



# Location Awareness in VMware® View™ 4.5 and Above

INFORMATION GUIDE

## Table of Contents

Abstract .....	3
Location Awareness in VMware View 4.5 and Above .....	3
A Platform for Location-Based Awareness Integration .....	3
Security Server to Limit Access .....	3
Tag-Based Entitlement .....	4
Endpoint Device Client Information .....	4
Active Directory Group Policy Example .....	6
Procedure for Creating Active Directory Group Policy .....	6
ThinApp and Location-Based Awareness .....	7
Setting Up Location-Based Printing .....	7
Find Out More .....	8
About the Author .....	8

## Abstract

Establishing role-based, policy-driven application access across multiple desktops is critical in medical and healthcare environments. In this paper, we describe the client attributes available at endpoint locations that can be used for role-based access control, enabling the dynamic association of users with locations. Information access and application privileges are determined by a user's role, an organization's policies, the type of desktop (such as kiosk, thin client, or PC), and device location.

The paper is intended for ISV software integration use.

## Location Awareness in VMware View 4.5 and Above

Together, VMware® View™ and ThinApp™ provide you with complete control to provision secure access to desktops, data, and applications based on endpoint device configuration, network location, and user identity.

From centralized datacenters that contain user identity and security profiles, endpoint locations, and network information, VMware View allows you to grant or restrict desktop or application access according to customizable policies.

VMware View works with Active Directory and makes it easy to manage unsafe endpoint devices and audit endpoint policies, on demand, to:

- Control desktop session timeout
- Restrict USB peripheral access
- Prevent file transfers and clipboard operations
- Map network printer operations
- Prevent attempts to breach data security

These features are of great value to the healthcare and public sectors, helping organizations comply with data security regulatory compliance mandates, such as Sarbanes-Oxley and HIPAA.

## A Platform for Location-Based Awareness Integration

To illustrate location-based awareness in VMware View, we will use the example of Doctor Jones, who can access clinical applications (like GE EMR or MEDITECH) and retrieve data from a patient contact management solution (for example, Carefx), from work and home.

### Security Server to Limit Access

VMware View provides the installation option of using View Connection Server as Security Server in a demilitarized zone (DMZ). This differentiates external access from internal access (within corporate firewall) to the desktops or endpoint device pools based on policy and regulatory requirements. You can configure the application wrapper and policy based on AD profiles associated with individual desktop or workgroup pools.

## Tag-Based Entitlement

It is simple for healthcare IT administrators to set up matching policies and tags associated with different connection servers and desktops to control access. In our example, this allows Doctor Jones to see 10 applications when at the clinic, and perhaps only 2 calendaring or non-sensitive applications from his desktop at home.

Most of the single signon (SSO) solutions allow user access based on “who you are” not “where you are.” VMware View adds additional control on a “per workstation” basis, providing the VMware View agent with physical device and network information when establishing the connection to the backend virtual desktop. This enables policy control based on “where you are.”

Fast profile access control, extended application-level policies, and flexible user authentication provide organizations the control and assurance they need to deliver applications to users regardless of location or device; this makes VMware View the ideal integration platform for healthcare environments.

## Endpoint Device Client Information

In View Manager Administration guide [http://www.vmware.com/pdf/view40\\_admin\\_guide.pdf](http://www.vmware.com/pdf/view40_admin_guide.pdf), pages 122 to 124 cover the ability to pass information about the client endpoint into the virtual machine. You can now pass the client name, IP address, and MAC into the virtual machine.

Table 1 lists the information sent to the guest machine agent for each client type.

CLIENT INFORMATION	WINDOWS	LINUX	DESCRIPTION
ViewClient_IP_Address	X	X	The IP address of the client device.
ViewClient_MAC_Address	X	X	The MAC address of the client device.
ViewClient_Machine_Name	X	X	The machine name of the client device.
ViewClient_TZID	X	X	The Olson time zone ID. When using View Client on Windows, this information is not available in the Volatile Environment in the desktop registry or in View Agent logs. It is sent using a private channel.  <b>Note:</b> To disable, set the Disable Time Zone Synchronization GPO to true.
ViewClient_Windows_Time zone	X	X	GMT standard time. When using View Client on Windows, this information is not available in the Volatile Environment in the desktop registry or in View Agent logs. It is sent using a private channel.

**Table 1:** Client Information Available in the Desktop

Third-party certified clients can also provide endpoint information. Note that in View Portal kiosk configuration, the following registry entities are not available.

- ViewClient\_Machine\_Name
- ViewClient\_Machine\_Domain
- ViewClient\_IP\_Address
- ViewClient\_LoggedOn\_Domainname
- ViewClient\_LoggedOn\_Username
- ViewClient\_MAC\_Address
- ViewClient\_Type

The following HKCU\Volatile Environment registry values are sent to the VMware View agent running in the virtual machine and are stored in the registry.

- ViewClient\_MachineName: TC01
- ViewClient\_IP\_Address: 10.10.10.1
- ViewClient\_MAC\_Address: 0a:0a:0a:0a:0a:0a

This information can be gathered every time you log in, so if a user changes location, you can see that change in the variables. This can be run with the CommandsToRunOnConnect once the VDM\_AGENT.ADM template has been configured in your AD and you have assigned the policies for CommandToRunOnConnect and/or CommandToRunOnReconnect option.

