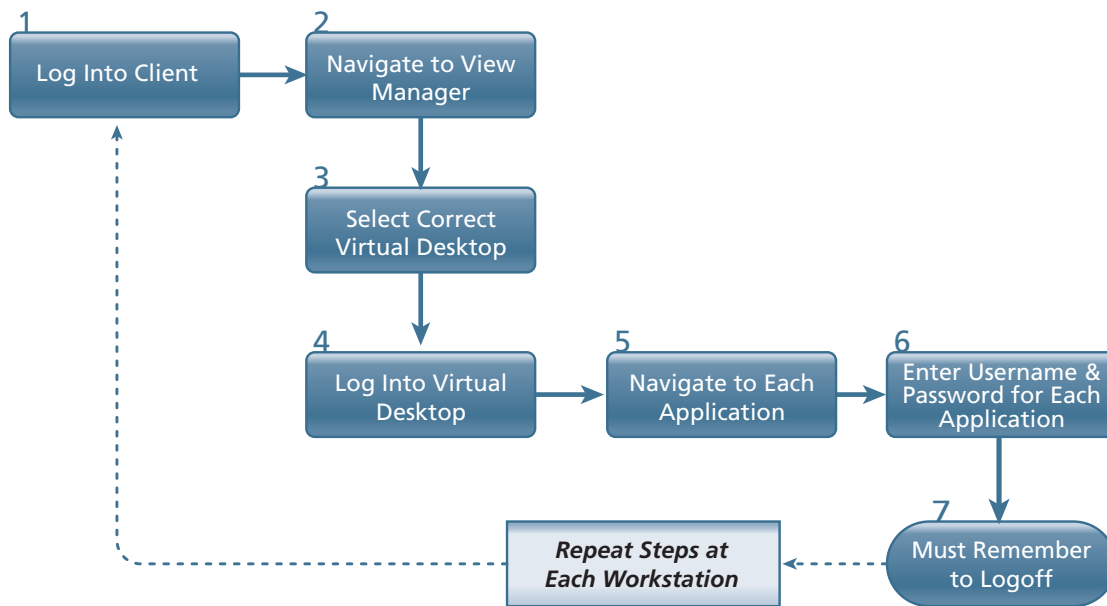


Figure 1: Steps to connect to applications in the VDI environment

1. Log into the client, whether a laptop, a workstation, or a desktop system in a private office.
2. Find the View Manager on the client.
3. Select the correct virtual desktop.
4. Log into the virtual desktop, by supplying the correct user ID and password.
5. Navigate to the right application.
6. Log into the application, supplying the user ID and password for the application.
7. Log off the application and the virtual desktop when leaving the workstation.

Roaming users that connect at many different workstations during the day must repeat this sequence of steps and logins many times, potentially using different IDs and passwords for each application. Even though applications within a VDI environment persist as long as the session is alive, many applications can time out due to inactivity to necessitate having to login again on a reconnection.

Each of these steps occurs in the context of someone trying to get their job done. Consider the clinician in a healthcare environment moving from a patient room to a shared workstation to an office. Each time they must execute these same steps. Their limited time with the patient is spent focusing more on technology rather than the patient.

Frustration, unattended and unsecure workstations, and weak, [shared passwords](#) are the inevitable consequences. And let's not overlook all of the calls to the IT helpdesk from forgotten or invalid passwords.

## AUTOMATED VDI ACCESS = FASTER ACCESS

Using an automated access solution, such as Imprivata OneSign Virtual Desktop Access™, you can replace the 7 steps with just a few simple user actions:

1. **Authentication** - The user authenticates at different workstations during the day with the single touch of a fingerprint or ID card. OneSign automatically connects the appropriate virtual desktop with the right applications to the user
2. **Application Access** - Once authenticated into their desktop, as users launch applications, their usernames and passwords are automatically filled in, providing direct access without the need to remember them all and enter them each time
3. **Security** - When finished at that workstation, the user can simply walk away. OneSign Secure Walk-Away® automatically locks the workstation, protecting sensitive applications and data.

