imprivata®

Product Documentation

Configuring Microsoft Azure Virtual Desktops

Shared Kiosks

Imprivata Enterprise Access Management 24.3

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 24.3

Configuring Azure Virtual Desktop for Shared 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 shared kiosks.

This document contains the following sections:

The Shared Kiosk Workflow

A shared kiosk let multiple users automatically connect to their own full virtual desktop from a shared local Windows endpoint.

Overview

When a shared kiosk is deployed:

- Generic credentials are used to automatically log into the local Windows endpoint and establish a Windows session.
- After a user authenticates on a shared local Windows endpoint, Imprivata Virtual Desktop Access automatically launches the virtual desktop.
- As a user authenticates on different shared Windows endpoints, they reconnect to their desktop virtualization session. This makes it appear as if the desktop, and all of the applications that are running on it, are "roaming" with them.

Example Workflow

The following details an example workflow:

1. The local Windows endpoint starts and establishes a Windows session using generic user credentials.
2. User 1 taps their proximity card to authenticate to the endpoint.
   - The virtual desktop for user 1 is automatically delivered to the local endpoint.

     If Microsoft detects that the user has multiple accounts, they are prompted to choose an account. This behavior only occurs the first time the user accesses the virtual desktop.
   - Everything associated with the virtual desktop, such as files, shares, and all other applications are available to them.
3. When user 1 is finished, they tap their proximity card to secure the endpoint.
4. User 1 continues their rotation, moving to a new location, and authenticates to a different Windows endpoint.
   - The virtual desktop for user 1 is reconnected (roamed) to the local endpoint.
   - The desktop and the applications are running in the same state as previously used.
5. When user 1 is finished, they tap their proximity card to secure the endpoint.
6. User 2 taps their proximity card to authenticate to the same shared Windows endpoint that user 1 was using.
   - The virtual desktop for user 2 is automatically delivered to the local workstation.
   - Everything associated with the virtual desktop, such as files, shares, and all other applications are available to them.

Before You Begin

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

Imprivata License Requirements

The following Imprivata licensed features are required:

- Virtual Desktop Access
- Authentication Management
- Single Sign-On

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.

Entra User Account to Grant Application Permissions

As part of the configuration process, you grant tenant-wide consent to let Imprivata Enterprise Access Management access your virtual desktops and authenticate your users.

Doing so requires a Microsoft Entra user account that can grant an application permission to the following APIs:

- Azure Virtual Desktop
- Microsoft Graph

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.

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.

Azure Virtual Desktop Configuration

In this section you:

- Grant Entra ID tenant-wide consent to Enterprise Access Management.
- Install the Imprivata agent on your virtual machines.
- Configure several registry settings to enable the virtual desktops for the workflow.

Step 1: Grant Tenant-Wide Consent and Assign Users

You grant tenant-wide consent to let Enterprise Access Management access your virtual desktops and authenticate your users.

Granting consent requires a Microsoft Entra user account that can grant an application permission to the following APIs:

- Azure Virtual Desktop
- Microsoft Graph

To grant consent:

1. Obtain the Imprivata application ID here.
2. Copy the following sample to build a URL:

   ```
   https://login.microsoftonline.com/<tenant_id>/adminconsent?client_
   id=<application_id>
   ```

   Where <*tenant_id*> specifies your Entra ID tenant ID and <*application_id*> specifies the Imprivata application ID.
3. Enter the URL into a browser to complete the consent process.
4. In the Microsoft Entra admin center, locate the **Imprivata AVD** application and do the following:
   a. Verify that Imprivata AVD has been granted consent to the following APIs:
      - Azure Virtual Desktop
      - Microsoft Graph
   b. Assign the required users and groups.

> **NOTE:**
> For more information, see the Microsoft documentation about reviewing application permissions and assigning users and groups to an application.

Step 2: Update Conditional Access Policies that Require MFA

Imprivata supports the integration with Azure Virtual Desktop and Windows 365 on Windows devices through the Imprivata AVD Microservice (Imprivata services). Consider the following:

- Azure Virtual Directory must be excluded from all conditional access policies that would require multifactor authentication (MFA) for Imprivata users.
- This exemption is required to allow communication between Imprivata services and Azure resources.

To configure the exception:

1. Locate the conditional access policy that applies to your Imprivata users.
2. Under **Target Resources**, click **All resources (formerly All Cloud apps)**.
3. Click **Exclude**, and then toggle **Select resources**.
4. Under **Select specific resources**, click **None** or any of the listed applications.
5. Search for **9cdead84-a844-4324-93f2-b2e6bb768d07**, and select **Azure Virtual Desktop**.
6. Repeat for all conditional access policies that would require MFA for Imprivata users.

