# Table of Contents

About the Validated Design Guide ........................................... 3  
Introduction ........................................................................ 4  
Audience ........................................................................... 4  
Business Case ....................................................................... 4  
What Is Mobile Secure Workplace? ........................................ 5  
  Mobility ........................................................................... 5  
  Security ........................................................................... 5  
  Management ..................................................................... 5  
User Profiles ......................................................................... 6  
Mobile Secure Workplace Architecture Overview .................... 8  
Key Components of the Architecture ....................................... 10  
  Core Components ................................................................ 10  
  Additional Components ..................................................... 10  
Solution Validation ................................................................. 11  
  Lab Equipment List ............................................................ 11  
  Solution Components ......................................................... 11  
  Optional Components ......................................................... 11  
Overview of Architecture ....................................................... 12  
  Datacenter ....................................................................... 13  
  Storage ............................................................................ 15  
  Networking ........................................................................ 16  
  Security ............................................................................ 17  
  RADIUS Two-Factor Authentication ...................................... 21  
  Single Sign-On for “Follow-Me Desktop” Experience ................. 22  
Management .......................................................................... 23  
  Endpoint Management ........................................................ 24  
  Persona Management ........................................................ 25  
Printing ................................................................................. 25  
  Optional: User-Installed Applications ................................. 25  
  User Connection Flow Sequence ......................................... 26  
Design Optimizations ............................................................... 27  
Summary ............................................................................... 28  
Appendix 1 ........................................................................... 29  
  Test Cases ....................................................................... 29  
  Functional Test Cases ........................................................ 29  
  Performance Validation Results ........................................... 30  
Appendix 2 ........................................................................... 34  
  How to Set Up Location-Based Printing on a Zero Client ........ 34
About the Validated Design Guide

VMware® Validated Design Guides provide an overview of the solution architecture and implementation. The validated designs and solutions have been created through architectural design development and lab testing.

The guide is intended to provide guidance for the introduction of proof of concepts, emerging new technology and architectures, as well as enhancement of customer use cases.

The Validated Design Guides:

• Incorporate generally available products into the design
• Employ repeatable processes for the deployment, operation, and management of components within the solution.

Validated Designs are tested for a specific use case or architectural practice on a limited scale and duration. These guides ensure the viability of theoretical designs or concepts in real world practices.

The Validated Design Guides provide an overview of the solution design and implementation guidance that includes:

• Use cases that are catered to the design
• Products that were validated as part of design testing
• Software that was used for each component of the design
• Configurations used to support the design test cases
• A list of design limitations and issues discovered during the testing
Introduction

This Validated Design Guide provides you an overview of the VMware Horizon™ Mobile Secure Workplace™ solution. The architecture uses products from VMware and its ecosystem of partners to build a comprehensive solution that satisfies the specific requirements of various use cases in enterprises such as mobility, bring your own device (BYOD), security, compliance, and printing.

This document will provide an overview of the various use cases, logical solution architecture, and results of the tested configuration. The solution is not exclusive to the products tested within the architecture. Consult your VMware representative for more information about how to modify the architecture with your preferred vendors.

Audience

This document is intended to assist solution architects, sales engineers, field consultants, advanced services specialists, and customers who will configure and deploy a virtual mobile secure workplace solution.

Business Case

Today’s workforce is no longer tethered to traditional stationary desktops. New devices have proliferated at companies of all sizes. Workers are increasingly mobile, and more than 60 percent of enterprise firms and 85 percent of SMB organizations are looking to initiate BYOD programs. Although end users are embracing these trends, IT departments—faced with tight budgets—are struggling with how to best support and manage these new devices while protecting corporate data as it is accessed across networks and locations.

A need to find a secure, streamlined and more cost-effective way to manage end users across devices and locations has become a top priority for many customers today.

Research shows that 97 percent of employees carry more than two devices and 50 percent of employees carry more than three devices. It is estimated that by the end of 2013, there will be more than 272 million tablets. With the popularity of these new devices and with companies increasingly supporting teleworking and remote working, it is becoming important to provide a way to enable secure access to workplaces over a wide variety of devices for end users across locations.
What Is Mobile Secure Workplace?

The VMware Horizon Mobile Secure Workplace solution provides an innovative way for IT to support device diversity and bring your own device initiatives by improving user access and mobility, streamlining application updates, enhancing data security, and delivering the highest-fidelity user experience.

