VMware Workspace Portal 2.1 Reviewer’s Guide
Previously VMware Horizon Workspace

WHITE PAPER
Table of Contents

Introduction .............................................................. 4
  What Is Workspace Portal? .......................................... 5
  Key Features ........................................................ 6
  Architecture ....................................................... 9
  Packaging and Licensing ......................................... 11
  Proof-of-Concept Checklist ...................................... 13

Installation .......................................................... 15
  Before Installation ............................................... 15
    Minimum Requirements for the vSphere Host ............... 15
    Minimum Requirements for the Virtual Appliance .......... 15
    Requirements for Network Configuration .................. 15
    Database Storage ............................................ 16
    Ports .......................................................... 16
    Web Browser Compatibility .................................. 17
  Installation Exercises .......................................... 17
    Exercise 1: Verify That the Environment Meets the Requirements ........................................... 17
    Exercise 2: Identify DNS Records and IP Addresses .......... 18
    Exercise 3: Gather Deployment Information ................ 18
    Exercise 4: Download the Workspace Portal OVA File ........ 19
    Exercise 5: Set Up the Workspace Virtual Appliance ..... 20

Configuration ...................................................... 28
  About Configuration ............................................ 28
  Configuration Exercises ....................................... 29
    Exercise 1: Configure the Workspace Portal Virtual Appliance ........................................... 29
    Exercise 2: Explore Administrative Services .............. 39
    Exercise 3: Explore End-User Tools ....................... 43
    Exercise 4: Custom Branding ................................ 45

Integrating with Horizon with View ............................ 50
  What Is View? ................................................... 50
  View Service Exercises ....................................... 51
    Exercise 1: Review the Prerequisites ........................ 51
    Exercise 2: Gather Configuration Data .................... 52
    Exercise 3: Configure the View Service .................. 52
    Exercise 4: Configure SAML Authentication in View ....... 60
    Exercise 5: Perform Verification, Sync, and Entitlement Tasks ........................................... 65
    Exercise 6: Access RDS-Hosted Applications from Workspace Portal ....................................... 67
    Exercise 7: Launch View Desktops from Workspace Portal .................................................. 69
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing ThinApp Packages</td>
<td>71</td>
</tr>
<tr>
<td>What Is ThinApp?</td>
<td>71</td>
</tr>
<tr>
<td>Exercises for ThinApp Packages</td>
<td>72</td>
</tr>
<tr>
<td>Exercise 1: Review the Prerequisites</td>
<td>72</td>
</tr>
<tr>
<td>Exercise 2: Gather Configuration Data</td>
<td>73</td>
</tr>
<tr>
<td>Exercise 3: Configure the ThinApp Packages Service</td>
<td>73</td>
</tr>
<tr>
<td>Exercise 4: Sync a ThinApp Repository to Workspace Portal</td>
<td>77</td>
</tr>
<tr>
<td>Exercise 5: Entitle Users or Groups to ThinApp Packages</td>
<td>78</td>
</tr>
<tr>
<td>Exercise 6: Add ThinApp Packages to Workspace Portal</td>
<td>84</td>
</tr>
<tr>
<td>Exercise 7: Add ThinApp Packages to Workspace Portal</td>
<td>85</td>
</tr>
<tr>
<td>Managing Citrix Published Applications</td>
<td>87</td>
</tr>
<tr>
<td>What Is XenApp?</td>
<td>87</td>
</tr>
<tr>
<td>Exercises for Citrix Published Applications</td>
<td>88</td>
</tr>
<tr>
<td>Exercise 1: Review the Prerequisites</td>
<td>88</td>
</tr>
<tr>
<td>Exercise 2: Gather Configuration Data</td>
<td>88</td>
</tr>
<tr>
<td>Exercise 3: Configure the Citrix Published Application Service</td>
<td>89</td>
</tr>
<tr>
<td>Exercise 4: Sync Citrix XenApp to Workspace Portal</td>
<td>91</td>
</tr>
<tr>
<td>Exercise 5: See Entitlements to Citrix Published Applications</td>
<td>94</td>
</tr>
<tr>
<td>Exercise 6: Manage Categories for Citrix Published Applications</td>
<td>96</td>
</tr>
<tr>
<td>Exercise 7: Launch Citrix Published Applications from Workspace Portal</td>
<td>99</td>
</tr>
<tr>
<td>Summary</td>
<td>102</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>102</td>
</tr>
<tr>
<td>About the Authors and Contributors</td>
<td>103</td>
</tr>
</tbody>
</table>
Introduction

Welcome to the VMware® Workspace™ Portal 2.1 Reviewer’s Guide, a comprehensive technical overview of VMware Workspace Portal. Workspace Portal enables you to build a self-service app store that provides your end users with access to any application from any device. As an IT professional, you can use Workspace Portal to deliver, manage, and secure enterprise assets and support Bring Your Own Device (BYOD) initiatives from a central location.

About This Guide
This guide provides a hands-on evaluation of some of the key features of Workspace Portal. It walks you through a series of exercises, each building on the one before. When you complete the exercises, you will have a working configuration and an understanding of the key features and capabilities of Workspace Portal in the context of meaningful use cases.

The installation and configuration sections present a basic deployment of a Workspace Portal appliance. You can then use your Workspace Portal appliance to entitle users to managed multi-device access to Microsoft Windows applications and VMware Horizon® with View™ desktops. In the remaining sections, you set up additional services in Workspace Portal to provide access to Remote Desktop Services (RDS)-hosted applications, VMware ThinApp® packages, and Citrix published applications.

This guide is designed for evaluation purposes and based on minimum resources to enable you to evaluate the capabilities and concepts of Workspace Portal without a dedicated test lab. This evaluation environment should not be used as a template for deploying a production environment.

Intended Audience
This guide is intended for IT professionals who are familiar with VMware vSphere® and new to VMware Workspace Portal, as well as media reviewers of the product. Familiarity with networking concepts, such as Active Directory, identity management, directory services, and Simple Mail Transfer Protocol (SMTP), is assumed. Knowledge of other technologies, such as ThinApp, VMware Horizon with View, Citrix application virtualization, and RSA SecurID, is also helpful.

Evaluation Support
This guide is not intended to substitute for product documentation. For detailed information regarding installation, configuration, administration, and usage of VMware products, refer to the online documentation. For additional questions, consult the online VMware knowledge base. For further assistance, contact a VMware sales representative or channel partner.

The following online resources, documentation, and self-help tools are available:

• VMware vSphere and VMware vCenter™ resources
  - Product overview
  - Product documentation
  - White papers and other resources
• VMware Workspace Portal resources
  - Product overview
  - Product documentation
  - White papers and other resources
What Is Workspace Portal?

Workspace Portal is a single, self-contained virtual appliance (VA) distributed as an Open Virtualization Archive (OVA) file. Workspace Portal provides a central, integrated repository where end users can access company resources from a variety of endpoint devices. These resources can include software-as-a-service (SaaS) applications, Windows applications, View desktops, RDS-hosted applications, ThinApp packages, and Citrix published applications.

Workspace Portal benefits both end users and IT administrators. Workspace Portal provides end users with a single workspace for all applications and resources. It enables IT administrators to manage users instead of devices and to offer advanced security and protection of corporate assets.

As an IT administrator, you can use the Web-based Workspace Portal management platform to create customized sets of applications, desktops, and workspaces for end users. You can also grant entitlements or integrate policies and entitlement filters from other systems, such as View or Citrix. End users can use Workspace Portal to access work resources, including desktops, browsers, shared corporate documents, and a variety of types of applications, all customized to their individual entitlements and devices. Your end users can access their desktops and applications using any device from any location, including thin clients, zero clients, PCs, Macs, iPads, Android devices, smartphones, Amazon Kindle Fires, and Google Chromebooks. This promotes employee productivity without compromising security or IT control.

Workspace Portal provides your end users with secure access to applications and files on a variety of devices, while at the same time allowing you to deliver, manage, and secure these assets centrally. Workspace Portal supports secure, single sign-on (SSO) to applications and virtual desktops from any computer or mobile device, and it meets the challenges of today’s fluctuating BYOD environments.
Key Features

Workspace Portal provides a secure virtual workspace that end users can use to access their applications and content at any time as they move between desktops, laptops, tablets, phones, or cars. IT teams manage only what they need to manage, instead of trying to control an employee’s entire device. This capability promotes security and compliance for all devices, regardless of ownership. Workspace Portal supports cloud-identity management, federating users’ identities so that a single authentication ticket is trusted across multiple systems. Users can access cloud-based services and SaaS and Web applications using single sign-on.

Workspace Portal 2.1 delivers the following features to enhance application resource management:

Simplified On-Premises Deployment

Workspace Portal is an easy-to-deploy, turnkey virtual appliance that can be deployed on any hypervisor supporting the OVA standard, such as vCenter, VMware vCloud Director®, VMware vSphere Client™, VMware vSphere Web Client, and VMware ESXi™. Workspace Portal also allows additional virtual appliances to be added as needed for scale and failover.

Reporting and Analytics

The new Workspace Portal dashboard provides improved usability and real-time deployment feedback, including user engagement (users, groups, application utilization) and system health.

![Workspace Portal Dashboard Reports and Analytics](image)

You can monitor Workspace Portal with external monitoring tools, collect logs from all virtual machines, and generate JMX MBean notifications for changes in health status. Workspace Portal now includes a user interface for diagnostics. Users and resource analytics and system health dashboards are available from the Workspace Admin Console.
Identity Architecture Enhancements
You can integrate Workspace Authentication Broker into other products, such as Edge Gateway, to provide authentication. Supported authentication types include Active Directory user name and password, Kerberos, and RSA SecurID. This flexibility enables different directory configurations for authentication, and directory synchronization to enable connecting to complicated Active Directory environments.

Enterprise Readiness
Workspace Portal has been enhanced by significantly reducing the elapsed time for calculating the changes to entitlement status of large numbers of users and applications. Enhancements to the Active Directory sync for Horizon resources ensure that new user entitlements always match the Workspace Portal user list.

VMware Horizon DaaS
VMware Horizon DaaS® desktops and applications are integrated and can be displayed through Workspace Portal. Desktop as a service (DaaS) is ideally suited for organizations that prefer IT as a service and require maximum flexibility with known costs. Cloud providers deliver full Windows desktops or applications from their cloud to a user on any device in any location, typically as a monthly subscription. In Workspace Portal, DaaS desktops and applications are launched using PCoIP, and can be accessed using SSO from Windows, Mac OS X, iOS, and Android devices.

AirWatch Mobile Device Management and Secure Content Locker
AirWatch® by VMware expands the mobile solution of Workspace Portal and enables secure mobile access to content by providing mobile device management (MDM), mobile application management, and mobile content management. AirWatch Secure Content Locker protects sensitive content in a corporate container and provides users with a central application to securely access even the most confidential materials from their mobile devices, such as patient charts, legal briefs, product inventory, and even financial reports. End users can use SSO from Workspace Portal to sign in to AirWatch Secure Content Locker™ and to enroll their devices. The AirWatch Secure Content Locker SAML app is preconfigured in the Workspace Portal cloud application catalog.

