VMware Horizon FLEX Solution Brief

VMware Horizon FLEX 1.8

WHITE PAPER

vmware®

Table of Contents

What Is VMware Horizon FLEX?

Traditionally, IT administrators have protected corporate data and applications and controlled costs by providing workers with company-issued, Windows-based laptops or desktops and by defining how and from where workers could access corporate applications and data.

However, the evolving workforce of today puts new demands on IT administrators. Road warriors must be productive when disconnected from the corporate network. More and more users demand Macs, even in organizations where Windows is the corporate computing standard. In addition, many companies are moving a significant percentage of their workforce from permanent to temporary or contract roles, eliminating traditional IT controls over corporate applications and data.

VMware Horizon® FLEX™ is a policy-based, containerized desktop solution that allows IT administrators to create, secure, and manage local desktops to meet the needs of workers with their own computers, road warriors, and Mac users in the enterprise. End users work within a restricted virtual machine on their endpoints and can be either connected or disconnected from the enterprise network.

Horizon FLEX is a combination of existing VMware products, with additional beneficial features. Horizon FLEX is composed of VMware Fusion® Pro, VMware Workstation Player™, VMware Mirage™ for Horizon FLEX, and the new Horizon FLEX Policy Server. The Horizon FLEX Client is composed of Fusion Pro and Workstation Player.

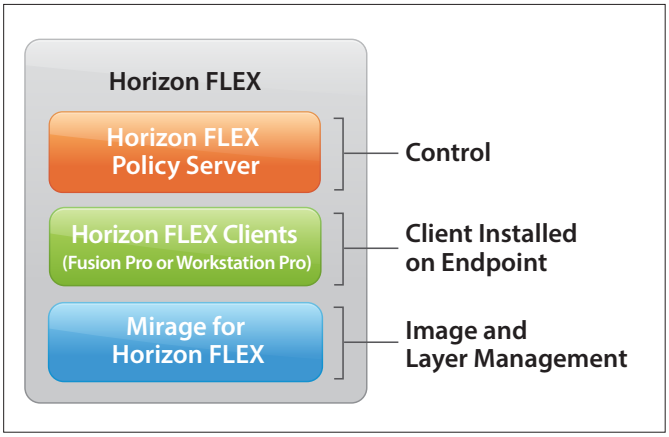

Figure 1: Horizon FLEX Package

With the Horizon FLEX package, administrators can create multiple restricted virtual machines (Horizon FLEX virtual machines) and entitle them to a variety of end users.

The Horizon FLEX solution complements existing VMware virtual desktop infrastructure (VDI) environments by allowing administrators to cater to both online and offline user requirements. Because the Horizon FLEX virtual machine is stored locally, corporate applications are accessible to the user even when offline.

With the Horizon FLEX virtual machine, IT can resolve the challenges presented by the intermittent network disconnection of bring-your-own-PC (BYOPC) and mobile users, while continuing to provide VDI desktops to other users.

Terminology for Horizon FLEX

The following terminology is used throughout this brief.

- **Horizon FLEX Client** – Combination of Fusion Pro and Workstation Player on the endpoint. The user connects to the Horizon FLEX Policy Server with the Horizon FLEX Client. One license key is used for both Fusion Pro and Workstation Player.
- **Fusion Pro** – Fusion Pro enables a user to connect to a restricted virtual machine from a Mac endpoint. In addition, the administrator creates a restricted virtual machine with Fusion Pro.

  Note: You can also use VMware Workstation Pro™ to create a Horizon FLEX virtual machine, but it is not included in the current Horizon FLEX bundle.
- **Workstation Player** – Workstation Player enables a user to connect to a restricted virtual machine from a Windows endpoint.
- **Mirage for Horizon FLEX** – The standard Mirage server that provides optional image management. The layering technology allows administrators to easily manage, back up, and patch virtual machine desktops.
- **Horizon FLEX Policy Server** – Handles the restricted virtual machine functionality. The administrator applies policies with the Horizon FLEX Policy Server.
- **Restricted virtual machine** – The administrator creates a restricted virtual machine with Fusion Pro. The user downloads this restricted virtual machine to a physical machine.
- **Horizon FLEX virtual machine or source virtual machine** – Other terms for the restricted virtual machine.
- **Host** – The physical computer on which the Horizon FLEX Client is installed.
- **Guest OS** – The operating system installed on the restricted virtual machine.
- **Guest content** – The applications and user data and settings installed on the restricted virtual machine.
- **Entitlement** – The assignment of restricted virtual machines to users. The administrator entitles Active Directory users and groups through the Horizon FLEX Policy Server. Users can access their entitled virtual machines from their Horizon FLEX Clients.

