Configuring OneSign 4.9 Virtual Desktop Access with Horizon View

HOW-TO GUIDE

vmware®

Introduction

This How-To Guide includes information about configuring OneSign® virtual desktop access (VDA) with View in VMware® Horizon™ 6. This document contains the following sections:

How To Use This Document

This How-To Guide is an overview of the installation and configuration process, highlighting critical areas on which you should focus.

Notes are important features or instructions

Best Practices are recommended methods that achieve the best results.

This is a warning or cautionary statement.

To view all OneSign documentation referred to in this How-To Guide, including other Tech Briefs and the *OneSign Administrator Guide*, go to the OneSign Documentation Library in the OneSign Administrator, or the OneSign Support Center at http://support.imprivata.com.

Before You Begin

Note the URL of the View Server

To support View VDA, OneSign must connect to a Connection Manager installed on the View server. You will need the URL of this server when configuring your View environment, and when configuring the OneSign connection to the View server. See Step 5: Configure OneSign's Connection to View.

Copy the Domain Certificate to the Thin Clients

To support View VDA, copy the domain certificate for the View Connection Broker and copy it to the endpoint computers.

Configuration

Step 1: Install VMware View Agent™ and Client Software

Before you configure OneSign desktop roaming for View, confirm your View environment.

- Install View Agent 4.0.1 or later on all VMs that will support OneSign.
- Install View Client 4.0.1 or later on all endpoint computers that will support OneSign.

When these are installed, be sure you can connect to the virtual desktop before continuing.

Step 2: Verify That the View Environment Is Configured Correctly

Before you install OneSign on View VMs and endpoint computers, perform the steps in the following sections to ensure your View environment is installed and configured correctly.

Verify the View Installation

Verify the following installations by viewing the software listed in the Windows Control Panel > Add and Remove Programs:

- Verify that View Agent 4.0.1 or later is installed on all VMs.
- Verify that View Client 4.0.1 or later is installed on all endpoint computers.

Step 3: Install OneSign on All VMs

To install View and OneSign 4.8 to all VMs:

1. Install View Agent on one VM.
2. Install OneSign on the same VM.
3. Clone the VM for all the installations you require.

Step 4: Install OneSign on All Endpoint Computers

OneSign must be installed on each endpoint computer on which View VDA will be used.

The OneSign installation can be pushed to groups of computers or installed on one computer at a time, depending on your organization's preferences. For complete installation details, see the OneSign Administrator Guide, Chapter 4: "Distributing the OneSign Agent."

To install OneSign on ProveID Embedded Linux thin clients, skip Step 4 and refer to the following documents: Configuring OneSign on Hewlett-Packard Smart Zero and ThinPro Thin Clients and Configuring OneSign on IGEL Linux Thin Clients.

Option 1: Push Install with MS Active Directory Group Policy

A common method for installing the OneSign Agent with multiple users is via an MSI push. You can distribute the OneSign Agent on users' computers by using Microsoft Active Directory's Group Policy to automatically push the package to user computers.

An MSI push requires minimal participation of end users.

Option 2: Installing the OneSign Agent from the Command Line

If you want to install the OneSign Agent on a single endpoint computer from the command line, see Installing the OneSign Agent from the Command Line.

Option 3: Deploying to Users for Self-Installation

Self-installation works best for experienced users. With this method, you pre-configure the installation, then send a notification email to one or more users from the OneSign Administrator. The email includes instructions to download the installation package and use the OneSign Installer to install OneSign. With this method, the OneSign Installer requires no manual configuration steps.

This is an easy way to roll out OneSign to early adopters.

Option 4: Installing the OneSign Agent Directly from the .msi File

You can also install the OneSign Agent on a computer directly from the .msi file. This method is similar to deploying to users for self-installation. With this method, the user must make several manual configurations during the OneSign Installer process.

Step 5: Configure OneSign's Connection to View

Configure OneSign's connection to the View server. To support VMware View VDA, OneSign must connect to a View Connection Manager installed on the View server.

1. In the OneSign Administrator, go to the **Properties** page > **Virtual Desktops** tab > **VMware View** section.
2. Enter the URL of each Connection Manager that will support OneSign.
3. Select **Allow authentication from VMware View clients**. This checkbox is **not** enabled by default. Once selected, uncheck it only when you need to stop OneSign service on all View endpoint computers.
4. Click **Save**.