Application Access Policies and Entitlements
As an IT administrator, you can apply access policies and define authentication strength per Web application. You can also base access to Web applications on network location and client type. During the initial setup, a global default policy is applied automatically. You can use the Web-based Workspace Portal management platform to create customized sets of applications, desktops, and workspaces for end users and groups. You can grant entitlements or integrate policies and entitlement filters from other systems such as Horizon with View or Citrix XenApp. You can augment security policies by deploying ThinApp packages on locked-down computers, and allow your end users to run their favorite applications without compromising security. You can also deploy, maintain, and update virtualized applications on USB sticks for greater portability. Workspace Portal performance improvements include faster user entitlement calculations, and easier bulk Active Directory uploads of users and groups.

Complex Active Directory Deployments
Workspace Portal now supports more flexible Active Directory configurations. You can integrate Workspace Portal with multiple Active Directory forests, and support directories that are single forest, single forest with multi-domain, or multi-forest with multi-domain:

- **Single Active Directory domain** – Workspace Portal supports single Active Directory domain, which is recommended for proof of concept.
- **Single forest with multi-domain** – Workspace Portal supports syncing users and groups from multiple domains within a single forest.
- **Multi-forest with multi-domain** – Workspace Portal supports multi-forest environments with a trust relationship to the domain, and users can store functionality if a proper trust relationship does not exist.

User stores associate an identity provider instance with users and groups in Workspace Portal. Users can choose which domain or store to log in to, and their preferences can be saved.
Centralized Application Management and Delivery
Workspace Portal provisions, distributes, and updates applications and enterprise services to employee devices in a dedicated workspace. Workspace Portal categorizes, publishes, and distributes applications into an application catalog—including Web applications, Citrix published applications, ThinApp packages, and View RDS-hosted applications—and preconfigures application preferences before distributing to employees.

Workspace Portal also enables the delivery of Windows applications that have been virtualized using ThinApp. Workspace Portal displays a user’s individual applications or View desktop on any device, without leaving a work footprint or data behind. You can also leverage legacy applications such as Windows and Web applications. End users can now reset View desktops from their Workspace User Portal.

Usability Enhancements for IT Administrators and End Users
Workspace Portal is now enhanced to make application resource management easier for both IT administrators and end users. With the HTML5-based design, everything is displayed as an application that can be accessed with a single click from desktops or devices. Usability enhancements such as move, application badging, and more have also been added to the Workspace User Portal. End users can now add their applications to Favorites, and group them in categories. The new action menu allows end users to easily reset their Horizon desktops as well as move subscribed applications to the top or bottom of the list, improving usability on mobile devices.

Support for Web Applications
Workspace Portal supports SSO to Web applications such as Outlook Web App, Microsoft Office 365, and SharePoint included in Office 365 Web applications, leveraging WS-Federation authentication. Outlook native client profile authentication is now supported, using a Workspace Portal-generated password in the Workspace User Portal.

View Hosted Application and View Desktop Delivery
Horizon with View (formerly Horizon View or VMware View) is a desktop virtualization solution that delivers virtual desktop services. View simplifies and automates the management of desktops and securely delivers desktops as a service to users. Workspace Portal delivers View virtualized desktops and RDS-hosted applications that are governed by policies and entitlements set in View. End users can now reset View desktops from their Workspace User Portal.

ThinApp Package Delivery to Windows Desktops
Workspace Portal delivers ThinApp packages with 32-bit and 64-bit applications to all Windows devices anywhere, using Windows DFS for application distribution. HTTP delivery is supported to non-domain member endpoints on Windows devices.

Citrix Published Application Delivery
Workspace Portal provides centralized identity and application access, including Citrix-based XenApp applications. From the Workspace User Portal, users can launch Citrix-based applications via XenApp 5.0 and later using single sign-on (SSO). As an IT administrator, you can entitle users and groups based on XenApp farm entitlements. Citrix Receiver must be installed on the client.
Architecture

Workspace Portal is now streamlined to a single virtual appliance and is installed on your network edge. Workspace Portal is packaged as an OVA file and can be deployed on top of any hypervisor supporting this standard, including vSphere, vSphere Client, vCenter, and ESXi. You can access the management interface from any Web browser. For the screenshots in this guide, the Workspace Portal virtual appliance was deployed with vSphere Client on vCenter.

Figure 3: The Streamlined Workspace Portal as a Single Virtual Appliance
Figure 4 shows a typical Workspace Portal deployment. This architecture leverages your current Active Directory and CIFS shares for ThinApp functionality. Note that this diagram shows an external database, as is recommended for a production environment.
Packaging and Licensing

Workspace Portal is available as a standalone product, a component of Horizon, and a key component of the VMware Workspace Suite™.

The Workspace Portal standalone product is licensed per named user, available in quantities of 10 or 100 licenses, and includes application management and ThinApp. For more information about pricing, see Purchasing Workspace Portal.

Workspace Portal is also a key component of Workspace Suite, which includes Horizon desktop virtualization, Workspace Portal, and AirWatch mobile device management. Workspace Suite is licensed per named user, for up to three personally owned or corporate-assigned devices per user, and unlimited use of desktops, laptops, thin clients, or zero clients per named user. For more information about pricing, see Purchasing Workspace Suite.

Workspace Portal is also offered as a component of Horizon in the VMware Horizon Advanced and Horizon Enterprise editions, available in two license models:

- **Per named user** – For virtual environments with staff members who need dedicated access to a virtual machine throughout the day
- **Per concurrent connection** – For virtual environments with a high number of users who share machines throughout the day, such as students and shift workers

For more information about pricing, see Purchasing Horizon with View.
Technical support on multiple levels is offered as well. For more information, see Purchasing VMware Support. The VMware Professional Services Organization is also available for consultation.

For additional information about packaging and licensing options, see

- VMware Horizon Pricing, Packaging, and Licensing
- VMware Product Evaluation
- VMware Product Guide
Proof-of-Concept Checklist

This guide introduces you to the Workspace Portal features and includes hands-on exercises to help you evaluate the product. The following checklist summarizes the exercises and provides a basic proof of concept. To explore each task in detail, see the corresponding section of the guide.

Prerequisites

- VMware vSphere Client environment
  - 2 vCPUs minimum
  - 6 GB minimum RAM
  - 36 GB minimum free disk space on datastore
  - Active Directory infrastructure
  - (Optional) Horizon with View 5.2 or later infrastructure
  - (Optional) ThinApp repository
  - (Optional) Citrix XenApp farm
- DNS configuration
  - IP addresses and DNS records
- Administrator user account in Active Directory to be used as a binding user
  - First name and last name
  - Display name
  - Email
  - Check Password never expires

Deploy Workspace Portal

- Before installation
  - Identify DNS records and DNS entries (see Exercise 2)
  - Gather installation information (see Exercise 3)
  - Download Workspace Portal OVA file (see Exercise 4)
  - In vSphere Client, select Deploy OVF Template (see Exercise 5)
- In the deployment wizard
  - Keep the name Workspace
  - Select the internal default datastore
  - Select port groups
  - Specify the time zone and IP addresses
  - After deployment, click Finish
  - Power on machine
- **CHECKPOINT:** Verify that Workspace Portal is fully powered on with no errors
Configure Workspace Portal

• Before configuration, gather configuration data (see Exercise 1)
• Use a Web browser to access Appliance Configurator at https://<WorkspaceHostname>:8443
• Click Get Started (see Exercise 2)
  - Set accounts and passwords
  - Select internal default database
  - Configure Active Directory settings
  - Configure Map User Attributes settings
  - Select users or groups
  - Click Push to Workspace to sync, and click Finish
• CHECKPOINT: Verify that a Setup is complete! message appears
• CHECKPOINT: Verify that the information is correct in the setup Summary window

Explore Workspace Portal

• Explore Workspace Portal administrative applications (see Exercise 2)
• Explore Workspace Portal end-user applications (see Exercise 3)
• Apply custom branding (see Exercise 4)

Set Up and Explore the View Service

• Configure the Horizon with View service (see Exercises 1, 2, and 3)
• Configure SAML authentication (see Exercise 4)
• Verify, sync, and entitle View pools to Workspace Portal users and groups (see Exercise 5)
• Access RDS-hosted applications from Workspace Portal (see Exercise 6)
• CHECKPOINT: Verify that you can launch View desktops from Workspace Portal (see Exercise 7)

Set Up and Explore the ThinApp Packages Service

• Configure ThinApp Packages service (see Exercises 1, 2, and 3)
• Sync ThinApp repository to Workspace Portal (see Exercise 4)
• Entitle users and groups (see Exercise 5)
• Make apps available in Workspace Portal (see Exercise 6)
• CHECKPOINT: Verify that you can launch ThinApp packages from Workspace Portal (see Exercise 7)

Set Up and Explore the Citrix Published Applications Service

• Configure Citrix Published Applications service (see Exercises 1, 2, and 3)
• Sync XenApp data (see Exercise 4)
• Verify entitlements to Citrix-based apps (see Exercise 5)
• Manage application categories (see Exercise 6)
• CHECKPOINT: Verify that you can launch XenApp published applications from Workspace Portal (see Exercise 7)
Installation

This section describes the prerequisites and recommended minimum requirements. Corresponding hands-on exercises are provided to walk you through the basic installation of a Workspace Portal instance. For more information, see the VMware Workspace Portal documentation.

Before Installation

Before you begin installation, make sure that your environment meets the minimum requirements for a Workspace Portal proof-of-concept deployment.

Minimum Requirements for the vSphere Host

VMware vSphere is a cloud operating system that manages large collections of infrastructure elements such as the CPU, storage, network, and data center. The vSphere Client is a Windows application that you can use to configure the host and to operate its virtual machines. VMware vCenter, another component of the vSphere suite, provides centralized management of virtual machines and ESXi hosts. You can also use an ESXi virtualization hypervisor for your Workspace Portal deployment. For additional Workspace Portal deployment options, see Installing and Configuring VMware Workspace Portal.

VMware Workspace Portal 2.1 supports the following versions of vCenter and ESXi:

<table>
<thead>
<tr>
<th>HOST</th>
<th>VERSION COMPATIBILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter</td>
<td>5.0 U3, 5.1 U2, 5.5</td>
</tr>
<tr>
<td>ESXi</td>
<td>5.0 U3, 5.1 U2, 5.5</td>
</tr>
</tbody>
</table>

Table 1: Recommended Minimum Requirements

For more information about the supported versions, see VMware Product Interoperability Matrixes.

Minimum Requirements for the Virtual Appliance

The following table summarizes the minimum supported hardware requirements for the Workspace Portal virtual appliance (`workspace-va`).