Key Benefits of Horizon FLEX

Using Horizon FLEX, administrators can

- Embrace Macs in the enterprise
- Enable offline productivity by providing users with corporate desktops that run locally on Windows or Mac endpoints
- Retain control of corporate applications and data by using policies to control USB device access, and copying and pasting
- Easily manage and maintain virtual machines using a centralized console
- Accommodate temporary workers and contractors with policy-based desktop expiration dates and remote lock

Remote lock is one of the exciting features that Horizon FLEX introduces. Remote lock allows administrators to instantly lock out a virtual machine and make it inaccessible to the user. This feature is useful in a scenario in which a user's contract expires prematurely.

Deploying Horizon FLEX

To access the restricted virtual machine, the user must first install the Horizon FLEX Client (Fusion Pro or Workstation Player) on a Mac or Windows endpoint. The user can then launch the Horizon FLEX Client to connect to the Horizon FLEX Policy Server and download the restricted virtual machine.

The administrator can mass-deploy the Horizon FLEX Client to Mac or Windows endpoints with standard package deployment tools, such as

- Apple Remote Desktop
- JAMF Casper Suite
- Microsoft System Center 2012 Configuration Manager

Note: You can include a restricted virtual machine as part of the deployment package.

Supported Host Operating Systems for Horizon FLEX

Users can run the Horizon FLEX Client and access their Windows corporate virtual machine from the following 64-bit host operating systems:

- Windows 7, Windows 8.1, and Windows 10
- Mac OS X 10.9, Mac OS X 10.10, and Mac OS X 10.11

Supported Guest Operating Systems for Horizon FLEX

Although Windows is the corporate standard, administrators can install either Windows or Linux in the guest operating system.

Following is a list of the supported guest operating systems in the Horizon FLEX desktop:

- Windows XP (32- and 64-bit), Windows 7 (32- and 64-bit), Windows 8.1, Windows 10, and Windows Server 2012 R2
- Ubuntu 14.04 and Ubuntu 15.10

Network Specifications for Horizon FLEX

The Horizon FLEX solution allows users to run corporate applications even when disconnected from the network. Virtual desktops are stored locally for a complete desktop experience that does not require a network connection.

A network connection between the Horizon FLEX Policy Server and the Horizon FLEX Client is required *only* in the following scenarios:

- For the initial download of the FLEX virtual machine
- To receive virtual machine restriction and policy updates

Note: You can also manage and update guest content if you use Mirage for Horizon FLEX. Users must connect to the network to receive updates to guest content.

The administrator specifies a download location (URL) for the Horizon FLEX virtual machine. The Horizon FLEX Policy Server must be accessible via HTTPS to the Horizon FLEX Client for the end user to download the virtual machine. After the user powers on the virtual machine and logs in, the user can access the virtual machine offline.

The administrator can also specify the number of days that the virtual machine can run without connecting to the Horizon FLEX Policy Server. When the time period is reached, the virtual machine is not usable. When the user regains access to the network, updates to the guest OS or virtual machine policies are applied.