Select the User Logon Format for View Authentication

In OneSign 4.8 HF2 and later, the user principal name (UPN) format (e.g., UserName@example.com) is used for authentication when launching View applications.

Previous releases of OneSign used the down-level logon name format (e.g., [DomainName]\UserName). You can disable the use of UPN and revert to down-level logon name format by creating the **DoNotUseUPN** registry key with a **Data Type** of **DWORD** and a value of **1** in one of the following locations:

- 32-bit computers: **HKEY_LOCAL_MACHINE\SOFTWARE\SSOProvider\VDI\View**
- 64-bit computers: **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SSOProvider\VDI\View**

Step 6: Create and Assign a Computer Policy for Endpoint Computers

Create, configure, and assign a computer policy that automates endpoint computer access to View. Endpoint computers and virtual desktops are assigned the Default Computer Policy unless:

- A different computer policy is manually assigned
- A different computer policy is automatically assigned by computer policy assignment rules

See Step 6c for details on manually and automatically assigning computer policies.

Review the Default Computer Policy settings to confirm that they are appropriate for your virtual desktop environment.

Step 6a: Create a Computer Policy for Endpoint Computers

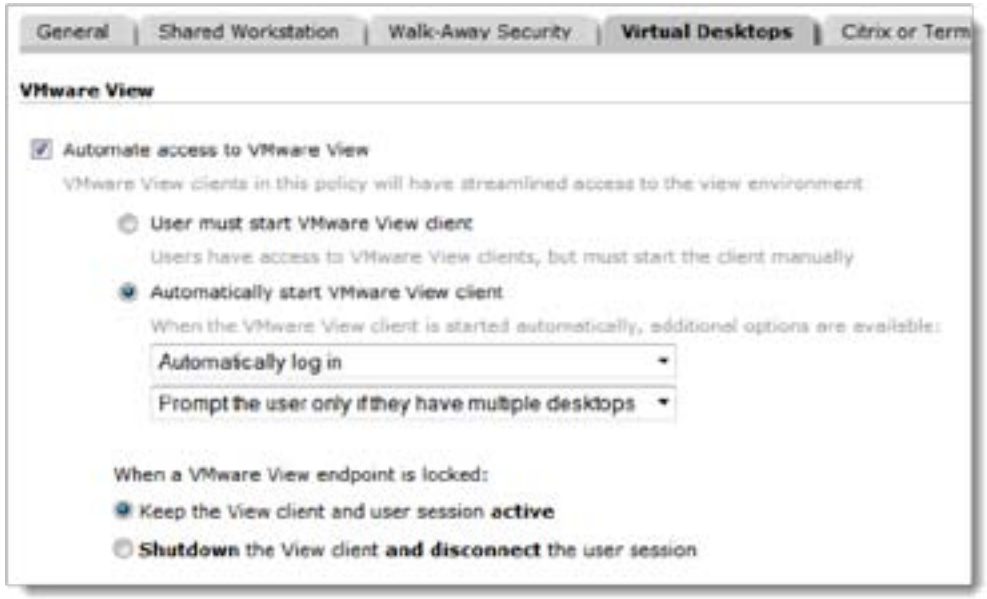
1. In the OneSign Administrator console, go to the **Policies** page > **Computer Policies**.

   You can select an existing computer policy from the list, or make a copy of the Default Computer Policy as a starting point. If you want to edit an existing computer policy, click the existing computer policy name, and skip to step 6b.

2. To copy the Default Computer Policy, click the checkbox next to **Default Computer Policy**, then click **Copy**.
3. Click **Default Computer Policy (2)**.
4. Rename the computer policy in the **Specify A Name** field.

Step 6b: Configure the Computer Policy to Endpoint Computers

1. Go to the **Virtual Desktops** tab > **VMware View** section.
2. Choose from the following options:
   - **Automatically start VMware View client**. The client will automatically authenticate users to View.
     - Select **Automatically log in** so the users are not prompted for their credentials.
     - Select **Prompt the user only if they have multiple desktops** to further streamline the virtual desktop experience for single-desktop users.




These options provide the most seamless and streamlined virtual desktop experience.

   - **User must start VMware View client**. Select this option if you want users to start the View client manually and then to authenticate to their desktops manually.