Step 3: 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 4: 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
RedirectionSupported	DWORD	HKLM\Software\SSOProvider\DeviceManager	Default value: 0 Set to: 1
RemoteOnly	DWORD	HKLM\Software\SSOProvider\DeviceManager	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 your local endpoints.
- Configure generic workstation-based credentials to automatically log into the local endpoint.
- Install the Imprivata agent on your local endpoints.
- Optionally, configure the **DesktopToAutoLaunch** registry key to override the desktop chooser.

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.

Step 3: Configure Generic Workstation-based Credentials

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

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 establish a Windows session.

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\CurrentVersion\Winlogon	Default value: 0 Set to: 1
DefaultUserName	STRING	HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon	The name of the generic user account.
DefaultPassword	STRING	HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon	The password of the generic user account.
DefaultDomainName	STRING	HKLM\Software\Microsoft\WindowsNT\CurrentVersion\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.

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 /?**.

Step 5: (Optional) Override the Desktop Chooser

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

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	HKLM\SOFTWARE\SSOProvider\VDI	<name_of_virtual_desktop_as_it_appears_in_the_chooser>

Imprivata Enterprise Access Management Configuration

In this section you:

- Configure a computer policy and assign it to your local endpoints.
- Configure a user policy and assign it to the users who require access to a virtual desktop.
- Import and deploy the AVD single sign-on application profile.
- Limit SSO to the Microsoft Remote Desktop client.

Step 1: Configure and Assign a Computer Policy

Configure a computer policy that automates access to virtual desktops and assign it to your local endpoints.

Configure a Computer Policy

To configure a 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 **Virtual Desktops** tab > **Microsoft Azure Virtual Desktops** section.
4. Select **Automate access to Azure Virtual Desktop**.
5. Choose one of the following options:
   - **Prompt the user only if they have multiple desktops**. If the user is entitled to one desktop, it launches automatically after login. If a user is entitled to multiple desktops, an Imprivata OneSign dialog prompts the user to choose a desktop.
   - **Always prompt the user to choose their desktop**. An Imprivata OneSign dialog always prompts the user to choose a desktop, regardless of how many desktops they are entitled to.

   > **NOTE**: If 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.

6. You can control the behavior when an endpoint computer is locked. Under When a Remote Desktop endpoint is locked, choose one of the following
   - **Keep the Remote Desktop and user session active**. This option preserves the user session. When a user logs back into an endpoint computer, or logs into another endpoint computer that is enabled for virtual desktop access, their desktop and applications are preserved just as they were when the endpoint computer was locked.
   - **Shutdown the Remote Desktop 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 an endpoint computer, or logs into another endpoint computer that is enabled for virtual desktop access, their desktop is relaunched.
7. 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: Configure and Assign a User Policy

Configure a user policy that automates access to virtual desktops and assign it to your users.

Configure a User Policy

To configure a user policy:

1. In the Imprivata Admin Console. go to the **Users** menu > **User Policies** page.
2. Do one of the following:
   - Click **Add** to create a new policy.
   - Click the name of an existing user policy to edit it.
3. Go to the **Virtual Desktops** tab, and select **Enable virtual desktop automaton**.

   By default, **Automate access to full VDI desktops** is enabled.
4. Select **Microsoft**, and click **Save**.

Assign the User Policy

To assign the user policy:

1. 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 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**, choose the policy you created, and click **OK**.

Step 3: Import and Deploy the AVD SSO Application Profile

By default, users are prompted to log into the Microsoft Remote Desktop client to launch a virtual desktop. Import the AVD SSO application profile to prevent your users from having to enter their credentials manually.

To import the profile:

1. Download and extract the application profile from here.
2. In the Imprivata Admin Console, go to the **Applications** menu, and click **Single sign-on application profiles**.
3. Click **Add App Profile** > **Import from file**, and import the profile.
4. From the list of application profiles, select **RemoteDesktopClient**, and then click **Deploy**.
5. Go to the **Deployment** section, and select **Deploy this Application?**.
6. Optional: By default, an application profile is configured to deploy to all users. If you want to limit the deployment to specific organizational units, groups, or users, uncheck **Deploy to All Users and Groups?** and do the following.
   a. Select the domain that contains the target users.
   b. Select **These OUs, groups, and users**.
   c. Do one, two, or all three of the following:
      - Click **Select OUs**, select the target organizational units, and then click **Done**.
      - Click **Select Groups**, select the target groups, and then click **Close**.
      - Enter a semi-colon separated list of specific users.
7. Leave the remaining settings unchanged.
8. Click **Save**.

Step 4: Limit SSO to the Remote Desktop Client

The AVD SSO application profile prevents users from having to manually enter their credentials to log into the Microsoft Remote Desktop client. However, by default, Microsoft prompts users to use the proxied credentials to stay signed into all other applications that use Entra ID as the identify provider.

To prevent users from being prompted, and to limit SSO to the Remote Desktop Client, configure the following registry key on your local endpoints.

Name	Type	Location	Value
BlockAADWorkplaceJoin	DWORD	HKLM\SOFTWARE\Policies\Microsoft\Windows\WorkplaceJoin	Default value: 0 Set to: 1