<table>
<thead>
<tr>
<th>COMPONENT (workspace-va)</th>
<th>MINIMUM vCPU</th>
<th>MINIMUM RAM</th>
<th>MINIMUM DISK SPACE</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Workspace Portal</td>
<td>2 vCPU</td>
<td>6 GB</td>
<td>36 GB</td>
</tr>
</tbody>
</table>

Table 2: Recommended Minimum Requirements for the Virtual Appliance

Requirements for Network Configuration

Workspace Portal connects to your existing Active Directory infrastructure, so you can sync users and groups for user authentication and management. Your Active Directory must be accessible in the same LAN as your Workspace virtual appliance. The Workspace Portal server must join the Windows domain if View or ThinApp services are enabled. The Workspace Portal host name must be in the same domain as the Active Directory domain it is joining.

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>MINIMUM REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS record and IP address</td>
<td>IP address and DNS record</td>
</tr>
<tr>
<td>Firewall port</td>
<td>Inbound firewall port 443 must be open for users outside the enterprise network to Workspace Portal</td>
</tr>
</tbody>
</table>

Table 3: Recommended Requirements for Network Configuration
Database Storage
An internal PostgreSQL database is included in the workspace-va for proof-of-concept testing. Note that for production, you must use an external database server (see the VMware Product Interoperability Matrixes for more details). You can convert and scale an internal PostgreSQL database to an external database at a later time. External database sizing includes 64 GB for the first 100,000 users and 20 GB for each additional 10,000 users.

You can use the internal PostgreSQL database for storage while testing the proof of concept. This supports a Workspace Portal deployment of no more than 1,000 users. For production, you must install and configure an external database server. For more information, see Installing and Configuring VMware Workspace Portal.

Ports
The ports you need for Workspace Portal depend on the deployment scenario. For the exercises in this guide, Workspace Portal connects to Active Directory in order to sync users and groups, and to connect to a ThinApp repository. The Workspace host name must be in the same domain as the Active Directory domain it is joining.

<table>
<thead>
<tr>
<th>PORT</th>
<th>SOURCE</th>
<th>TARGET</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Browsers</td>
<td>workspace-va</td>
<td>HTTPS</td>
</tr>
<tr>
<td>8443</td>
<td>Browsers</td>
<td>workspace-va</td>
<td>Administrator port</td>
</tr>
<tr>
<td>443</td>
<td>workspace-va</td>
<td>workspace-va</td>
<td>HTTPS</td>
</tr>
<tr>
<td>25</td>
<td>workspace-va</td>
<td>SMTP</td>
<td>TCP port to relay outbound mail</td>
</tr>
<tr>
<td>389, 636, 3268, 3269</td>
<td>workspace-va</td>
<td>Active Directory</td>
<td>Default values; ports are configurable</td>
</tr>
<tr>
<td>5432</td>
<td>workspace-va</td>
<td>Database</td>
<td>Default value for the PostgreSQL database</td>
</tr>
<tr>
<td>389, 443</td>
<td>workspace-va</td>
<td>View server</td>
<td>Access to View server</td>
</tr>
<tr>
<td>443</td>
<td>workspace-va</td>
<td>ThinApp repository</td>
<td>Access to ThinApp repository</td>
</tr>
<tr>
<td>5500</td>
<td>workspace-va</td>
<td>RSA SecureID system</td>
<td>Default value; port is configurable</td>
</tr>
<tr>
<td>53</td>
<td>workspace-va</td>
<td>DNS server</td>
<td>TCP/UDP Each workspace-va must have access to the DNS server on port 53, and allow incoming SSH traffic on port 22</td>
</tr>
<tr>
<td>88, 135, 465</td>
<td>workspace-va</td>
<td>Domain controller</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>TCP: 9300-9400 UDP: 54328</td>
<td>workspace-va</td>
<td>workspace-va</td>
<td>Audit needs</td>
</tr>
</tbody>
</table>

Table 4: Recommended Requirements for Ports
Web Browser Compatibility
The Workspace Portal Admin Console is a Web-based application that is included when you install Workspace Portal. The following table summarizes the supported Web browsers you can use to access and use the Workspace Portal interfaces:

<table>
<thead>
<tr>
<th>WEB BROWSER</th>
<th>OPERATING SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 10 and 11</td>
<td>Windows</td>
</tr>
<tr>
<td>Google Chrome 34.0 or later</td>
<td>Windows and Mac OS X</td>
</tr>
<tr>
<td>Mozilla Firefox 28 or later</td>
<td>Windows and Mac OS X</td>
</tr>
<tr>
<td>Safari 6.1.3 and later</td>
<td>Mac OS X</td>
</tr>
</tbody>
</table>

Table 5: Supported Web Browsers

Note: You cannot launch Citrix-based applications in Internet Explorer 8. You must use a later version of Internet Explorer.

For more information about minimum requirements, see Installing and Configuring VMware Workspace Portal. For more information about the compatibility of current and previous versions of VMware products and components, see the VMware Product Interoperability Matrixes.

Installation Exercises
The following hands-on exercises help you evaluate the process of preparing your environment and installing your Workspace Portal instance. The exercises are sequential and build upon one another, so make sure to complete each exercise in this section before going to the next. Before you install Workspace Portal, verify that your environment meets the recommended requirements, identify or set up IP addresses and DNS records, and gather the network information you need for the Workspace Set Up wizard.

- Exercise 1: Verify that the environment meets the requirements
- Exercise 2: Identify DNS records and IP addresses
- Exercise 3: Gather deployment information
- Exercise 4: Download the Workspace Portal OVA file
- Exercise 5: Set up the Workspace virtual appliance

Note: This proof-of-concept demonstration was deployed using vSphere Client on vCenter 5.1. The screenshots for the exercises were taken on a Mac running Windows 7 with VMware Fusion® 6.

Exercise 1: Verify That the Environment Meets the Requirements
Before deploying Workspace Portal, verify that your environment meets the recommended minimum requirements. Review the requirements described in Before Installation, and verify that the resources you have allocated to your Workspace virtual appliance meet the minimum requirements for the following:

- **VMware vSphere host** – Use vSphere, vCenter, or ESXi.
- **Workspace Portal** – Use the recommended requirements for the exercises in this guide.
- **Network configuration** – Make sure that inbound firewall port 443 is open for users outside the enterprise network to Workspace Portal.
- **Database storage** – Use the internal default PostgreSQL database for testing the proof of concept only. For production, install an external database server.
- **Ports** – Reserve the recommended ports for the exercises in this guide.
- **Web browser compatibility** – Use the recommended Web browsers for the exercises in this guide.

After verifying that your environment meets the requirements for deployment, proceed to the next exercise to identify or set up IP addresses and DNS records.
Exercise 2: Identify DNS Records and IP Addresses

Now that you have verified that minimum requirements for deployment are met, identify or create DNS entries for the Workspace. Workspace Portal requires a DNS entry and a static IP address. Forward DNS entries are required, and reverse DNS entries are optional. A-records are DNS address records that point domain and host names to static IP addresses. PTR records are pointer records that map an IPv4 address to the canonical name on the host. Because every organization administers its IP addresses and DNS records differently, ask your network administrator for a DNS record and IP address before you begin installation.

Reverse lookup is optional. If you are implementing reverse lookup, define a PTR record on the DNS server to ensure that the virtual appliance uses the correct network configuration.

You can use the DNS records in the following table by replacing the sample entries with your own data.

<table>
<thead>
<tr>
<th>A-RECORD HOST NAME</th>
<th>A-RECORD ADDRESS</th>
<th>PTR RECORD HOST NAME</th>
<th>PTR RECORD ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>my-workspace-va.company.com</td>
<td>10.114.196.70</td>
<td>PTR my-workspace-va.company.com</td>
<td>70.196.114.10.in-addr-arpa</td>
</tr>
<tr>
<td>my-connector-va.company.com</td>
<td>10.114.196.71</td>
<td>PTR my-connector-va.company.com</td>
<td>71.196.114.10.in-addr-arpa</td>
</tr>
</tbody>
</table>

Table 6: Examples of Forward and Reverse DNS Records and IP Addresses

Note: DNS host names that are over 15 characters or contain underscores might cause failures when syncing ThinApp packages. If this happens, make sure that the Workspace virtual appliance short host name meets these criteria.

When the DNS configuration is complete, it is recommended that you verify that the reverse DNS lookup is properly configured. For example, the virtual appliance command `host IP_address` should resolve to the DNS name lookup.

Exercise 3: Gather Deployment Information

After identifying or creating DNS records and IP addresses, use the following deployment information checklist to gather the network information you need when installing Workspace Portal.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>YOUR NETWORK INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workspace fully qualified domain name (FQDN)</td>
<td></td>
</tr>
<tr>
<td>WORKSPACE NETWORK INFORMATION</td>
<td></td>
</tr>
<tr>
<td>• IP address of the virtual appliance</td>
<td></td>
</tr>
<tr>
<td>• DNS server name</td>
<td></td>
</tr>
<tr>
<td>• Default gateway address</td>
<td></td>
</tr>
<tr>
<td>• Netmask or prefix</td>
<td></td>
</tr>
<tr>
<td>AD DOMAIN CONTROLLER</td>
<td></td>
</tr>
<tr>
<td>• Active Directory server name</td>
<td></td>
</tr>
<tr>
<td>• Active Directory domain name</td>
<td></td>
</tr>
<tr>
<td>• Bind DN user name and password</td>
<td></td>
</tr>
<tr>
<td>• Base DN</td>
<td></td>
</tr>
<tr>
<td>• Active Directory user name and password with privileges to join computers to the domain</td>
<td></td>
</tr>
<tr>
<td>OPTIONAL SSL CERTIFICATE</td>
<td></td>
</tr>
<tr>
<td>• SSL certificate</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> You can also add the SSL certificate after deployment.</td>
<td></td>
</tr>
<tr>
<td>• Private key</td>
<td></td>
</tr>
</tbody>
</table>
ITEM | YOUR NETWORK INFORMATION
--- | ---
WORKSPACE LICENSE KEY | • Workspace license key
  **Note:** The license key is entered in the Workspace administration console in the **Settings > Global Settings** tab after installation is complete.

ADMINISTRATION PASSWORD | • Workspace administrator account password
• Virtual appliance root account password
• SSH user account password for remote login

---

Table 7: Deployment Information Checklist

After you gather the information you need to install the Workspace VA, proceed to the next exercise to download the OVA files.

**Exercise 4: Download the Workspace Portal OVA File**

Now that you have prepared the environment and gathered the DNS records and other network information that you need, you are ready to download the Workspace Portal package files.

Download the [Workspace Portal OVA package](#) file from the VMware Web site under Desktop and End-User Computing.

**Note:** Approximately 2 GB of disk space are required on the target machine when you download.

After you successfully download the Workspace Portal OVA package file, proceed to the next exercise to prepare for deployment by setting up DNS entries for Workspace Portal.
Exercise 5: Set Up the Workspace Virtual Appliance

Now that you have the downloaded OVA file, you are ready to deploy it. You can start this exercise at any time after downloading. **Note:** In the Workspace Portal user interface, the OVF Template and the OVA file are equivalent.