Here is an example of how it can be used. Values on the guest virtual machine can be as follows:

```
HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\Configuration\CommandsToRunOnConnect
Command1="wscript.exe c:\reconnectscript.vbs"
```

```
HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\Configuration\
CommandsToRunOnReconnect Command1="wscript.exe c:\reconnectscript.vbs"
```

Write the script to look something like the following. The string from the msgbox below will pop up in a small window:

```
-Begin Script-
Const HKEY_CURRENT_USER = &H80000001

Set wmiLocator=CreateObject("WbemScripting.SWbemLocator") Set wmiNameSpace =
wmiLocator.ConnectServer(".", "root/default") Set objRegistry = wmiNameSpace.
Get("StdRegProv")

sPath = "Volatile Environment"

lrc = objRegistry.GetStringValue(HKEY_CURRENT_USER, sPath, "ViewClient_Machine_
Name", vMachine) lrc = objRegistry.GetStringValue(HKEY_CURRENT_USER, sPath,
"ViewClient_IP_Address", vIP) lrc = objRegistry.GetStringValue(HKEY_CURRENT_
USER, sPath, "ViewClient_MAC_Address", vMAC)

msgbox "The Remote Device Name is " & vMachine & " @ " & vIP & " (" & vMAC &
") "
```

-End Script-

This simple example script shows that you can pass information to applications and map devices such as printers to a specific user at an actual location. The possibilities are myriad.

## Active Directory Group Policy Example

One way to implement Active Directory group policies in View Manager is to create an Organizational Unit (OU) for your VMware View desktops, and link one or more Group Policy Objects (GPOs) to that OU. You can use these GPOs to apply group policy settings to your VMware View desktops and to enable loopback processing.

You can configure policies on your Active Directory Server, or on any computer in your domain. This example shows how to configure policies directly on your AD server.

**Note:** Because every VMware View environment is different, you might need to perform different steps to meet your organization's specific needs.

### Procedure for Creating Active Directory Group Policy

#### 1. Create an OU for VMware View Desktops

To apply group policies to VMware View desktops without affecting other Windows computers in the same Active Directory domain, you can create an OU specifically for your VMware View desktops.

#### 2. Create GPOs for VMware View Group Policies

You can create GPOs to contain group policies for View Manager Components and location-based printing, and then link them to the OU for your View desktops.

#### 3. Add VMware View ADM Templates to a GPO

To apply View Manager Component group policy settings to your VMware View desktops, you add their ADM Template files to GPOs.

#### 4. Enable Loopback Processing for View Desktops

When you enable loopback processing, User Configuration settings that usually apply to a computer apply to all the users that log in to that computer instead.

## ThinApp and Location-Based Awareness

ThinApp is an application virtualization solution that simplifies application deployment. While ThinApp does not offer any location awareness or metering/monitoring-specific technologies, it does support and work with other technologies that can enable a ThinApp packaged application to be somewhat “location aware” or have its usage metered/monitored.

For example, ThinApp supports Active Directory Group Security authentication. Assigning an AD User Security group (or groups) to a ThinApp packaged application ties it to any system on the specific domain, against which an Active Directory user may authenticate. And while it is not documented, ThinApp also supports AD Computer Security groups.

Since any validation logic can be scripted—and virtually anything can be scripted with ThinApp—you can use an embedded VBS script to ensure the ThinApp packaged application launches where you want, for whom you want, when you want, and how you want. See the ThinApp Blog Article “Adding Non-Active Directory Validation Logic to a ThinApp Package” (<http://blogs.vmware.com/thinapp/2009/01/adding-non-acti.html>) for more details on this.

It should also be noted that one of ThinApp’s strengths is the ability to plug into any existing ESD and metering/monitoring solution. Using third-party tools, administrators can also accomplish some of these same “location restriction” goals. VMware has specifically partnered with Concept Software—makers of the SoftwareKey Metering solution for ThinApp (<http://www.softwarekeymetering.com>)—which can restrict any application (not just a ThinApp packaged app) to a system/user with any number of validation checks and parameters.

The ThinApp runtime (also known as the “Virtual Operating System”) by default has no knowledge of the client information and attributes. ThinApp is only an application virtualization solution to make applications behave according to scripted validation logic. However, you can embed the location-based awareness logic into the VB scripting prior to the packaging. This is very likely a possibility.

## Setting Up Location-Based Printing

The location-based printing feature maps printers that are physically near client systems to VMware View desktops, enabling users to print to their local and network printers from their View desktops.

Set up location-based printing by configuring the Active Directory group policy setting AutoConnect Location-based Printing for VMware View, which is located in the Microsoft Group Policy Object Editor in the **Software Settings** folder under **Computer Configuration**.

**Note:** The policy is computer-specific, not user-specific. Computer-specific policies apply to all VMware View desktops, regardless of who connects to the desktop.

The AutoConnect Location-based Printing for VMware View group policy setting is a name translation table. You use each row in the table to identify a specific printer and define a set of translation rules for that printer. The translation rules determine whether the printer is mapped to the VMware View desktop for a particular client.

When a user connects to a VMware View desktop, View Manager compares the client system to the translation rules associated with each printer in the table. If the client system meets all of the translation rules set for a printer, or if a printer has no associated translation rules, View Manager maps the printer to the VMware View desktop during the user’s session.

You can define translation rules based on the client system’s IP address, name, and MAC address, and the user’s name and group. You can specify one translation rule, or a combination of several translation rules, for a specific printer.

## Find Out More

For information or to purchase VMware products, call 1-877-4VMWARE (outside of North America dial +1-650-427-5000), [www.vmware.com/products](http://www.vmware.com/products), or search online for an authorized reseller. For detailed product specifications and systems requirements, please refer to the VMware View and ThinApp install and configure guide.

## 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.

