Product Documentation

Configuring Citrix XenDesktop

Imprivata Enterprise Access Management 25.3

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 25.3

This document includes information about configuring Imprivata Virtual Desktop Access with Citrix XenDesktop. An Imprivata Virtual Desktop Access license is required.

This document includes the following sections:

Before You Begin

Software Requirements

Review the following:

- Verify that the Citrix XenDesktop environment is functioning normally, independent of Imprivata, before installing and configuring Imprivata components.
- Review the Imprivata Enterprise Access Management with SSO Supported Components matrix to confirm that your environment meets all of the minimum or recommended Citrix and endpoint device requirements.

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.

Session Persistence Using COOKIEINSERT

Session persistence maintains the connection between an endpoint and the Citrix Storefront after load balancing is performed. A common way to maintain session persistence is to use the endpoint source IP address. However, customers who use Network Address Translation (NAT) in front of a NetScaler load balancer cannot use this persistence method, because endpoints appear to have the same IP address at the load balancer.

Those customers must use the NetScaler COOKIEINSERT session persistence method. This method causes the NetScaler to insert a cookie into client requests, which the NetScaler uses to track the server to which the connection belongs.

To enable session persistence using COOKIEINSERT, perform this procedure **after** you have completed all steps in the main Installation Sequence section further below.

1. Configure the Citrix NetScaler's Persistence type to be COOKIEINSERT and specify a cookie name to use, for example, persistcookie.
2. Specify the same cookie name in your endpoints using either method a or b.

   In both methods, VALUE is the cookie name you specified in the Citrix NetScaler:

a. **For Imprivata ProveID Embedded Linux endpoints:**

   Add a new configuration option to the imprivata.conf configuration file on the endpoints, using one of two methods:

   - Add this new section to the imprivata.conf file:
     ```
     [citrix]
     cookie-insert = VALUE
     ```
   - Or run this command from the endpoint system prompt:
     ```
     /usr/lib/imprivata/runtime/bin/configuration-editor citrix --cookie-insert VALUE
     ```

b. **For Windows endpoints:**

   Configure the cookie name using this Registry key:
   ```
   HKLM\Software\SSOProvider\VDI\CookieInsertName String VALUE;
   ```

3. Reboot the endpoints.

Troubleshooting

An Imprivata agent log file entry that indicates a problem with this session persistence method is:

`Failed to get COOKIEINSERT token` – The Imprivata agent failed to get the cookie from the header. Make sure that the cookie names are the same on the NetScaler and the endpoints.

Citrix Workspace App Configuration

After installing Citrix Workspace app, additional configuration is required to support Enterprise Access Management.

If you have not completed the configuration, see *Configuring Citrix Workspace App for* Enterprise Access Management in the Online Help.

NOTE: Citrix Workspace app is not required for ProveID Embedded–enabled thin clients.

Note the Citrix Connection Information

Imprivata agents communicate with known Citrix stores. The following table details the types of URLs that can be used to configure the connection to the Citrix store and the endpoints on which they are supported.

URL type	Examples	Endpoint type
Citrix DaaS	• https://example.cloud.com	You can use this URL for Windows endpoints only.
Store Front	• https://citrix-xendesk.example.com/Citrix/Store/ • https://citrix-xenapp.example.com/Citrix/Store/	You can use this URL for Windows endpoints only.
StoreFront Web Site	• https://citrix-xendesk.example.com/Citrix/StoreWeb/ • https://citrix-xenapp.example.com/Citrix/StoreWeb/	You can use this URL for Windows and PIE endpoints.
XenApp Services (PNAgent)	• https://citrix-xendesk.example.com/Citrix/Store/PNAgent/config.xml • https://citrix-app.example.com/Citrix/Store/PNAgent/config.xml	You can use this URL for Windows and PIE endpoints.

Configure Citrix for Native Connections to Stores

Additional Citrix configuration is required to support native connections to Citrix StoreFront stores. The Citrix store must be configured with the following authentication methods to support Imprivata OneSign:

- User name and password
- Domain pass-through
- HTTP basic — Even if the store is configured for HTTPS, this authentication method is required.

To configure the required authentication methods:

1. Open Citrix Studio.
2. Go to **Citrix StoreFront** > **Receiver for Web**.
3. Select the store you want to manage.
4. In the **Store Web Receiver** pane, click **Choose Authentication Methods**.
5. Click **Add/Remove Methods** and enable the required methods.