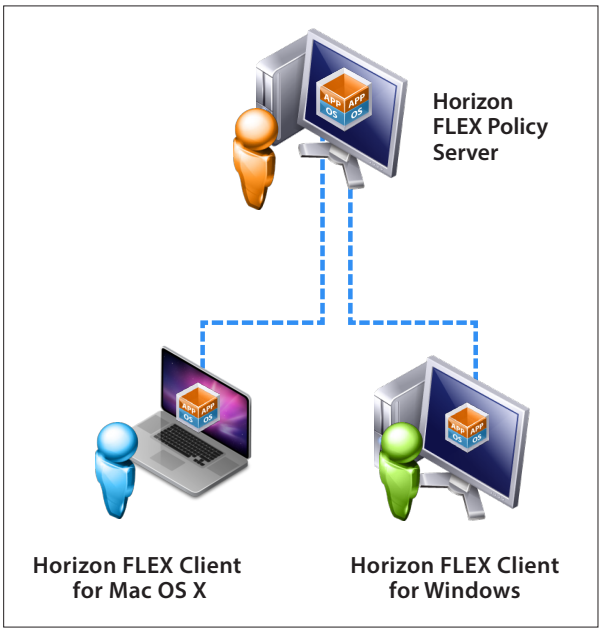

Figure 2: Horizon FLEX Policy Server for Central Management of Desktops

Administrative Functions in the Horizon FLEX Policy Server

You can manage and control containerized desktops with the new Horizon FLEX Policy Server. After the Horizon FLEX license has been applied to Mirage for Horizon FLEX, the Horizon FLEX Policy Server is activated.

Administrators can perform a myriad of tasks, including

- Manage an inventory of restricted virtual machines
- Browse a list of users and groups in the Active Directory service
- Entitle users and groups to one or more restricted desktops
- Specify virtual machine policies for a given entitlement
- Prevent user access to restricted virtual machines with remote lock
- Examine virtual machine details and status at any given point in time

Restricted Virtual Machine Policies

The administrator can define a specific set of policies for a Horizon FLEX virtual machine from the Horizon FLEX Policy Server Web management user interface.

Figure 3 shows the New Policy window and the various policy and restriction settings. Details of these policies follow.

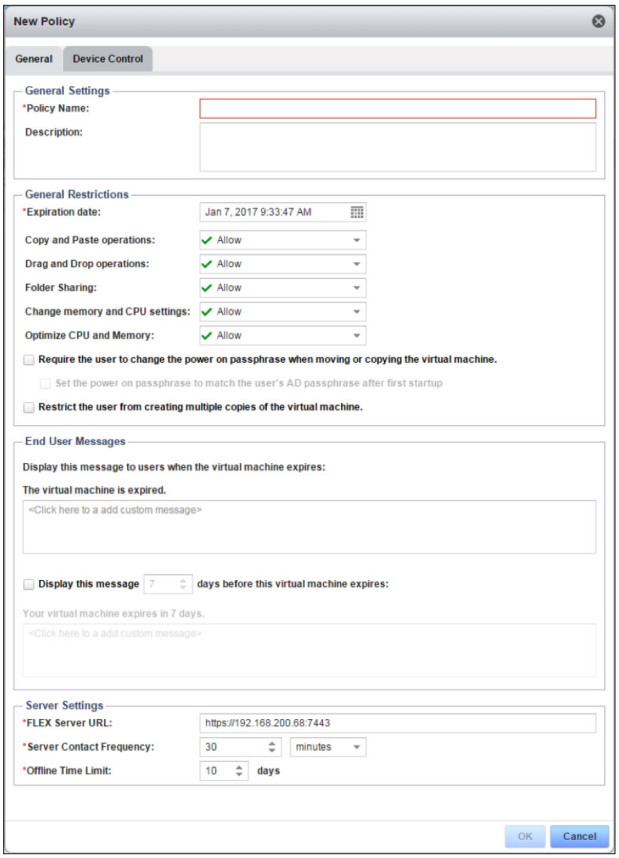

Figure 3: New Policy Window in the Horizon FLEX Policy Server

General Settings in New Policy Window
General Settings include setting a **Name** and **Description** for the virtual machine policy.

General Restrictions in New Policy Window
General Restrictions apply to all users entitled to a virtual machine. Field explanations follow.

- **Expiration date** – You can configure the virtual machine to expire at a specific date and time.
- **Use of USB devices** – You can allow or block USB device access in the virtual machine. You can also allow only specific USB classes or devices.
- **Copy and Paste operations** – You can control copy-and-paste and drag-and-drop functionality between the host and the virtual machine.
- **Drag and Drop operations** – You can control drag-and-drop functionality between the host and the virtual machine.
- **Passphrase** – You can choose whether to require the user to change the power-on passphrase when moving or copying the restricted virtual machine.
- **Single instance** – You can prevent the user from using a second copy of a virtual machine.
- **CPU and memory** – You can give permission to end users to edit the CPU and memory settings for the virtual machines. You can also set the virtual machine to automatically optimize itself based on the host system's resources.

