# BEST PRACTICES FOR DELIVERING MICROSOFT OFFICE 365 IN VMWARE HORIZON 7

**vm**ware®

# Table of Contents

**vmware**®

**vm**ware®

# Best Practices for Delivering Microsoft Office 365 in VMware Horizon 7

## Introduction

This article explores the use of Microsoft Office 365 in a VMware Horizon® 7 environment, including tips and best practices that can improve performance and application manageability. For information beyond the scope of this document, see Additional Resources.

This version of the document covers Horizon 7 On-Premises. Another version of this document will cover Horizon Cloud on Azure.

This document is for:

• VMware Horizon 7.9 and later

• VMware Dynamic Environment Manager 9.9 and later

• VMware App Volumes 2.18 and later

**Note**: The terminology has changed in App Volumes 4.0. AppStacks are now called Packages. This document will refer to them as AppStacks.

### Purpose

This guide is to help you use VMware Horizon 7 to deliver Microsoft Office 365 ProPlus to your end users.

### Intended Audience

This guide is intended for IT administrators who want to expand their use of VMware Horizon 7. Familiarity with VMware vSphere and VMware vCenter Server is assumed, as is familiarity with other technologies, including networking and storage in a virtual environment, Active Directory, identity management, and directory services.

### What Is VMware Horizon 7 with Microsoft Office 365?

This section briefly describes VMware Horizon 7 and Microsoft Office 365 in preparation for using them together.

### What is VMware Horizon 7?

VMware Horizon 7 is a family of desktop and application virtualization solutions designed to deliver Windows and Linux virtual desktops and published applications. Horizon 7 enables organizations to deliver virtualized or remote desktop services and applications to end users from centralized VMware vSphere servers. The VMware Horizon 7 solution includes several components, of which View is the main one.

JMP is the next-generation desktop and application delivery platform from VMware and is a key component of VMware Horizon®. It enables you to focus on defining outcomes based on business needs instead of maintaining and troubleshooting environments. JMP leverages non-persistent machines, VMware App Volumes, and VMware Dynamic Environment Manager technologies to untangle the operating system, applications, and user personalization. By doing so, all the component pieces together can be automatically assembled on demand to deliver Just-in-Time desktops and apps to any device. JMP lets you deliver Windows as a service.

Horizon 7 allows IT to deliver virtual desktops and applications, including RDS published applications and Windows 10 VM Hosted applications. All of this can be accessed from one digital workspace which efficiently provides end users with the resources they need.

### What is Microsoft Office 365?

Microsoft Office 365 is a service that provides secure access to the suite of Office products from the cloud. Instead of buying and installing a new version of the suite whenever you need to upgrade, the products are updated automatically so users always work with the most current versions. User-based licenses can be applied to 15 different devices: 5 mobile phones, 5 tablet-style devices, and 5 PCs or Macs. Even if the Office desktop is not installed on the device, Office 365 provides the suite of applications from the

cloud through the browser. The license follows each user across devices, providing a consistent experience offline or online, across all supported devices. In addition to the familiar suite of Office products—Word, Excel, PowerPoint, and Outlook—Office 365 also includes OneDrive, Teams, SharePoint, and OneNote.

For more information, see:

- What is Office 365?

- Microsoft Office 365 Support

- Microsoft Office 365 ProPlus

## Configuring Office 365 ProPlus for Horizon 7

This section explains how to deploy Office 365 ProPlus to a shared computer VMware Horizon 7 environment using nonpersistent virtual desktop infrastructure (VDI) or Remote Desktop Services (RDS) and Shared Computer Activation (SCA). Office 365 ProPlus must be used to leverage Shared Computer Activation. Office 365 ProPlus offers both Office 2016 and 2019.

- **Nonpersistent Virtual Desktop Infrastructure (VDI)** – Nonpersistent VDI are based on stateless desktop images where the remote user is unable to configure a desktop instance as the desktop virtual machine is refreshed at the end of the session. This stateless architecture has many advantages, such as being easier to support and having lower storage costs. Other benefits include a limited need to back up the virtual machines and easier, less expensive disaster recovery and business continuity.

- **Remote Desktop Services** – RDS is a Microsoft Windows component that allows users to access remote computers, session-based desktops, virtual desktops, applications in the data center, and virtual machines over a network connection. VMware Horizon 7 supports Remote Desktop Session Host (RDSH), a role in RDS. RDSH servers host the Windows applications and desktops that are accessed by remote users over the network connection.

- **VM Hosted Applications** - (New Feature as of Horizon 7.9) A pool of nonpersistent floating desktops which can be used to publish applications like RDS. For more information, see VM Hosted Applications.

- **Shared Computer Activation** – SCA is an activation mode used to deploy Office 365 ProPlus to multiple users sharing a single computer. A typical example of SCA is the deployment of Office 365 ProPlus using floating non-persistent desktops, which enables multiple users to access and run Office 365 ProPlus programs simultaneously on remote computers.

**Note**: Use SCA for multiple users sharing the same machine, whether physical or virtual. For multiple users assigned individual computers, such as dedicated Horizon 7 desktops, you can use the standard Microsoft install media with a product key to install Office 365 ProPlus, as you would with traditional endpoint desktops.

The main areas of consideration are as follows:

- Deploy Office 365 by using Remote Desktop Services

- Overview of the Office Deployment Tool

- Overview of shared computer activation for Office 365 ProPlus

## Understanding How Shared Computer Activation Works

Shared Computer Activation (SCA) is the activation mode to use when a virtual machine is shared among multiple users, such as with published resources on RDSH, and with floating desktop pools provisioned with VMware Instant Clone. After enabling SCA and installing Office 365 ProPlus on a shared computer, the following sequence of events takes place for each user:

1. The user logs in to the Horizon 7 system.
2. The user launches an Office 365 ProPlus application, such as Word.
3. Behind the scenes, Office 365 ProPlus contacts the Office Licensing Service through the Internet to obtain a licensing token for the user.
4. The Activate Office window prompts the user for their account information to verify that the user is licensed to use Office 365 ProPlus.

**vmware®**
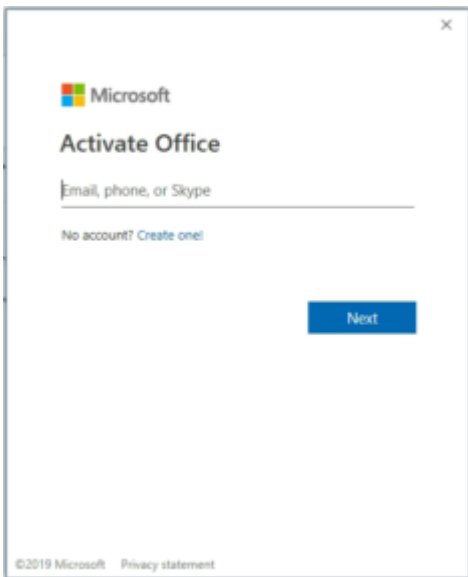
**Figure 1**. Microsoft Office Activation Window

**Note**: Each licensing token is unique to that specific user, for that specific shared computer. This licensing token does not enable this user to access other computers within the Horizon 7 system. Likewise, this licensing token does not enable other users to access Office 365 ProPlus. In both cases, access is obtained by repeating the same sequence of steps.

Federation support allows for automatic activation and is configured by Windows Group Policy Objects using the Office 2016 Administrative Template files. For more information, see the Office 2016 Administrative Template files (ADMX/ADML) and Office Customization Tool.

You can also use VMware Workspace ONE Access to provide single sign-on into Office 365 resources.

For more information, see VMware Workspace ONE Access Integration with Office 365.