Enable Control+Alt+Delete for Virtual Desktops

Imprivata recommends that control + alt + delete is enabled for all virtual desktops that you are configuring.

1. From the domain controller, open the **Group Policy Management Console**.
2. In the required domain, select the group policy object that applies to the virtual desktops and click **Edit**.
3. In the Group Policy Management Editor, go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies**.
4. Select **Security Options**.
5. Select **Interactive logon: Do not require CTRL+ALT+DEL** and right-click.
6. Select **Properties** > **Define this policy setting** > **Disabled** and click **OK**.

Citrix DaaS Connections

If you are managing your deployment through the Citrix Cloud, complete the following before you configure Imprivata Virtual Desktop Access.

> **NOTE:**
> Citrix DaaS connections are supported on Windows endpoints only.

Create a Citrix Cloud OAuth Client

A Citrix Cloud OAuth client is required to allow Enterprise Access Management to access Citrix Cloud APIs.

To create the client:

1. From the Citrix Cloud admin console, go to **Identity and access management** > **API Access** > **Workspace API**.
2. Enter a user-friendly display name. For example, Imprivata client.
3. Specify an email address to receive notifications about the client.
4. Create either a public or private client with the following configuration:
   a. Set **Require users to accept consent when accessing this client** to **No**.
   b. Set **Require Proof Key** to **Yes**.
   c. Set **Will the consuming Application require Offline Access** to **No**.
5. Add **http://localhost:60000** as a redirect URL.

   If you are unable to use port 60000, you can specify any other dynamic port range by setting the following registry key (DWORD) on all of your endpoints:
   `HKEY_LOCAL_MACHINE\SOFTWARE\SSOProvider\ISXAgent\CitrixCloudDefaultServerPort`

   > **NOTE:**
   > This port is used internally by the Imprivata agent on the endpoint. The port does not need to be opened or exposed for external access.

6. Create the client.
7. If you have created a private client, copy or download the client secret.

   You require the secret when configuring the Imprivata connection to your Citrix store(s).

   > **NOTE:**
   > The client secret cannot be retrieved again. If you lose it, you will need to rotate it.

Locate the Client ID and Application ID

Configuring the Imprivata connection to the Citrix store requires the following:

- A client ID
- An application ID
- If you created a private client, the client secret.

To locate the client and application ID:

1. From the Citrix Cloud admin console, go to **Identity and Access Management** > **API access** > **Workspace API**.
2. Locate your client, and note the client ID and application ID.
3. If you created a private client and do not have the client secret, edit the client. Editing the client gives you the option to rotate the secret and copy it.

Configure Imprivata Web SSO for SAML Authentication

SAML authentication eliminates the need to send a user name and password between Enterprise Access Management and Citrix when authenticating Enterprise Access Management users.

Using SAML authentication requires that you configure Imprivata Web SSO.

> **NOTE:**
> It is also recommended that you configure Citrix Federated Authentication Service (FAS). If you do not configure Citrix FAS, users are prompted to log in manually after the virtual resources are launched.

Step 1: Configure a Connection to the Imprivata Cloud

Imprivata provides you with an Enterprise ID and one-time cloud provisioning code. This information is required to configure a connection to the Imprivata cloud.

1. In the Imprivata Admin Console, click the **gear** icon, and then click **Cloud connection**.
2. Enter your Enterprise ID and cloud provisioning code.
3. Click **Establish Trust**.

Step 2: Retrieve the Imprivata SAML Metadata and Certificate

Configuring Citrix as the Service Provider requires the Imprivata IdP metadata and the x.509 certificate.

To retrieve the required information:

1. In the Imprivata Admin Console, click the **gear** icon, and then click **Web app login configuration**.
2. Click **View and copy Imprivata (IdP) SAML metadata**.

3. Copy and save the following:
   - The entity ID URL.
   - The SSO post URL.
   - The SLO post URL.
4. Download the Imprivata IdP certificate.

Step 3: Configure Citrix Cloud as the SAML Service Provider

Configuring Citrix as the Service Provider requires the Imprivata SAML metadata and certificate.