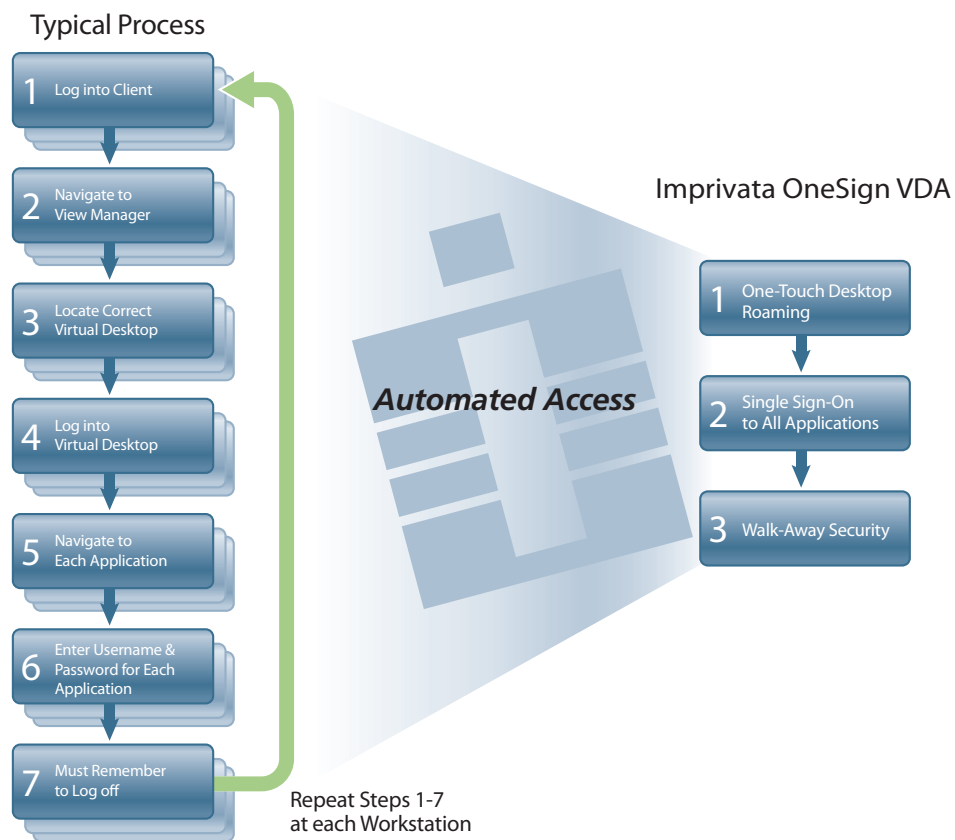


Figure 2: Streamlining application access and logoff

## STREAMLINED, SECURE ACCESS WITH IMPRIVATA ONESIGN VIRTUAL DESKTOP ACCESS™

Imprivata OneSign® is an identity and [access management](#) platform that integrates user authentication, user access, [password management](#) and access auditing in one secure, easy-to-manage appliance. Imprivata OneSign simplifies access control with centrally managed authentication and access policies integrating physical and IT security across an entire organization.

Imprivata OneSign Virtual Desktop Access (VDA) integrates with VDI environments such as VMware View 4.5 and Oracle's Sun Ray to automate the process of logging in to desktops and applications—while extending security across the entire workflow. The Imprivata OneSign appliance can run on a physical or virtualized server.

By streamlining and securing user access, OneSign VDA:

- Improves virtual desktop user productivity and workflow
- Embeds transparent security
- Integrates location awareness in roaming and security policies

*Let's look at how OneSign VDA delivers all three components:*

### ONESIGN VDA = IMPROVED VDI USER PRODUCTIVITY AND WORKFLOW

OneSign VDA gives users fast, convenient access to applications delivered via VMware View or Oracle Sun Ray by providing:

- **Fast, Secure Desktop Roaming:** Rather than going through a complete login process every time they change location, users should be able to simply touch a fingerprint pad or card reader to call up their desktop and any running applications. Virtual desktops should be personalized according to the individual's job function and preferences.
- **Single Sign-On:** Enables rapid access to applications without the need to enter usernames and passwords for each one. Launch an application and OneSign will automatically fill in the user's username and password and log them in. Fast, and nothing to remember, or more importantly, forget.
- **Workflow Continuity:** As users change locations, their desktop should follow them, maintaining state as appropriate. This eliminates the time sink of connecting and disconnecting from various applications from each new location. When a user reconnects to their desktop from a new location, they should be able to reconnect to their previously established desktop session.