## Requirements for Using Nonpersistent VDI and RDS with Office 365 ProPlus

To deploy Office 365 ProPlus with Horizon 7, you must meet the following basic requirements:

• An Office 365 plan that includes Office 365 ProPlus

• Office Customization Tool

• Supported version of Office 365 ProPlus

  • You can download the Office 365 ProPlus software to your local network using the Office Deployment Tool.
  • Office 365 ProPlus is available in a 32-bit and a 64-bit version, and either version can be used.
  • To decide which to pick, see Choose between 64-bit and 32-bit version of Office.

• A supported version of VMware Horizon 7

• A supported version of VMware Horizon Agent:

  • Windows 10
  • Other Operating Systems

• A reliable network connection between the Horizon 7 systems and the Internet

  • The Office Licensing Service, a component of Office 365 ProPlus, issues temporary activation licenses to shared machines when the user is authenticated. The shared systems contact the Office Licensing Service through the Internet to obtain a license for each Office 365 ProPlus user. The connection requires Internet connectivity to obtain the license, as well as to renew it, which occurs every few days. Other programs, such as Outlook, require connectivity to communicate with Exchange provided by Office 365 services. You also need the Internet to download or update Office 365 ProPlus.

# Using the Office Deployment Tool

It is recommended that you use the Office 2016 Deployment Tool (ODT), a Microsoft management technology for installation and configuration. You can use the ODT to download the install media, configure SCA mode, configure which languages to install, determine which products to install and which to exclude, set up automatic updates, and more. You make these configurations by modifying the XML file that the ODT accesses during setup. The ODT uses Click-to-Run, a Microsoft technology for installing and updating Office products.

For more information, see Overview of the Office Deployment Tool.

## Office 365 ProPlus Click-to-Run

Click-to-Run is a Microsoft technology to expedite the processes of installing and updating Office products. Using Click-to-Run technology, installations can be performed on demand, and remotely from the Internet.

As with traditional Office deployments using MSI-based installations, Office 365 Click-to-Run is not available for Microsoft Volume Licensing and can be only downloaded by the ODT.

## Using the Office 365 ProPlus Configuration XML Editor

Your configuration choices are stored in the Office 365 ProPlus Configuration XML Editor, which the Office 2016 Deployment Tool uses during installation. The following example was created with the Office 365 ProPlus Configuration XML Editor, and shows downloading and installing the Office media.

Using the example configuration file provided below, the Office installation media is downloaded to a local network file share. A source path specifies where the Office 365 ProPlus installation media is located.

```
<Configuration ID="1a15b285-688c-443f-a550-7ac57495ad8b">
  <Add OfficeClientEdition="64" Channel="Broad" SourcePath="\\server\share"
AllowCdnFallback="FALSE" ForceUpgrade="TRUE">
    <Product ID="O365ProPlusRetail">
      <Language ID="en-us" />
      <ExcludeApp ID="Access" />
      <ExcludeApp ID="Groove" />
      <ExcludeApp ID="OneDrive" />
      <ExcludeApp ID="OneNote" />
      <ExcludeApp ID="Publisher" />
      <ExcludeApp ID="Lync" />
      <ExcludeApp ID="Teams" />
    </Product>
  </Add>
  <Property Name="SharedComputerLicensing" Value="1" />
  <Property Name="PinIconsToTaskbar" Value="TRUE" />
  <Property Name="SCLCacheOverride" Value="0" />
  <Property Name="AUTOACTIVATE" Value="0" />
  <Property Name="FORCEAPPSHUTDOWN" Value="FALSE" />
  <Property Name="DeviceBasedLicensing" Value="0" />
  <Updates Enabled="FALSE" />
  <RemoveMSI />
  <Display Level="None" AcceptEULA="TRUE" />
</Configuration>
```

**Figure 2**. Example of configuration.xml file

## Enabling Shared Computer Activation on Nonpersistent VDI and RDS

The Office Deployment Tool and the configuration.xml file are used to install Office 365 ProPlus on the shared computer (such as a nonpersistent VDI desktop or RDS server), and to enable shared computer activation for that computer. Add the following lines when you create the configuration.xml file:

```
<Display Level="None" AcceptEULA="True" />
```

```
<Property Name="SharedComputerLicensing" Value="1" />
```

**Note**: You can use Windows Group Policy Objects to override the default settings specified during installation. The Group Policy templates are located at the Microsoft Download Center.

**vm**ware®

For more information, see Configuration Options for the Office Deployment Tool.

# Installing and Configuring Office 365 on Horizon 7 Systems

This section provides a high-level overview of the process of installing Office 365 ProPlus in a Horizon 7 VDI and RDS environment.

## Install Office 365 ProPlus

1. Install and configure Windows desktop OS for VDI or Windows Server for RDS. Make sure to optimize the image with the VMware OS Optimization Tool.
2. (If RDSH) Install and configure the Remote Desktop Session Host role service.
    1. Horizon 7.10 and later will detect and automatically install the role during Horizon Agent install.
    2. **Note**: It may need to reboot twice to install the role and then the agent.
3. Install and configure the Horizon Agent.
4. Create a shared directory on a file server for the Office files (`\\FileServer\OfficeShare`).
5. Download and extract the Office Deployment Tool to the file share you created.
6. Create the configuration.xml files that are used to download and configure Office 365 ProPlus. Make sure the following lines are included:
   `<Display Level="None" AcceptEULA="True" />`
   `<Property Name="SharedComputerLicensing" Value="1" />`
   **Note**: Do not install OneDrive Desktop or OneDrive (Groove).
7. Download Office 365 ProPlus to a file share on your local network using the Office Deployment Tool and the configuration.xml file. From an elevated command prompt, run `setup.exe`.
   `\\FileServer\OfficeShare\setup.exe /download`
   `\\FileServer\OfficeShare\Configuration.xml`
8. Install Office 365 ProPlus on the VDI desktop or RDS server (install to the master virtual machine if using Instant Clone Technology or View Composer) using the Office 2016 Deployment Tool along with the `configuration.xml` file. From an elevated command prompt, run `setup.exe` using the ODT. Specify the /configure parameter and provide a location to the configuration.xml file:
   `\\FileServer\OfficeShare\setup.exe /configure`
   `\\FileServer\OfficeShare\Configuration.xml`
9. Wait until the command completes. Do not start and activate any of the Office programs at this time. The installation process can take several minutes to finish, and a progress window is not displayed.
   **Note**: When installing Office 365 ProPlus as part of a base image, make sure not to activate Office 365 ProPlus prior to provisioning the shared machines. This prevents temporary product keys from being installed during the image creation process. Users activate Office 365 ProPlus by logging in with their account credentials.
10. Install the OneDrive sync app per machine via `OneDriveSetup.exe /allusers`. For more information, see Installation Instructions.

# Considerations for Deploying Office 365 ProPlus to a Horizon 7 Environment

This section provides best practices, guidelines, tips, and optimizations for your deployment.

• Shared Computer Activation

• Microsoft FSLogix

• VMware Dynamic Environment Manager (DEM)

• VMware App Volumes

• Microsoft One Drive Sync App

• Microsoft Outlook

**vm**ware®

• VMware Workspace ONE Access

• Tips and Optimizations

## Shared Computer Activation

This section discusses several considerations when you use shared computer activation in your deployment.

• **Internet connectivity** – Because the shared computer must contact the Office Licensing Service on the Internet to obtain or renew a licensing token, reliable connectivity between the shared computer and the Internet is necessary.

• **Licensing token renewal** – The licensing token that is stored on the shared computer is valid for up to seven days, whether or not the user logs in during that time. As the expiration date for the licensing token reaches 50%, Office 365 ProPlus automatically attempts to renew the licensing token while the user is logged in. After seven days, the licensing token expires. The next time the user launches an Office 365 ProPlus program, Office 365 ProPlus contacts the Office Licensing Service on the Internet to get a new licensing token.