This solution enables you to address the following three key requirements:

**Mobility**

The Mobile Secure Workplace solution built on VMware Horizon View™ places desktops in the datacenter and provides access to the datacenter through any device. With a multitude of client devices supported, the desktops can be accessed from any workstation, thin client, or mobile device. This enables true BYOD support and, with session persistence, enables session mobility across devices—so you get to use the same desktop from different devices. With Persona Management and optional user-installed applications support, the Mobile Secure Workplace solution provides true session persistence across devices and sessions. In addition to providing session persistence across devices, VMware Horizon View uses PCoIP protocol to deliver the best desktop user experience from any device.

**Security**

With support for end-user access via two-factor authentication (RSA SecurID, RADIUS authentication, etc.), the Mobile Secure Workplace solution emphasizes data and application security in the organization. In addition to providing the right level of access to the right resources, it also simplifies patch management and update management. Since all the desktops are in the datacenter, the Mobile Secure Workplace solution helps IT administrators update and patch the desktops to the latest version. This ensures that no vulnerabilities exist in the environment due to unpatched or orphaned systems. Also since the data resides in the datacenter, and is protected by VMware vShield™, it provides superior security for the environment.

**Management**

One of the key challenges facing organizations today is the ability to manage and get an overview of the environment, desktops, access policies, and service levels. The Mobile Secure Workplace solution, with optionally integrated VMware vCenter™ Operations Manager™, provides an integrated dashboard with intelligent response on all desktop-related events, which helps IT administrators to provide the right amount of intervention and guidance when virtual infrastructure performance looks to be exceeding an expected range of behavior. The solution can also include vCenter Configuration Manager (vCM) for importing suggested configurations and to meet regulatory compliance requirements.
User Profiles

In a typical organization, there are multiple user profiles with unique requirements. This solution architecture caters to the following five distinct user profiles.

<table>
<thead>
<tr>
<th>USER PROFILE</th>
<th>CHARACTERISTICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office-Based Information Worker</td>
<td>Workers with a broader skill set that require assimilation and manipulation of information or input from multiple sources. Examples include higher-level back-office functions, such as finance, IT, and mid-level management. These users will require a relatively broad application portfolio. They will also need some level of control over how they access applications and data, but not full administrative control. They are unlikely to be mobile, but might work from more than one fixed location. They will require multi-channel communication and collaboration capabilities for working with peers.</td>
</tr>
<tr>
<td>Content / Media Worker / Software Developer</td>
<td>Workers with a high level of expertise in an area of creativity or science that requires detailed manipulation of content. These are the traditional power users. Examples include engineers, graphic designers and some developers. They typically require a narrow, but specialized, portfolio of applications. They are unlikely to be mobile and will normally work from a single, fixed location. They will also need some level of control over how they access applications and data, but not full administrative control, and may be ring-fenced from other corporate functions. They will require high levels of computation capability and graphical display. They may also require specialist peripheral devices.</td>
</tr>
<tr>
<td>Home Office Worker</td>
<td>Workers with a broader skill set that require assimilation and manipulation of information or input from multiple sources. These workers also need to roam within a defined area or set of areas such as a campus or office, or traditionally work from home. Examples include remote workers, teachers, doctors, and higher-level managers.</td>
</tr>
<tr>
<td>Traveling Worker</td>
<td>Workers who spend at least 50 percent of their time in a non-office or non-campus location. They will typically be oriented to a single function, often customer facing. Examples include sales and service representatives. They typically require access to only a narrow portfolio of applications and only create information content in a highly structured manner. They will not require control over how they access applications or data, but will need access from almost any location within geographic boundaries. They typically tend to use laptops.</td>
</tr>
<tr>
<td>VIP</td>
<td>Business executives who will typically require access to only a small number of applications, but they will expect control over how they access these applications and corporate data. They will need to be mobile and typically tend to use tablets and laptops.</td>
</tr>
</tbody>
</table>

Table 1: Business User Profiles Considered in the Mobile Secure Workplace Architecture
These five business user profiles can be transposed to three distinct user workload profiles as listed below:

<table>
<thead>
<tr>
<th>USER PROFILE</th>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Worker</td>
<td><strong>Application Profile:</strong> MS Office, Adobe, IE, Firefox, Chrome, Outlook, SaaS applications (using JRE), Windows applications (Notepad, Calculator), multimedia players (Flash, WMP, etc.), antivirus, WebEx&lt;br&gt;<strong>Network Profile:</strong> LAN&lt;br&gt;<strong>Security Profile:</strong> Audit capability and GPO settings for UX policy; and antivirus and DLP (data loss protection – RSA and Symantec)&lt;br&gt;<strong>Other:</strong> Multi-monitor; print to nearest printer</td>
</tr>
<tr>
<td>Power User</td>
<td><strong>Application Profile:</strong> MS Office, Adobe, IE, Firefox, Chrome, Outlook, SaaS applications (using JRE), Windows applications (Notepad, Calculator), multimedia players (Flash, WMP, etc.), antivirus, WebEx, media and development environments&lt;br&gt;<strong>Network Profile:</strong> LAN and WAN&lt;br&gt;<strong>Security Profile:</strong> Two-factor authentication, audit capability and GPO settings for UX policy; data encryption and antivirus&lt;br&gt;<strong>Other:</strong> Multi-monitor; print to nearest printer</td>
</tr>
<tr>
<td>Mobile Knowledge Worker</td>
<td><strong>Application Profile:</strong> MS Office, Adobe, Outlook, IE, Firefox, Chrome, SaaS applications, Windows applications, multimedia players (Flash, QuickTime, etc.), antivirus, Webex&lt;br&gt;<strong>Network Profile:</strong> LAN and WAN&lt;br&gt;<strong>Security Profile:</strong> Two-factor authentication, audit capability and GPO settings for UX policy; data encryption and antivirus; auto disconnect upon connecting to new device&lt;br&gt;<strong>Other:</strong> Print to nearest printer</td>
</tr>
</tbody>
</table>

Table 2: User Workload Profiles

The validated design in this document supports the unique requirements of these user profiles and also helps the IT team manage the environment securely.
Mobile Secure Workplace Architecture Overview

The following diagram shows the logical topology for the Mobile Secure Workplace solution:

Figure 1: Mobile Secure Workplace Reference Architecture
The architecture consists of two virtual machine clusters, the *management cluster* and *virtual desktop cluster* for scalability purposes. In addition, the third-party software management or add-on functions including the ecosystem partner products for printing, user-installed applications, security, SIEM, system management, and antivirus, can be segmented into the third resource boundary.

The management cluster includes all the management components required for the VMware Horizon View base architecture along with vCenter Operations Manager and vShield-related VMware products. The virtual desktop cluster is dedicated to host the stateless virtual desktops, accessed by the end users. The environments are segregated to effectively utilize the underlying hardware resources, and support storage layer tiering where required.

The management architecture can host multiple connection servers, load balanced to provide redundancy and availability. Enterprise users can access the closest desktop immediately by accessing the network of load balancers using a single namespace, and remote users can access the environment using View Security Servers deployed in the demilitarized zone (DMZ). Usage of security servers enables the end users to access the desktops via PCoIP and have a better user experience.

The architecture is built based on the standard reference architectures published by VMware and is scalable.
Key Components of the Architecture

Though the architecture is vendor agnostic, below is a list of components that are part of the architecture:

**Core Components**

- **vSphere and vCenter** - The solution is built on top of vSphere, the industry-leading virtualization platform. There are many benefits to using the vSphere platform and more information on the platform can be found on the VMware Web site.

- **VMware Horizon View** - The central component of the solution architecture is VMware Horizon View, which is the industry-leading virtual desktop infrastructure (VDI) product.

- **VMware vShield** - VMware vShield provides best-in-class security to the virtual desktop environment. vShield Endpoint with the hypervisor-based Antivirus protection (from our leading AV vendors), provides tremendous benefits in terms of management and ease of use for the environment. In addition, vShield App and vShield Edge products add security to the environment. Visit the VMware Web site for more information on the vShield line of products.

- **ThinPrint** - Most of the use cases catered to by this solution have a location-aware printing requirement. ThinPrint software, OEM’d by VMware, provides the functionality of location-aware printing from many devices. More information about ThinPrint can be found on the ThinPrint Web site.

**Additional Components**

- **Management** - One of the biggest challenges faced by the IT group is on-demand management of the entire environment and an ability to proactively identify and plan the infrastructure. VMware vCenter Operations Manager for Horizon View provides the management infrastructure required for the environment.

- **Compliance** - One of the key requirements of many vertical industries is the ability to manage compliance to various industry regulations. VMware vCenter Configuration Manager helps organizations achieve their compliance requirements.

- **Persona Management and User-Installed Applications** - Many use cases defined in the solution have a requirement to persist user information across sessions. But the biggest cost savings, both in terms of CapEx and OpEx, can be achieved by using stateless desktops. To effectively achieve this, Horizon View has a feature called Persona Management to maintain user data and profile persistence across stateless sessions. In addition to the profile persistence, some use cases require support for user-installed applications. This can be achieved by using some of our partner products.

The next section of the document details the architecture as it was built for testing within the lab environment at VMware.
Solution Validation

The solution implemented in the lab was sized to scale to many thousands of desktops per the sizing guidelines provided in VMware published reference architectures. The architecture was built in pods or building blocks for easy scalability. For the functional testing aspects, the solution was implemented with 250 desktops and was deployed on the following hardware in the validation.