To configure Citrix as the SP:

1. In the Citrix Cloud console, go to the menu, and click **Identity and Access Management**.
2. From the **Authentication** page, add Imprivata as an IdP.
   Be sure to specify SAML 2.0 as the authentication type.
3. Connect to your new IdP, and specify an administrator sign-in URL.
4. Download the service provider SAML metadata and save it to an XML file.
   You require the metadata when configuring the Imprivata SSO application profile for SAML.
5. Enter the following Imprivata IdP metadata that you copied from the Imprivata Admin Console:
   a. The entity ID
   b. The SSO post URL
   c. The SLO URL
6. Upload the Imprivata x.509 certificate.
7. Note the following Citrix Identity Platform attributes. You must map these attributes to your user directory (domain) when configuring the Imprivata application profile for SAML:
   - cip_sid
   - cip_upn
   - cip_email
   - cip_oid

Step 4: Locate the Workspace URL

You require your Workspace URL when configuring the Imprivata connection to your virtual resources.

To locate the URL:

1. In the Citrix Cloud console, go to the menu, and click **Workspace configuration**.
2. From the **Authentication** page, copy and save your Workspace URL.

Step 5: Configure an Imprivata Web SSO Application Profile

An Imprivata Web SSO application profile is required to configure SAML authentication.

To configure the application profile:

1. In the Imprivata Admin Console, click **Applications** > **Single sign-on application profiles**.
2. Click **Add App Profile** > **Application using SAML**.
3. Enter an application profile name and user-friendly name.
4. Click **Get SAML metadata**, select **From XML**, and upload the SP SAML metadata XML file.
5. Map the following Citrix Identity Platform attributes to your user directory (domain):
   - cip_sid
   - cip_upn
   - cip_email
   - cip_oid
6. Save the application profile and deploy it to your users.

Step 6: Configure Citrix Federated Authentication Service

After you configure Web SSO for SAML authentication, it is recommended that you configure Citrix FAS. If you do not configure Citrix FAS, users are prompted to log in manually after the virtual resources are launched.

For more information, see Configuring Support for Citrix Federated Authentication Service.

Installation Sequence

Step 1: Install the Latest Citrix Software

Before you configure Imprivata Virtual Desktop Access for Citrix XenDesktop, confirm your Citrix XenDesktop is operating normally.

BEST PRACTICE: Install the latest supported version of the Citrix Virtual Desktop agent on all VMs on which the Imprivata agent will be installed. Install the latest supported version of Citrix Workspace app on all endpoint computers on which the Imprivata agent will be installed.

Step 2: Verify the Citrix XenDesktop Environment is Configured Correctly

Before you install the Imprivata agent on XenDesktop VMs and endpoint computers, verify that your Citrix XenDesktop environment is installed and configured correctly.

Verify the Citrix Installation

Verify the following installations by viewing the software listed in the Windows **Control Panel** > **Add and Remove Programs**:

- Verify that the Citrix Virtual Desktop agent is installed on all VMs.
- Verify that the Citrix Workspace app is installed on all endpoint computers.

Verify XenDesktop Catalogs

1. On the XenDesktop server, start Citrix Studio.

   In Citrix cloud or hybrid cloud environments, use the Citrix control plane.
2. Click **Machine Catalogs** in the navigation tree to display your catalogs.
3. Open a catalog to view all of the VMs in the catalog.

Verify XenDesktop Groups

1. In Citrix Studio, click **Delivery Groups** in the navigation tree to display your delivery groups.

   In Citrix cloud or hybrid cloud environments, use the Citrix control plane to navigate to your delivery groups.
2. Open a Delivery Group to view the list of VMs in the group.

To verify group settings, right-click one of the Desktop Groups and select **Edit Desktop Group**.

Verify XenDesktop Store Settings

In Citrix Studio, go to **Citrix StoreFront** > **Receiver for Web** in the navigation tree.

Verify the Citrix XenDesktop store settings and note the respective store URLs (Web Site or XenApp Services). For more information, see your Citrix user documentation.

Step 3: Install the Imprivata Agent on All VMs

To install the Citrix Virtual Desktop agent and the Imprivata agent to all VMs:

1. Install the Citrix Virtual Desktop agent on one VM.
2. Install the Imprivata agent on the same VM.
3. Clone the VM for all the installations you require.

Step 4: Install the Imprivata Agent on All Endpoint Computers

The Imprivata agent must be installed on each endpoint computer on which Citrix XenDesktop 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. For complete installation details, see "Deploying the Imprivata Agent" in the Imprivata Online Help.

NOTE: To configure Imprivata ProveID Embedded Linux thin clients, skip this step and see the following articles: Configuring ProveID Embedded on HP Smart Zero and ThinPro Thin Clients and Configuring ProveID Embedded on IGEL Linux Thin Clients.

