# Configuring Kiosk Mode

## VMware Horizon 6.0 with View

WHITE PAPER

vmware®

## Table of Contents

# Introduction

Many organizations provide interactive customer kiosks in public places where users can perform specific tasks without having to log in. VMware Horizon® with View supports this "anonymous use" functionality with View kiosk mode. Endpoint devices configured as kiosk clients display View virtual desktops and allow users to perform a limited set of functions specified by the Horizon administrator.

## How Kiosk Mode Works

Kiosk mode associates a View virtual desktop with the MAC address or client ID of a kiosk endpoint device rather than with a user's login credentials. The endpoint device can be a zero client, a thin client, or a locked-down PC running either Windows or Linux.

When a kiosk user activates an input device—for instance, by pressing a key or clicking a mouse button—the kiosk client contacts a View Connection Server. The View Connection Server authenticates the client, connects it to a View virtual machine running in kiosk mode, and launches a remote desktop session. The session is then displayed on the endpoint device.

The kiosk user is normally presented with a session that displays either a View desktop with a limited set of applications or a single, dedicated application that appears to be running on the kiosk endpoint. The infrastructure is user-transparent.

With View kiosk mode

- Users do not have access to the operating system or file system of the View desktop.
- No user authentication is required.
- No user data is preserved.
- There is no need for persistent virtual desktops.

These considerations mean that kiosk functionality can be provided at low cost, with inexpensive endpoints, non-persistent virtual desktops, and no additional storage. Very little is required of IT resources beyond initial setup and provisioning.

## Authentication

Using MAC addresses or client IDs to associate View virtual desktops with kiosk *devices* rather than with *users* simplifies the authentication model.

Although kiosk users might be required to provide authentication information for certain applications, they do not ordinarily log in to the View desktop. In most cases, they simply use the session or application that is presented to them.

In some circumstances, however, an administrator might require all kiosk users to log in to the View desktop with the same, predetermined username and password. This scenario can be desirable when use of the kiosk or an application is restricted to a known set of users, such as company employees or registered students, but is not available to the general public. In this case, people who know the password can use the kiosk, but these users are not identified by personal credentials.

Because kiosks are usually placed in public locations, kiosk mode is not recommended for transactions that require transfer of sensitive information, such as credit card numbers, user email addresses and passwords, or patient records.

For general information on View security, including comments about kiosk mode, see the VMware Horizon with View Security Hardening Overview.

### Supported Features and Limitations

Commonly used View features supported in kiosk mode include

- USB redirection – When a client session for a kiosk desktop is established, USB peripherals attached to a client endpoint are connected immediately to the View desktop.
- Printing – Virtual printing is enabled by default.
- Multiple monitors – Kiosk endpoints are not usually set up with multiple monitors, but kiosk mode supports the capability by distributing the remote View desktop across all monitors attached to the kiosk endpoint. Kiosk users cannot alter the display mode.
- Flash URL redirection – Flash content can be streamed from Adobe Media Servers to kiosk endpoints.
- Multimedia redirection (MMR) – Multimedia content can be streamed to kiosk endpoints.

The following limitations apply to View kiosk mode:

- Real-Time Audio-Video (RTAV) is supported on many thin clients and PCs but is not supported on zero clients.
- Hosted applications that use Remote Desktop Services (RDS) servers are not supported in kiosk mode.
- Configuration of kiosk mode on View desktops hosted on Remote Desktop Session Host (RDSH) servers requires a custom user account (see step 7 under Configuring Clients).

# Planning and Preparation

Use the following guidelines to set up the View environment and to prepare for configuration of the kiosk client AD accounts:

- Determine the purpose, type, and location of the kiosk endpoints.
- Prepare the hardware for the kiosk endpoints, if necessary.
- If using PCs as kiosk endpoints, install Horizon Client software.
- Attach USB peripherals, if any, to the kiosk endpoints.

The instructions for setting up View desktops in kiosk mode are similar to those for setting up other non-persistent View desktops. Additional steps needed to configure clients in kiosk mode are described in the following sections:

- Preparing Active Directory for Kiosk Mode
- Preparing Desktops for Kiosk Mode
- Configuring and Connecting Kiosk Clients

# Kiosk Client Device Types

Most traditional desktop and portable computing devices, such as PCs, have memory and storage capabilities as well as processors, and they can function whether connected to a network or not. Zero clients have no memory or storage and only limited processing ability, and they can function only with a network connection. Thin clients also depend on a network connection, but they often have some software installed on them, such as an operating system or device drivers.