Lab Equipment List

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>FUNCTION / DESCRIPTION / VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>5 - 1U servers with 2 Intel Xeon E7 8837 2.67GHz processors, 96GB RAM</td>
</tr>
<tr>
<td></td>
<td>1 - 3U servers with 2 Intel Xeon E7 8837 2.67GHz processors, 128GB RAM</td>
</tr>
<tr>
<td>Hard drives</td>
<td>8 – 300GB Intel 320 SSD Drives</td>
</tr>
<tr>
<td></td>
<td>8 – 600GB 7200RPM HDD</td>
</tr>
<tr>
<td>Attached storage</td>
<td>iSCSI storage array, Raw Disk Capacity: 8TB, Raw Flash Cache 160GB, 24GB RAM, 4 – 1GbE network ports</td>
</tr>
<tr>
<td>Networking</td>
<td>Unmanaged layer 2 – 10/100 24 port switch</td>
</tr>
</tbody>
</table>

Table 3: Lab Equipment

Solution Components

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>FUNCTION / DESCRIPTION / VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere</td>
<td>5.0.1</td>
</tr>
<tr>
<td>vSphere with vCenter</td>
<td>5.0</td>
</tr>
<tr>
<td>VMware Horizon View</td>
<td>5.1</td>
</tr>
<tr>
<td>VMware Horizon View Composer</td>
<td>3.0</td>
</tr>
<tr>
<td>vShield Edge™, vShield App™, and vShield Endpoint™</td>
<td>5.0.1</td>
</tr>
<tr>
<td>SSO with RADIUS</td>
<td>Safenet Authentication Manager v6.1.7</td>
</tr>
<tr>
<td>Desktop antivirus</td>
<td>Trend Micro Deep Security</td>
</tr>
</tbody>
</table>

Table 4: Solution Components

Optional Components

<table>
<thead>
<tr>
<th>PRODUCT</th>
<th>FUNCTION / DESCRIPTION / VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Operations Manager for Horizon View</td>
<td>1.0</td>
</tr>
<tr>
<td>Load balancer</td>
<td>BigIP GTM LTM APM</td>
</tr>
<tr>
<td>Microsoft System Center</td>
<td>System Center 2012</td>
</tr>
<tr>
<td>Liquidware Lab</td>
<td>ProfileUnity</td>
</tr>
<tr>
<td>Data security</td>
<td>Verdasys</td>
</tr>
<tr>
<td>Follow Me desktop session roaming</td>
<td>HID NaviGO</td>
</tr>
</tbody>
</table>

Table 5: Optional Components
Overview of Architecture

In the Mobile Secure Workplace design it is important to separate the management and desktop components into two discrete blocks of infrastructure. In the design we created a management cluster and a Horizon View pod in order to establish a subscription- or consumption-based model. This methodology is important in order to scale the solution easily, as another pod can be plugged into the architecture as required and services can be extended to accommodate the expansion. Third-party services were also grouped together as a separate virtual appliance (vApp) entity in order to provide performance isolation.

vShield networking was configured to provide the security architecture, specifically around virtual desktop communication and application protocol flow in and out of the management, services, and desktop pool security zones.

In order to satisfy the mobility and security specifications in this design, the architecture leveraged several third-party solutions.
Datacenter

This diagram shows how each software component was deployed on each host.

![Datacenter Configuration in Three Clusters](image)

The datacenter was configured with three clusters: management, virtual desktop, and View Services (for third-party products).
A snapshot of the environment is provided below:

![Figure 3: Datacenter Environment](image)

The infrastructure components required for the environment are configured in the management cluster, and the View Services components are configured in the View Services cluster.

The management cluster includes two Active Directory virtual machines for redundancy, a vCenter server with SQL virtual machine, and a Certificate Authority for RADIUS authentication, using SafeNet Authentication Manager.

The View Services cluster includes the View Connection Server, vCenter Compliance Manager, vShield Security Manager, and View Security Servers. These form the core and optional services required for the environment, to satisfy the requirements of the five user profiles discussed earlier.

Separate resource pools were added for each one of the user profiles. The five user profiles were transposed to three technology profiles: Knowledge Worker, Power User, and Mobile Knowledge Worker. The virtual desktops for each one of the profiles will be created within these resource pools. The vShield Edge product was configured to ensure that these resource pools are segregated and cannot talk to each other.

In addition to the above clusters, for the validation, the environment included a View Planner instance to launch workloads.
Storage

For the Mobile Secure Workplace design, the typical storage configuration can be logically segregated into two clusters: management and VDI. The management cluster is in turn is segmented into general, SQL, vShield and third-party. The VDI cluster is segregated into virtual desktops and User / Corporate data segments, following the logical segregation of workloads in these datastores.

