Product Documentation

Configuring Microsoft Windows 365

Virtual Kiosks

Imprivata Enterprise Access Management 26.1

Contacting Imprivata

20 CityPoint, 480 Totten Pond Road, 6th Floor

Waltham, MA 02451 USA

Phone: 781-674-2700

Toll-Free: 1-877-OneSign

Fax: 1 781 674 2760

Support: 1 800 935 5958 (North America)

Support: 001 408-987-6072 (Outside North America)

https://www.imprivata.com

support@imprivata.com

Copyright and Legal Information

Trademark Information

Legal Notices

Document revision 26.1

Configuring Windows 365 Cloud PC for Virtual Kiosks

This document details how to configure Microsoft Windows 365 Cloud PC and Imprivata Virtual Desktop Access for virtual kiosks.

This document contains the following sections:

Configuring Windows 365 Cloud PC for Virtual Kiosks **3**
- The Virtual Kiosk Workflow 4
  - Overview 4
  - Example Workflow 4
- Before You Begin 5
  - Imprivata License Requirements 5
  - Software Requirements 5
  - Local Endpoint Requirement 5
  - Microsoft Entra Single Sign-on and the Host Pool 5
- Windows 365 Configuration 5
  - Step 1: Install the Imprivata Agent on the Windows 365 Virtual Desktop 7
    - Use the Installation Wizard 7
    - Use a Third-Party Software Distribution Tool 7
  - Step 2: Enable the Virtual Desktop for the Workflow 8
- Windows Endpoint Configuration 8
  - Step 1: Verify that Endpoints can Access the Imprivata Web Service 8
  - Step 2: Install the Microsoft Windows App 9
- Require the Use of the Windows App 9
- Prevent Windows App from Spanning Multiple Monitors 9
  - Step 3: Configure Generic Workstation-based Credentials 9
    - Session Persistence 10
    - Create a Generic User Account 10
    - Configure the Endpoint to Login with the Generic Credentials 10
  - Step 4: Install the Imprivata Agent on Endpoints 10
    - Use the Installation Wizard 10
    - Use a Third-Party Software Distribution Tool 11
    - Disable the Imprivata Agent 11
- Imprivata Enterprise Access Management Configuration 12

The Virtual Kiosk Workflow

A virtual kiosk lets multiple users share a virtual desktop and use the same applications under the correct credentials. Users access the virtual desktop from a shared local Windows endpoint.

Allowing users to share the same virtual desktop helps to reduce the overhead associated with maintaining a virtual desktop for each user.

Overview

When a virtual kiosk is deployed:

- Generic credentials are used to log into the local Windows endpoint and automatically launch a Windows 365 session.

  In this workflow, you configure the virtual desktop to launch automatically. Imprivata Virtual Desktop Access does not launch the virtual desktop.
- While the virtual desktop remains running and logged in with the generic credentials, users authenticate to the Imprivata agent, which provides session-based access to applications that are enabled for SSO.
- When the Imprivata agent detects a user switch, Imprivata Enterprise Access Management either shuts down the open applications on the virtual desktop, or can keep an application open but switch the user that is logged in.

Example Workflow

The following details an example workflow:

1. The local Windows endpoint starts.
   - The endpoint establishes an Azure Virtual Desktop session using generic user credentials and launches the virtual desktop.
   - The desktop continues to run under the generic credentials.
2. User 1 taps their proximity card to authenticate and begins working with applications.
   - **Application A** is configured to remain open after a user logs off.

     Epic Hyperspace configured with the Imprivata Connector for Epic Hyperdrive is an example of this configuration.
   - **Application B** is enabled for SSO and is profiled with the Imprivata Application Profile Generator (APG) to shut down automatically after a user logs off.

   The Imprivata Citrix or Terminal Server agent manages SSO for these applications.
3. User 1 also opens **Application C**, which is not profiled with the Imprivata APG.
4. User 1 does not close any of their applications and taps their proximity card to secure the endpoint.

- The Azure Virtual Desktop session remains open.
- The Enterprise Access Management session is locked but not logged off.

5. User 2 taps their proximity card to authenticate.
   - **Application A**: The Imprivata Citrix or Terminal Server executes the logoff sequence to switch users with the application. Depending on the application settings, the same screen that User 1 was viewing appears. For example, the same patient chart appears.
   - **Application B** shuts down.
   - **Application C** remains open in the exact same state as User 1 left it.
6. User 2 taps their proximity card to secure the endpoint.

> **NOTE:**
> Configuring the Imprivata Connector for Epic Hyperdrive and SSO application profiles is beyond the scope of thisguide. For more information, see the Imprivata Connector for Epic Hyperdrive Configuration Guide andthe "SSO" section in the Imprivata Enterprise Access Management — SSO Help.

Before You Begin

Before you begin, be sure that you meet the following prerequisites:

Imprivata License Requirements

An Authentication Management or Single Sign-On license is required for this workflow.