Thin and zero clients are less expensive to acquire than PCs, and their maintenance cost is minimal. In some settings, however, such as public libraries, it can be more economical to repurpose old PCs as kiosks than to buy new hardware.

PCs have more local processing power than thin or zero clients, but they also require maintenance and tend to be less secure. For a more detailed discussion of types of clients, see Key Considerations in Choosing a Zero Client Environment for View Virtual Desktops in VMware Horizon and the VMware Compatibility Guide.

# Setting Up the View Environment

In most cases, kiosks are added to an existing View deployment. If the View environment is not yet set up, refer to the following documentation:

- View Installation
- Setting Up Desktop and Application Pools in View
- Reviewer's Guide for View in Horizon 6

## Preparing Active Directory for Kiosk Mode

As a best practice, do not use the same View Connection Server to handle both a production environment and clients in kiosk mode. Instead, use dedicated View Connection Server instances, and create dedicated organizational units (OUs) and groups in Active Directory for kiosk client accounts. This practice simplifies client configuration and can help to prevent intrusions.

For more detailed information, see *Prepare Active Directory and View for Clients in Kiosk Mode* in View Administration and *Create an OU for View Machines* in Setting Up Desktop and Application Pools in View.

## Preparing Desktops for Kiosk Mode

To prepare View desktops to run in kiosk mode

1. Create a virtual machine template for the guest operating system as explained in *Creating Virtual Machine Templates* in the Setting Up Desktop and Application Pools in View guide.
2. Install the View Agent on the virtual machine template.

   The View Agent Virtual Printing component includes the ThinPrint driver.

   Virtual printing does not require installation of printer drivers on the remote View desktop. For more information, see Configuring Printing.

   Because kiosk passwords are usually unknown, kiosks should not be shut down automatically in most settings. To enable user access to the kiosks at any time, configure the guest Windows OS so that clients are never locked when left unattended.

3. In View Administrator, create a floating-assignment desktop pool.

   On the Desktop Pool Settings page, select **Refresh Immediately** in the **Delete or refresh machine on logoff** option. This option prevents inadvertent changes in settings from being preserved and applied for future kiosk users. Other desktop pool settings include whether to log out automatically after the session disconnects.

4. Entitle the kiosk client or group to this desktop pool.

   If requiring kiosk users to log in with the same credentials, create an Active Directory group for the kiosks they can access. It is easier to identify kiosk clients by their group name than by individual MAC addresses. Setting up an AD group for kiosks is optional, but the kiosk clients must have entitlement to the pool regardless of whether users are required to log in with a password.

   For more information, see *Pools for Kiosk Users* and *Add Entitlements to a Desktop or Application Pool* in the Setting Up Desktop and Application Pools in View guide.

5. Install the kiosk application or applications, if any, on the View desktop virtual machine template.

   For information on associating VMware ThinApp applications with the desktop pool, see Assigning ThinApp Applications.

6. Configure View policies and group policy objects (GPOs), for instance to enable or disable USB devices.

   For more information, see *Setting Policies in View Administrator* and *Configuring Settings for Client Sessions* in the View Administration guide.

# Configuring and Connecting Kiosk Clients

Horizon Client software is pre-installed on many thin and zero clients. See the VMware Compatibility Guide for a current list of compatible units, or contact the vendor for Horizon Client updates. To use PCs instead of thin or zero clients as kiosk endpoints, install Horizon Client on each PC.

To perform configuration tasks such as establishing communication, setting up applications, and assigning custom Client IDs instead of using MAC addresses, use View Administrator on the View Connection Server. No View or kiosk configuration tasks are performed on the endpoint devices except for installation of Horizon Client software where necessary.

Use the `vdmadmin` command with the `-Q` option from the View Connection Server to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and to display information about their configuration. The `vdmadmin` directory location is automatically set in the system PATH: `C:\Program Files\VMware\VMware View\Server\tools\bin`.

For help with the `vdmadmin` command, type

```
vdmadmin -help
```

## Configuring Clients

Perform the following steps to configure clients in kiosk mode.

1. Set default values for the organizational unit (OU), password expiration, and group membership of clients in kiosk mode. For example:

   ```
   vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=MYORG,DC=com"
   -noexpirepassword -group kc-grp
   ```

2. Verify that the defaults are set.

   **vdmadmin -Q -clientauth -getdefaults**

3. To create an account for a client based on its MAC address, use the appropriate command to discover the MAC address. Skip this step if using a custom account name.