End User Messages in New Policy Window
In End User Messages, the administrator can choose to do the following:

- Display an expiration message to the user when the virtual machine expires
- Display a warning message to the user before the virtual machine expires
- Set the number of days before expiration that the warning message is shown

Server Settings in New Policy Window
Server settings apply to the Horizon FLEX Policy Server. Field explanations follow.

- **FLEX Server URL** – Specify the URL and port number for the Horizon FLEX Policy Server.
- **Server contact frequency** – You can specify how frequently in minutes, hours, or days the Horizon FLEX Client must check the Horizon FLEX Policy Server for policy updates. The virtual machine always attempts to contact the Horizon FLEX Policy Server at the specified time, but policy updates are retrieved only when the user is online. If this time is exceeded, the virtual machine uses the last retrieved policy set.
- **Offline Time Limit** – You can specify how long the virtual machine is allowed to run without contacting the Horizon FLEX Policy Server. This period must be greater than the server contact frequency. If this time is exceeded, the user receives a warning message, and the virtual machine becomes inaccessible. When the virtual machine can contact the Horizon FLEX Policy Server, the virtual machine again becomes accessible. The administrator does not need to reactivate the virtual machine.

Applying Security Measures

The administrator can apply security measures to a Horizon FLEX virtual machine. The Wipe feature is used to delete a virtual machine from a user's desktop so that its data is lost, and the Lockout feature prevents a user from accessing a virtual machine.

Figure 4 shows the Wipe button that is available from the Virtual Machines tab on the Horizon FLEX Policy Server Web management user interface, and Figure 5 shows the Lockout button.