The general datastore cluster in the management segment consists of Active Directory, DNS, View Connection Manager, View Security Servers, etc. All general infrastructure components are located in this segment. Storage best practices are followed when the datastores are created (e.g., two instances of AD, VCM, and VSS are located in two separate datastores for failover protection). Follow Storage Best Practices when designing a production environment.

The SQL logical cluster contains the datastores for all SQL databases used for Composer, vCenter, etc., and the vShield cluster contains the datastores for all vShield virtual machines. In addition, a separate datastore cluster hosts all third-party software such as user-installed application support.

The VDI logical cluster contains datastores for virtual desktops and user and corporate data.

Typically, the management logical cluster can be Fibre Channel or iSCSI and the virtual desktop datastores are in SSD for faster performance. The user data and corporate data are located in NFS datastores.

The diagram below shows the storage configuration for the environment.

Figure 4: Storage Configuration
In this lab design, the management logical cluster (general, SQL, vShield and third-party virtual machine datastores) is located in iSCSI datastores. The VDI cluster (virtual desktops) is located in SSD and the user data is located in NFS datastores. For production environments, VMware recommends that IT administrators review Storage Best Practices documentation on the best storage options for various types of virtual machines.

**Networking**

For this architecture, vSphere network distributed switch technology was leveraged to simplify the configuration for Mobile Secure Workplace.

![Network Diagram](image)

**Figure 5:** Network Overview of the Environment

Standard VLANs were used to segregate vSphere management, services management, and desktop virtual machine traffic. In this configuration all uplink ports were configured as VTP trunk ports into the vSphere hosts. All networking was then broken out at the virtual distributed switch (vDS) level.
**Security**

The figure below illustrates how the vShield App Security Zones were set up for communication between the management components and the desktop pools.

vShield Edge allows us to control the application traffic flows between discrete components at a granular level. vShield Edge was used to segregate the management cluster from the desktop cluster. It can also be used to segregate pools of desktops which have stringent security requirements.

vShield App was used as a load balancer for the internal View Connection Managers, used exclusively by users inside the corporate network.

The external connections are load balanced via network load balancers.

---

**Figure 6: vDS Portgroup Layout**

**Figure 7: vShield App Security Zone Setup**
A screenshot of the vShield Edge configuration for the Management and DMZ networks is shown below:

![vShield Edge Configuration for Management and DMZ Networks](image1.png)

**Figure 8:** vShield Edge Configuration for Management and DMZ Networks

vShield Edge is also used to segregate the Management and User Profile pools. A screenshot of vShield Edge configuration for the Management and Knowledge Worker profile pool is shown below:

![vShield Edge Configuration for Management and Knowledge Worker Profile Pool](image2.png)

**Figure 9:** vShield Edge Configuration for Management and Knowledge Worker Profile Pool
vShield Edge is configured around each user profile pool to ensure that data does not cross over between user profile pools, but only between Management and User profile pools. A sample configuration for the Knowledge Worker profile pool is shown below:

![Knowledge Worker Profile Pool](image)

**Figure 10:** Knowledge Worker Profile Pool
Firewall rules were also established to restrict data movement. A snapshot of the firewall rules is shown below:

![Firewall Rules](image)

Figure 11: Firewall Rules
RADIUS Two-Factor Authentication

Horizon View supports a variety of two-factor authentication devices including RSA SecurID, RADIUS compliant One-Time Password token, contacted / contactless card, and smart cards. This architecture employed the RADIUS authentication feature in View 5.1 using a SafeNet RADIUS server to authenticate all users.

The RADIUS client was first added to the View Connection Server from the Windows Server Manager folder > Roles > NPS (Local) > RADIUS Clients and Servers > Radius Clients. A snapshot of the configuration is provided below:

![Creating New RADIUS Client](image)

Figure 12: Creating New RADIUS Client
Once the RADIUS client was added to the server, it was paired with the View Connection Server using the Horizon View administrator dashboard, by editing the Connection Server settings in the administrator console, and selecting RADIUS authentication from the 2-factor Authentication drop down menu in the Authentication tab.

![View Connection Authentication Server Settings](image)

The RADIUS server information was populated using the Create New Authenticator button. This provides enhanced authentication using OTSP.

**Single Sign-On for “Follow-Me Desktop” Experience**

One of the key features of Mobile Secure Workplace is session persistence. This enables the user to disconnect and reconnect to their desktop session from and between any device. This feature is enabled in Horizon View by default. In addition to the standard feature, this architecture also employs HID NaviGO for easier tap-in access to desktops. This feature enables the user to disconnect a desktop session from one device and reconnect to it from another device. The session state, along with the user profile information, is preserved across sessions, thereby providing true mobility across devices.
Management

The View Connection Manager shows the health of various components deployed within the infrastructure (not including the third-party products). This basic level of information can be sufficient for many organizations.

