imprivata®

Product Documentation

Configuring VMware Horizon View RDS Hosted Applications

Imprivata Enterprise Access Management 24.2

Configuring Support for VMware Horizon View RDS Hosted Applications

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 Imprivata Virtual Desktop Access with VMware Horizon View RDS hosted applications. Imprivata Authentication Management and Virtual Desktop Access licenses are required for this feature.

NOTE: To configure support for VMware Horizon View virtual desktops, see Configuring Support for VMware View Virtual Desktops.

This document contains the following sections:

Before You Begin

Note the URL of the VMWare View Connection Manager

To support VMware Horizon View RDS hosted applications (RDS hosted applications), Imprivata must connect to a VMware Horizon Connection Manager. You need the URL of this broker when configuring your VMware View environment, and when configuring the Imprivata connection to the VMware App applications. See Step 6: Configure Imprivata's Connection to VMware View

Note the Names of the RDS Hosted Applications

When configuring Imprivata's connection to the VMware Horizon Connection Manager, you enter the name of each VMware application to be published to endpoint computers. These applications include:

- A Remote Desktop Services (RDS) virtual desktop.

> **NOTE:** Although you can publish an RDS virtual desktop, it is considered an application.

- The applications that are deployed to and launched from an RDS desktop.

You must spell the application names exactly the same, including spacing and capitalization, as they appear in the VMware View Horizon Administrator console. See Step 6: Configure Imprivata's Connection to VMware View

Copy the Domain Certificate to the Thin Clients

To support RDS hosted applications, copy the domain certificate from the VMware Horizon Connection Manager and add it to all 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.

Imprivata Virtual Desktop Access reconnects to any existing application sessions, including those that:

- You have configured the user policy to automatically launch.
- Users have launched manually.

Installation Sequence

Step 1: Install the VMware View Agent and Client Software

Before you configure Imprivata with RDS hosted applications:

- Review Imprivata Enterprise Access Management Supported Components to confirm your VMware View agent and client versions are supported by Imprivata.
- View the software listed in the Windows **Control Panel** > **Add Remove Programs** for all VMware virtual machines (VMs) and endpoint computers. Verify that the:
  - VMware View agent is installed on all VMs.
  - VMware Horizon View Client (View Client) is installed on all endpoint computers.

Step 2: Configure the View Client to Reconnect to Open Applications

After a workstation lock/unlock, users may be inadvertently disconnected from RDS hosted applications that are automatically launched. Configuring the View Client to automatically reconnect to open applications prevents users from having to manually launch the disconnected applications.

Complete the following on all endpoint computers:

1. From the endpoint computer, open the View Client.
2. From the gear icon menu, click **Applications** > **Reconnect automatically to open applications.**
3. Click **OK**.

Step 3: Install the Imprivata Agent on all Virtual Machines

To install the Imprivata agent to all VMs:

1. Install the Imprivata agent on one VM.
2. Clone the VM for all of the installations you require.

Step 4: Install the Imprivata Agent on all RDS Session Hosts

Install the Imprivata Citrix or Terminal Server agent on each RDS session host. For complete installation details, see "Deploying the Imprivata Agent" in the Imprivata Online Help.

Step 5: Install the Imprivata Agent on All Endpoint Computers

The Imprivata agent must be installed on each endpoint computer on which VMware View 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.

Step 6: Configure Imprivata's Connection to VMware View

To support RDS hosted applications, Imprivata agents must communicate with one or more VMware Horizon Connection Managers.

1. In the Imprivata Admin Console, go to the **Computers** menu > **Virtual desktops** page > **VMware Horizon – Apps** section.
2. Enter the URL of each VMware Horizon Connection Manager. To add more than one server, click **Add another server**.
3. From **Authenticate using**, select the type of credentials that apply to the applications on the specified server.
4. Enter the application names. You can enter:
   - One or more RDS virtual desktops.
   - One or more applications that are deployed to and launched from an RDS desktop.

NOTE: You must spell the application names exactly the same, including spacing and capitalization, as they appear in the VMWare View Horizon Administrator console.

Select the User Logon Format for VMware View 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 7: Create and Assign a Computer Policy for Endpoint Computers

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

Endpoint computers and virtual applications 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 7a: 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 7b.
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 7b: Configure the Computer Policy to Endpoint Computers

1. Click the **Virtual Desktops** tab and go to the **VMware Horizon – Apps** section.
2. Select **Automate access to VMware Horizon**.
3. You can control the behavior when an endpoint computer is locked:
   - Select **Keep the VMware Horizon client and user session active** to preserve the user session. When a user logs back into the endpoint computer or roams to another endpoint computer that is enabled with VMware Horizon, their applications are preserved just as they were when the endpoint computer is locked.
   - Select **Shutdown the VMware Horizon client and disconnect the user session** to help optimize resource consumption and minimize the total number of active sessions in use in the enterprise. When a user logs back into the endpoint computer (or another endpoint computer with VMware View enabled), their applications relaunch.
4. Select the servers that the endpoint computers should use.