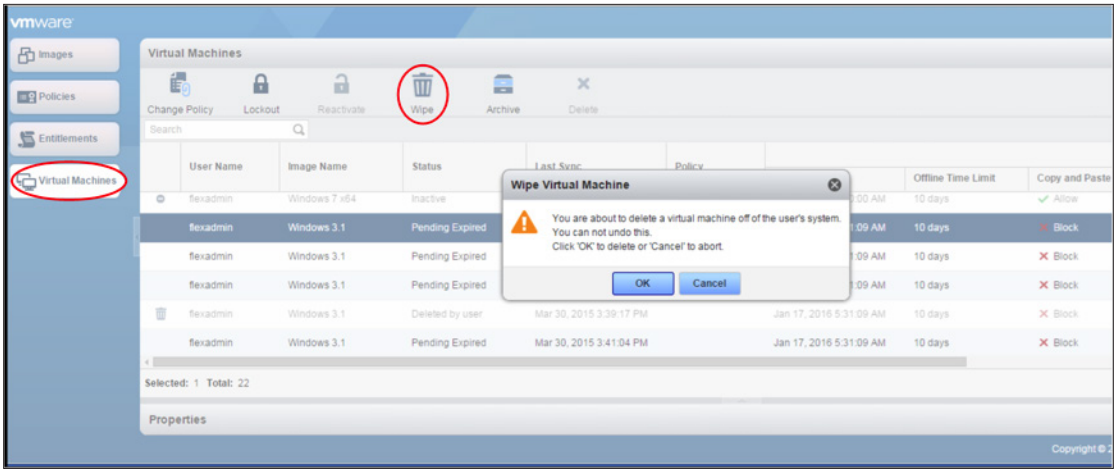

Figure 4: Wipe Feature in the Horizon FLEX Policy Server

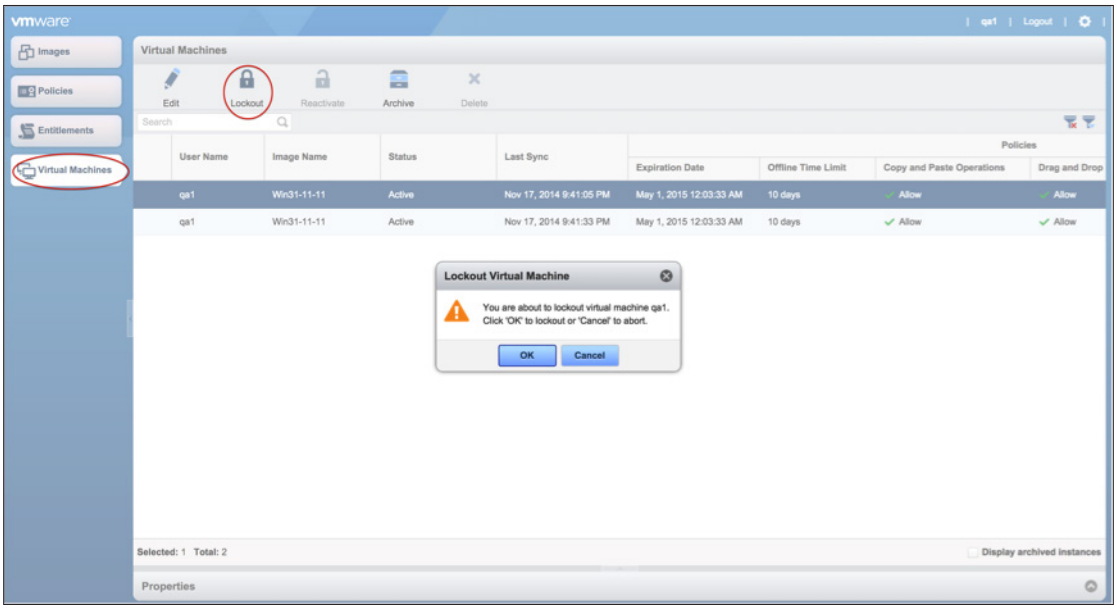

Figure 5: Lockout Feature in the Horizon FLEX Policy Server

The administrator logs in to the Horizon FLEX Policy Server Web management user interface to wipe or lock out a restricted virtual machine.

Procedure to Apply a Security Measure

1. Log in to the Horizon FLEX Policy Server Web management user interface.
2. Click the **Virtual Machines** tab.
3. Select a restricted virtual machine.
4. Click either **Wipe** or **Lockout**.
5. Click **OK** to confirm the security measure.

The status of this virtual machine changes to either Pending Wipe or Pending Lockout. Upon next contact with the Horizon FLEX Policy Server, the virtual machine is deleted or locked out.

Basic Administrator and User Workflows for Horizon FLEX

Horizon FLEX allows administrators to centrally manage and maintain restricted virtual machines while users access these virtual machines locally. Details of basic administrator and user workflows follow.

Administrator Workflow

The administrator prepares a restricted virtual machine for the user, as outlined in Figure 6.