• **Reduced functionality mode** – If the user is not licensed for Office 365 ProPlus, or if the user closes the Activate Office dialog box, no licensing token is obtained. Office 365 ProPlus is not activated and is now in reduced functionality mode. This means that the user can view and print Office 365 ProPlus documents but cannot create or edit documents. Office 365 ProPlus displays notification that most features are turned off.

• **Activation limits** – Normally, you can install and activate Office 365 ProPlus on five computers or fewer. Using Office 365 ProPlus with SCA enabled does not count against the five-computer limit. Microsoft allows a single user to temporarily activate Office 365 ProPlus on what it considers a reasonable number up to 20 of shared computer devices per week within a given time period. The user gets an error message in the unlikely event the limit is exceeded. For more information, see Troubleshoot issues with shared computer activation for Office 365 ProPlus.

## Microsoft FSLogix

Microsoft FSLogix is a set of solutions to allow a nonpersistent user connected to VDI or RDSH to have a persistent experience by redirecting the user profile (Profile Container) or just the Office 365 Configuration (Office Container) to a VHD(x) file on a network share.

### Disclaimer
*FSLogix is one of many third-party solutions that work with VMware Horizon. While this tutorial shows example models for integration, VMware assumes no responsibility in providing support for the use of FSLogix software with VMware products. As with any profile management technology, proper design, component redundancy, backup, and other management practices are imperative to ensure a good user experience and to prevent loss of user data. VMware provides this tutorial to demonstrate functional compatibility of the FSLogix Profile Container with Horizon JMP components. For design guidance of Horizon see the VMware Workspace ONE and Horizon Reference Architecture. For guidance on sizing, scaling, and maintaining the FSLogix components, please consult Microsoft.*

### FSLogix Profile Container
The FSLogix Profile container redirects the entire user profile to a network location in a VHD(x) file for nonpersistent environments.

### FSLogix Office Container
The FSLogix Office Container redirects only areas of the profile that are specific to Microsoft Office and is a subset of Profile Container. Office Container allows Office Settings to roam in non-persistent environments. The Office Container will allow Office Activation to roam and captures local data such as the OneDrive cache and the Outlook OST for cached mode.

Details on setup and configuration of FSLogix:

• FSLogix Overview

• Download and Install FSLogix

• Configure FSLogix Office Container

• Configure FSLogix Profile Container

• Microsoft FSLogix Entitlement Requirements

**vm**ware®

The following document goes into detail on setup and configuration of FSLogix with JMP and Horizon Cloud on Azure. The setup and configuration process are the same for FSLogix Profile Containers and Office Containers:

• Integrating FSLogix Profile Containers with the VMware Horizon Just-In-Time Management Platform (JMP)

• Integrating FSLogix Profile Containers with VMware Horizon Cloud Service on Microsoft Azure

## VMware Dynamic Environment Manager (DEM)

VMware Dynamic Environment Manager (DEM) (formally called VMware User Environment Manager) is a profile and policy management solution that supports personalization and dynamic policy configuration across virtual, physical, and cloud-based Windows desktop environments. You can use DEM to simplify policy management by replacing and unifying problematic, unmaintainable, or complex login scripts and profile logic. You can map environmental settings, such as networks and printers, and dynamically apply end-user security policies and customizations. DEM ensures that each user's settings and customizations follow that user from one location to the next, regardless of the endpoint used to access the user's resources.

Office 365 ProPlus benefits from DEM like an MSI-based Office installation does, regardless of the deployment method and service-centric model. DEM can be used to persist Windows and application settings such as Office 365 across non-persistent sessions as well as manage the user environment. Examples of user environment settings are:

• ADMX settings

• Application Blocking

• Privilege Elevation

• File Type Associations

• Horizon Smart Polices

• Folder Redirection

• Printer Mappings and more

Pre-Defined settings can be used to configure language or other application settings per user or device. DirectFlex in DEM will detect when an application is launched and environmental settings such as printer mappings or mapped drives can be executed in real-time when the application that needs them is run.

For more information, see VMware Dynamic Environment Manager and the Quick-Start Tutorial for VMware User Environment Manager.

## VMware App Volumes

VMware App Volumes is a Windows application delivery and application life-cycle-management solution which can be used with Horizon 7 and RDSH virtual environments. App Volumes uses application containers called AppStacks (Packages in App Volumes 4), which are read-only virtual disks that contain all the components—such as executables and registry keys—required to run an application. When an AppStack is deployed, it does not require end-user installation, and it is available for use within seconds. You can use App Volumes to deliver native Windows applications, virtualized Windows applications such as ThinApp packages, and applications to be targeted for published applications on both RDSH and VM Hosted Applications.

AppStacks work on both Horizon 7 VDI, VM Hosted Applications and RDSH. For RDSH servers and VM Hosted Applications the AppStack is delivered to the machine and attached when the service starts up so all users can access the applications. App Volumes extends the manageability of Office 365 ProPlus for these environments with one-to-many provisioning to simplify the process of deploying, upgrading, and patching the systems.

Writable Volumes are read/write volumes assigned per user. There are three types of Writable Volume templates:

• **Profile Only**:  Contains the users' profile and allows it to roam across sessions.

• **UIA Only**:  Allows user installed applications which will roam across non-persistent sessions. An example is Office 365 Plug-Ins.

• **UIA plus Profile**: Contains the users' profile and allows the user to install applications. Both the applications installed, and the profile will roam across nonpersistent sessions.

Writable volumes are only available on virtual desktops - they are not available on RDSH. For more information about App Volumes, see VMware App Volumes. For more information on installing Office products in App Volumes, see Installing and Using Microsoft Office Products with VMware App Volumes 2.x.

## Microsoft One Drive Sync App

OneDrive for Business is not officially supported for RDSH or for nonpersistent VDI deployments. The new OneDrive sync app should be used. For more information, see Use the sync app on virtual desktops. This new sync app is installed once per machine and all users share a single installation of OneDrive. This will help speed up the logon process and reduce sprawl as there is only one copy of onedrive.exe on a system.

Do not install OneDrive Desktop or OneDrive (Groove) as part of configuring the XML with the Office Configuration tool. Instead, run the onedrivesetup.exe file that is included in the download with the /allusers switch to do the machine installation of OneDrive. If there is an existing Office install, remove all OneDrive clients and install the OneDrive sync app in the same way. For more information, see Directions on Installing the OneDrive sync app per machine.

### OneDrive Files On-Demand

OneDrive Files On-Demand leverages the Windows 10 Fall Creators update (1709) and the OneDrive Sync Client to simplify the user experience with cloud storage accessibility. We recommend always using Files on-Demand. With Files On-Demand, you can access all your files in the cloud without having to download all of them and use storage space on your system. All your OneDrive online files can be seen in File Explorer and work just like every other file on your system. You will be able to open online-only files from within any desktop or Windows Store apps using the Windows file picker.

The files and subfolders within OneDrive are accessible on-demand and have a blue cloud icon indicating the content state is online. The online files report details such as date modified, type, size and are searchable behaving much like traditional Windows files. However, the files are zero bytes in size on the local storage. Accessing an online file by double-clicking downloads the data to the default local storage location. Files that are downloaded are indicated with a green check icon as viewed from OneDrive.