To set up the Workspace Portal virtual appliance:

1. In vSphere Client, click **File > Deploy OVF template.**

   ![Figure 6: Begin Deploying the Workspace Portal OVA Package](image)

2. On the Source page, browse to the location or type the specific URL of the OVA package that you downloaded earlier, and then click **Next.**

   ![Figure 7: Indicate Location of the OVA Package in the Deploy OVF Template Wizard](image)
3. On the OVF Template Details page, verify the data, and then click **Next**.

![Figure 8: Verify Template Details](image)

4. On the End User License Agreement page, read the agreement, click **Accept**, and then click **Next**.

![Figure 9: Accept End User License Agreement](image)
5. On the Name and Location page, type a unique, case-sensitive name to identify this Workspace Portal virtual machine, select the location for the template, and then click **Next**.

![Set Name and Location of Workspace Portal Deployment](image1.png)

**Figure 10:** Set Name and Location of Workspace Portal Deployment

6. On the Host / Cluster page, select the host or cluster to run the deployed template, and then click **Next**.

![Indicate the Host or Cluster](image2.png)

**Figure 11:** Indicate the Host or Cluster
7. On the Resource Pool page, select the resource pool in which to deploy the template, and then click Next.

Figure 12: Set Resource Pool Where Workspace Portal Will Be Deployed

8. On the Storage page, select the location to store the virtual machine files, and then click Next.

Figure 13: Set Storage Location
9. On the Disk Format page, select the Thin Provision disk format in which to store the Workspace Portal files for evaluating the proof of concept, and then click **Next**.

![Set Disk Format](image1.png)

**Figure 14: Set Disk Format**

10. On the Network Mapping page, map the networks that Workspace Portal should use to networks in your inventory, and then click **Next**.

![Set Network Mapping](image2.png)

**Figure 15: Set Network Mapping**
11. On the Properties page, customize the settings for your deployment, and then click **Next**.

![Set Application and Networking Properties](image)

Figure 16: Set Application and Networking Properties

- **Connector Only Install** – To perform a basic installation, leave the check box deselected.
- **Timezone setting** – Select the correct time zone.
- **Customer Experience Improvement Program** – By default, this option is enabled to assist VMware to improve the quality of this product by automatically sending anonymous data statistics about version and component usage patterns. You can disable this option by deselecting the check box.
d. **Networking Properties** - To configure a static IP address, enter the address for the following items. If you do not enter an address, Dynamic Host Configuration Protocol (DHCP) is used.

- **Host Name** – Host name for this virtual machine (underscores and special characters are not supported)
- **Default Gateway** – Default gateway address for this virtual machine
- **DNS** – Domain name servers for this virtual machine, comma-separated

**Note:** Do not use UTF-8 characters when creating the domain name because they cause problems when logging in through non-ASCII user stores.

- **IP Address** – IP address for the interface
- **Netmask** – Netmask or prefix for the interface

12. On the Ready to Complete page, verify the settings, and then click **Finish**. This can take a few minutes to complete. 

![Verify Deployment Settings](image-url)
13. In vSphere Client, right-click the Workspace Portal virtual appliance that you just deployed, and select **Power On** to start the virtual appliance.

![Power On the Virtual Appliance](image18)

Figure 18: Power On the Virtual Appliance

14. Wait until the virtual appliance is completely powered on. This can take a few minutes. When the virtual appliance initialization is complete, the blue Welcome window appears.

![Welcome to the Workspace Portal Appliance](image19)

Figure 19: Welcome to the Workspace Portal Appliance

After successfully deploying the Workspace Portal OVA package, proceed to the next chapter to configure the virtual appliance using the Appliance Configurator.
Configuration

Now that you have downloaded and deployed Workspace Portal, you are ready to start initial configuration. This section describes the key elements of the configuration procedure for Workspace Portal, identifies the data required, and provides hands-on exercises that walk you through the initial configuration process using the Appliance Configurator.

About Configuration

When the virtual appliance initialization is complete, the blue Welcome window appears. The Welcome window contains two URLs to applications on the Workspace Portal virtual appliance.

![Welcome window](image)

**Figure 20:** Click the First URL to Launch the Application Configurator

Click URL#1 to launch the Application Configurator, where you can complete first-time setup. At any time after the first click, URL#1 launches the Workspace Admin Console where you can use Workspace Portal. URL#2 works only after you complete the initial configuration exercises. These links are described more fully in Explore Administrative Tools.
Configuration Exercises

Now that you are familiar with the configuration process, you are ready to begin the initial configuration of Workspace Portal. This section provides hands-on exercises to walk you through the initial configuration process of your deployment, to explore the tools and applications in more detail, and to apply customized branding to your Workspace Portal instance. The configuration exercises are sequential and build upon one another, so make sure to complete each exercise in this section before going to the next.

- Exercise 1: Configure the Workspace Portal virtual appliance
- Exercise 2: Explore administrative tools
- Exercise 3: Explore end-user tools
- Exercise 4: Apply customized branding

Exercise 1: Configure the Workspace Portal Virtual Appliance

With the networking data that you gathered using the Configuration Information Worksheet, you are ready to begin the configuration process.

To configure the Workspace Portal virtual appliance:

1. Click the first URL in the Welcome window to start the Workspace Setup wizard (https://<WorkspaceHostname>).
2. On the Get Started page of the Appliance Configurator, you can preview the process, and then click **Continue**.

![Get Started](image)

*Figure 22: Get Started*
3. On the Set Passwords page, type the passwords for the appliance administrator account, appliance root account, and remote user account, and then click **Continue**.

   **Note:** If the password confirmation does not match the password, a red X appears.

![Set Passwords](image-url)
4. On the Select Database page, select **Internal Database**.

   **Note:** The internal database is provided for proof-of-concept testing only. An external database is recommended for production and for migration from earlier versions of Workspace Portal. You can transfer from an internal database to an external database at any time. For more information about database considerations, see *Installing and Configuring Workspace Portal*.

   ![Select Database](image)

   **Note:** If you are using the internal default database, the process is instantaneous. If you are using an external database, it takes a few minutes to set up tables, schemas, and so on.
5. On the Configure Directory page, type the directory information, and then click **Continue**.

![Configure Directory](image)

**Figure 25: Configure Directory**

- **Directory Type** – For this proof-of-concept exercise, select **Active Directory** from the drop-down menu.
- **Use SSL** – For this proof-of-concept exercise, leave this field blank.
- **Use DNS Service Location** – For this proof-of-concept exercise, leave this field blank.
- **Server Host** – Type the server address, such as 123.45.54.321, or ad.mycorp.com.
- **Server Port** – Type the server port number.
- **Search Attribute** – Select the account attribute that contains the user name from the drop-down menu.
- **Base DN** – Type the DN from which to start account searches.
- **Bind DN** – Type the DN of the account that can search for users.
- **Bind Password** – Type the password for the account that can search for users.
6. On the Map User Attributes page, select the attributes from the drop-down menus, and then click Continue.

- **Email** – Select from the drop-down menu.
- **FirstName** – Select from the drop-down menu.
- **LastName** – Select from the drop-down menu.
- **UserName** – Select from the drop-down menu.
- **Phone** – Select from the drop-down menu.
- **Disabled** – Select from the drop-down menu.
- **UserPrincipalName** – Select from the drop-down menu. This is used in connection with the View exercises.

**Note:** When you set an attribute as required, users without the attribute are removed from VMware Workspace the next time Directory Sync executes.

- **Domain** – Select from the drop-down menu.
- **DistinguishedName** – Select from the drop-down menu.
7. On the Select Users page, you can accept the defaults that filter Active Directory users from syncing to Workspace Portal. Select user attributes and search conditions from the drop-down lists and enter the filter values in the text box.

Figure 27: Select Users

- **Enable Directory Sync** – Select the check box.
- **Enter the DN for Users** – Provide the user and administrative user domain names.
- **Apply Filters to Exclude Users** – Leave blank.
8. On the Select Groups page, use the **Available Groups** text box to search for the Active Directory Groups to add to Workspace Portal, and then click **Add**. When you are finished selecting groups, click **Continue**.

   **Note:** This information is required later for the **View exercises**, but you can do it any time after Workspace Portal is set up.

![Select Groups](image-url)
9. On the Push to Workspace Portal page, click **Push to Workspace**.

![Figure 29: Push to Workspace Portal](image)

10. Wait until the synchronization is complete. This might take a few minutes.

![Figure 30: Push to Workspace Portal](image)
11. On the Setup Review page, click **Finish** to start the Workspace Admin Console.

![Setup Review](image1)

**Figure 31: Setup Review**

When the first-time setup is complete, the Workspace Admin Console dashboard appears.

![Workspace Admin Console Dashboard](image2)

**Figure 32: VMware Workspace Portal Dashboard**

You have now successfully completed the first-time setup. Proceed to the next exercise to explore the administrative applications and services included in Workspace Portal for IT administrators.
Exercise 2: Explore Administrative Services

After completing the first-time setup, you are now ready to explore the services and applications that Workspace Portal provides for IT administrators, starting with the VMware Workspace Portal Administrative Services Links.

The Services Links page contains shortcuts to the three administrative Web applications that Workspace Portal provides for IT administrators. Bookmark this page so that you can return to it easily (https://<workspaceHostname>:8443):

- Appliance Configurator
- Workspace Admin Console
- Connector Services Admin
Appliance Configurator

The Appliance Configurator is one of the administrative Web applications in Workspace Portal. You use the Appliance Configurator to manage the database, update certificates, enable Syslog, change the administrative password, and manage various other infrastructure functions. Sign in as the WorkspacePortal administrator with the password that you set during first-time setup. You can access Appliance Configurator from the Workspace Admin Console on the Settings tab by clicking the VA Configuration tab, and then the Manage Configuration button. For more details, see Installing and Configuring Workspace Portal.

1. From the Services Links page (https://<workspaceHostname>:8443), click Appliance Configurator.

2. In the Sign In window, type the administrator password that you set up during configuration.
3. The first time you visited the Appliance Configurator, the Welcome to Workspace Setup window was displayed (Figure 21 in Exercise 1). Any time you launch the Appliance Configurator subsequently, the navigation menu is displayed.

![Figure 35: Appliance Configurator Navigation Bar Opens to Database Connection Setup](image)

At any time after initial setup, you can revisit the Appliance Configurator to modify the setup. In the exercises that follow, you use the other two Web applications—Workspace Admin Console and Connector Services Admin—to evaluate Workspace Portal.

**Workspace Admin Console**

The Workspace Admin Console is one of the administrative Web applications in Workspace Portal. You use the Workspace Admin Console to set up the resource catalog and administer users and groups, entitlements, and reports.

1. Navigate to the Workspace Admin Console by selecting one of the following options:
   - From the Services Links page (https://<workspaceHostname>:8443), click Workspace Admin Console.
   - From your Web browser, go to https://<workspaceHostname>/admin.
2. In the Sign In window, type your Active Directory administrator user name and password to log in to Workspace Portal.

![Figure 36: Workspace Portal Sign-in Window](image)
3. Review the Workspace Admin Console dashboard to verify that the system is functioning as expected.

