imprivata®

Product Documentation

Configuring VMware View Virtual Desktops

Imprivata Enterprise Access Management 24.2

Installing and Configuring Support for VMware Horizon Virtual Desktops

NOTE:
Beginning with 24.2, Imprivata OneSign and Imprivata Confirm ID have been renamed to Imprivata Enterprise Access Management.

Some interfaces in the Imprivata Admin Console, Imprivata Appliance Console, and documentation may retain the older Imprivata OneSign and Imprivata Confirm ID product names.

This document includes information about configuring VMware Horizon virtual desktops to support Imprivata Virtual Desktop Access. Imprivata Authentication Management and Virtual Desktop Access licenses are required for this feature.

NOTE:
To configure support for VMware Horizon View RDS hosted applications, see Configuring Virtual Desktop Access with VMware Horizon View RDS Hosted Applications in the OneSign or Confirm ID online help or a PDF version of that topic.

This document contains the following sections:

Installing and Configuring Support for VMware Horizon Virtual Desktops **2**
- Before You Begin 3
  - Note the URL of the VMware Horizon Server 3
  - Copy the Domain Certificate to the Thin Clients 3
  - Session Persistence 3
- Installation Sequence 3
  - Step 1: Install VMware Horizon Agent and Client Software 3
  - Step 2: Install the Imprivata Agent on All VMs 3
  - Step 3: Install the Imprivata Agent on All Endpoint Computers 4
  - Step 4: Configure Imprivata's Connection to VMware Horizon 4
  - Step 5: Create and Assign a Computer Policy for Endpoint Computers 4
  - Step 6: Create and Apply a User Policy 6
  - Step 7: (Optional) Override the Desktop Chooser 7
- Troubleshooting 8
  - Enabling VMware Menu Bar 8
  - Enabling USB Devices on VMware Horizon Virtual Desktops 8
  - Enabling the Imprivata USB Receiver for Hands Free Authentication on VMware Horizon Virtual Desktops 8
  - Enabling Proximity Cards 9
  - Troubleshooting UPN Format for VMware Horizon Authentication 9
  - User Credentials are not Passed to the Virtual Desktop 10
  - Multiple Client Sessions Launch at VMware Horizon Virtual Desktops on Windows 10
  - Branding Login and Enrollment Screens 11

Before You Begin

Note the URL of the VMware Horizon Server

To support VMware Horizon Virtual Desktop Access, Imprivata must connect to a VMware Horizon Connection Manager (Connection Manager) installed on the VMware Horizon server. You will need the URL of this server when configuring your VMware Horizon environment, and when configuring the Imprivata connection to the VMware Horizon server. See Step 4: Configure Imprivata's Connection to VMware Horizon.

Copy the Domain Certificate to the Thin Clients

To support VMware Horizon Virtual Desktop Access, copy the domain certificate for the Connection Manager and copy it to the endpoint computers.

Session Persistence

Session persistence (roaming) is managed by your virtual environment, not Imprivata Virtual Desktop Access. If your virtual environment is configured correctly for session persistence, Imprivata Virtual Desktop Access seamlessly roams user sessions, on authentication, to the endpoint computers in your environment.

NOTE: For more information about configuring session persistence, see your vendor–specific documentation.

Installation Sequence

Step 1: Install VMware Horizon Agent and Client Software

Before you configure Imprivata desktop roaming for VMware Horizon, review Imprivata Enterprise Access Management Supported Components or Imprivata Enterprise Access Management Supported Components to confirm your VMware Horizon agent and client versions are supported by Imprivata. An Imprivata Authentication Management license is required to enable desktop roaming.

Be sure you can connect to the virtual desktop before continuing.

Before you install the Imprivata agent on VMware Horizon VMs and endpoint computers, view the software listed in the Windows **Control Panel** > **Add and Remove Programs**:

- Verify that VMware Horizon agent is installed on all VMs.
- Verify that VMware Horizon Client is installed on all endpoint computers.