![Figure 14: View Connection Manager System Health](image-url)
For organizations that require enhanced monitoring and management, including capacity planning, the Mobile Secure Workplace solution integrates the VMware vCenter Operations Manager for Horizon View product. This product, when integrated, provides end-to-end visibility of the Horizon View environment. The patented analytics and integrated approach to performance, capacity, and configuration management deliver simplified health and performance management along with a better end-user experience, since issues can be identified and solved proactively.

In addition to the above analytics, the architecture also supports adding more third-party analytics and monitoring tools to suit any organizational needs.

**Endpoint Management**

The OS, applications, and settings on the endpoint also need to be managed. When these endpoints run an embedded version of Microsoft Windows, they can be managed in much the same way as a physical desktop. Endpoint management tools can be used to automate and simplify the task of provisioning and monitoring the desktop virtualization endpoints. Network-based services such as Dynamic Host Configuration Protocol (DHCP) and file servers can also be used to provision and update endpoints.

There are many endpoint management solutions available in the market. For this architecture, we used the System Center Configuration Manager (SCCM) to manage the Windows-based endpoints. In addition to the OS updates and patches being delivered by SCCM, the software was also used to deliver ThinApp packages to the endpoints. If the organization’s endpoints consist of a mix of Windows and other endpoints, multiple third-party software products can be used to manage them.
Persona Management

In a traditional physical desktop with local storage, all of the changes a user makes to their profile are stored on the local hard disk in their profile. In the virtual desktop world, desktops come in two flavors: dedicated desktops (also known as persistent desktops) in which users are assigned a specific desktop and use that desktop each time they log in; and floating desktops (also known as non-persistent) which provide the user any available desktop for each session. For dedicated desktops, the user’s profile is stored in the persistent data disk. But dedicated desktops are not storage efficient, increasing the total cost of ownership for the solution.

The Mobile Secure Workplace solution employs floating desktops with Persona Management enabled. This feature seamlessly preserves a user’s profile on a network share for safe keeping between sessions in either floating or dedicated desktops. Persona persists data and settings stored in the profile without specific knowledge of how a particular application works. This enables the architecture to be more storage efficient. The Persona Management feature is also efficient during login times, since it downloads only the files that Windows requires, such as user registry files. Other files are copied to the desktop when the user or an application opens them from the profile folder, thus increasing efficiency.

Printing

The location-based printing feature, enabled by ThinPrint and built into Horizon View, helps map printers that are physically close to the thin clients in an enterprise. In this architecture, location-based printing was enabled by configuring the Active Directory group policy setting AutoConnect Location-based Printing for VMware View, which is located in the Microsoft Group Policy Object Editor in the Software Settings folder under Computer Configuration. Since this policy is device specific and not user specific, the user always gets to print to the printer closest to the device. This also enables the printer to print to locally attached printers (at homes for home office employees). Detailed information on the ThinPrint GPO configuration is provided in the Appendix.

This solution does not include location-aware printing from mobile devices or laptops. There are numerous third-party software products which enable secure printing from mobile devices. More information can be found in the Secure Printing with VMware View paper.

Optional: User-Installed Applications

In any enterprise, there are some user profiles which require support for user-installed applications. This feature is in addition to the profile persistence feature offered by Persona Management. The Mobile Secure Workplace design uses the Liquidware Labs ProfileUnity FlexApp product to enable the user to install their own applications in a floating desktop, and have that application persist across sessions. The FlexApp product enables the applications to be stored separately from the Windows operating system while integrating them at logon. There are other third-party applications which also enable this function.
User Connection Flow Sequence

The diagram below illustrates the virtual desktop connection path after a user initiates the Horizon View client and logs in to the environment.

The internal network users reach the appropriate Connection Server via the load balancer, while the WAN users reach the Connection Server via the View Security Servers. After authentication using RADIUS OTSP, the user is presented user-installed applications. User-installed applications are snapped to the Virtual Desktop at the time of assignment, making the environment efficient.
Design Optimizations

Storage
This design uses the View Storage Accelerator feature to optimize the storage array configuration.

![Figure 17: View Storage Accelerator Feature Enabled](image)

This feature optimizes the environment for Reads and can significantly lower the IOPS required from the array.

Horizon View Composer
In this design, the Composer was deployed as a standalone server for scalability and failover purposes.