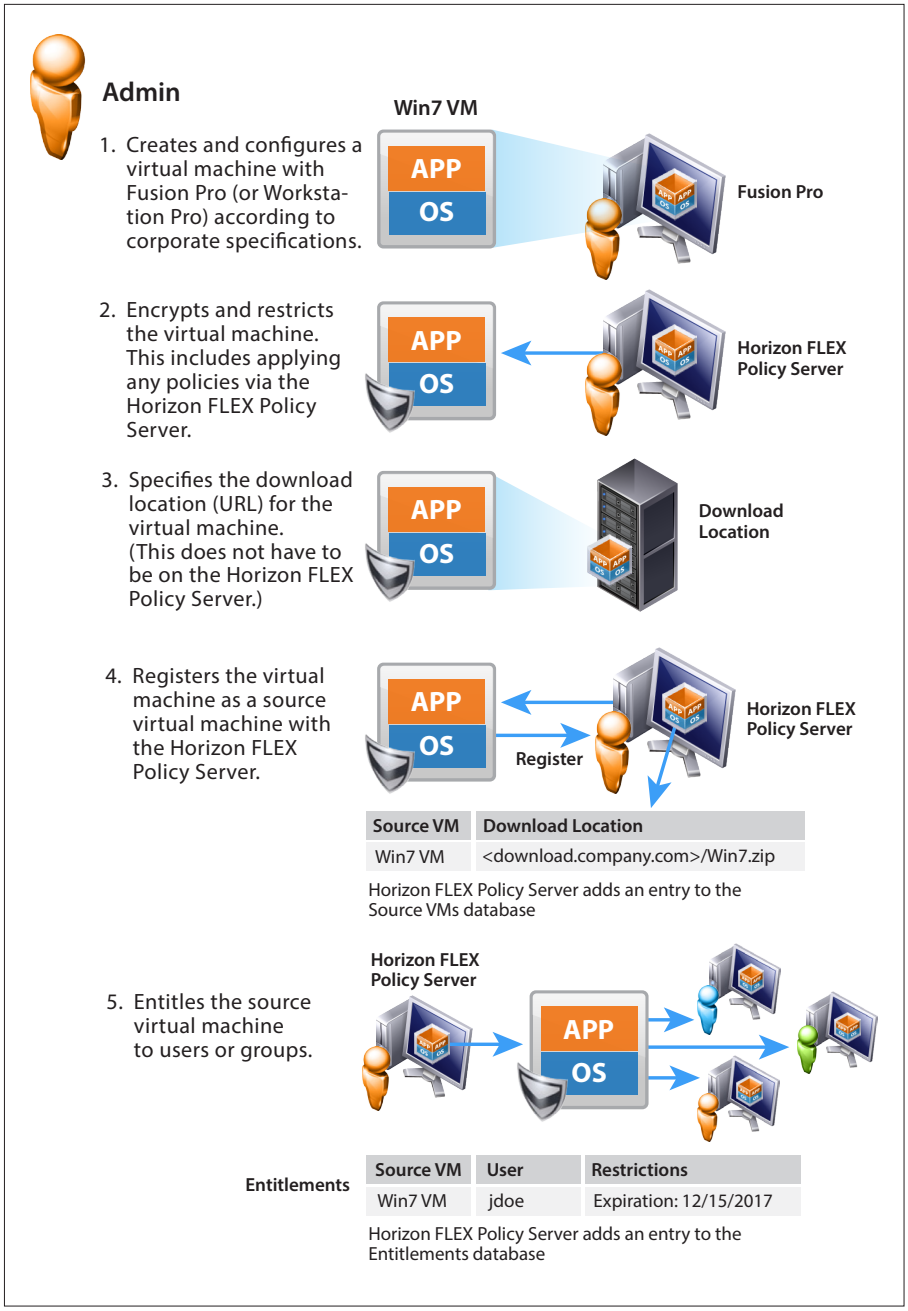

Figure 6: Administrator Workflow

User Workflow

The user can access the restricted virtual machine as illustrated in Figure 7.