Step 2: Install the Imprivata Agent on All VMs

To install VMware Horizon and Imprivata to all VMs:

1. Install the VMware Horizon agent on one VM.
2. Install the Imprivata agent on the same VM.
3. Clone the VM for all the installations you require.

Step 3: Install the Imprivata Agent on All Endpoint Computers

The Imprivata agent must be installed on each endpoint computer on which VMware Horizon Virtual Desktop Access will be used.

The installation can be pushed to groups of computers or installed on one computer at a time, depending on your organization's preferences. See "Deploying the Imprivata Agent" in the online help for instructions on installing agents. Choose the method that suits your environment.

NOTE:
To configure Imprivata ProveID Embedded on Linux thin clients, see Configuring ProveID Embedded on Linux Thin Clients in the OneSign or Confirm ID online help or in a PDF of that topic.

Step 4: Configure Imprivata's Connection to VMware Horizon

Configure Imprivata's connection to the VMware Horizon server. To support VMware Horizon Virtual Desktop Access, Imprivata must connect to a VMware Horizon Connection Manager installed on the VMware Horizon server.

1. In the Imprivata Admin Console, go to the **Computers** menu > **Virtual Desktops** page > **VMware Horizon – Desktops** section.
2. Select **Allow authentication from VMware Horizon clients**.
3. Enter the URL of each Connection Manager that will support Imprivata.
4. Click **Save**.

Select the User Logon Format for VMware Horizon Authentication

By default, Imprivata OneSign uses the down-level logon name format (such as [DomainName]\UserName) for authentication when launching VMWare View applications.

To disable the use of the down-level logon name format and to enable the user principal name (UPN) format (such as UserName@example.com), create the **DoNotUseUPN** registry key with a **Data Type** of **DWORD** and a value of **0** in the following location:

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

This is only applies to Imprivata environments configured and licensed for Authentication Management.

Step 5: Create and Assign a Computer Policy for Endpoint Computers

Create, configure, and assign a computer policy that automates endpoint computer access to VMware Horizon.

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.

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

Step 5a: Create a Computer Policy for Endpoint Computers

1. In the Imprivata Admin Console, go to the **Computers** menu > **Computer policies** page.

   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 5b.
2. To copy the Default Computer Policy, select **Default Computer Policy** , then click **Copy**.
3. Click **Default Computer Policy (2)**.
4. Rename the computer policy in the **Name** field.

Step 5b: Configure the Computer Policy to Endpoint Computers

1. Go to the **Virtual Desktops** tab > **VMware Horizon** section.
2. Select **Automate access to VMware Horizon** to have Imprivata automatically handle login behavior for VMware Horizon endpoint computers.
3. Choose from the following options:
   - **Prompt the user only if they have multiple desktops**
   - **Always prompt the user to choose their desktop**

   

   NOTE: If you are configuring single-user computers, and a user is entitled to multiple desktops, you can prevent them from having to choose which one to launch by configuring a registry key (**DesktopToAutoLaunch**) on the Windows endpoint. For more information, see Step 7: (Optional) Override the Desktop Chooser.
4. You can control the behavior when an endpoint computer is locked. Under **When a VMware Horizon 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 VMware Horizon enabled) their desktop and applications are preserved just as they were when this endpoint computer was locked.
   - **Shutdown the VMware Horizon 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 VMware Horizon enabled) their desktop will relaunch.

5. Select the Connection Managers that the endpoint computers should use.

> **NOTE**: To update the list of available Connection Managers, click **Add or modify Connection Managers**.

6. Click **Save**.

Step 5c: Assign the Computer Policy to Endpoint Computers

Assign the computer policy you just created to endpoint computers.

Manually Assigning the Computer Policy

1. In the Imprivata Admin Console, go to the **Computers** menu > **Computers** page.
2. Select the computers to which you want to assign the computer policy. You can use **Search for Computers** to enter search criteria.
3. Select **Apply Policy**.
4. Select **Choose a policy for selected computers**, choose the policy from the list, and then click **Apply Policy**.