Changes made to the downloaded, locally available files, are synced to the online repository on an ongoing basis. When using an FSLogix Container or App Volumes Profile Only or Profile Plus UIA Writable Volume the downloaded files will be available for the next Instant Clone desktop the user receives. See Solutions for Desktops for details on using the FSLogix Office Container with Office Activation and DEM. From the context menu in OneDrive, there is an option to set the files as Always keep on this device. Those files will remain local in the FSLogix Container or Writable Volume (Profile Only or Profile plus UIA).
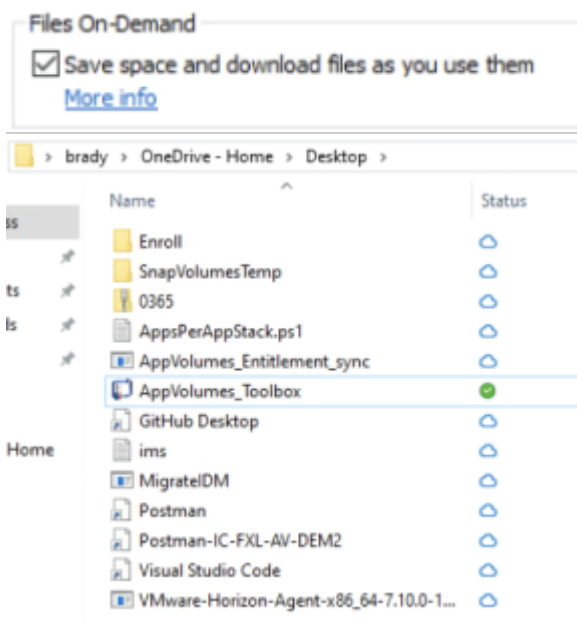


**Figure 3**. OneDrive Files on-Demand

For more information, see the following additional resources:

• One Drive on Virtual Desktops

• Installing the One Drive Sync App Per Machine

• Files On-Demand

• OneDrive Backup

## Microsoft Outlook

This section describes areas of consideration when using the Outlook product within Office 365 ProPlus, in a VMware Horizon 7 environment. The main areas of consideration are understanding Outlook Cached Exchange Mode and optimizing Outlook for Office 365 ProPlus and RDSH.

### Understanding Outlook Cached Mode

In many cases, Cached Exchange Mode is the recommended option for Office 365 deployments. When using a Microsoft Exchange email account on Internet connections, Cached Mode can improve performance. Cached Mode saves a local copy of your mailbox data on your computer. Outlook accesses this cached copy instead of the cloud, resulting in faster response times.

If Cached Exchange Mode is not enabled, all the data for operations is stored and retrieved from the cloud, which can be time-consuming and slow down performance. With Cached Mode you can access your downloaded data even if the network connection is broken, and you can continue to work offline until your network connection is restored. By contrast, when the default Online Mode is enabled, Outlook accesses Office 365 on an ongoing basis and does not cache anything locally.

To enable Outlook Cached Mode for Office 365 ProPlus on a Horizon 7 system:

• Use Outlook 2013 SP1 or later

• Define Exchange Cached Mode in Windows Group Policy Objects

• Configure Full items or only headers in Windows Group Policy Objects

An App Volumes Writable Volume (Profile Only or UIA plus Profile), or FSLogix container can be used to persist the cached Outlook data across nonpersistent sessions. For more details, see FSLogix Office Container with Office Activation and DEM.

## VMware Workspace ONE Access

VMware Workspace ONE Access (formerly called VMware Identity Manager) is an offering that provides application provisioning, a self-service catalog of applications and virtual desktops, conditional access controls, and single sign-on (SSO) for software-as-a-service (SaaS), web, cloud, and native mobile applications. VMware Workspace ONE Access provides your IT team with a central location for the management of user provisioning and access policy with directory integration, identity federation, and user analytics.

VMware Workspace ONE Access provides SSO support for Office 365 to trust the VMware Workspace ONE Access service for authentication to the Office 365 applications. In addition, Workspace ONE Access provides federation support with the ability to configure outbound provisioning of users and groups to Azure Active Directory that is used by Office 365.

For more information, see VMware Workspace ONE Access Integration with Office 365.

## Tips and Optimizations

When you use Office 365 ProPlus in a Horizon 7 environment, the following considerations may be helpful.

• Do not enable automatic updates for Office 365 when using Instant Clone Technology or View Composer. Apply updates manually to the base image. The Office updates can be configured using Group Policies and the Office Administrative Template.

• **Note**: Policy templates are frequently updated by Microsoft, be sure to always have the latest version.

• VMware OS Optimization Tool (OSOT) – This tool helps optimize Windows systems for use with VMware Horizon 7. The optimization tool includes customizable templates to enable or disable Windows system services and features, per VMware recommendations and best practices, across multiple systems. Since most Windows system services are enabled by default, the optimization tool can be used to easily disable unnecessary services and features to improve performance.

• Microsoft Support and Recovery Assistant (SaRA) for Office 365 - The Microsoft Support and Recovery Assistant works by running tests to figure out what's wrong and offers the best solution for the identified problem. It can currently fix Office, Office 365, or Outlook problems. If the Microsoft Support and Recovery Assistant cannot fix a problem for you, it will suggest next steps and help

you get in touch with Microsoft support.

• Patching Office 365 in nonpersistent systems – The following list the best practices for updating and maintaining Office 365 ProPlus in nonpersistent VDI or RDS system.
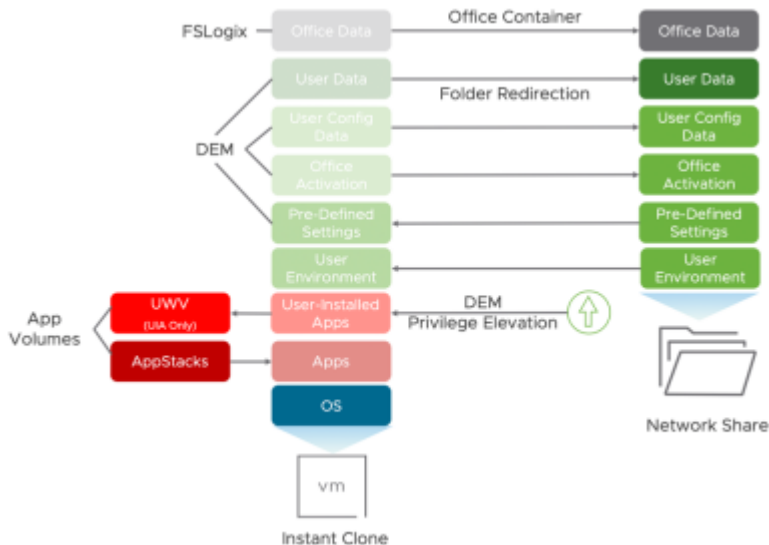
- Turn off default patching - disable updates
- Turn off user interaction or point to empty path
- Integrate Office builds into Windows image monthly

# Solutions for Desktops

This section offers recommended solutions when using Office 365 with Horizon 7 non-persistent desktops. There are several solutions outlined. Each provides persistence of Office 365 activation and user data across non-persistent desktop sessions.

## FSLogix Office Container + Dynamic Environment Manager + App Volumes

In this scenario, we are using the Microsoft FSLogix Office Container to persist the Office 365 configuration data, including Office activation across non-persistent user sessions. The Office Container allows all Office 365 settings and local data such as the One Drive cache or Outlook OST data to roam. FSLogix is configured either via registry or GPO as to which components of Office 365 will be persisted. This information is shared to a VHD(x) file on a network file share. The FSLogix Office Container is designed to be used in conjunction with another profile management solution. Since the Office Container only captures a subset of the user profile, another solution must be used to capture the remaining required data. In addition, the Office Activation data is encrypted via DPAPI and must be decrypted to be used across non-persistent sessions. We can use Dynamic Environment Manager (DEM) to do this. The following locations need to be roamed across non-persistent sessions: `<AppData>\Microsoft\Crypto` and `<AppData>\Microsoft\Protect`.