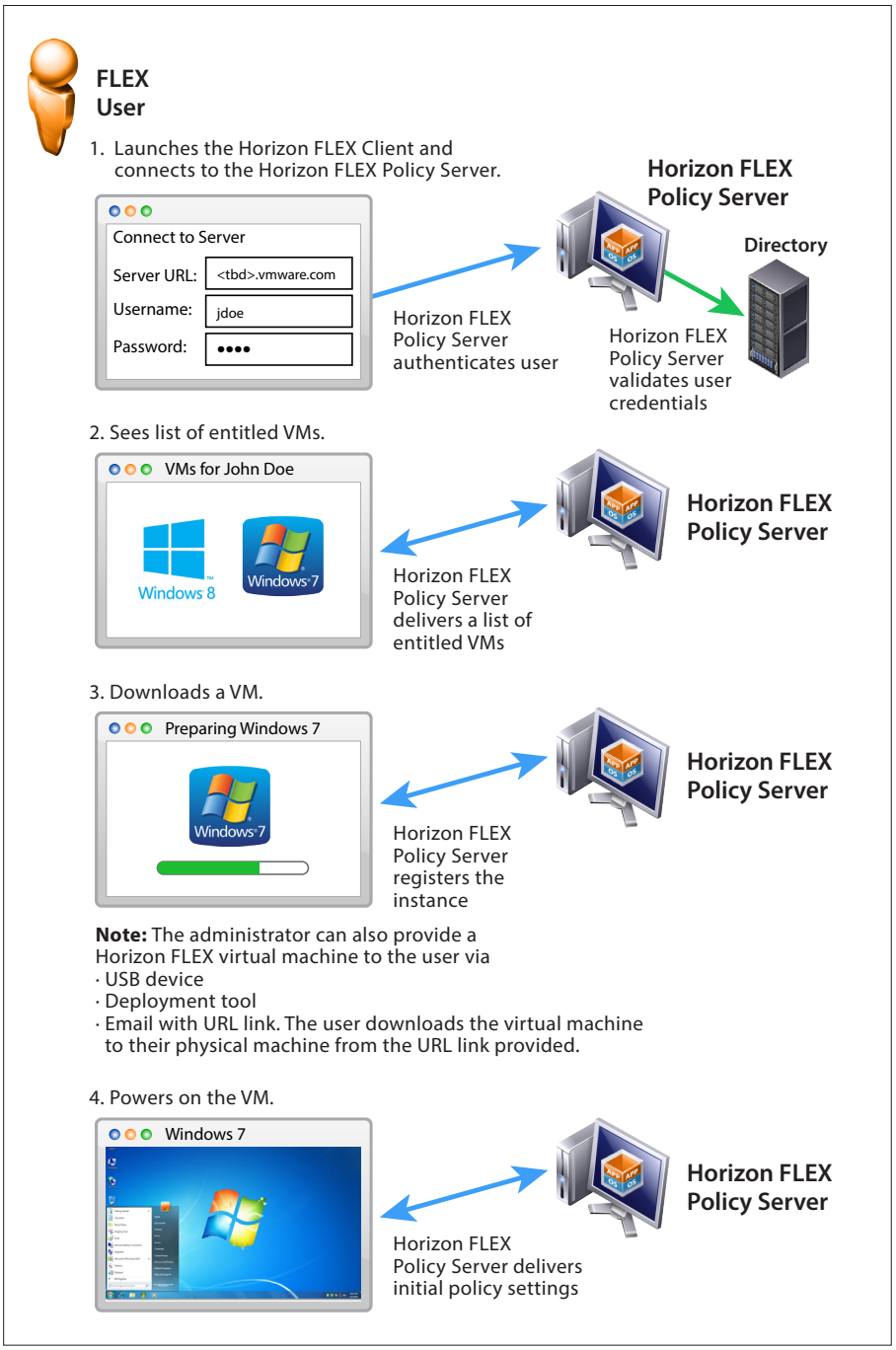

Figure 7: User Workflow

Use Cases

Horizon FLEX solves a broad number of enterprise use cases:

- **Bring Your Own PC (BYOPC)** – Supports employees using their own computer for work, or those employees assigned a Mac at work even though a Windows computer is "standard issue."
- **Temporary or contract workers** – Enables temporary or contract workers to access the applications and data they need while protecting corporate data, especially if users have their own computers and might not always work onsite.
- **Disconnected workers** – Supports employees who are not always connected to the corporate network, for example, road-warrior sales reps, or consultants or employees working from home.
- **Regional office workers** – Supports workers in regional offices who need to exchange confidential information with the home office using a standard set of corporate applications.
- **Development and training** – Supports development, testing, and training efforts that require an isolated environment that is hardware- and operating-system–agnostic.

Bring Your Own PC

IT administrators are forced to support a heterogeneous environment with the recent BYOPC revolution. IT can no longer define the rules when it comes to hardware type or how users access the corporate network. Employees want flexibility to choose their own personal machine, and many of these are Macs. In an effort to reduce costs, companies might not want to provide laptops to new employees. Supporting different user machines presents challenges in terms of security and data protection.

CHALLENGE	SOLUTION
User support – Employees want flexibility to use their own computers for work, and more and more of these computers are Macs. IT administrators are forced to support multiple user environments (Windows and Macs), and companies do not have time or budget to up-skill Windows IT staff.	Users can run a standardized, corporate Windows desktop on their own Mac or Windows machines, eliminating the need to provide support for Mac OS X. From a centralized server, IT can manage and maintain the Horizon FLEX Windows virtual machine without impacting the native OS on the endpoint.
Security risk – Personal machines pose security risks. Granting access to the corporate network allows users to access corporate applications and potentially capture sensitive data.	IT administrators can create restricted and encrypted virtual machines, reducing security concerns. The virtual machine is locked down and can be set to expire when the contract expires, protecting corporate applications and data. Copy-and-paste functions can also be restricted, along with USB access.

Temporary or Contract Workers

Increasingly, many companies employ temporary and contract workers. These workers often have their own laptops and work from home, making it difficult for IT administrators to maintain security.

CHALLENGE	SOLUTION
Data access – Granting corporate access to contractors poses security risks if users launch corporate applications from their personal computers. After a contract has expired, the applications remain on the user's machine, allowing them to capture sensitive data.	IT administrators can create restricted and encrypted machines, reducing security concerns. The desktop is locked down and can be set to expire at a predefined date and time, thus protecting corporate applications and data. As an increased security measure, the Horizon FLEX virtual machine can be "poison-pilled" at any time. Copy-and-paste functions can be restricted, along with USB access. If the contract is renewed, administrators can also renew the virtual machine, saving time and effort.