![Workspace Admin Console Dashboard](image)

In the exercises that follow, you use the Workspace Admin Console to set up the resource catalog of applications and desktops, and administer your users, groups, and entitlements.

**Connector Services Admin**

The Connector Services Admin is one of the administrative Web applications in Workspace Portal. You use the Connector Services Admin to configure the directory, set up authentication brokers, and administer other enterprise integrations, such as virtual desktops and remote applications. Integrations include ThinApp, View and Application pools, and Citrix-published resources. You can also check directory sync status and alerts.

1. Navigate to the Connector Services Admin by selecting one of the following options:
   - From the Services Links page (https://<workspaceHostname>:8443), click **Connector Services Admin**.
   - From your Web browser, go to https://<workspaceHostname>:8443/hc/admin.

2. In the Login window, type the password you set during configuration to verify that your access to the Connector Services Admin is functioning.

![Connector Services Admin Login Window](image)
3. Review the About window.

![Figure 39: Connector Services Admin About Window](image)

In the exercises in the following chapters, you use the Connector Services Admin to set up integrations to View, to a ThinApp repository, and to a Citrix XenApp farm.

After you have explored the three main applications for IT administrators, proceed to the next exercise to explore the user interfaces that Workspace Portal provides for your end users.

**Exercise 3: Explore End-User Tools**

Now that you are familiar with the administrative applications for IT administrators, you are ready to explore the Workspace User Portal (also called App Portal). The Workspace User Portal contains the two interfaces that Workspace Portal provides for end users: My Apps and App Center.

Sign in to the Workspace User Portal using your Active Directory user name and password. Workspace Portal opens by default to the My Apps window. From My Apps, you can go to App Center to display all applications and desktops that you are entitled to access as an end user. You can also return to your IT administrator status in the Admin Console by clicking the **Administration Console** link in the drop-down menu in the upper right.

![Figure 40: The Users’ App Portal Includes App Center and My Apps](image)
The Workspace App Portal includes the following applications for end users:

- **My Apps**
- **App Center**

### Workspace My Apps

My Apps provides users with the ability to manage the applications to which they are entitled, and to access those applications without reentering their login credentials. Users can drag and drop the application icons on their My Apps page to rearrange them. When users remove applications from their My Apps page, the applications remain available in the App Center.

Sign in with your Active Directory user name and password, which launches the Workspace My Apps window. My Apps displays all applications and desktops that you are entitled to access as an end user. From here you can move, organize, and favorite the applications and desktops entitled to you. You can also return to the Admin Console by clicking the **Administration Console** link in the drop-down menu in the upper right.

### Workspace App Center

Sign in with your Active Directory user name and password, which launches the Workspace User Portal (also called App Portal). The application opens by default to the My Apps window. Click **App Center**, which displays all applications and desktops that you are entitled to access as an end user. End users can group apps in their Workspace Web app portal by marking applications as favorites and by filtering applications by category.

App Center provides users with self-service category filtering, which shows the latest applications added. The App Center is designed to scale to thousands of desktop and Web applications. End users can now add their applications to Favorites, and group them in categories. The new action menu allows end users to easily reset their Horizon desktops, as well as to move subscribed applications to the top or bottom of the list, which is ideal on mobile devices.

After you have completed the configuration and setup of Workspace Portal, and explored the tools and applications included in Workspace Portal for both IT administrators and end users, you can proceed to the next exercise to explore the expanded custom branding options. The latest release enables you to configure custom branding for desktops, browsers, and mobile devices.
Exercise 4: Custom Branding

You can apply enterprise branding to customize company icons, logos, fonts, background, and title for your application. The customized branding is then displayed in the Sign-In, User Portal, and Administration Console windows, in Web browser page titles, and as background colors and text fonts.

To customize the User Portal window to display company branding:

1. Log in to the Workspace admin console (https://<workspaceHostname>/admin), and click Settings > Custom Branding.

   ![Custom Branding](image)

   Figure 41: Applying Custom Branding

2. Customize the brand name and logo as follows:
   
   a. **Logo** – Click **Upload**, and upload your company logo as a JPEG, PNG, or GIF file to appear on the Sign In, User Portal, and Administration Console windows.
   
   b. **Favicon** – Click **Upload**, and upload a JPEG, PNG, GIF, or ICO file to appear in the Web browser page title.
   
   c. **Company Name** – Type the company name to appear in the Web browser page title.
   
   d. **Product Name** – Type the product name to appear in the Web browser page title.
3. Customize the sign-in screen and verify the results.

![Customizing the Sign-In Screen](image)

- **Background Color** – Type the hexadecimal color code, and verify the result in the preview.
- **Masthead color** – Type the hexadecimal color code, and verify the result in the preview.
- **Background Highlight** – Choose whether to enable the background highlight.
- **Background Pattern** – Choose whether to enable the background pattern.
- **Masthead Pattern** – Choose whether to enable the masthead pattern.
- **Image (Optional)** – Upload an image as a JPEG, PNG, or GIF file up to 1400 x 900 pixels.
- **Logo** – Upload your company logo as a JPEG, PNG, or GIF file up to 350 x 100 pixels.
- Check the results in the preview to verify your changes.
4. Customize your users’ view of Workspace Portal on the Web, and verify the results in the My Apps and App Name previews.

![Portal (Web view)](image)

**Figure 43: Customizing the Portal Web View**

- **Background Color** – Type the hexadecimal color code, and verify the result in the preview.
- **Name and icon Color** – Type the hexadecimal color code, and verify the result in the preview.
- **Lettering effect** – Click the arrow and select a lettering effect from the drop-down menu.
- **Background Highlight** – Choose whether to enable the background highlight.
- **Background Pattern** – Choose whether to enable the background pattern.
- **Image (Optional)** – Upload an image as a JPEG, PNG, or GIF file up to 1400 x 900 pixels.
- **g. Verify the results in the My Apps and App Name previews.**
5. Customize your users’ view of Workspace Portal on tablets and mobile devices, and verify the results in the tablet and mobile device previews.

![Portal (Mobile and Tablet views)](image)

**Figure 44: Customizing the Portal Mobile and Tablet Views**

- **a. Background Color** – Type the hexadecimal color code, and verify the result in the preview.
- **b. Title bar color** – Type the hexadecimal color code, and verify the result in the preview.
- **c. Title color** – Type the hexadecimal color code, and verify the result in the preview.
- **d. Name color** – Type the hexadecimal color code, and verify the result in the preview.
- **e. Lettering effect** – Select a lettering effect from the drop-down menu.
- **f. Title Bar pattern** – Choose whether to enable the background pattern.
- **g.** Choose whether to use the same values for both the Launcher and the Catalog.
- **h.** Verify the results in the tablet and mobile device previews.
6. Choose whether to enable the first-time user tour.

![First-Time User Tour](image)

Figure 45: Enabling the First-Time User Tour

7. Customize user portal bookmarks on your end users’ mobile devices.

![Customizing Mobile Device Options](image)

Figure 46: Customizing Mobile Device Options

a. **Web Clip Icon** – Click **Upload**, and upload an icon as a JPEG or PNG file up to 512 x 512 pixels.

b. **Web Clip Title** – Type a new short title of fewer than 20 characters.

8. Click **Save**.

9. Verify that your changes appear the next time you log in or launch Workspace Portal.

When you have verified that the setup was successful and the customized branding appears as it should, configuration is complete and your Workspace Portal appliance is set up. You can now use your Workspace Portal appliance to entitle your users to managed multi-device access to your company applications, including Windows applications, software-as-a-service (SaaS) applications, and View desktops. By configuring additional services, you can also use Workspace Portal to provide your end users with access to RDS-hosted applications, ThinApp packages, and Citrix published applications. You can explore these Workspace Portal services in any order:

- **View service**
- **ThinApp Packages service**
- **Citrix Published Applications service**
Integrating with Horizon with View

After you successfully install and configure Workspace Portal, you can use the various Workspace Portal services to perform specialized tasks. You can enable and configure each service either during setup or at a later time. You can explore the services in this guide in any order. This section describes how to configure the View service. The ThinApp and Citrix XenApp services are described in Manage ThinApp Packages and Manage Citrix Published Applications.

Configuring the View service integrates Workspace Portal with an existing deployment of Horizon with View, allowing you to sync information about your available View pools and entitlements from the View Connection Server to Workspace Portal. Your end users can then launch their View desktops and RDS-hosted applications from Workspace Portal. To configure the View service, you must join the Active Directory domain, sync the View Connection Server with it, and enable SAML authentication.

What Is View?

View is a component of VMware Horizon that delivers virtualized and remote desktops and applications through a single platform and supports end users with access to Windows and online resources. When configured as an integrated service of Workspace Portal, View provides end users with access through a single, unified workspace.

With View, IT departments can run remote desktops and applications in the data center and deliver these desktops and applications to employees as a managed service. End users gain a familiar, personalized environment that they can access from multiple devices anywhere throughout the enterprise or from home. Administrators gain centralized control, efficiency, and security by having desktop data in the data center. For more information, see the Horizon with View product page.
View Service Exercises

These hands-on exercises help you evaluate the benefits of integrating an existing View deployment with Workspace Portal. The exercises are sequential and build upon one another, so make sure to complete each exercise before going on to the next.

This section includes the following exercises:

- Exercise 1: Review the prerequisites
- Exercise 2: Gather configuration data
- Exercise 3: Configure the View service
- Exercise 4: Configure SAML authentication in View
- Exercise 5: Perform verification, sync, and entitlement
- Exercise 6: Access RDS-hosted applications from Workspace Portal
- Exercise 7: Launch View desktops from Workspace Portal

Exercise 1: Review the Prerequisites

To integrate Workspace with View, the environment where you are deploying Workspace Portal must meet the following criteria:

- VMware Workspace Portal deployed and configured
- VMware Horizon with View
  - Version 6.0 supports both View desktops and RDS-hosted applications
  - Version 5.2 supports only View desktops
- View pools, desktops, and RDS-hosted applications
- View entitlements set for Active Directory users and groups
- DNS entry and an IP address that uses reverse lookup available for each View Connection Server in your View setup (Workspace Portal requires reverse lookup for View Connection Servers, View Security servers, and load balancers)

**Important:** Unlike the optional reverse lookup for Workspace Portal, reverse lookup for View Connection Server is required. If reverse lookup is not properly configured, the Workspace Portal integration with View fails.

- Active Directory users and groups synchronized with View pool entitlements to Workspace Portal

See Installing and Configuring Workspace Portal for more details.