   Windows client:

   **C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe printEnvironmentInfo**

   Linux client:

   **vmware-view -printEnvironmentInfo -s *connection_server***

4. Add accounts for clients in kiosk mode.

   The View Connection Server creates a user account and password for each client based on the client's MAC address, which it uses to authenticate the client when connecting it to the View desktop. From the administrator's point of view, it is usually more convenient to establish a client ID that assigns a name to the client than to use the MAC address.

   Either use the **vdmadmin** command to create a client ID using the kiosk endpoint's MAC address, or create an account name with up to 20 characters, beginning with the string **custom-**.

   The following example adds an account for a client specified by its MAC address, with an automatically generated password that never expires.

   **vdmadmin -Q -clientauth -add -domain *MYORG* -clientid 00:10:db:ee:76:00 -group kc-grp -genpassword -noexpirepassword**

   The following example adds an account for a named client in the specified OU group, and specifies a password to be used with the client. Any kiosk user can use this password, but it is ordinarily distributed only to a restricted group of users.

   **vdmadmin -Q -clientauth -add -domain *MYORG* -clientid custom-csh1 -ou "ou=kou,DC=*MYORG*,DC=com" -password "VMware1!"**

5. Enable authentication of clients in kiosk mode for each View Connection Server instance, as in the following example:

   **vdmadmin -Q  -enable -s *connection_server***

6. Verify the configuration of kiosk clients, for example:

   **vdmadmin -Q -clientauth -list**

7. For RDSH servers, entitle the client account to the View desktop by logging in to the RDSH server and adding the account name to the RDS Kiosk Users group: **Control Panel** > **System and Security** > **System** > **Remote settings** > **Select users** > **Add**.

## Connecting Clients

By default, the account name is based on the MAC address of the kiosk endpoint and has an automatically generated password. To assign a client ID instead of the MAC address, specify the client ID in the form *custom-xxxxx*.

For example, to connect a Windows client with an assigned client ID and password:

**vmware view.exe -unattended -serverURL 192.168.13.245 -userName custom-csh1 -password "VMware1!"**

**Note:** It is not necessary to specify the **-userName** option for clients in kiosk mode when using the MAC address of the client device.

To connect a Linux client:

**vmware-view --kioskLogin --fullscreen --once --noninteractive --nomenubar -s *connection_server***

For information about using the **vmware-view** command, see *Running Horizon Client from the Command Line* in the Using VMware Horizon Client for Windows guide or *Using the Horizon Client Command-Line Interface and Configuration Files* in the Using VMware Horizon Client for Linux guide.

For zero clients and thin clients, contact the vendor for the kiosk mode options used to connect to the View Connection Server.

If the View Connection Server successfully authenticates the kiosk client, and a View remote desktop is available, the View Connection Server starts a remote session and displays it on the kiosk endpoint.

For more information about command-line options for kiosk mode, see *Setting Up Clients in Kiosk Mode* and *Configuring Clients in Kiosk Mode Using the -Q Option* in the View Administration guide.

# Optional Configuration Tasks

This section offers tips for setting up kiosk client accounts.

## Displaying Kiosk Client Accounts

The following command-line example shows how to display connected kiosk endpoints currently authenticated by the View Connection Server:

```
vdmadmin –Q –clientauth –list
Client Authentication User List
==========================================================================
GUID : acdbf1ea-91e8-4635-af67-1d68d2b0c977
ClientID : custom-gch1
Domain : vmware-view
Password Generated : false
GUID : af645bdb-e1be-44cb-a2c9-8d59aca95416
ClientID : custom-gch2
Domain : vmware-view
Password Generated : true
GUID : 89df116f-8d22-4945-8d81-e6325711c68e
ClientID : custom-gch3
Domain : vmware-view
Password Generated : true
GUID : 9948528a-76b8-4efa-a50c-ba1554ce5f4e
ClientID : cm-12_34_56_78_9a_bc
```

```
Domain : vmware-view
Password Generated : false
Client Authentication Connection Servers
=======================================
Common Name : VIEW-BROKER
Client Authentication Enabled : true
Password Required : false
```

## Removing Kiosk Client Accounts

The following example shows how to remove the client ID for a kiosk endpoint:

```
vdmadmin -Q —clientauth —clientid custom-csh1 —domain vmware-view —remove
Client authentication user was removed successfully.
```

The following example shows how to remove all client IDs:

```
vdmadmin -Q -clientauth —removeall
Are you sure you want to remove all Client Authentication users? YES/NO>: yes
```

## Assigning ThinApp Applications

Use View Administrator to distribute and manage applications that have been packaged with ThinApp. To have the kiosk endpoint access certain application groups, prepare the guest operating system with applications in the base image, or associate the ThinApp applications with the desktop pool. Kiosk mode supports both local and streaming deployment of ThinApp packages.