![Figure 18: View Composer Server Settings as Standalone](image)
Summary

The Mobile Secure Workplace design provides workload optimization for VDI mobility and security in the desktop computing environment. This architecture, built with VMware Horizon View and ecosystem partner products, was tested for the integration of various products to provide a validated end-to-end solution. This design can be used to build a Mobile Secure Workplace solution in your organization. The architecture, while tightly integrated, is also built to be modular, so customers can pick and choose the various components that fit their specific needs. The architecture is also scalable per the guidelines provided in the VMware Horizon View reference architectures.

This design caters to the three key virtual desktop requirements in any organization: Mobility, Security and Management. With BYOD support and session persistence across devices with Persona Management, this design enables true mobility for the end users in an organization.

Integration with VMware vShield Endpoint, App and Edge products allows the infrastructure boundary to be clearly identified. Virtual machines are secure from external virus threats by offloading the detection to the vShield secure virtual machine, and internal data breaches can be avoided by a virtual resource boundary segregation.

Finally, with support from vCenter Operations Manager for Horizon View, the design provides IT professionals the ability to see the infrastructure from a single integrated dashboard, managing the service levels for their organization as well as capacity planning.

The Mobile Secure Workplace design employs various third-party components to support the end-user requirements. These third-party components can be replaced with the customer’s preferred vendors. This design provides the ability to modularly replace various components, while achieving the same results described in this design.
Appendix 1

Test Cases

For this architecture, the test cases cover three key features: Mobility, Security, and Management. In addition to the test cases explained below, the VMware ecosystem of partners conducted their own testing to see how their products integrate with this solution. More information on partner testing will be found in the How-To Guides for this solution.

Below is an overview of the key test cases and their results.

Functional Test Cases

Mobility

<table>
<thead>
<tr>
<th>#</th>
<th>TEST CASE</th>
<th>DESCRIPTION</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BYOD</td>
<td>Connect to a virtual desktop via Horizon View clients in Windows laptop, Mac, thin client, iPhone, iPad, and Android device</td>
<td>Pass</td>
</tr>
<tr>
<td>2</td>
<td>User Experience</td>
<td>Access common office applications (MS Word, MS Excel, MS PowerPoint, Adobe Acrobat Reader and Windows Media Player) from thin client and mobile devices with good to great user experience</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>Session Mobility</td>
<td>Connect to a desktop session from Windows system, disconnect, and connect back to the same session using a Mac (with all the profile and user data intact)</td>
<td>Pass</td>
</tr>
</tbody>
</table>

Table 6: Mobility Test Case Summary

Security

<table>
<thead>
<tr>
<th>#</th>
<th>TEST CASE</th>
<th>DESCRIPTION</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Virus Protection</td>
<td>After AV is updated using vShield Endpoint, use EICAR file to test the AV protection</td>
<td>Pass</td>
</tr>
</tbody>
</table>
| 2 | Environment Access | Confirm that desktop access is not provided when the following are used:  
- Incorrect password  
- Incorrect OTSP passcode  
- Deactivated user name | Pass   |
| 3 | Desktop Access     | Ensure that user gets access to the correct desktop pool by testing access and the inability to access desktops in other pools | Pass   |
| 4 | Pool Security      | Ensure that desktops in one pool cannot access resources in another pool, except for the management and View Services cluster | Pass   |
| 5 | Data Protection    | Ensure data protection by:  
- Changing GPO and testing that user cannot download any data to USB  
- Changing GPO and testing that user cannot download any data to host computer | Pass   |

Table 7: Security Test Case Summary
### Management

<table>
<thead>
<tr>
<th>#</th>
<th>TEST CASE</th>
<th>DESCRIPTION</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alerts on Unauthorized Access</td>
<td>Ensure that alerts are generated for unauthorized access to the environment, desktop pools and GPO policy violation</td>
<td>Pass</td>
</tr>
<tr>
<td>2</td>
<td>Capacity Planning</td>
<td>Generate capacity planning data from vCenter Operations Manager</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>Virtual Machine Status</td>
<td>Ensure that virtual machines that missed any updates are reported in vCenter Operations Manager</td>
<td>Pass</td>
</tr>
</tbody>
</table>

Table 8: Management Test Case Summary

### Performance Validation Results

In addition to the manual functional tests, the design was tested using View Planner for workload.

The graphs below detail the results from View Planner for 64 virtual machines with a heavy workload running three iterations with un-tuned images.

![CPU Usage Test Results](image)
Figure 20: Memory Usage Test Results
Figure 21: Application Network Bit Rate Test Results
Figure 22: Datastore Byte Rate Test Results

Appendix 2
How to Set Up Location-Based Printing on a Zero Client

Step 1: Reinstall Agent
If you followed the optimization guide when you first set up your Horizon View environment you were told to disable Virtual Printing in a Zero Client environment. This was recommended because ThinPrint was not supported in a Zero Client environment and therefore CPU cycles were wasted by enabling this feature. With VMware View 4.5 and later, location-based printing is supported, so the Virtual Printer component is needed. To enable this, re-run the View Agent installer, select Modify and change the Virtual Printing setting, as seen below.