After you review the minimum requirements needed for configuration, proceed to the next exercise to gather the data needed to configure the View service.
Exercise 2: Gather Configuration Data
Now that you have verified that you have the minimum configuration requirements, you can gather the required data listed in the following Configuration Data Worksheet.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>YOUR CONFIGURATION DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory fully qualified domain name (FQDN)</td>
<td></td>
</tr>
<tr>
<td>Active Directory user account with privileges to join computers to the domain</td>
<td></td>
</tr>
<tr>
<td>Initial View Connection Server FQDN</td>
<td></td>
</tr>
<tr>
<td>FQDN for client access (load balancer address)</td>
<td></td>
</tr>
<tr>
<td>Active Directory user account with read privileges in View Administrator</td>
<td></td>
</tr>
</tbody>
</table>

Table 8: Configuration Data Worksheet for the View Service

When you finish gathering the data required for configuration, proceed to the next exercise to configure the View service.

Exercise 3: Configure the View Service
Now that you have the data you need for configuration, you can start setting up the View service.

To configure the View service in Workspace Portal:
2. Log in using administrator credentials.
3. On the Join Domain page, provide the data that you gathered during Exercise 2: Gather Configuration Data, and then click Join Domain.

Figure 48: Typing Domain Information into the Join Domain Wizard
4. On the Join Domain page, verify that the message **Values have been saved** appears in the upper left.

![Figure 49: Domain Successfully Joined](image)

5. In the left navigation bar, click **Map User Attributes**, select the **Required** check box next to **userPrincipalName** to enable it, and then click **Save**.

![Figure 50: Mapping User Attributes](image)
6. In the left navigation bar, click **View Pools**, type the Connection Server data, make sure that the **Perform Directory Sync** check box is selected, and then click **Save**.

![Figure 51: Enabling and Configuring View Desktops](image)
7. In the Last Sync box in the lower right, click **Sync Now** to sync Workspace and the Active Directory configuration from View.
8. On the Select Users page, accept the defaults, and then click **Continue**.

Figure 53: Accepting Selected Users
9. On the Select Groups page, accept the defaults, and then click **Continue**.

![Figure 54: Accepting Selected Groups](image-url)
10. On the Push to Workspace page, verify the scheduled changes, and then click **Push to Workspace**.

![Figure 55: Pushing to Workspace](image)

11. On the View Pools page, verify the scheduled changes, and then click **Save and Continue**.

![Figure 56: Saving and Continuing](image)

**Note:** From now on before syncing, verify that the values for **View Client Access URL** and **View Client Access Port** on the View Pools page are compatible with those on the Edit Network Range page. To open the Edit Network Range page, click **Workspace Settings > Network Ranges > Edit**. Verify that a compatible external client access URL for the View service is available.
12. The View Pools page is displayed, indicating that Workspace Portal has the View Connection Server certificate.

![Figure 57: Verifying the View SSL Certificate](image)

When you have successfully configured the View service, proceed to the next exercise to enable and configure SAML authentication.
Exercise 4: Configure SAML Authentication in View

Now that you have successfully configured the View service, you can configure SAML authentication in View.

To configure SAML authentication:

1. Log in to your View Administrator with an administrative user account.
2. In the left navigation bar, select View Configuration > Servers.

3. Select the first Connection Server that you configured in Exercise 3: Configure the View Service, and then click Edit.
4. In the Authentication tab, select **Allowed** from the drop-down menu, and then click **Manage Authenticators** to add Workspace Portal as an SAML authenticator.

Figure 60: Click Manage Authenticators

5. In the Manage Authenticators dialog box, click **Add**, and then click **OK**.

Figure 61: Add Authenticators
6. In the Add SAML 2.0 Authenticator dialog box, configure the new authenticator with an appropriate label, description, and the URL for your Workspace Portal, and then click **OK**.

![Configure New Authenticator](image)

**Figure 62: Configure New Authenticator**

7. If you are using a self-signed SSL certificate, you are prompted to verify the certificate by clicking **View Certificate**.

![Verify Server Certificate](image)

**Figure 63: Verify Server Certificate**
8. Review the information, and then click **Accept**.

![Certificate Information](image)

**Figure 64: Certificate Information**
9. Return to the Workspace Portal wizard to confirm that all certificates are valid, and click **Save** to complete the configuration.

   **Note:** If you selected manual synchronization, click **Sync Now** on the View Pools page to sync the View pools to Workspace Portal.

10. Repeat this procedure for every View Connection Server instance in the replica group.

    For more information, see the **Enable a SAML 2.0 Authenticator** section of Integrating VMware Workspace Portal and VMware Horizon View.

    When all View Connection Servers in your replica group are set up, proceed to the next exercise to verify that the View pools and entitlements display properly in Workspace Portal.
Exercise 5: Perform Verification, Sync, and Entitlement Tasks

Now that you have successfully completed the setup for all View Connection Servers in the replica group, you are ready to verify that the View pools and entitlements display properly in Workspace Portal.

To verify, sync, and grant entitlements:

2. Log in using administrator credentials.
3. Verify that the dashboard has updated to include the View pool information.

4. On the Catalog tab, click the down arrow next to Any Application Type, select View Desktop Pools, and then under Application, select a desktop pool.
5. Verify that the View pools are listed in the interface. Then log out and log back in as a user entitled to use the View desktop.

![Figure 68: View Pool Entitlements Window](image)

6. Verify that you can see the desktop entitlements, and then launch a connection to a desktop from the VMware Workspace Portal Web interface. You can launch the desktop either through the locally installed View Client, or through your browser.

![Figure 69: Workspace Portal Web Interface](image)

When you have finished verifying that View pools and entitlements display properly in Workspace Portal, proceed to the next exercise to access a View-hosted application from Workspace Portal.
Exercise 6: Access RDS-Hosted Applications from Workspace Portal

After the Workspace Portal and View integration is set up, your entitled users can access the available RDS-hosted applications in their Workspace Portal catalog. Hosting applications on RDS servers is a new feature of View, and does not require any additional configuration. View is set up with hosted applications, and the integration enables Workspace Portal to display them.

**Note:** VMware Horizon Client™ must be installed on every desktop. See Installing and Configuring Workspace Portal for details.

To launch RDS-hosted applications from the Workspace Portal catalog:

1. Log in to Workspace Portal as a user, and click the **App Center** button in the upper right.

   ![Figure 70: Logging in to Workspace Portal as a User](image)

2. In the App Center, select a hosted application, and click **Add App**.

   **Note:** Horizon Client must be installed on every desktop.

   ![Figure 71: Adding a Hosted Application to My Apps](image)
3. Click the **My Apps** button in the upper right, and then click the hosted application to launch it from Workspace Portal.

![Figure 72: Launching a Hosted Application from Workspace Portal](image)

When you have successfully accessed a hosted application from Workspace Portal, proceed to the next exercise to access a View desktop from Workspace Portal.
Exercise 7: Launch View Desktops from Workspace Portal

Now that the Workspace Portal and View integration is set up, your entitled users can access the available View desktops in their Workspace Portal catalog. As long as the View integration is set up, Workspace Portal can display desktops from View.

Note: Horizon Client must be installed on every desktop. See Installing and Configuring Workspace Portal for details.

To launch View desktops from the Workspace Portal catalog:

1. Log in to Workspace Portal as a user, and click the App Center button in the upper right.

![Figure 73: Logging in to Workspace Portal as a User](image1)

2. In the left pane of the App Center, click Desktop, select a View desktop, and click Add App.

   Note: The Horizon Client must be installed on every desktop.

![Figure 74: Adding a View Desktop to My Apps](image2)
3. Click the **My Apps** button in the upper right, and then click the hosted application to launch it from Workspace Portal.

![Launching a View Desktop from Workspace Portal](image)

*Figure 75: Launching a View Desktop from Workspace Portal*

Now that you have set up and explored the View service supported by Workspace Portal, you can explore the other Workspace Portal services in any order:

- ThinApp packages service
- Citrix published applications service
Managing ThinApp Packages

After you successfully install and configure Workspace Portal, you can use the various Workspace Portal services to perform specialized tasks. You can enable and configure each service during setup or at a later time. You can explore the services described in this guide in any order.

This section provides a set of exercises to walk you through the process of setting up the ThinApp Packages service in your Workspace Portal instance. The ThinApp Packages service streamlines application management by providing access to ThinApp packages from a Windows network share. As an administrator, you can load the ThinApp packages using the Workspace Connector Services Admin, and entitle users and groups to each package using the Workspace Administration Console. This enables your end users to launch these applications using their Workspace Portal.

If you have a repository of ThinApp packages that is compatible with and meets the requirements of Workspace Portal, you can use the exercises in this section to explore this optional service.

What Is ThinApp?

ThinApp is an application virtualization tool that is included in Workspace Portal, and is also available standalone. ThinApp can package conventional Windows applications to make them more portable.

ThinApp virtualizes applications by decoupling them from their underlying operating systems, and encapsulating the application files and registry into a single ThinApp package. You can then deploy and manage the package independently from its underlying operating system. The virtualized application continues to behave the same across different configurations.

You can use ThinApp to simplify the migration of legacy Windows applications such as applications based on Internet Explorer 6 to Windows 7 systems. You can augment security policies by deploying ThinApp packages on locked-down computers, and allow your end users to run their favorite applications without compromising security. You can also deploy, maintain, and update virtualized applications on USB sticks for greater portability.
Exercises for ThinApp Packages

This section provides hands-on exercises to help you evaluate the key features of using ThinApp functionality with Workspace Portal. To add ThinApp packages to your Workspace Portal catalog, you must have a ThinApp repository already set up and ready to integrate with Workspace Portal before proceeding with the ThinApp exercises. The exercises within this section are sequential and build upon one another, so ensure that you complete each exercise before going to the next.

This section includes the following exercises:

- **Exercise 1: Review the prerequisites**
- **Exercise 2: Gather configuration data**
- **Exercise 3: Configure the ThinApp Packages service**
- **Exercise 4: Sync the ThinApp repository to Workspace Portal**
- **Exercise 5: Entitle users or groups to ThinApp packages**
- **Exercise 6: Add ThinApp packages to Workspace Portal**
- **Exercise 7: Launch ThinApp packages from Workspace Portal**

**Exercise 1: Review the Prerequisites**

To use Workspace Portal to manage your ThinApp packages, you need a ThinApp repository that contains your ThinApp packages. You point your Workspace Portal to that repository and sync the packages. When this is done, the ThinApp packages become available in the Workspace Portal catalog, and you can then entitle them to your end users and groups.

After integrating your Workspace Portal system with your ThinApp repository (see [Installing and Configuring Workspace Portal](#)), you can view the ThinApp packages from the repository in your catalog, and manage them using Workspace Portal. You can entitle users and groups, and configure license-tracking information for each ThinApp package. See the [Workspace Portal Administrator’s Guide](#) and [VMware ThinApp](#) for more details.

Verify that the following prerequisites are in place before starting the exercises in this section:

- **ThinApp repository** – Verify that you have a repository of ThinApp packages on a network share.
- **Key information** – Gather the following information:
  - Uniform Naming Convention (UNC) path to the network share folder
  - Active Directory domain name
  - Credentials of an administrative account with rights to join the domain
- **Windows devices** – ThinApp packages can run only on Windows endpoints and View desktops.
- **Workspace for Windows** – Verify that Workspace for Windows is installed on each Windows endpoint so that your users can launch ThinApp packages from those devices (see [VMware Workspace Portal User Guide](#) for more information).
- **Enabled ThinApp packages** – Ensure that each ThinApp package is enabled for Workspace Portal (formerly called Horizon Application Manager) when packaged (see [Manage with VMware Horizon Application Manager](#) in the ThinApp User’s Guide or [Using VMware Horizon Application Manager to Manage Deployment and Entitlement of ThinApp Packages](#) for more information).