**Figure 4**. Non-persistent desktops with FSLogix Office Container, DEM and App Volumes

This can be accomplished by either creating a new personalization template and add `<AppData>\Microsoft\Crypto` and `<AppData>\Microsoft\Protect` under `[IncludeFolderTrees]` or by creating a configuration file for the built-in **Personal Certificates - AppData NOT redirected**. This will save the setting to the profile archive and will be imported on each system with DEM and then the Office Activation data can be decrypted.
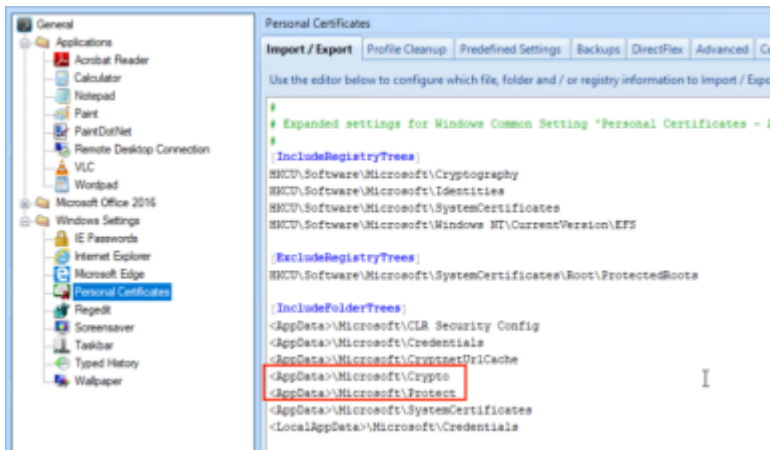
**Figure 5**. Roam Office Activation Encryption Keys with DEM

In addition to the roaming the folder for DPAPI, DEM will be used for the following:

• **User Configuration Data** - Capture configuration data for applications, and Windows Settings outside of Office applications. This data is roamed across non-persistent desktop sessions. Note that when using the FSLogix Office Container, you do not need to use the DEM templates for Microsoft Office.

• **User Environment** - You can use the User Environment tab of the Management Console for creating and managing user environment settings. The settings are applied at login and logout. Examples are Horizon Smart Policies, Application Blocking, Privilege Elevation or Folder Redirection.

• **Privilege Elevation** - Allow users that are not admins the ability to install software. This is used in conjunction with an App Volumes UIA only Writable Volume. This will allow installed applications to roam across non-persistent systems. For more information, see Privilege Elevation Feature Walk Through.

• **Pre-Defined Settings** - Settings can be applied to an application automatically. An example is pre-populating server names in an application or choosing a default language.

• **Folder Redirection** - Redirect user data folders to a file share to make them available across non-persistent sessions. An example is the Documents folder.

App Volumes will be used to provide applications in addition to what is installed in the base image through AppStacks, and to also provide the ability for non-admin users to install applications that will be roamed across non-persistent desktop sessions using a UIA Only Writable Volume in conjunction with Privilege Elevation in DEM.



**Figure 6**. UIA Only Writable Volume

## Dynamic Environment Manager + App Volumes

In this scenario, we are using Dynamic Environment Manager (DEM) and App Volumes to provide persistence of the Office 365 data including licensing activation across non-persistent sessions. App Volumes will be used to assign a UIA + Profile Writable Volume to each user. This type of Writable Volume will roam the entire user profile as well as allow users to install applications that will be available across non-persistent sessions. This will be used to roam all the Office 365 activation data as well as local user data including data like the OneDrive Cache or the Outlook OST file. Since the entire profile is redirected to the Writable Volume, there is no need to configure DEM to roam the individual folder locations required by DPAPI. There is also no need for folder redirection in this use case. Everything (Office activation data, Office user data, general user data) is stored in the profile and redirected to the Writable Volume. App Volumes will also be used to provide applications in addition to what is installed in the base image through AppStacks, and to also provide the ability for non-admin users to install applications that will be roamed across non-persistent desktop sessions using a Profile plus UIA Writable Volume in conjunction with Privilege Elevation in DEM.
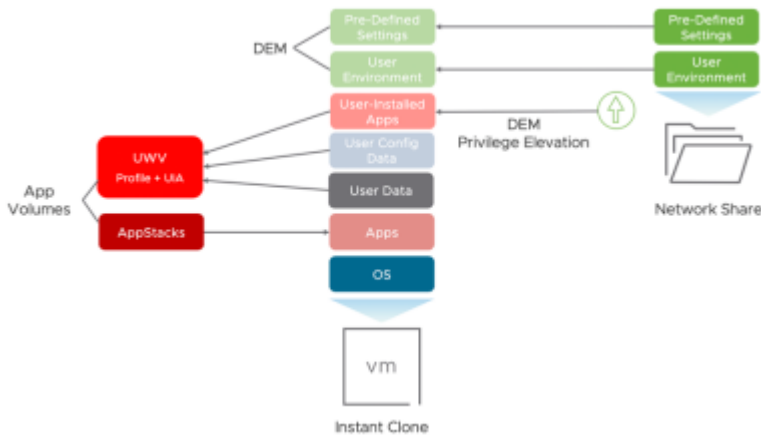
**Figure 7**. Dynamic Environment Manager + App Volumes
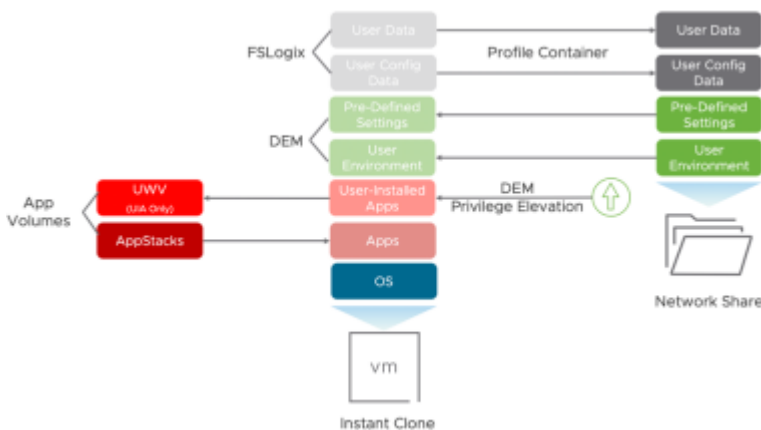
DEM will be used for the following:

• **User Environment** - You can use the User Environment tab of the Management Console for creating and managing user environment settings. The settings are applied at login and logout. Examples are Horizon Smart Policies, Application Blocking, Privilege Elevation or Folder Redirection.

• **Privilege Elevation** - Allow users that are not admins the ability to install software. This is used in conjunction with an App Volumes Profile plus UIA Writable Volume. This will allow installed applications to roam across non-persistent systems. For more information, see Privilege Elevation Feature Walk Through.

• **Pre-Defined Settings** - Settings can be applied to an application automatically. An example is pre-populating server names in an application or choosing a default language.
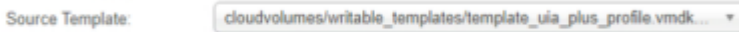


**Figure 8**. UIA plus Profile Writable Volume

## FSLogix Profile Container + DEM + App Volumes

In this scenario, the FSLogix Profile Container is combined with DEM and App Volumes to provide persistence of the user experience and the Office 365 data across non-persistent desktops. FSLogix is configured either via registry or GPO. The profile is then redirected to a VHD(x) file on a network file share. The FSLogix Profile Container redirects the entire user profile, so there is no need to redirect the folders for DPAPI data or for user folder redirection. Everything (Office activation data, Office user data, general user data) is in the profile and redirected to the FSLogix Profile Container VHD(x) file.



**Figure 9**. Microsoft FSLogix Profile Container, Dynamic Environment Manager and App Volumes

DEM will be used for the following:

• **User Environment** - You can use the User Environment tab of the Management Console for creating and managing user environment settings. The settings are applied at login and logout. Examples are Horizon Smart Policies, Application Blocking, Privilege Elevation or Folder Redirection.