## **ONESIGN VDA = PRODUCTIVITY GAINS + TRANSPARENT SECURITY ACROSS THE WORKFLOW**

Too often, productivity and security are seen as trade-offs. By adding OneSign VDA to your virtual desktop environment, you have the opportunity to improve both, by layering security in a transparent fashion throughout the VDI workflow—from session start to logoff.

### ***Session Start: Applying Strong Authentication***

The adoption of VDI is a perfect opportunity to eliminate the security risks associated with the inherent weaknesses of passwords. We all know that people with too many passwords to remember will erode security by writing their passwords down or setting them all to the same easy, obvious string.

The solution is twofold: enable strong authentication beyond just a username and password, and provide single sign-on capabilities so that users won't have to remember all their various passwords; manage them for the user. With this strategy, knowing a password is not enough to gain access, and users won't need to write passwords down and stick them to their monitors.

Using Imprivata OneSign VDA, you can easily add strong authentication factors to your virtual desktop login and application sign-on. OneSign supports a number of authentication technologies, so you can choose the method that works best for your users and environment. For example, many notebooks have built-in fingerprint devices. Adding a biometric factor to the login ensures that only the actual user can access their desktop.

Proximity cards are pervasive in healthcare and government industries, and can easily be added to authentication processes. Workstations equipped with a card reader allow users to quickly login with a tap of the card or a tap + entry of a PIN. OneSign also supports tokens and other methods.

Once the user has authenticated initially, repeated reconnections during the day require only the tap of the proximity card or press of the fingerprint, without additional need to enter additional data.

Combining **strong authentication** with single sign-on offers convenience and productivity gains with protection from phishing, password theft, and other unauthorized access. Together with a complete audit trail of virtual desktop access, OneSign helps to ensure that essential data and applications are well protected from misuse and unauthorized access.

### ***Application Launch: Audit and Control***

When deploying the VDI desktop, apply the principle of least privilege; putting only those applications appropriate for the user and their role on the desktop. This reduces the possibility of unauthorized access and eliminates the clutter on the desktop with applications that are not appropriate to the user's role.

Maintaining a secure audit log of application access gives you constant visibility into who is accessing which applications—when and from where. Combining strong access controls with constant audit and visibility is key to protecting applications and data from unauthorized access and misuse.

### Transaction-level Authentication

You can require that the user re-authenticate (via proximity card or fingerprint) when performing a particularly sensitive transaction. Examples of these transactions might include writing prescriptions in healthcare, transferring funds in the financial industry, or authorizing programs in government agencies.

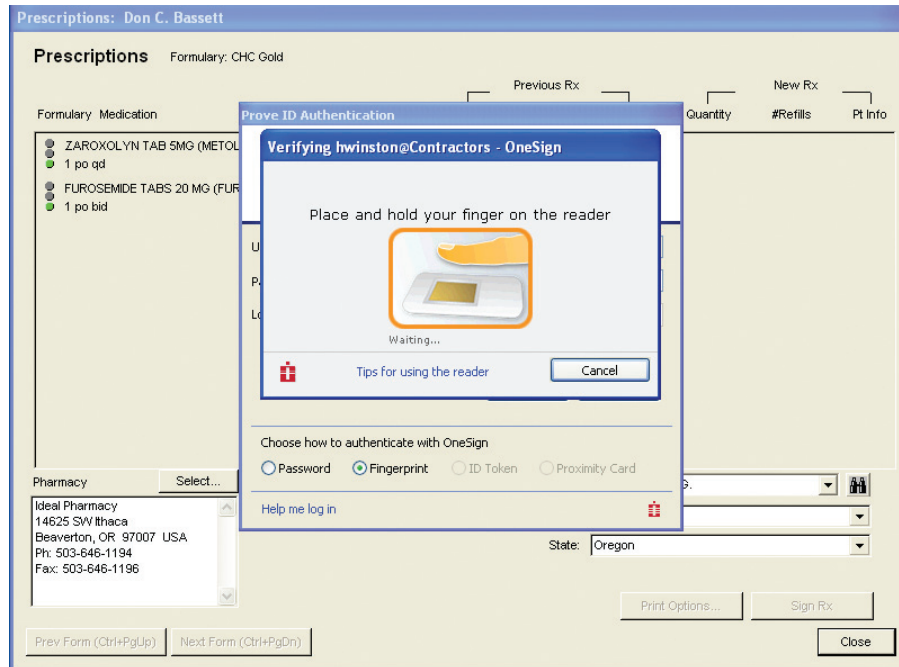


Figure 3: A user may be challenged to re-authenticate during an important transaction

Challenging users to perform this quick re-authentication increases your confidence that the right user is at the workstation at this critical juncture.