Software Requirements

Verify that your Windows 365 environment:

- Is functioning normally, independent of Imprivata Enterprise Access Management, before installing and configuring Enterprise Access Management components.
- Meets the minimum or recommended Windows 365 and endpoint device requirements. For more information, see the Imprivata Enterprise Access Management Supported Components matrix.

Local Endpoint Requirement

Local endpoints must be Entra ID joined .

Microsoft Entra Single Sign-on and the Host Pool

Authenticating users using Microsoft Entra SSO is not supported.

Verify that Microsoft Entra SSO is not enabled in the RDP properties of your host pool.

Windows 365 Configuration

In this section you

- Install the Imprivata agent on your virtual desktops.
- Configure a series of registry settings to enable the virtual desktops for the workflow.

Step 1: Install the Imprivata Agent on the Windows 365 Virtual Desktop

Install the Imprivata shared kiosk (type 2) agent on the virtual desktops that will be delivered to your users.

Use the Installation Wizard

To install the Imprivata agent:

1. In the Imprivata Admin Console, click **Computers** > **Deploy agents**.
2. Download the agent installer from the **Deployment Procedure** section.
3. Run the installation wizard.

Completing the installation requires you to:

- Enter the FQDN or IP address of the Imprivata appliance to which the agent must connect to obtain the enterprise topology.
- Select the **Shared Kiosk Workstation** agent.

> **NOTE:**
> Launching the Imprivata agent installer directly requires you to execute the MSI from an elevated command prompt. You cannot directly run the installer by either double-clicking the MSI or right-clicking the MSI and running it as an administrator. This requirement does not apply to deployments performed through Microsoft Endpoint Configuration Manager (SCCM) or any other third-party software deployment tool.

Use a Third-Party Software Distribution Tool

To deploy the Imprivata agent using a third–party software distribution tool:

1. In the Imprivata Admin Console, click **Computers** > **Deploy agents**.
2. Download the agent installer from the **Deployment Procedure** section.
3. Deploy and run the Imprivata agent installation using the following syntax:
   ```
   msiexec.exe /i "<path_to_installer>\ImprivataAgent.msi
   IPTXPRIMSERVER="https://<appliance_FQDN>/sso/servlet/messagerouter"
   AGENTTYPE=2
   ```

The **IPTXPRIMSEVER** value specifies the appliance to which the Imprivata agent should connect to obtain the enterprise topology.

Consider the following:

- This syntax represents the required installation parameters. For a complete list of supported parameters, see "Distributing the Imprivata Agent from the Command Line" in the Imprivata Enterprise Access Management Online Help.

- The Imprivata agent installer supports standard msiexec options. For more information on these commands, run **msiexec /?**.

Step 2: Enable the Virtual Desktop for the Workflow

Configure the following registry settings on the virtual desktop to enable it for this workflow:

Name	Type	Location	Value
LockRemoteSessionWithAgentOnClient	DWORD	HKLM\Software\SSOProvider\ISXAgent	Default value: 0 Set to: 1
LockVirtualSessionWithHotKey	DWORD	HKLM\Software\SSOProvider\ISXAgent	Default value: 0 Set to: 1
RedirectionSupported	DWORD	HKLM\Software\SSOProvider\DeviceManager	Default value: 0 Set to: 1
RemoteOnly	DWORD	HKLM\Software\SSOProvider\DeviceManage	Default value: 0 Set to: 1
disablecad	DWORD	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\System	Default value: 0 Set to: 1

Windows Endpoint Configuration

In this section you:

- Verify that your local endpoints can access the Imprivata web service.
- Install the Microsoft Remote Desktop client on the local endpoints.
- Configure generic workstation-based credentials to automatically log into the local endpoint and deliver the virtual desktop.
- Install the Imprivata agent on the local endpoints.

Step 1: Verify that Endpoints can Access the Imprivata Web Service

Your local endpoints must be able to access the Imprivata web service endpoint URL (`https://avd.cloud.imprivata.com/`).

Coordinate with your network administrators to make sure that network restrictions do not prevent access to the Imprivata web service.

NOTE:
The Imprivata web service is not accessible via a web browser. The URL serves as the address through which the endpoint interacts with the web service.

Step 2: Install the Microsoft Windows App

The Microsoft Windows App lets your users connect to a virtual desktop.

For more information about getting started with Window App, see the Microsoft documentation.

> **NOTE:**
> Support for Windows 365 Cloud PC requires the use of the Windows App. If the Remote Desktop Client is installed on the local endpoint, you can either uninstall it or enforce the use of Windows App using the `ViewerType` registry value.

> **NOTE:**
> Using a web browser to connect to the virtual desktop is not supported.

Require the Use of the Windows App

The `ViewerType` registry value can be used to enforce the use of the Windows App, if the Remote Desktop Client is also installed on the local endpoint. Setting this value to `1` enforces the use of Windows App.