   NOTE: To update the list of available servers, click **Add or modify VMware servers**.
5. Click **Save**.

Step 7c: Assign the Computer Policy to Endpoint Computers

Assign the computer policy to the endpoint computers.

Manually Assigning the Computer Policy

To assign the computer policy:

1. In the Imprivata Admin Console, go to the **Computers** menu > **Computers** page.
2. Select the computers to which to assign the computer policy. You can use **Search for Computers** to enter search criteria.
3. Click **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**.

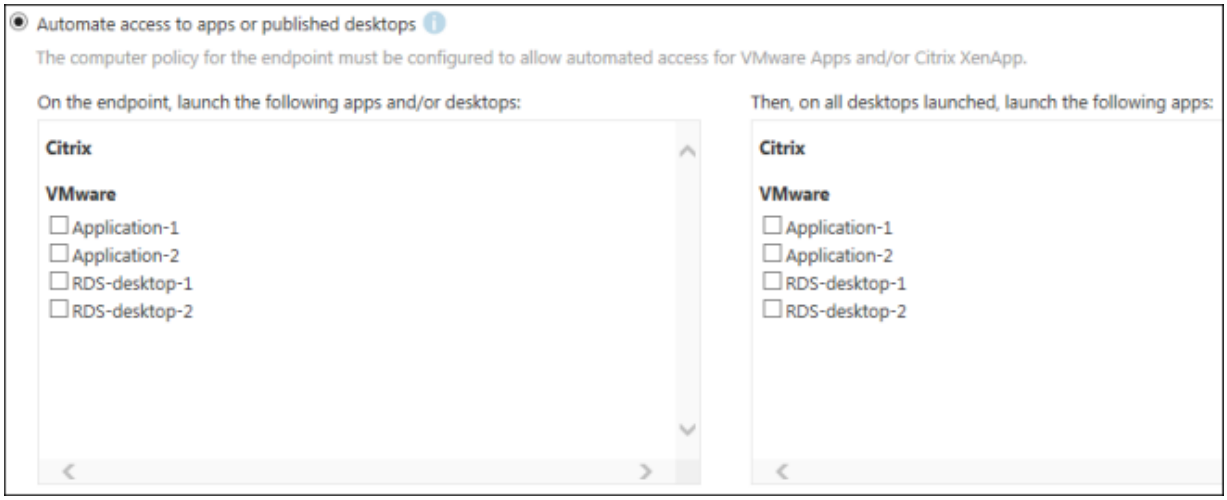
BEST PRACTICE: When assigning a computer policy to ProveID Embedded thin clients only, select **Imprivata agent type** > **ProveID Embedded**.

Step 8: Create and Apply a User Policy

Create and apply a user policy that automates user access to RDS hosted applications.

Step 8a: Create a User Policy

1. In the Imprivata Admin Console, go to the **Users** menu > **User policies** page.
2. 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 6.
3. To copy the Default User Policy, select **Default User Policy**, and then click **Copy**.
4. Click **Default User Policy (2)**.
5. Rename the user policy.
6. Click **Virtual Desktops**.
7. Select **Enable virtual desktop automation** > **Automate access to apps or published desktop**. The list of applications configured in Step 6: Configure Imprivata's Connection to VMware View are listed in two panes.



8. Configure one of the following:
   - If you only want to automatically launch applications, select the applications from the left pane. Do not select applications from the right pane.
   - If you only want to automatically launch an RDS desktop, select the RDS desktop from the left pane. Do not select applications from the right pane.
   - If you want to automatically launch an RDS desktop and individual applications, which are not on top of the desktop, select the RDS desktop from the left pane and the applications from the left pane.
   - If you want to automatically launch applications on top of an RDS desktop, select the RDS desktop from the left pane, and then select the applications from the right pane.
9. Click **Save**.

Step 8b: Apply a User Policy

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

   You can view additional pages of users without losing your selections. The users that you select are saved and a counter on the top of the page lists the number of selected users.

   BEST PRACTICE: To select multiple users more efficiently, use the **Search for Users** tool at the top of the **Users** page. The tool offers search parameters for refining your results.

3. Click **Apply Policy**.
4. Choose a policy, and then click **OK**.

Troubleshooting

Enabling USB Devices on VMware View RDS Desktops

By default, the VMware Horizon View RDS virtual desktop does not enable devices plugged into a USB port on a Windows endpoint computer. To enable the support of a USB port, 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 the following location:

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

Enabling Proximity Cards on Thin and Zero Clients

To enable detection of proximity card events by the Imprivata agent on the VMware Horizon View RDS 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 View Authentication

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

- **UseInteractive** — This key has no effect on RDS hosted applications.
- **DisableDomainName** — if set to **1**, VMware View 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**

Branding Login and Enrollment Screens

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