Kiosk Mode with VMware® View™ 4.5 and Above

WHITE PAPER

vmware

Table of Contents

Abstract 3
Introduction 3
Creating Kiosk Client ID 4
Provisioning Desktop Pool and Entitlement 6
Connecting Kiosk Client 6
Assigning ThinApp Groups 6
Automatic USB Redirection 6
Kiosk Mode Vertical Use Cases 7
Healthcare Use Case. 7
Hospitality 8
Education 8
Summary 9
About the Author 9
Acknowledgements 9

Abstract

To stay competitive, an organization must balance customer service with operational efficiencies. One way to do this is through innovative self–service solutions, such as a customer kiosk. This freestanding, interactive system can streamline the customer experience by providing information, processing registration and payments, and more. This document provides a feature introduction on Kiosk Mode in VMware® View™ 4.5 and above, and deployment scenarios for various verticals.

Introduction

Self-service kiosks can be used in many different situations, such as healthcare, hospitality, and education. For example, a majority of patients claim that the most challenging part of a hospital or doctor visit isn't the visit itself—it's the check-in process. A kiosk station can help simplify the patient experience by allowing them to update their personal information, order prescription refills, and pay their balances without having to wait in line.

Application-specific peripherals such as proximity card readers, biometric identification, insurance card scanners, privacy screens, and payment transaction devices streamline patient and work flow, improve financial performance, ensure HIPAA privacy compliance, and provide patients with dramatically improved service. Eliminating paper forms means the information does not have to be re-entered, increasing accuracy and reducing administrative overhead.

VMware View 4.5 and above supports the "hidden" Kiosk Mode, which transparently connects the locked-down endpoint or thin client directly to a remote desktop session. Users do not need to specifically launch a VMware View Client. All configuration and provisioning is executed in background. The user is presented with a familiar interface—a dedicated kiosk application running on a virtual desktop session. VMware View implements any additional authentication mechanisms that are required for secure transactions, while securing the physical network against tampering and snooping. All devices connected to the network are trusted. For example, automatic USB device redirection and connection can be enabled to allow secure connectivity for allowable local devices.

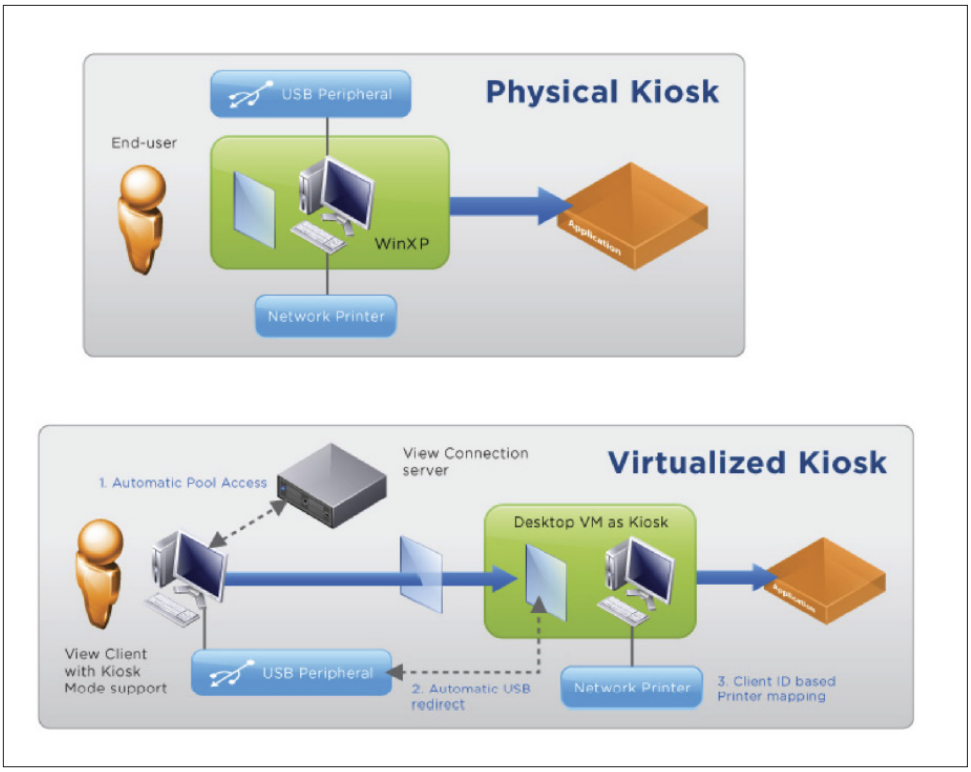

Figure 1: Physical Kiosk versus Virtualized Kiosk

Creating Kiosk Client ID

In View Manager Administration console, you can create a floating pool with a "Refresh on Logoff" option for Kiosk Mode usage.

The admin uses the vdmadmin command from the View Connection Server command line to set the connection broker to Kiosk Mode. Please note this command needs to be executed for each instance, as in the following example.

`vdmadmin -Q –enable -s servername` where servername is your connection server hostname instance.