### Locking or Ending Sessions

The move to VDI gives you the opportunity to set and enforce policies around desktop sessions. For example, should a user need to re-authenticate after a certain period of idle time? How much idle time is allowed before the session times out and the desktop locks? With the VDI infrastructure, these decisions can be integrated throughout the overall VDI environment.

Unattended workstations are a common security issue. A user, once authenticated, may walk away to answer a question or handle an emergency. You need to set policies around how long a workstation can be unattended, and to automate the process of locking down public workstations when an authorized user is not present.

**OneSign Secure Walk-Away®** is an option that protects workstations with the potential for public access. It uses a video camera that monitors the presence or absence of an authenticated user in front of the workstation. Once the user walks away, it locks the workstation, and provides instant re-authentication when the user returns. The user does not need to do anything special to take advantage of this security. If they do not return, another user wanting to access that workstation can easily disconnect the previous user and gain access with their own credentials.

Walk-away security is particularly important for workstations where many people move through the area (such as workstations in reception areas, public spaces or patient rooms.)



*Figure 5: Secure Walk-Away automatically detects the presence or absence of the user*

## **ONESIGN VDA = ROAMING WITH LOCATION AWARENESS**

As any real estate agent will tell you, location always matters. For roaming users, you want to deliver the same consistent desktop experience, with location-aware intelligence built in to streamline workflow and to enhance security.

OneSign VDA gives your VDI environment location-aware operations for devices, applications, and data.

### **Devices**

With OneSign VDA, when a user switches locations, the devices available to them change automatically. For example, the default printer will change depending on the location of the workstation.

### **Applications**

OneSign VDA enables you to set applications to be sensitive to location as well. You can tailor the presentation or appearance of an application depending on location—hiding personal emails at public workstations, for example. In a patient room, the clinician may automatically be presented with the electronic health record application.

### **Location-Specific Data**

Location information can be used to filter which data is presented to the end user.

For example, government workers may only be able to access documents with specific clearance levels when they have keyed into a secure facility. Or a physician may automatically get the data for the patients on the second floor when using a workstation on that floor.

Imprivata One-Sign VDA supports all of these types of location awareness, and fully supports the roaming user according to security policies.

## CONSIDERATIONS FOR SUCCESSFUL VDI ADOPTION

As you implement or design a VDI environment in your organization, consider the following strategies for success:

1. Maintain and protect end-user workflows. Protecting user productivity throughout the transition and beyond is essential to your organization. Technology is merely the means to the end of your core mission.
2. Secure the virtual environment with strong authentication and single sign-on. With centralized control of the desktop deployment, you have a unique opportunity to enhance security. Combining single sign-on with strong authentication ensures that the tighter access controls are coupled with the convenience of a single login.
3. Leverage location awareness to improve productivity and security. Eliminate the productivity drains and security risks of user roaming by integrating location-aware capabilities in your VDI infrastructure.
4. Remember that a quick win requires happy users. Include end users on your implementation team, and make sure you understand their workflows. If you make the users' lives more difficult, you are bound to suffer from slow and/or incomplete adoption. Protect and enhance the user experience, and your VDI solution has a much better chance of success.

## CONCLUSION

Imprivata OneSign Virtual Desktop Access™ is an automated access solution that gives users fast, convenient and secure access to applications, so you can realize the cost, efficiency and security benefits of desktop virtualization.

Imprivata OneSign VDA:

- o Improves virtual desktop user productivity and workflow
- o Embeds transparent security
- o Integrates location awareness into roaming and security policies

To learn more, visit [http://www.imprivata.com/onesign\\_virtual\\_desktop](http://www.imprivata.com/onesign_virtual_desktop).



Offices In:  
Belgium • Germany  
Italy • Singapore  
UK • USA

1 877 ONESIGN  
1 781 674 2700  
[www.imprivata.com](http://www.imprivata.com)

WP-VDAGOCO-Ver1-1110