For more information, see *Managing ThinApp Applications in View Administrator* in the View Administration guide.

## Provisioning Desktop Pools and Creating Entitlements

The **vdmadmin** command does not support the configuration of entitlements. To create desktop pools and entitlements, use View Administrator on the View Connection Server.

## Configuring Policies for Kiosk Clients

Use View Administrator on the View Connection Server to manage desktop pools and configure kiosk client settings.

Configure specific kiosk endpoints with Windows GPOs and scripts, and add specific applications to the Windows startup application list.

If the kiosk has a physical keyboard, disable all function keys and keystroke sequences, such as Control+Alt+Delete, that can override kiosk mode.

### Configuring Automatic USB Redirection

Although access to USB devices is convenient, it can also expose the environment to data theft and malware. USB devices are currently enabled by default when the View desktop session is launched or the devices are plugged in. The following GPO policies are set to `true` at connection:

- **ConnectUSBOnStartup** – Connect all USB devices to the desktop on launch.
- **ConnectUSBOnInsert** – Connect USB devices to the desktop when they are plugged in.

To control which USB devices are redirected, configure GPO settings for the View Agent or Horizon Client. To disable USB devices, set the USB Access policy to `Deny` in View Administrator. The default value for this policy is `Allow`. The USB Access settings in View Administrator override the USB connection settings for a client in kiosk mode.

For more information, see *View Policies* in the View Administration guide, *Overview of Setting Up USB Redirection* in Setting Up Desktop and Application Pools in View, and USB Device Redirection, Configuration, and Usage in VMware Horizon with View.

### Configuring Printing

Virtual printing gives kiosk users access to local or network printers without requiring that additional printer drivers be installed in the View desktop. In virtual printing, the printers connected to the client are redirected to the View desktop.

To make virtual printing available to kiosk users, install the Virtual Printing component of View Agent, which includes the ThinPrint driver, on the View desktop. Kiosk users can set preferences for print quality, double-sided printing, and so on from their View desktop sessions.

## Summary

VMware Horizon with View offers a versatile kiosk mode to facilitate the use of unattended, self-service kiosks in public and semi-public locations where anonymous access to specific applications is required. Configuration options provide convenient user functionality at minimal acquisition (CapEx) and maintenance (OpEx) costs.

This paper describes View kiosk mode and provides references to more detailed material to help administrators and decision makers design and implement virtual kiosks.

# About the Authors and Contributors

Gary Sloane, Consulting Editor, VMware, and Karen Smith, formerly of VMware, updated this paper for Horizon 6 with View.

An earlier version of the paper was written by Cynthia Hsieh, formerly of VMware.

The following people helped to update and review this paper:

- Stephane Asselin, Senior End-User-Computing Architect, VMware
- Peter Brown, Senior Research and Development Manager, VMware
- Dean Flaming, Senior Technical Marketing Manager, VMware
- Rick Li, Senior Member of the Technical Staff, Enterprise Desktop Quality Engineering, VMware
- Jessica Lu, Technical Staff, Enterprise Desktop Quality Engineering, VMware
- Jack McMichael, Solutions Consultant, VMware
- Felix Yan, Senior Member of the Technical Staff, Enterprise Desktop, VMware
- Victor Zhang, Technical Staff, Enterprise Desktop Quality Engineering, VMware

To comment on this paper, contact us at twitter.com/vmwarehorizon.

# Additional Resources

- Configuring Kiosk Mode in VMware View Manager 4.5 and Later (KB 1028287)
- Extra configuration required when setting up kiosk mode for a View desktop or application on an RDS host (KB 2081492)
- Key Considerations in Choosing a Zero Client Environment for View Virtual Desktops in VMware Horizon
- Reviewer's Guide for View in Horizon 6
- Setting Up Desktop and Application Pools in View
- USB Device Redirection, Configuration, and Usage in VMware Horizon with View
- Using VMware Horizon Client for Linux
- Using VMware Horizon Client for Windows
- VMware Compatibility Guide
- VMware Horizon with View Security Hardening Overview
- VMware Horizon View 6 Desktop Virtualization Cookbook
- VMware View 5 – Configure and Deploy Clients in Kiosk Mode

vmware

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