Automatically Assigning the Computer Policy

Computer policy assignment rules let you assign a policy to existing endpoint computers and make sure that the policy is automatically assigned to endpoint computers that are added later.

To use a rule to assign the computer policy:

1. In the Imprivata Admin Console, go to the **Computers** menu > **Computer policy assignment** page.
2. Click **Add new rule**.
3. Name the rule and select the assignment criteria.
4. Select the policy you created and click **Save**.

> **BEST PRACTICE:** When assigning a computer policy to ProveID Embedded thin clients only, select **Imprivata agent type** > **ProveID Embedded**.

Step 6: Create and Apply a User Policy

Create and apply a user policy that automates user access to VMware Horizon.

Step 6a: Create a User Policy

1. In the Imprivata Admin Console, go to the **Users** menu > **User policies** page.

   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, select **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 **Enable virtual desktop automation**.
7. Select **Automate access to full VDI desktops** to have Imprivata automatically handle login behavior for VMware Horizon endpoint computers. Roaming users with this policy will have streamlined access to the VMware Horizon environment.
8. Click **Save**.

Step 6b: Apply a User Policy

1. To apply a user policy to other users, in the Imprivata Admin Console, go to the **Users** menu > **Users** page.
2. Select the users to which you want to apply the user policy.

   You can view additional pages of the **Users** list without losing your selections. The users you have selected are tracked and displayed on a counter at the top of the page.

   

   BEST PRACTICE: To select multiple users more efficiently, use the **Search for Users** tool at the top of the **Users** page. 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**.

Step 7: (Optional) Override the Desktop Chooser

By default, when a user is entitled to multiple desktops, they are prompted to choose which one to launch.

If you are deploying single-user computers, you can override this behavior by configuring a registry key (**DesktopToAutoLaunch**). This registry key streamlines desktop access by letting you specify which desktop should automatically launch for the user on the Windows endpoint.

To specify which desktop should be launched:

1. From the endpoint, open the Registry Editor.

2. Create the following registry key:

Name	Data Type	Location	Value
DesktopToAutoLaunch	String	HKEY_LOCAL_ MACHINE\SOFTWARE\SSOProvider\VDI	*<name_of_virtual_desktop_ as_it_appears_in_the_ chooser>*

Troubleshooting

Enabling VMware Menu Bar

By default, Imprivata ProveID Embedded does not display the VMware desktop menu bar (shade bar). You can use the ProveID Embedded configuration editor to modify the behavior.

To run the configuration editor, open a terminal and enter the following:

```
/usr/lib/imprivata/runtime/bin/configuration-editor
```

The following example configures the thin client to display the menu bar:

```
usr/lib/imprivata/run/bin/configuration-editor menubar
```

The following example configures thin client to hide the menu bar:

```
usr/lib/imprivata/run/bin/configuration-editor nomenubar
```

Enabling USB Devices on VMware Horizon Virtual Desktops

The VMware Horizon virtual desktop does not by default enable devices plugged into a USB port on a Windows endpoint computer.

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\SSOProvider\VDI\View**

Enabling the Imprivata USB Receiver for Hands Free Authentication on VMware Horizon Virtual Desktops

The Imprivata USB Receiver for Hands Free Authentication for Imprivata Confirm ID is not enabled by default on VMware Horizon View virtual desktops.

1. Open the Registry Editor.
2. Navigate to the appropriate location:
   - 64-bit computers: **HKEY_LOCAL_MACHINE\SOFTWARE\SSOProvider\DeviceManager**
3. Locate **RedirectionSupported** and change the **Value** to **1**.
4. Create the **RemoteOnly** registry key with a **Data Type** of **DWORD** and a **Value** of **1**.