• **Privilege Elevation** - Allow users that are not admins the ability to install software. This is used in conjunction with an App Volumes UIA only Writable Volume. This will allow installed applications to roam across non-persistent systems. For more information, see Privilege Elevation Feature Walk Through.

• **Pre-Defined Settings** - Settings can be applied to an application automatically. An example is pre-populating server names in an application or choosing a default language.

App Volumes will be used to provide applications in addition to what is installed in the base image through AppStacks, and to also provide the ability for non-admin users to install applications that will be roamed across non-persistent desktop sessions using a UIA Only Writable Volume in conjunction with Privilege Elevation in DEM.
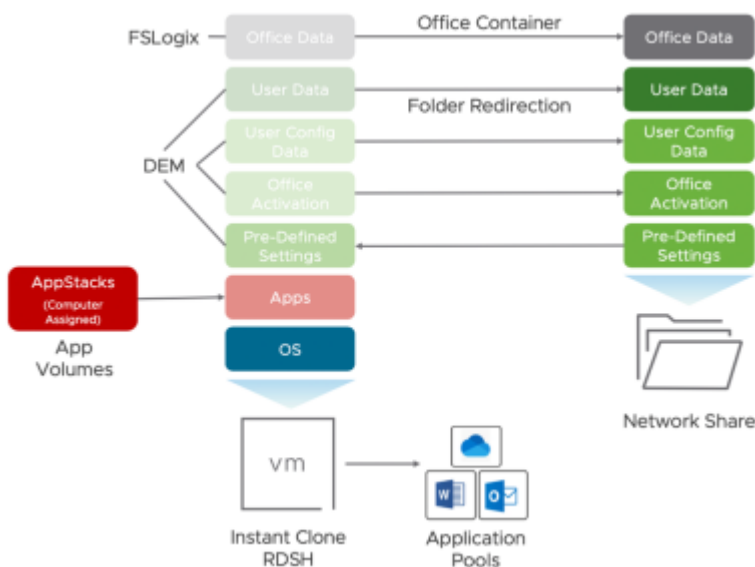
This solution is covered in detail in: Integrating FSLogix Profile Containers with the VMware Horizon Just-In-Time Management Platform (JMP).

# Solutions for RDSH

The following solutions cover using Remote Desktop Services Host (RDSH) to deliver Microsoft Office. These solutions provide persistence of the Office activation data, as well as user data, such as the OneDrive cache or the Outlook Cached Mode OST file.

## Instant Clone RDSH - FSLogix Office Container + DEM + App Volumes

In this scenario, we are using the Microsoft FSLogix Office Container to persist the Office 365 configuration data, including Office activation across non-persistent user sessions. The Office Container will allow all Office 365 settings and local data such as the One Drive cache or Outlook OST data to roam. FSLogix is configured either via registry or GPO as to which components of Office 365 will be persisted. This information is shared to a VHD(x) file on a network file share. The FSLogix Office Container is designed to be used in conjunction with another profile management solution. Since the Office Container only captures a subset of the user profile, another solution must be used to capture the remaining required data. In addition, the Office Activation data is encrypted via DPAPI and must be decrypted to be used across non-persistent sessions. We can use Dynamic Environment Manager (DEM) to do this. The following locations need to be roamed across non-persistent sessions: `<AppData>\Microsoft\Crypto` and `<AppData>\Microsoft\Protect`.



**Figure 10**. Instant Clone RDSH with FSLogix Office Container + DEM + App Volumes

This can be accomplished by either creating a new personalization template and add `<AppData>\Microsoft\Crypto` and `<AppData>\Microsoft\Protect` under `[IncludeFolderTrees]` or by creating a configuration file for the built-in **Personal Certificates - AppData NOT redirected**. This will save the setting to the profile archive and will be imported on each system

with DEM and then the Office Activation data can be decrypted.
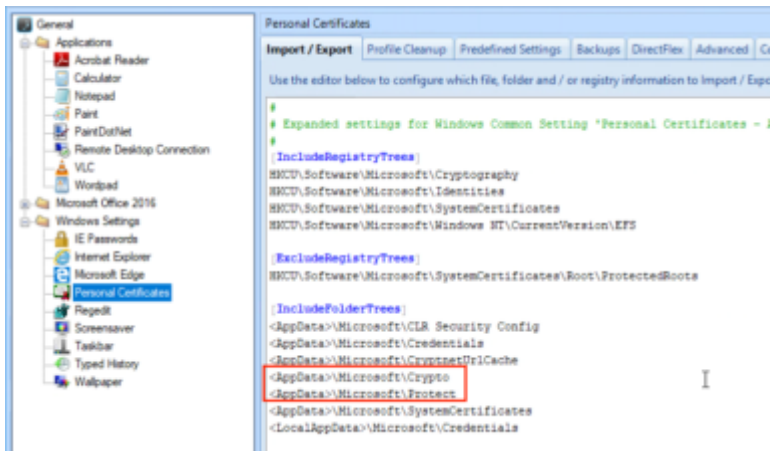


**Figure 11**. Roam Office Activation Encryption Keys with DEM

In addition to the roaming the folder for DPAPI, DEM will be used for the following:

• **User Configuration Data** - Capture configuration data for applications, and Windows Settings outside of Office applications. This data is roamed across non-persistent desktop sessions. Note that when using the FSLogix Office Container you do not need to use the DEM templates for Microsoft Office.

• **User Environment** - You can use the User Environment tab of the Management Console for creating and managing user environment settings. The settings are applied at login and logout. Examples are Horizon Smart Policies, Application Blocking, Privilege Elevation or Folder Redirection.

• **Pre-Defined Settings** - Settings can be applied to an application automatically. An example is pre-populating server names in an application or choosing a default language.

• **Folder Redirection** - Redirect user data folders to a file share to make them available across non-persistent sessions. An example is the Documents folder.

App Volumes can be used to deliver computer attached AppStacks to the RDSH servers. The AppStacks will be attached when the computer starts up, then can be published to end-users as application pools. The best practice is to assign computer attached AppStacks to the Organizational Unit in Active Directory which contains the RDSH servers.
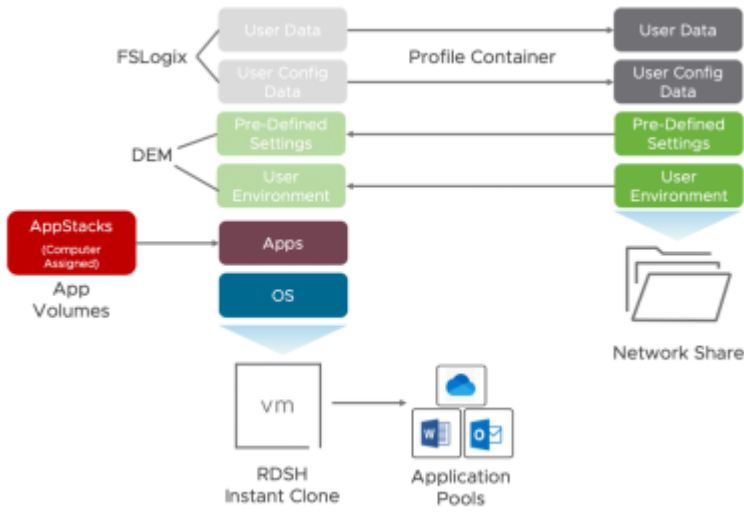


**Figure 12**. Computer attached AppStack assigned to an Organizational Unit

## Instant Clone RDSH - FSLogix Profile Container + DEM + App Volumes

In this scenario, the FSLogix Profile Container is combined with DEM and App Volumes to provide persistence of the user experience and the Office 365 data across non-persistent desktops. FSLogix is configured either via registry or GPO. The profile is then redirected to a VHD(x) file on a network file share. The FSLogix Profile Container redirects the entire user profile, so there is no need to redirect the folders for DPAPI data or for user folder redirection. Everything (Office activation data, Office user data, general user data) is in the profile and redirected to the FSLogix Profile Container VHD(x) file.