Disconnected Workers

Some companies have a large mobile workforce. Workers who travel frequently, like sales representatives and consultants, are often unable to get secure network access to corporate data and applications. In some organizations, managing an ever-growing client list can also pose issues.

CHALLENGE	SOLUTION
Remote and offline workers – Road warriors are unable to get secure network access to corporate data and applications needed for client appointments.	Road warriors have a local desktop, allowing them to leverage corporate data and applications even when offline, turning downtime into productive time. When the user is back online, updates to policies or the Horizon FLEX virtual machine are applied.
Isolate and safeguard client data – Over time, adding clients and files increases file management complexity for users and makes it harder to find the appropriate file for a client when needed.	IT can provide consultants with one or more Horizon FLEX virtual machines per physical machine. Consultants can allot one virtual machine to each client, making it easier to isolate, manage, maintain, and locate client files and applications.

Regional Office Workers

Regional offices, dealerships, and franchises might need to create and submit confidential reports, like revenue or inventory, to other regional offices or to the central office. These regional offices might also need a way to maintain reports locally. IT staff might not be available in every branch to ensure that security policies are enforced.

CHALLENGE	SOLUTION
Regular reports with confidential data – Regional offices need to send regular confidential reports to the head office while maintaining consistency across all branches. However, a regional office might not have IT staff onsite to support or reinforce security best practices, exposing the organization to potential risk.	IT can provide each regional office with a restricted, encrypted desktop that contains the applications needed to provide the head office with required reports. Horizon FLEX includes policies that can be applied to a local virtual machine to secure those reports, including restrictions on USB device access and copying and pasting.

Development and Training

Development, testing, and training efforts often require an isolated environment that is hardware- and operating-system–agnostic. Providing a consistent training environment presents a challenge as more schools adopt a BYOPC approach. In addition, developers and testers might require a Linux environment but still need access to Windows-based productivity tools.

CHALLENGE	SOLUTION
Isolated environment – Companies providing large-scale training, universities and schools, and developers and testers all need an isolated environment in which to perform their tasks. More and more of these users prefer to use Macs, but still require Windows-only applications.	Horizon FLEX can deliver preconfigured applications, tailored for a specific class in an isolated, locked-down virtual machine. Users have the flexibility of running this restricted virtual machine on their own machine or on one provided for them. Engineers can use native Windows tools and applications on a machine of their choice.

Summary

VMware Horizon FLEX is a containerized desktop solution that allows businesses to accommodate emerging modes of working, such as BYOPC, temporary or contract workers, and disconnected users. Organizations can deploy and control standardized Windows virtual machine desktops to groups of employees, a challenge that has been difficult or costly to address. IT can now give Mac users, contractors, and disconnected workers access to a secure corporate desktop in a cost-effective package without sacrificing security and corporate compliance.

IT administrators can create, secure, and manage restricted virtual machines from a centralized location, while users run their virtual machines locally. Horizon FLEX complements and extends an existing VDI environment, allowing flexibility for a broad spectrum of users.

The VMware Horizon FLEX solution offers you

- Secure delivery of a Windows virtual machine desktop on any Mac or Windows computer, managed from a single solution
- Horizon FLEX Policy Server to enforce corporate compliance
- Management of virtual machines from a centralized server without impacting the host OS on the endpoint
- Robust security features and granular control with restricted and encrypted virtual machines
- Desktops that can be used with or without a network connection
- Virtual machine expiration dates and remote lock

Author and Contributors

Andy Morris, Senior Product Line Marketing Manager, End-User Computing, VMware, revised this paper to update the supported host and guest operating systems in Horizon FLEX 1.8. Gina Daly, Technical Writer in End-User-Computing Technical Marketing, VMware wrote the original version of this paper.

Contributors to this document include

- Surendra Gupte, Staff Engineer, Personal Desktops, End-User Computing, VMware
- Nicolas Rochard, Director, Product Marketing, End-User Computing, VMware
- Nannette Vilushis, Senior Product Marketing Manager, End-User Computing, VMware
- Kristina De Nike, Product Line Manager, End-User Computing, VMware

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

Additional Resources

For more information, see the Horizon FLEX product Web page.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com