Enabling Proximity Cards

To enable detection of proximity card events by the Imprivata agent on the VMware Horizon virtual desktop, create the **RedirectionSupported** registry key with a **Data Type** of **DWORD** and a value of **1**:

- 64—bit computers: **\HKLM\Software\SSOProvider\DeviceManager**

To prevent simultaneous RF IDeas reader access by two Imprivata processes, create the **RemoteOnly** registry key with a **Data Type** of **DWORD** and a value of **1**:

- 64—bit computers: **\HKLM\Software\SSOProvider\DeviceManager**

Troubleshooting UPN Format for VMware Horizon Authentication

If you have enabled the UPN format for authentication, Imprivata OneSign supports additional registry-based configuration for launching VMware Horizon to better support UPN format credentials. These registry values allow more fine-grained control of the launch process:

- **UseInteractive** — if set to **1**, VMware Horizon does not use the **–nonInteractive** option on the command line. If set to **0**, it is on the command line.
- **DisableDomainName** — if set to **1**, VMware Horizon will not issue the **–domainName** option on the command line. If set to **0**, it will appear on the command line.
- **useDomainName** — a string value that allows the customer to specify an alternate domain name. The Imprivata-derived domain name is used by default.

Set these registry keys with a **Data Type** of **DWORD**:

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

Configuration Options

Set the following registry keys as indicated below to configure the presentation of the VMware Horizon virtual desktop. These configurations should fully automate the connection process, unless the user has multiple entitlements.

Virtual Desktop with No VMware Horizon Interface or Toolbar

With this configuration the VMware Horizon user interface and toolbar will not be displayed on the virtual desktop:

- **UseInteractive** = 1
- **DisableDomainName** = 0
- **DomainName** = Your alternate domain name, if needed.

Virtual Desktop Displays VMware Horizon Interface and Toolbar

With this configuration the VMware Horizon user interface and toolbar will be displayed on the virtual desktop:

- **UseInteractive** = 1
- **DisableDomainName** = 0
- **DomainName** = Your alternate domain name, if needed.

The desktop toolbar in the virtual desktop will be displayed unless a Group Policy Object has removed it.

User Credentials are not Passed to the Virtual Desktop

If users are prompted to log into the virtual desktop after successfully logging into the endpoint computer, verify that the VMware client sessions are enabled for SSO.

To verify that SSO is enabled:

1. Log into the VMware Horizon View Administrator console.
2. Click **View Configuration** > **Global Settings**.
3. Go to the **General** section and verify that **Single sign-on (SSO)** is **Enabled**.
4. If it is set to **Disabled**, click **Edit**, select **Enabled**, and then click **OK**.

Multiple Client Sessions Launch at VMware Horizon Virtual Desktops on Windows

In a specific situation, multiple instances of a VMware Horizon client launch for VMware Horizon virtual desktops on Windows endpoints. End-users may or may not notice the icons for the multiple instances in the right corner of the Windows task bar on the endpoints.

This situation occurs if multiple VMware Horizon Connection Managers are specified in the computer policy assigned to the endpoint computers. This specification occurs in Step 5b: Configure the Computer Policy to Endpoint Computers.

If this problem occurs, implement the following fix. Create the **AutoBalancerMode** Windows registry key with a **Data Type** of **DWORD** on the endpoint computers. This key can enable automatic load balancing among the multiple Connection Managers specified in the computer policy.

Create the key at this location:

For 64-bit computers: **HKEY_LOCAL_MACHINE\SOFTWARE\SSOProvider\VDI\AutoBalancerMode**

Specify one of these values for the DWORD:

- **2**: Randomly pick a Connection Manager in the computer policy and launch one instance of a Horizon Client for it.
- **1**: Pick the first available Connection Manager in the computer policy and launch one instance of a Horizon Client for it.

This DWORD value is also available, but it will not fix the problem:

- **0** (default, disabled): No load balancing. For each Connection Manager in the computer policy, launch a Horizon Client instance.

Branding Login and Enrollment Screens

You can display your corporate logo on Imprivata login and enrollment screens for Imprivata single-user and kiosk workstations. See "Branding the Login and Self-Service Experience" in the Imprivata Online Help.