The FSLogix Profile Container is covered in detail in: Integrating FSLogix Profile Containers with the VMware Horizon Just-In-Time Management Platform (JMP).

**Figure 13**. RDSH Instant Clone + FSLogix Profile Container + DEM + App Volumes

DEM will be used for the following:

• **User Environment** - You can use the User Environment tab of the Management Console for creating and managing user environment settings. The settings are applied at login and logout. Examples are Horizon Smart Policies, Application Blocking, Privilege Elevation or Folder Redirection.

• **Pre-Defined Settings** - Settings can be applied to an application automatically. An example is pre-populating server names in an application or choosing a default language.

App Volumes can be used to deliver computer attached AppStacks to the RDSH servers. The AppStacks will be attached when the computer starts up, then can be published to end-users as application pools. The best practice is to assign computer attached AppStacks to the Organizational Unit in Active Directory which contains the RDSH servers.



**Figure 14**. Computer attached AppStack assigned to an Organizational Unit

# VM Hosted Applications

As of Horizon 7.9, there is a new feature in Horizon called VM Hosted Applications. This allows floating Instant Clone pools to be used as a source for Application Pools. This is a great solution for publishing Office 365 applications. The advantages are:

• Publish application that do not run on a server OS

• Want to run applications on Windows 10

• Same deployment and configuration process as a normal desktop

• Publish UWP apps as well as any Win32 application

• One-to-One user to machine assignment, which prevents a user from impacting performance for another user as can happen in RDSH

• No need for RDS CALs

## Requirements for VM Hosted Applications

• Horizon 7.9 server or later

• Horizon 7.9 agent or later

• Horizon Client 5.1 or later

• Instant Clone Floating Pool

• Windows 10 1803 or later

For more information, see VM Hosted Applications Feature Walkthrough.

A floating Instant Clone pool is created as usual; choose the session type of Application or Desktop & Application to enable this feature. Desktop & Application allows the pool to be accessed via users for both Desktops and Applications. Note that users can only use one type (Desktop or Application) at a time.
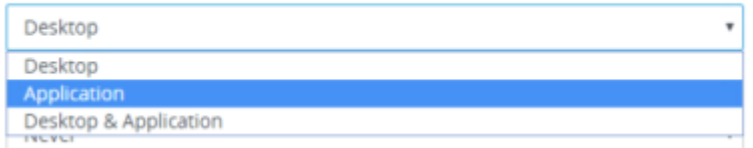


**Figure 15**. Choosing Application Session Type

After the pool is created, go through the standard Application Pool creation process, except choose Desktop Pool and select the name of the Pool you just created. You can then either select applications to publish manually or automatically.
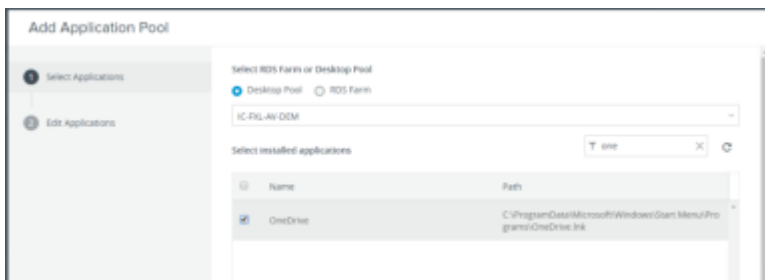


**Figure 16**. Adding Application Pool

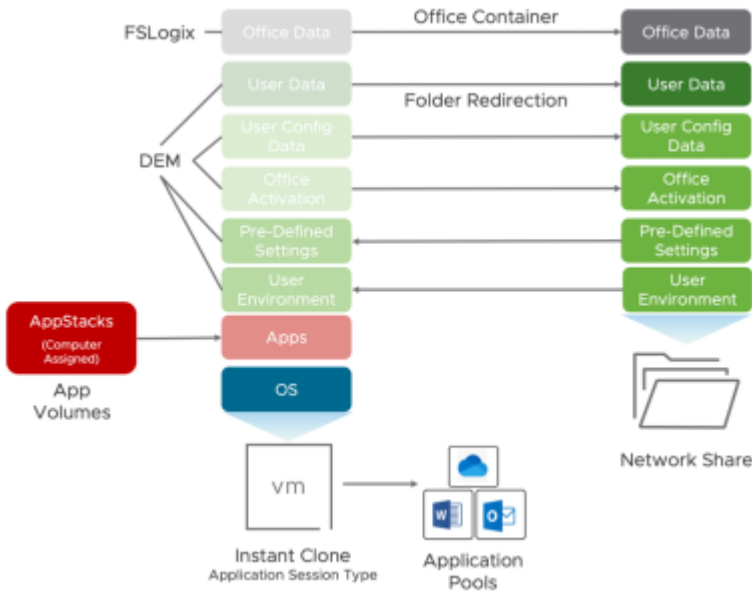Entitlement is done the same and the published apps look the same to the user as RDSH hosted applications do.
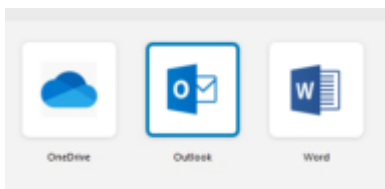


**Figure 17**. VM Hosted Applications in the Horizon Client

**Note**: Do not use a UIA Writable Volume or Privilege Elevation in this use case, as users only interface with the applications which are published.

## VM Hosted Applications + FSLogix Office Container + DEM + App Volumes

In this scenario, we are using the Microsoft FSLogix Office Container to persist the Office 365 configuration data, including Office activation across non-persistent user sessions. The Office Container will allow all Office 365 settings and local data such as the One Drive cache or Outlook OST data to roam. FSLogix is configured either via registry or GPO as to which components of Office 365 will be persisted. This information is shared to a VHD(x) file on a network file share. The FSLogix Office Container is designed to be used in conjunction with another profile management solution. Since the Office Container only captures a subset of the user profile, another solution must be used to capture the remaining required data. In addition, the Office Activation data is encrypted via DPAPI and must be decrypted to be used across non-persistent sessions. We can use Dynamic Environment Manager (DEM) to do this. The following locations need to be roamed across non-persistent sessions: `<AppData>\Microsoft\Crypto` and `<AppData>\Microsoft\Protect`.

**Figure 18**. VM Hosted Applications + FSLogix Office Container + DEM + App Volumes

This can be accomplished by either creating a new personalization template and add `<AppData>\Microsoft\Crypto` and `<AppData>\Microsoft\Protect` under `[IncludeFolderTrees]` or by creating a configuration file for the built-in **Personal Certificates - AppData NOT redirected**. This will save the setting to the profile archive and will be imported on each system with DEM and then the Office Activation data can be decrypted.
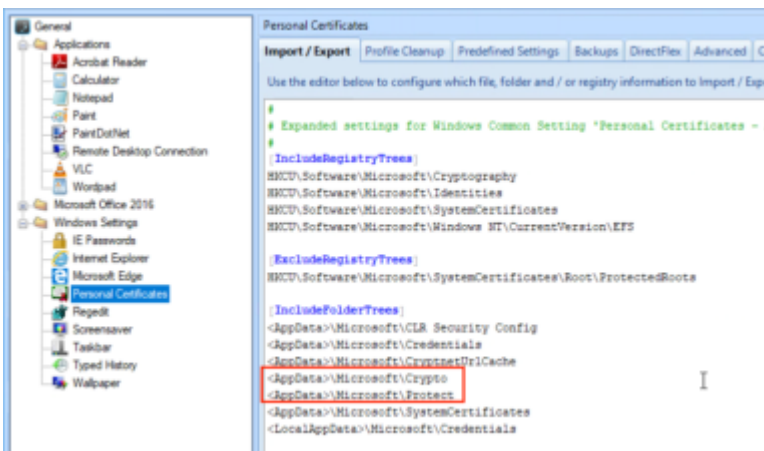


**Figure 19**. Roam Office Activation Encryption Keys with DEM

In addition to the roaming the folder for DPAPI, DEM will be used for the following:

• **User Configuration Data** - Capture configuration data for applications, and Windows Settings outside of the Office applications. This data is roamed across non-persistent desktop sessions. Note that when using the FSLogix Office Container, you do not need to use the DEM templates for Microsoft Office.