See [Installing and Configuring VMware Workspace Portal](#) for more details.

After you review the prerequisites, proceed to the next exercise to gather the data needed to configure the ThinApp Packages service.
Exercise 2: Gather Configuration Data

Now that you have verified that you have the prerequisites, you can gather the required data listed in the following Configuration Data Worksheet.

Gather the following information so that it is available as you complete the exercises in this section:

<table>
<thead>
<tr>
<th>ITEM</th>
<th>YOUR CONFIGURATION DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory domain</td>
<td></td>
</tr>
<tr>
<td>Active Directory user name of an administrative account with rights to join the domain</td>
<td></td>
</tr>
<tr>
<td>Active Directory password of an administrative account with rights to join the domain</td>
<td></td>
</tr>
<tr>
<td>User name for a user account that has read access to the network share</td>
<td></td>
</tr>
<tr>
<td>Password associated with the network share account</td>
<td></td>
</tr>
<tr>
<td>Uniform Naming Convention (UNC) path to the network share folder</td>
<td></td>
</tr>
</tbody>
</table>

Table 9: Configuration Data Worksheet for the ThinApp Packages Service

When you finish gathering the data, proceed to the next exercise to configure the ThinApp Packages service.

Exercise 3: Configure the ThinApp Packages Service

After you verify that your environment meets the prerequisites, you can enable Workspace Portal to locate your ThinApp packages.

To join your Workspace Connector instance to an Active Directory domain:

2. In the left navigation pane, select **Join Domain**.

Figure 78: Connector Join Domain

3. On the Join Domain page, type the information for the Active Directory domain, and click **Join Domain**.
   a. **AD Domain** – Type the fully qualified domain name of the Active Directory, such as HS.TRIDOT.COM.
   b. **AD Username** – Type the username of an account in the Active Directory which has permissions to join systems to that domain.
   c. **AD Password** – Type the password associated with the AD Username.
   d. The Join Domain page displays a message indicating that you have now joined the domain.
4. Enable Workspace Portal to access the stored ThinApp packages:

![Image of VMware Workspace Portal](image.png)

**Figure 79:** Connector – Packaged Apps – ThinApp

- In the left navigation pane, select **Packaged Apps – ThinApp**.
- In the upper right, select the **Enable packaged applications** check box.
- Provide the following information:
  1. **AD Password** – Type the Active Directory password.
  2. **Path** – Type the path to the shared ThinApp repository folder in UNC path format, such as `\server\share\subfolder`.
  3. **Choose Frequency** – Select the time interval at which you want the Connector to sync the data. For a weekly interval, set the day and time of day. For a daily interval, set the time.
  4. **Enable account based access** – Select the check box if you want to use account-based access.
  5. **Share User** – Type the user name for a user account that has read access to the network share.
  6. **Share Password** – Type the password associated with the Share User account.
vii. Verify that the information is correct, and then click Save.
A message confirms that the values have been saved and indicates the last sync status.

![Image of the ThinApp saved screen]

**Figure 80:** Connector Packaged Apps – ThinApp Saved

After you have enabled the ThinApp Packages service, proceed to sync the Workspace Portal service with your ThinApp repository.
Exercise 4: Sync a ThinApp Repository to Workspace Portal
Now that you have configured the ThinApp Packages service, you are ready to synchronize the ThinApp information with Workspace Portal.

To sync your ThinApp repository with Workspace Portal:

1. In the Advanced tab of Workspace Connector Services Admin under Packaged Apps – ThinApp, verify the information in all required fields, update any if necessary, and then click Save.

2. When you are satisfied that all information is accurate, click Sync Now to sync the ThinApp packages with Workspace Portal.
3. Wait until the sync completes. This can take several minutes.

When the synchronization is complete, proceed to the next exercise to grant the entitlements to ThinApp packages.

**Exercise 5: Entitle Users or Groups to ThinApp Packages**

Now that your Workspace Portal configuration is complete, you can entitle users and groups to access Windows applications that have been captured as ThinApp packages. Note that all users must have Workspace for Windows installed on their Windows systems to run the ThinApp packages to which they are entitled. Entitled users can view and launch applications from Workspace Portal on their own systems. If you remove the entitlement, the user can no longer see an application. You can grant entitlements in two ways: by entitling one or more users to a specific ThinApp package, or by adding one or more entitlements to a specific user or group.

- Grant entitlements to specific ThinApp packages
- Grant entitlements to specific users or groups
Grant Entitlements to Specific ThinApp Packages
This exercise starts by describing how to entitle users or groups to a specific ThinApp package. Note that you can also grant ThinApp package entitlements to a specific user or group.


![Admin Console Sign-In](image)

Figure 84: Admin Console Sign-In

2. In the Admin Console, click the Catalog tab.

3. In the Any Application Type drop-down menu, select ThinApp Packages, and then click the specific ThinApp package to entitle users to.

![Searching the Catalog for ThinApp Packages](image)

Figure 85: Searching the Catalog for ThinApp Packages
4. In the left pane under Application Info, click **Entitlements**, and then click **Add group entitlement** or **Add user entitlement**.

![Modify application](image)

**Figure 86:** Add Group or Individual Entitlements

5. Select the check box of all groups or users that you want to entitle.

![Add Group Entitlement](image)

**Figure 87:** Indicate Who Gets Entitled
6. From the drop-down menu, select the Deployment Type, and then click **Save**.

![Figure 88: Indicate Type of Deployment](image)

- **Automatic** – Users or groups can access the ThinApp package the next time they log in to the Workspace Portal.
- **User-Activated** – Users or groups activate the ThinApp package in their Workspace Portal.

You have now entitled users or groups to a specific ThinApp package. Next, see how to add entitlements to a specific user or group.

**Grant Entitlements to Specific Users or Groups**

This exercise describes how to grant ThinApp package entitlements to specific users or groups. Note that you can also grant users or groups entitlements to a specific ThinApp package.

1. In the Workspace Admin Console, in the **Users & Groups** tab, click either **Users** or **Groups**.

![Figure 89: Selecting Groups](image)
2. Click the name of the specific user or group to entitle, and then click **Add entitlement**.

![Add Entitlement to Selected Group](image1)

**Figure 90:** Add Entitlement to Selected Group

3. In the Application Type drop-down menu, select **ThinApp Packages**.

![Select ThinApps for Application Type](image2)

**Figure 91:** Select ThinApps for Application Type

4. Select the ThinApp packages that you want to make available to this user or group.
5. From the drop-down menu, select the Deployment method and then click **Save**:

![Add entitlements for a group](image-url)

**Figure 92: Indicate Type of Deployment**

- **Automatic** – Users have immediate access to the ThinApp package the next time they log in to Workspace Portal.
- **User-Activated** – Users activate the ThinApp package in Workspace Portal to use the virtualized application.

After entitling the users and groups to use the identified ThinApp packages, proceed to the next exercise to see how you can make new ThinApp packages available in the Workspace Portal catalog.
Exercise 6: Add ThinApp Packages to Workspace Portal

When the ThinApp Packages service is enabled and your Workspace Portal deployment is integrated with ThinApp, you can make new ThinApp packages available in the catalog by adding them to the ThinApp repository that is integrated with your Workspace Portal, and then synchronizing the two systems.

To make new ThinApp packages available in your Workspace Portal catalog:


![Connector Services Admin Login](image)

2. In the ThinApp repository, create a subfolder for each new ThinApp package using ASCII characters.

3. Copy the files for each ThinApp package, such as EXE and DAT files, to the subfolder.

4. Sync Workspace Portal with the ThinApp repository by choosing one of the following options:
   - Wait for the next scheduled sync.
   - Manually sync using the ThinApp Packages page of the Connector Web interface.

See the VMware Workspace Portal Administrator’s Guide for more details.

After making new ThinApp packages available, proceed to the next exercise to verify that the ThinApp packages are visible from Workspace Portal.
Exercise 7: Launch ThinApp Packages from Workspace Portal

Now that the Workspace Portal and ThinApp integration and ThinApp package entitlements are complete, your entitled users can access the available ThinApp packages in their Workspace Portal catalog.

**Note:** The Workspace for Windows application must be installed on every Windows endpoint. See [Installing and Configuring Workspace Portal](#) for details.

To launch ThinApp packages from the Workspace Portal catalog:

1. Log in to Workspace Portal as a user, and click the **App Center** button in the upper right.

![Figure 94: Logging in to Workspace Portal as a User](image)

2. Verify that the ThinApp packages you synced in Exercise 6 are displayed in the App Center, select one ThinApp package, and then click **Add App**.

   **Note:** The Workspace for Windows application must be installed on the Windows endpoint.

![Figure 95: Adding a ThinApp Package to My Apps](image)
3. Click the **My Apps** button in the upper right, and then click the ThinApp package to launch it from Workspace Portal.

![Launching a ThinApp Package from Workspace Portal](image)

Figure 96: Launching a ThinApp Package from Workspace Portal

Now that you have set up and explored the ThinApp service supported by Workspace Portal, you can explore the other Workspace Portal services in any order:

- **View service**
- **Citrix published applications service**
Managing Citrix Published Applications

After you successfully install and configure Workspace Portal, you can use the various Workspace Portal services to perform specialized tasks. You can enable and configure each service during setup or at a later time. You can explore the services in this guide in any order.

When the Citrix Published Application service is enabled, access to Citrix published applications is enabled. This section describes how you can use this service to streamline management of Citrix published applications, and provides a set of exercises to walk you through the process.

What Is XenApp?

Citrix XenApp is a virtualization product that is hosted on groups of servers called XenApp farms. Integration enables your end users to launch XenApp published applications from within Workspace Portal using their well-known Active Directory user name and password. End users can access entitled applications (SaaS, ThinApp, RDS-hosted applications, and Citrix published applications), along with files and desktops, through the Workspace Admin Console.

Integration enables you to leverage existing hardware and software and still gain the productivity advantages of Workspace Portal. XenApp entitlement permissions are still managed through XenApp farms, and there is no VMware code on the XenApp server or receiver. Moreover, there is no dependency on load balancers.
Exercises for Citrix Published Applications

This section provides hands-on exercises to help you evaluate the benefits of adding Citrix published applications to your Workspace Portal catalog. You must have a XenApp farm already set up and ready to integrate with Workspace Portal before proceeding with the exercises. The exercises within this section are sequential and build upon one another, so make sure to complete each exercise before going to the next.