![Figure 23: VMware View Agent Installer](image)

![Figure 24: VMware View Agent Virtual Printing Setting](image)

Step 2: Install the Print Driver
The printer driver needs to be installed on the virtual machine; to do this we need to install the print driver into the OS.
Windows XP
To install a print driver on Windows XP open **Printers and Faxes**, right click anywhere in the white space and go to **Server Properties**. From there choose the **Drivers** tab and select **Add**. Follow the wizard to add the driver you need.

![Figure 25: Adding a Print Driver in Windows XP](image)

Windows 7
Server Properties is not available on Windows 7. Instead you have to install the driver by going through the **Add Printer** wizard. Select **Add a local printer**, follow the directions in the wizard, and and add the printer driver on the driver selection screen.

![Figure 26: Adding a Print Driver in Windows 7](image)

As a final step you will need to delete the printer that you just created.

**Step 3: Set Up DLL on Domain Controller**
In this step we will be registering a DLL, adding an ADM file to Group Policy, and configuring the Group Policy
itself. These files enable additional features in Group Policy that allow location-based printing to work.

Register the Location-Based Printing Group Policy DLL File
Please review Setting Up Location-Based Printing in the latest VMware Horizon View Administration Guide for complete details.

Before you can configure the group policy setting for location-based printing, you must register the DLL file TPVMGPoACmap.dll. VMware provides 32-bit and 64-bit versions of the TPVMGPoACmap.dll file on your View Connection Server.

install_directory\VMware\VMware View\Server\Extras\GroupPolicyFiles\ThinPrint

Procedure
1. Copy the appropriate version of TPVMGPoACmap.dll to your Active Directory server or to the domain computer that you use to configure group policies.
2. Use the regsvr32 utility to register the TPVMGPoACmap.dll file.
   a. For example: regsvr32 "C:\TPVMGPoACmap.dll"

Step 4: Set Up Group Policy
Enable Loopback Processing for Horizon View Desktops
Please review Add View ADM Templates to a GPO in the latest VMware Horizon View Administration Guide for complete details.

To make User Configuration settings that usually apply to a computer apply to all of the users that log in to that computer, enable loopback processing.

Prerequisites
• Create GPOs for the Horizon View component group policy settings and link them to the OU that contains your Horizon View desktops.
• Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.

Procedure
2. Right-click the OU that contains your Horizon View desktops and select Properties.
3. On the Group Policy tab, click Open to open the Group Policy Management plug-in.
4. In the right pane, right-click the GPO that you created for the group policy settings and select Edit.
   a. The Group Policy Object Editor window appears.
5. Expand the Computer Configuration folder and then expand the Administrative Templates, System, and Group Policy folders.
6. In the right pane, right-click User Group Policy loopback processing mode and select Properties.
7. On the Setting tab, select Enabled and then select a loopback processing mode from the Mode dropdown menu.
8. Click OK to save your changes.

Set Up AutoConnect Map Additional Printers
Please review Configure the Location-Based Printing Group Policy in the latest VMware Horizon View Administration Guide for complete details.
The screen shot illustrates how to set up a printer to connect to All IP Ranges, All Client Names, All Mac Addresses, and All User Groups. The Printer Name will be **TEST-NETWORK**, it will use the HP LaserJet 4 driver (which was installed in Step 2), and it will connect on the IP address of **192.168.100.5**.

![Sample Printer Setup](image)

**Figure 27: Sample Printer Setup**

**Important:** Print Driver is case sensitive (and space sensitive)—the driver name must match the driver name from the virtual machine exactly as it appears on the virtual machine. This may mean that if you have one network printer and use it from both XP and Windows 7, you may need to set up multiple mappings to the same printer.

**Troubleshooting**

Open a command prompt and go to this directory: `C:\Program Files\VMware\VMware Tools\`

From within that directory run these commands:

```plaintext
tpautoconnect.exe –d all
```

- This will delete all printers created by ThinPrint

```plaintext
tpautoconnect.exe –v –i vmware –a COM1 –F 30
```

- This command is the same command that is run by the TP process. The only difference is that instead of running the process with the quiet flag (`-q`) we want to run it in verbose mode (`-v`). This will help us see if there are any errors.

**Common Errors**

**Can’t get Client Name** - This error most likely means that the Group Policy is not taking effect.

**No suitable client protocol found.** - This error can be ignored. Following this error you should see your printer’s map.