Each kiosk station has a unique ClientID to connect to View Connection Server. Instead of creating a user directly in the Active Directory, you will use the command vdmadmin to create a ClientID with kiosk station's MAC address. Alternatively, you can create an account name with up to 20 characters, which must begin with the string "Custom-". Any client in Kiosk Mode can use such an account. For added security, View Client in View 4.5 and above rejects any attempt to log in using an account for a kiosk client. In the example below, optionally, you can create a "kiosk" Organizational Unit (OU) group in Active Directory. This simplifies the process of entitling the OU to the desktop pool.

```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmadmin -Q –clientauth –add –
clientid 00:1A:A0:1B:44:90 –domain vmware-view –ou "ou=kou,dc=vmware-view,dc=com" Client
authentication user was added successfully.
```

Note: An IT manager can add the vdmadmin directory location to the system PATH to save lengthy typing. Below is a Command line example of how to remove Client_ID.

```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmadmin -Q —clientauth —clientid
custom-csh1 —domain vmware-view —remove Client authentication user was removed
successfully.

C:\Program Files\VMware\VMware View\Server\tools\bin>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

GUID                                : 6c6c0d50-2735-4fb5-90da-49673bee4b9c
ClientID                            : cm-00_1A_A0_1B_44_90
Domain                              : vmware-view
Password Generated                  : true

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

The example below shows how to display connected kiosk stations currently authorized by the View Connection Server.

```
C:\Program Files\VMware\VMware View\Server\tools\bin>vdmadmin -Q -clientauth —removeall
Are you sure you want to remove all Client Authentication users? YES/NO>: no
```

Provisioning Desktop Pool and Entitlement

The **vdmadmin** command line tool does not support entitlement configuration. You must use the View Manager Administration console to create desktop pools and entitlements.

Connecting Kiosk Client

The kiosk client installation script is launched from the command line using wswc, with the key required information ClientID (MAC by default, can be a custom ID). ClientID only needs to be specified when authenticating using a client account name in the form "Custom-xxxxx". For example:

```
C:\Program Files\VMware\VMware View\Client\bin>wswc -unattended -serverurl 192.1
68.13.245 -username custom-csh1
```

Assigning ThinApp Groups

VMware View supports ThinApp provisioning directly from View Manager. You can assign the ThinApp repository by assigning the file share's UNC path. If you would like to have the kiosk station access certain application groups, you can either prepare the guest virtual machine with applications in the base image or associate the ThinApp group to the desktop pool.

Automatic USB Redirection

Unlike the typical View desktop instance, you don't need to manually enable or add USB devices from the View desktop stub. Instead, USB peripherals are automatically connected when the desktop session is established.

If you have set USB policy in the View Manager console to allow or disallow USB devices access within the virtual session, the settings will automatically override the USB connection setting in the kiosk client.

Kiosk Mode Vertical Use Cases

Healthcare

Kiosk stations are networked into a central database that contains patients' electronic healthcare records (EHR), and feature a camera, credit card reader, printer, and a very cool biometric authentication device.

Typically, the USB peripherals are not redirected automatically in View desktop and you need to manually connect the device. When the kiosk client session is established, supported USB peripherals are connected immediately to the virtual desktop session. The following GPO policies are set to TRUE at connect:

ConnectUSBOnStartup
Connect all USB devices to the desktop on launch.

ConnectUSBOnInsert
Connect USB devices to the desktop when they are plugged in.

The IT manager does not need to set the value for the policy in Kiosk Mode.

The kiosk client connects the endpoint hardware device seamlessly to the guest virtual machine. If you are working with single-sign-on (SSO) solution for desktop policy, application wrapping, or role-based application access, you can continue to apply the SSO within the guest virtual machine.

However, as the ClientID access is generic each time, for example using custom-csh1 to access the virtual desktop, the typical "Follow Me Desktop" use case will not apply in the Kiosk Mode.

For location-based printing, you can refer to the "ThinPrint GPO Configuration for Location-Based Printing" Information Guide. If the local printer is attached directly as a local peripheral connected direct with the kiosk, VMware View utilizes the ThinPrint to print to local printer. However, if it's a networked printer with an IP address, it will require the IT Administrator to enable to Group Policy Object for "AutoConnect Map Additional Printers for VMware View."

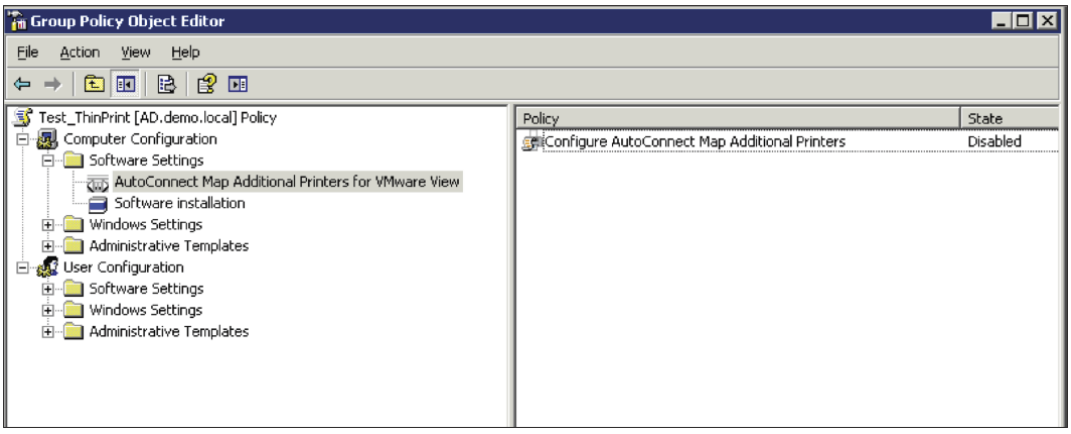

Figure 2: Modify.Software.Settings.in.View.Connection.Server.GPO

If all kiosk stations can send print jobs to a central printer, you can assign an Organizational Unit (OU) to print to the designated printer from the GPO. The printer can also be set based on its MAC address. Alternatively, configure each printer map to the kiosk station individually according to its dedicated client ID.

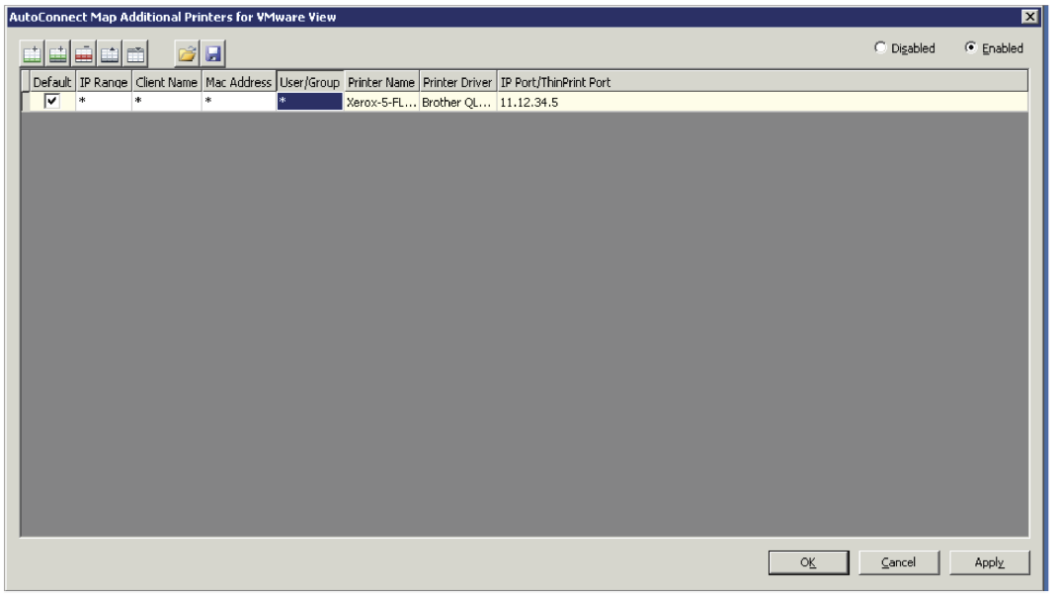

Figure 3: Enter.Manually.or.batch.import.the.network.printer.mapping.

Hospitality

In airports, trains or hotels, it's common to see ticketing check-in platforms. Kiosk Mode can be used to provide:

- A kiosk ticket printer, by configuring ClientID-based printing/location-based printing
- Driver license or credit card authentication, using USB redirection for a reader
- Timeout or walk away policy, by configuring auto logoff from session

Education

Universities everywhere are realizing the cost savings and benefits of kiosks for automated registration, financial aid information, course catalogs, directories, way finding, academic and athletic event calendars, student ID validation, and more. Kiosk Mode can be configured to:

- Video viewing using Control Multimedia Redirection policy
- Set Auto logoff/walkaway policy
- Use a USB device to read a student or faculty ID card and establish access rights, using Automatic USB redirection

University client end points offer great opportunities for layering web-based applications, which can significantly reduce staffing budgets and assist with campus process flows during periods where there are sharp spikes in demand, such as registration, parent weekends, athletic events, etc.

Summary

Kiosk Mode provides easy command line options with endless possibilities for individual software vendors (ISV) or system integrators. For more details, see the following chapters from the VMware View Administrator's Guide on the VMware View product site at http://www.vmware.com/products/view/:

- Running View Client from the Command Line
- Setting up Clients in Kiosk Mode

About the Author

Cynthia Hsieh is a Senior Technical Marketing Manager at VMware. She focuses on application integration, proof of concepts, and security subjects. Hsieh's previous background includes product management positions at Wyse, Trend Micro, Oracle, and Yahoo.

Acknowledgements

Thank you for the content validity and guidance provided by Gerald Cheong, Lan Nguyen K and Lebin Cheng.

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