• **User Environment** - You can use the User Environment tab of the Management Console for creating and managing user environment settings. The settings are applied at login and logout. Examples are Horizon Smart Policies, Application Blocking, Privilege Elevation or Folder Redirection.

• **Pre-Defined Settings** - Settings can be applied to an application automatically. An example is pre-populating server names in an application or choosing a default language.

• **Folder Redirection** - Redirect user data folders to a file share to make them available across non-persistent sessions. An example is the Documents folder.

App Volumes can be used to deliver computer attached AppStacks to the VM Hosted Application desktops. The AppStacks will be attached when the computer starts up, then can be published to end-users as application pools. The best practice is to assign computer attached AppStacks to the Organizational Unit in Active Directory which contains the desktops.
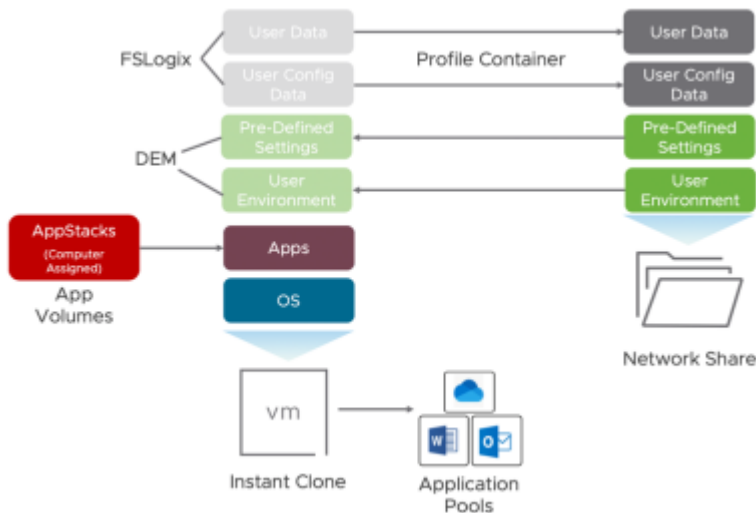
| | Entity | | Name | | Status | | |
|---|---|---|---|---|---|---|---|
| | BETA\MWEUC OU:Desktops.Horizon_CDH | | Desktops | | Assigned | | |

**Figure 20**. Computer attached AppStack assigned to an Organizational Unit

## VM Hosted Applications + FSLogix Profile Container + DEM + App Volumes

In this scenario, the FSLogix Profile Container is combined with DEM and App Volumes to provide persistence of the user experience and the Office 365 data across non-persistent desktops. FSLogix is configured either via registry or GPO. The profile is then redirected to a VHD(x) file on a network file share. The FSLogix Profile Container redirects the entire user profile, so there is no need to redirect the folders for DPAPI data or for user folder redirection. Everything (Office activation data, Office user data, general user data) is in the profile and redirected to the FSLogix Profile Container VHD(x) file.

The FSLogix Profile Container is covered in detail in: Integrating FSLogix Profile Containers with the VMware Horizon Just-In-Time Management Platform (JMP).



**Figure 21**. VM Hosted Applications + FSLogix Office Container + App Volumes

DEM will be used for the following:

• **User Environment** - You can use the User Environment tab of the Management Console for creating and managing user environment settings. The settings are applied at login and logout. Examples are Horizon Smart Policies, Application Blocking, Privilege Elevation or Folder Redirection.

• **Pre-Defined Settings** - Settings can be applied to an application automatically - an example is pre-populating server names in an application or choosing a default language.

App Volumes can be used to deliver computer attached AppStacks to the RDSH servers. The AppStacks will be attached when the computer starts up, then can be published to end-users as application pools. The best practice is to assign computer attached AppStacks to the Organizational Unit in Active Directory which contains the RDSH servers.

# Summary and Additional Resources

## Summary

This guide provides tips to help IT administrators use VMware Horizon 7 to deliver Microsoft Office 365 ProPlus applications to end users. The guide discusses the implementation of Microsoft Office 365 ProPlus in a VMware Horizon 7 environment using the shared computer model with Shared Computer Activation and provides tips and best practices that can improve performance and

application manageability.

## Additional Resources

For more information, you can explore the following resources:

- What is Office 365?

- Microsoft Office 365 Support

- Microsoft Office 365 ProPlus

- Microsoft Office 2016 Administrative Template files and Office Customization Tool

- Office Deployment Tool

- Microsoft Office Administrative Template Files

- Microsoft Office 365 Determine the deployment method to use

- Microsoft Office 365 Identity and Azure Active Directory

- Microsoft Office 365 Plan Options

- Microsoft Office 365 Client Configuration Service

- Microsoft Office 365 Network planning and performance tuning

- Microsoft Office 365 Network and migration planning

- Microsoft Support and Recovery Assistant

- OneDrive Sync App

- Configuration options for the Office Deployment Tool

- Troubleshoot issues with shared computer activation for Office 365 ProPlus

- FSLogix Overview

- Download and Install FSLogix

- Configure FSLogix Office Container

- Configure FSLogix Profile Container

- Microsoft FSLogix Entitlement Requirements

- Integrating FSLogix Profile Containers with the VMware Horizon Just-In-Time Management Platform (JMP)

- VMware App Volumes

- VMware App Volumes Documentation

- VMware App Volumes Provisioning Recipe for Microsoft Office 365

- VMware Horizon 7 Activity Path

- VMware Horizon 7 Content on TechZone

- VMware Horizon 7 Documentation

- VMware Horizon Support Center

- VMware Workspace ONE Access

- VMware Identity Manager Integration with Office 365 for Single Sign-on and Provisioning

- VMware Knowledge Base

- VMware OS Optimization Tool

- VMware Dynamic Environment Manager Activity Path

- VMware Dynamic Environment Manager Documentation

## Change Log

The following updates were made to this guide.

| Date | Description of Changes |
|------|------------------------|
| 2020-02-10 | • Updated requirements, tips, procedures, and additional resources.<br>• Rebranded VMware Identity Manager and User Environment Manager. |

# Authors and Contributors

## Authors

- Chris Halstead, EUC Staff Architect, End-User-Computing Technical Marketing, VMware

- Cindy Heyer Carroll, Technical Writer, End-User-Computing Technical Marketing, VMware

## Contributors

- Josh Spencer, EUC Staff Architect, End-User-Computing Technical Marketing, VMware

- Frank Anderson, VMware Alumni

## Reviewers

- Jim Yanik, Senior Manager in End-User-Computing Technical Marketing, VMware

- William Uhlig, EUC Private Sector C1 Solutions Engineer, VMware

- Darren Hirons, Senior Solution Engineer, VMware


To comment on this paper, contact VMware End-User-Computing Technical Marketing
at euc_tech_content_feedback@vmware.com.

**vm**ware®