Location	Default state	Set to
HKLM\Software\SSOProvider\VDI\AVD\ViewerType	Not configured. If both clients are installed on the local endpoint, Imprivata Virtual Desktop Access falls back to the Remote Desktop Client.	1

Prevent Windows App from Spanning Multiple Monitors

By default, the Windows App spans all monitors when it opens. The `DisableMultiMonitor` registry value can be used to prevent the default behavior. Setting this value to `1` prevents the Windows App from spanning multiple monitors.

Location	Default state	Set to
HKLM\Software\SSOProvider\VDI\AVD\DisableMultiMonitor	Not configured. Windows App spans all monitors when it opens.	1

Step 3: Configure Generic Workstation-based Credentials

A generic user account is required to automatically log into the local endpoint and establish a session with the virtual desktop.

Session Persistence

Session persistence (roaming) can result in users obtaining an incorrect session when moving from one shared workstation to another.

To prevent roaming, you can take one of the following actions:

- Create a unique generic user for each shared local endpoint in the environment.
- Disable session roaming in your Azure Virtual Desktop environment.

Create a Generic User Account

When creating a generic user account, consider the following:

- When adding the generic user to your user directory, be sure that the account is not enrolled in EAM.
- These credentials are only used to automatically log in to the local endpoint and deliver the virtual desktop.
- The generic user account must have access to the virtual desktop, and the endpoint must be configured to automatically launch the virtual desktop.

  Imprivata Virtual Desktop Access does not launch the virtual desktop.

Configure the Endpoint to Login with the Generic Credentials

Configure the following registry settings to configure the local endpoint to automatically boot and authenticate to Windows using the generic workstation-based credentials.

Name	Type	Location	Value
AutoAdminLogon	STRING	HKLM\Software\Microsoft\WindowsNT\Winlogon	Default value: 0 Set to: 1
DefaultUserName	STRING	HKLM\Software\Microsoft\WindowsNT\Winlogon	The name of the generic user account.
DefaultPassword	STRING	HKLM\Software\Microsoft\WindowsNT\Winlogon	The password of the generic user account.
DefaultDomainName	STRING	HKLM\Software\Microsoft\WindowsNT\Winlogon	If using a domain user, set this value to the required domain.

Step 4: Install the Imprivata Agent on Endpoints

Install the shared-kiosk workstation (type 2) agent on your local endpoints.

The Imprivata agent is only required on the local endpoints for the USB-redirection of authentication devices. After you install the agent, you disable it from launching.

Use the Installation Wizard

To install the Imprivata agent:

1. In the Imprivata Admin Console, click **Computers** > **Deploy agents**.
2. Download the agent installer from the **Deployment Procedure** section.
3. Run the installation wizard.

Completing the installation requires you to:

- Enter the FQDN or IP address of the Imprivata appliance to which the agent must connect to obtain the enterprise topology.
- Select the **Shared Kiosk Workstation** agent.

> **NOTE:**
> Launching the Imprivata agent installer directly requires you to execute the MSI from an elevated command prompt. You cannot directly run the installer by either double-clicking the MSI or right-clicking the MSI and running it as an administrator. This requirement does not apply to deployments performed through Microsoft Endpoint Configuration Manager (SCCM) or any other third-party software deployment tool.

Use a Third-Party Software Distribution Tool

To deploy the Imprivata agent using a third–party software distribution tool:

1. In the Imprivata Admin Console, click **Computers** > **Deploy agents**.
2. Download the agent installer from the **Deployment Procedure** section.
3. Deploy and run the Imprivata agent installation using the following syntax:
   `msiexec.exe /i "<path_to_installer>\ImprivataAgent.msi IPTXPRIMSERVER="https://<appliance_FQDN>/sso/servlet/messagerouter" AGENTTYPE=2`

The **IPTXPRIMSEVER** value specifies the appliance to which the Imprivata agent should connect to obtain the enterprise topology.

Consider the following:

- This syntax represents the required installation parameters. For a complete list of supported parameters, see "Distributing the Imprivata Agent from the Command Line" in the Imprivata Enterprise Access Management Online Help.
- The Imprivata agent installer supports standard msiexec options. For more information on these commands, run **msiexec /?**.

Disable the Imprivata Agent

The Imprivata agent is only required on local endpoints for the USB-redirection of authentication devices. The Imprivata Citrix or Terminal Server agent on the virtual desktop manages user authentication.

Configure the following registry key to disable the Imprivata agent.

Name	Type	Location	Value
DisableLaunch	DWORD	HKLM\Software\SSOProvider\ISXAgent	Default value: 0 Set to: 1

Imprivata Enterprise Access Management Configuration

This workflow does not require a user policy or a computer policy with settings specific to Imprivata Virtual Desktop Access.

Configure these policies to meet the needs of your organization.