3. You can control the behavior when an endpoint computer is locked. Under **When a VMware View endpoint is locked**, choose one of the following:
   - **Keep the View client and user session active.** This option preserves the user session; when a user logs back into this endpoint computer (or another endpoint computer with View enabled) their desktop and applications are preserved just as they were when this endpoint computer was locked.
   - **Shutdown the VMware View client and disconnect the user session.** This option helps optimize resource consumption and minimizes the total number of active sessions in use in the enterprise. When a user logs back into this endpoint computer (or another endpoint computer with View enabled) their desktop will relaunch.
4. ***Optional:*** You can uncheck specific Connection Managers that you do not want used by endpoint computers with this policy. Under **Available VMware View Connection Managers**, the **Add or modify Connection Managers** link brings you to the **Virtual Desktops** tab on the **Properties** page.
5. When you are done creating the computer policy, click **Save** at the bottom of the page.

Step 6c: Assign the Computer Policy to Endpoint Computers

Assign the computer policy you just created to endpoint computers.

Manually Assigning the Computer Policy

1. Go to the **Users**, **Computers**, and **Domains** page > **Computers** tab.
2. Check the checkboxes next to the computers to which you want to assign the computer policy.
3. Select **Apply Policy.**
4. Select **Apply a specific policy** and the name of the policy you've created.
5. Click **OK**.

Automatically Assigning the Computer Policy

Use computer policy assignment rules to assign a computer policy to existing endpoint computers, and to automatically assign a policy to endpoint computers added in the future.

1. Go to the **Users**, **Computers**, and **Domains** page > **Computer Policy Assignment** tab.
2. Click **Add New Rule**.
3. Name the assignment rule.
4. Select one of the following options:
   - **Computer IP address:** enter the range of IP addresses to include in this computer policy.
   - **Computer host name:** a computer matches if its host name contains the text entered in this field.
   - **OneSign agent type:** choose an agent type from the list. This option works best if this computer policy is to be used for only one agent type.

When assigning a computer policy to only ProveID Embedded thin clients, select **OneSign agent type**> **ProveID Embedded**.

5. In the field **Apply this computer policy**, select the computer policy you've created.

   There is no **Save** button. These rules are saved automatically as you create them.

Step 7: Create and Apply a User Policy

Create and apply a user policy that automates user access to View.

Step 7a: Create a User Policy

1. In the OneSign Administrator, go to the **Policies** page > **User Policy** tab.

   You can select an existing user policy from the list, or make a copy of the Default User Policy as a starting point. If you want to edit an existing user policy, click the existing user policy name, and skip to step 5.

2. To copy the Default User Policy, click the checkbox next to **Default User Policy** , then click **Copy**.
3. Click **Default User Policy (2)**.
4. Rename the user policy in the **Policy Name** field.
5. Click the **Virtual Desktops** tab.
6. Select **Automate access to VMware View** to have OneSign automatically handle login behavior for View endpoint computers. Roaming users with this policy will have streamlined access to the View environment.
7. Click **Save**.

Step 7b: Apply a User Policy

1. To apply a user policy to other users, go to the **Users**, **Computers and Domains** page > **Users** tab.
2. Select the checkboxes next to the users to which you want to apply the user policy.

   You can view additional pages of the **Users** list without losing your selections. OneSign keeps track of all the users you have selected and displays a counter above the **Users** tab.

Best Practice: To select multiple users more efficiently, use the **Search For Users** tool at the top of the Users tab. Search for Users offers several search parameters for refining your results.

3. Click **Apply Policy**. The Apply Policy dialog box opens.
4. Choose the policy from the drop-down list, then click **OK**.

Troubleshooting

Enabling USB Devices on View Endpoint Computers

The View virtual desktop does not by default enable devices plugged into a USB port on the endpoint computer. To change this behavior, create one of the following registry keys with a **Data Type** of **DWORD** and a value of **1**:

- **connectUSBOnInsert** — Connects a USB device to the foreground desktop when the device is plugged in
- **connectUSBOnStartup** — Connects all USB devices to a desktop when it is launched

Add the key in one of the following locations:

- 64-bit computers: **\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SSOProvider\VDI\View**
- 32-bit computers: **\HKEY_LOCAL_MACHINE\SOFTWARE\SSOProvider\VDI\View**

Branding Login and Enrollment Screens

You can display your corporate logo on OneSign login and enrollment screens for OneSign single-user and kiosk workstations. See the Tech Brief Customizing OneSign, “Replacing the OneSign Logo in Authentication Dialogs.”

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