imprivata®

Product Documentation

Configuring Microsoft Azure Virtual Desktops

Virtual Kiosks

Imprivata Enterprise Access Management 25.1

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 25.1

Configuring Azure Virtual Desktop for Virtual Kiosks

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 details how to configure Microsoft Azure Virtual Desktop and Imprivata Virtual Desktop Access for virtual kiosks.

This document contains the following sections:

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 an Azure Virtual Desktop 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 Azure Virtual Desktop environment:

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

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.

Azure Virtual Desktop 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 Azure Virtual Desktop

Install the Citrix or Terminal Server agent (type 3) 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 **Citrix or Terminal Server** agent.

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=3
   ```

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

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 Remote Desktop Client

The Microsoft Remote Desktop client lets your users connect to a virtual desktop.

For more information about the Remote Desktop client and how to install it, see the Microsoft documentation.

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

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.

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

In this section you:

- Configure a computer policy and assign it to your local endpoints.
- Configure an extension object.
- Configure a computer policy and assign it to your virtual desktops.

NOTE:
This workflow does not require that you configure a user policy with settings that are specific to Imprivata Virtual Desktop Access.

Step 1: Configure and Assign a Computer Policy for Endpoint Computers

Configure a computer policy that lets your local endpoints function as virtual kiosks.

Configure the Computer Policy

To configure the computer policy:

1. In the Imprivata Admin Console, go to the **Computers** menu > **Computer Policies** page.
2. Do one of the following:
   - Click **Add** to create a new policy.
   - Click the name of an existing computer policy to edit it.
3. Go to the **Shared Workstation** tab > **Kiosk Workstations** section.
4. Select **Allow Fast User Switching with Citrix or Terminal Servers**.
5. Click **Save**.

Assign the Computer Policy

Assign the computer policy to your local endpoints.

Manually Assign the Computer Policy

To manually assign 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.
3. Click **Apply Policy**.
4. Select **Choose a policy for the selected computers**, select the policy from the list, and click **Apply Policy**.

Automatically Assign 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 automatically 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**.

Step 2: Secure the Virtual Desktop Session

Under certain circumstances, when the local endpoint connects to the virtual desktop, the session is unlocked. This might result in a non–Enterprise Access Management user gaining access to the virtual desktop.

To prevent this behavior and to ensure that the virtual desktop session remains locked until an Enterprise Access Management user authenticates, you can configure an extension object.

To configure the extension object,

1. In the Imprivata Admin Console, go to the **gear** icon menu, and click **Extensions**.
2. Go to the **Procedure code** section, and click **View/Edit**.
3. Click **Add**.
4. Enter a name, and click **Click here to choose an event**.
5. Under **Agents Events**, click **Agent Startup**.
6. Specify the following procedure code:
   `rundll32.exe user32.dll,LockWorkStation`
7. Specify that the code be written and executed as a batch script (`bat`), and click **Save**.

Step 3: Configure and Assign a Computer Policy for Virtual Desktops

Configure a computer policy that lets your virtual desktops function as virtual kiosks.

To configure the computer policy:

1. In the Imprivata Admin Console, go to the **Computers** menu > **Computer Policies** page.
2. Do one of the following:
   - Click **Add** to create a new policy.
   - Click the name of an existing computer policy to edit it.
3. Go to the **Citrix or Terminal Server** tab > **Authenticating generic user or anonymous Citrix XenApp or Terminal Server sessions** section.
4. Select **The XenApp or Terminal Server Windows session user and Imprivata user are not always the same**.
5. If not already selected, select **Always trust the Citrix or Terminal Server**.
6. Go to the **Fast User Switching** section, and under **Endpoints with an installed agent**, select **Allow Fast User Switching with the remote server if allowed in the computer policy**.
7. Select the computer policy you created for your local endpoints.
8. Go to **Extensions** tab, select **Enable Procedure Code Extension Object?**, and enable the procedure code you created.
9. Save the computer policy and assign it to your virtual desktops.