This section includes the following exercises:

• Exercise 1: Review the prerequisites
• Exercise 2: Gather configuration data
• Exercise 3: Configure the Citrix Published Application service
• Exercise 4: Sync Citrix XenApp to Workspace Portal
• Exercise 5: See entitlements to Citrix published applications
• Exercise 6: Manage categories for Citrix published applications
• Exercise 7: Launch Citrix published applications from Workspace Portal

Exercise 1: Review the Prerequisites

Verify that the following prerequisites are in place before starting the exercises in this section:

• Workspace Integration Broker – Verify that the Workspace Integration Broker is installed and configured (See Installing and Configuring Workspace Portal for more details).
• Citrix XenApp farm – Verify that a Citrix XenApp deployment is set up with XenApp published applications.
• Citrix Receiver – Verify that a platform-appropriate Citrix Receiver is installed on each endpoint device so that your users can launch Citrix published applications from those devices.

After reviewing the prerequisites, proceed to the next exercise to gather configuration data.

Exercise 2: Gather Configuration Data

Now that you have verified that your environment meets the prerequisites for the exercises in this chapter, you are ready to gather the configuration data, to have ready for the exercises that follow.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>YOUR CONFIGURATION DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN of the Integration Broker to sync with</td>
<td></td>
</tr>
<tr>
<td>Server port</td>
<td></td>
</tr>
<tr>
<td>Version of XenApp server farm</td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td></td>
</tr>
<tr>
<td>Transport type of your Citrix server configuration</td>
<td></td>
</tr>
<tr>
<td>Port used by your Citrix server configuration</td>
<td></td>
</tr>
</tbody>
</table>

Table 10: Configuration Data Worksheet for the Citrix Published Applications Service

After gathering your configuration data, proceed to the next exercise to enable and configure the Citrix Published Applications service.
Exercise 3: Configure the Citrix Published Application Service

Now that you have gathered the configuration data you need, you are ready to configure the Citrix Published Application service. You can use this service to view all Citrix published applications and entitlements from your catalog in Workspace Portal. You can entitle users and groups only through your XenApp system, and then view those entitlements through Workspace Portal.

To set up the Citrix Published Application service:

2. On the Advanced tab, click Published Apps – Citrix.
   
   **Note:** All of the specifications in this exercise are typed into this Published Apps – Citrix page.
3. In the upper left, select the Enable Citrix-based Applications check box.

4. In the Sync Integration Broker fields, type the following information:
   - **Sync Integration Broker** – Type the fully qualified domain name of the Integration Broker to sync with.
   - **Server Port** – Type the port number for the Integration Broker to sync with.
   - **SSL** – For the purposes of this proof-of-concept exercise, leave the SSL check box deselected.
5. Scroll down, and in the SSO Integration Broker fields, choose one of the following options:

- Click the **Use same as Sync Integration Broker** button.
- Type the fully qualified domain name of the Integration Broker and server port number to get the SSO token.

6. Scroll down, and in the Server Farms fields, type the following information:

- **Version** – Select the version from the drop-down menu.
- **Server name** – You can leave this blank.
- **Servers** – You can edit or reorder servers.
- **Transport type** – Select the same transport type used in your Citrix server configuration.
- **Port** – Make sure to type the same port number that is used in your Citrix server configuration.
7. In the remaining fields, provide the information as follows:

![Figure 102: Server](image)

- **Deployment Type** – Select the type of deployment to use for entitling your Citrix published applications from the drop-down menu.
- **Sync categories from server farms** – Select the check box to enable.
- **Choose Frequency** – Select the frequency to sync from the drop-down menu.

8. Confirm that the information you provided is accurate, and then click **Save**.

After enabling and configuring the Citrix Published Application service, proceed to sync the Workspace Portal service with your existing Citrix XenApp repository.

**Exercise 4: Sync Citrix XenApp to Workspace Portal**

Now that you have set up the Citrix Published Application service, you are ready to synchronize Workspace Portal with Citrix XenApp. Although you can see your Citrix published applications from the Workspace Connector Services Admin, you cannot make changes to the Citrix published applications from the Workspace Portal service. When changes are made on the Citrix side, such as adding a new server farm or entitling new users to an application, you must sync XenApp with Workspace Portal to transfer the new information.

To sync your Citrix deployment with Workspace Portal:

2. On the Advanced tab, click **Published Apps – Citrix**.

![Figure 104: Navigating to Sync in Workspace Connector Services Admin](image)

3. Verify the information, update if necessary, and then click **Save**.

![Figure 105: Verifying, Updating If Necessary, and Saving](image)
4. When you are satisfied that all information is accurate, click **Sync Now** to sync Citrix with Workspace Portal.

![Figure 106: Syncing Now](image)

5. Wait until the sync completes. This can take several minutes.

![Figure 107: Waiting for Sync to Complete](image)

After verifying that Workspace Portal is synchronized with your existing Citrix XenApp repository, proceed to the next exercise to inspect the entitlements to Citrix published applications.
Exercise 5: See Entitlements to Citrix Published Applications

Now that you have verified that your Workspace Portal is synced to your Citrix XenApp repository, you are ready to examine Citrix entitlements. You can view all Citrix published applications and entitlements in your Workspace Portal resource catalog, but you cannot make changes. You can entitle users and groups only through your Citrix XenApp system.

To view user and group entitlements to Citrix published applications:


2. See which users and groups are entitled to a specific Citrix published application:
   a. Click the Catalog tab.
   b. Click Any Application Type > Citrix Published Applications.
   c. Click a specific application.
   d. In the Entitlements tab, see lists of group and user entitlements in separate rows.
3. See which Citrix published applications have been entitled to a specific user or group:
   a. Click the **Users & Groups** tab.
   b. Click either **Users** or **Groups**.
   c. Click the name of the specific user or group.
   d. In the **Entitlements** tab, see entitled Citrix published applications in the Citrix Published Applications table.

After verifying that your Citrix published applications and entitlements are visible in the Workspace Admin Console, proceed to the next exercise to create Workspace Portal categories for the Citrix published applications.
Exercise 6: Manage Categories for Citrix Published Applications

Now that you have verified that Citrix published applications are displayed in your Workspace Admin Console, you can create application categories. Categories are filters to help you search for applications. If you have a large number of applications, you can organize them by category, and then search by both application type and by category. You can apply multiple categories to an application. You can apply categories to any type of application, not just Citrix published applications.

When you sync, any categories created in your Citrix deployment appear in Workspace Portal, but not the reverse. Categories created in Workspace Portal never appear in your Citrix deployment. If you edit a category in your Citrix deployment, the new name is displayed in Workspace Portal the next time you sync. However, the original category name also persists in Workspace Portal, and can be edited or manually deleted.

To create new categories:


2. In the Workspace Admin Console, click the Catalog tab.

3. Click the name of an application, and then click Details on the left.
4. In the **Categories** text box on the right, type the new category to add. In the following screenshot, the new category is Graphics Apps.

![Figure 114: Adding New Application Category](image1)

5. Click the **Catalog** tab again to return to the list of applications. Notice that the new Graphics Apps category has now been applied to the Paint application.

![Figure 115: Returning to Catalog Search Field](image2)
6. Click the down arrow beside Any Category, and select the new category from the drop-down menu.

![Figure 116: Searching by Category](image)

7. Verify that Workspace Portal displays only applications that are categorized as Graphics Apps.

![Figure 117: Verifying the Category Filter](image)

After creating new categories for your Citrix published applications, proceed to the next exercise to view the Citrix published applications from the user perspective.
Exercise 7: Launch Citrix Published Applications from Workspace Portal
Now that you have explored some of the options available through the enabled Workspace Portal Citrix Published Application service, your users can access the Citrix published applications from their client devices. In this exercise, you log in as a user to verify the user experience.

Note: To access Citrix published applications from Workspace Portal, the Citrix Receiver must be installed on the endpoint device.

Figure 118: Verifying that Citrix Receiver is Installed Before Launching

To access Citrix published applications from Workspace Portal:
1. Log in to Workspace Portal as a user, and click the App Center button in the upper right.
2. In the App Center, select a Citrix published application, and click Add App.
   
   Note: The Citrix Receiver must be installed on your endpoint device.

Figure 120: Adding a Citrix Published Application to My Apps

3. Click the My Apps button in the upper right.
4. In My Apps, click the icon of any Citrix published application to verify that it is published from XenApp.

Figure 121: Inspecting a Citrix Published Application from Workspace Portal
5. Click the published application to launch it from Workspace Portal.

Now that you have set up and explored the Citrix Published Applications service supported by Workspace Portal, you reached the end of the review exercises. You can explore the VMware Workspace Portal Documentation to find out how to set up a more complex production environment, or review the services covered in the reviewers guide in any order:

- View service
- ThinApp Packages service
- Citrix Published Applications service
Summary

The topics covered in this guide include the key features and benefits of using VMware Workspace Portal for secure, single sign-on to applications and virtual desktops from any endpoint device and any location. The guide provides an overview of Workspace Portal functionality, architecture, and components. Exercises are provided to walk you through the basic installation and deployment process, including initial configuration. Three main services—integration with external products including View, ThinApp, and Citrix XenApp—are described and exercises provided to help you explore and evaluate the benefits of Workspace Portal functionality.

The topics presented in this document provide enough information to set up and operate a basic Workspace Portal deployment. For access to product download sites and additional documentation of more complex deployments, see the Additional Resources section of this document. For comprehensive information about all Workspace Portal options, see VMware Workspace Portal Documentation.

Additional Resources

For more information about VMware Workspace Portal, review the following resources:

- VMware Workspace Portal Documentation
- Workspace Portal OVA package file download
- VMware Knowledge Base
- VMware Product Interoperability Matrixes
- Installing and Configuring Workspace Portal
- Workspace Portal features
- Workspace Portal product page
- Workspace Portal Product Evaluation Center
- VMware Product Guide
- Horizon product page
- VMware Horizon with View Documentation
- VMware Horizon Pricing, Packaging, and Licensing
- Workspace Portal Support Center
- VMware Professional Services Organization
About the Authors and Contributors

This version of the Reviewer’s Guide was updated by Cindy Heyer, Technical Writer, End-User Computing, VMware.

With special thanks for the contributions of

• Karen Zelenko, Staff Program Manager, Cloud R&D, End-User Computing, VMware
• Balaine Wightman, Staff Engineer, Cloud R&D, End-User Computing, VMware
• Ravi Chayanam, Sr. Manager, R&D, Cloud R&D, End-User Computing, VMware
• Kevin Strohmeyer, Sr. Director, Product Marketing, Workspace Portal Services, End-User Computing, VMware
• Debbie Rishel, Senior Web Marketing Manager, Web Marketing, End-User Computing, VMware
• Rory Clements, Group Manager, Solution Management, End-User Computing, VMware
• Candace Harrison, Staff Technical Writer, Tech Pubs, VMware

The Reviewer’s Guide was originally written by

• Rory Clements, Group Manager, Solution Management, End-User Computing, VMware
• Muthu Somasundaram, Product Line Marketing Manager, End-User Computing, VMware

To comment on this paper, contact the VMware End-User Computing Solutions Management and Technical Marketing Team at twitter.com/vmwarehorizon.