Step 5: Configure the Imprivata Connection to Citrix XenDesktop

Imprivata agents communicate with known Citrix stores. To configure the connection:

1. In the Imprivata Admin Console, go to the **Computers** menu > **Virtual Desktops** page > **Citrix XenDesktop** section.
2. Enter the URL that should be used to connect to the Citrix store.
3. If you are managing your deployment through the Citrix Cloud, enter the client ID, application ID, and if the client is private, the client secret.
4. **Optional**: Click **Add another server** to add additional Citrix stores.

5. **Optional**: Select **Use SAML authentication**.
6. Click **Save**.

Step 6: Create and Apply a Computer Policy for Endpoint Computers

Configure a new computer policy for endpoint computers supporting Citrix XenDesktop.

Endpoint computers and virtual desktops are assigned the Default Computer Policy unless a different computer policy is assigned. Review the Default Computer Policy settings to confirm that they are appropriate for your virtual desktop environment.

Step 6a: Create a Computer Policy for Endpoint Computers

To create a computer policy:

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 6b.
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 6b: Configure a Computer Policy for Endpoint Computers

To configure the computer policy:

1. Go to the **Virtual Desktops** tab > **Citrix XenDesktop** section.
2. Select **Automate access to Citrix XenDesktop**.
3. Choose 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 Enterprise Access Management dialog prompts the user to choose a desktop.
   - **Always prompt the user to choose their desk**. An Enterprise Access Management dialog always prompts the user to choose a desktop, regardless of how many desktops they are entitled to.

   > **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 8: (Optional) Override the Desktop Chooser.
4. You can control the behavior when an endpoint computer is locked. Under **When a XenDesktop endpoint is locked**, choose one of the following:

- **Keep the XenDesktop 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 XenDesktop enabled) their desktop and applications are preserved just as they were when this endpoint computer was locked.
- **Shutdown the XenDesktop 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 XenDesktop enabled) their desktop will relaunch.

5. Select the servers that the endpoint computers should use.

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

6. Click **Save**.

Step 6c: Apply Computer Policy to Endpoint Computers

Apply the computer policy you just created to 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 you want 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 the selected computers**, select the policy from the list, and 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 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**.

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

Step 7: Create and Apply a User Policy

Create and apply a user policy that automates user access to Citrix XenDesktop.

Step 7a: Create a User Policy

To 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. **Automate access to full VDI desktops** is selected by default. Imprivata automatically handles login behavior for XenDesktop endpoint computers. Roaming users with this policy will have streamlined access to the XenDesktop environment.
8. Click **Save**.

Step 7b: Apply a User Policy

To apply a 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** 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** tab. Search for Users offers several search parameters for refining your results.
3. Click **Apply Policy**.
4. Choose the policy from the drop-down list, then click **OK**.

Step 8: (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 Enterprise Access Management on Citrix XenDesktop Shared Kiosk Workstations

This topic describes how to enable Enterprise Access Management on Citrix XenDesktop shared kiosk workstations by invoking the Credential Providers utility (**ISXCredProvDiag.exe**) and adding all Enterprise Access Management credential providers to the Citrix list of allowed credential providers, or "allowlist."

Adding Enterprise Access Management Credential Providers via the Enterprise Access Management Credential Providers UI

To add all Enterprise Access Management credential providers to the Citrix allowlist via the Enterprise Access Management Credential Providers UI, perform the following steps on each kiosk workstation:

1. Run **ISXCredProvDiag.exe** to open the Credential Providers window.
2. Click **Create Citrix Allowlist**. All Enterprise Access Management credential providers are added to the Citrix allowlist.

> **NOTE:** This button is only available when the Citrix Virtual Agent is installed. To determine if the Citrix agent is installed, the Imprivata OneSign Credential Providers utility looks for the **[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA]** and **[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters\{FF525C75-290A-411A-98B6-2729537D6F38}]** registry keys.

Adding Enterprise Access Management Credential Providers via the Command Line

On each kiosk workstation, run **ISXCredProvDiag.exe** from the command line with the parameter **/addcitrix** or **/ac**. This adds all Imprivata OneSign credential providers and wrappers to the **[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\CredentialProviderWhitelist]** registry key. The **/addcitrix** parameter is the same as the existing **/wrapall** parameter.

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.