Product Documentation

Configuring Citrix XenApp Published Desktops

Imprivata Enterprise Access Management 25.2

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 25.2

Table of Contents

Configuring Citrix XenApp Published Desktops

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 support for Citrix XenApp® published desktops.

Before You Begin

Software Requirements

Review the following:

- Verify that the Citrix XenApp environment is functioning normally, independent of Imprivata, before installing and configuring Imprivata components.
- Review the Imprivata Enterprise Access Managementwith 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.

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.

BEST PRACTICE: Limit the delivery of an application to one instance per user. If the application is distributed across multiple servers in the farm, limiting the instance ensures that the Citrix broker roams the session that the user was previously using. For more information about configuring application delivery, see the Citrix 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.

Citrix Stores and XenApp Services

Stores that are configured with a XenApp Services URL must be enabled for prompt authentication. See this Citrix Documentation topic for configuration details.

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 Cloud	• 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.

Note the Published Application Names

Note the exact name, as it appears in the Citrix Web Interface or Citrix StoreFront, for each XenApp published desktop and application you want to auto-launch. Configuring the Imprivata connection to the Citrix environment requires that you enter each name with the same spelling, spacing, and capitalization.

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 Enterprise Access Management:

- 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.

Citrix Cloud Connections

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

NOTE:
Citrix Cloud 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.

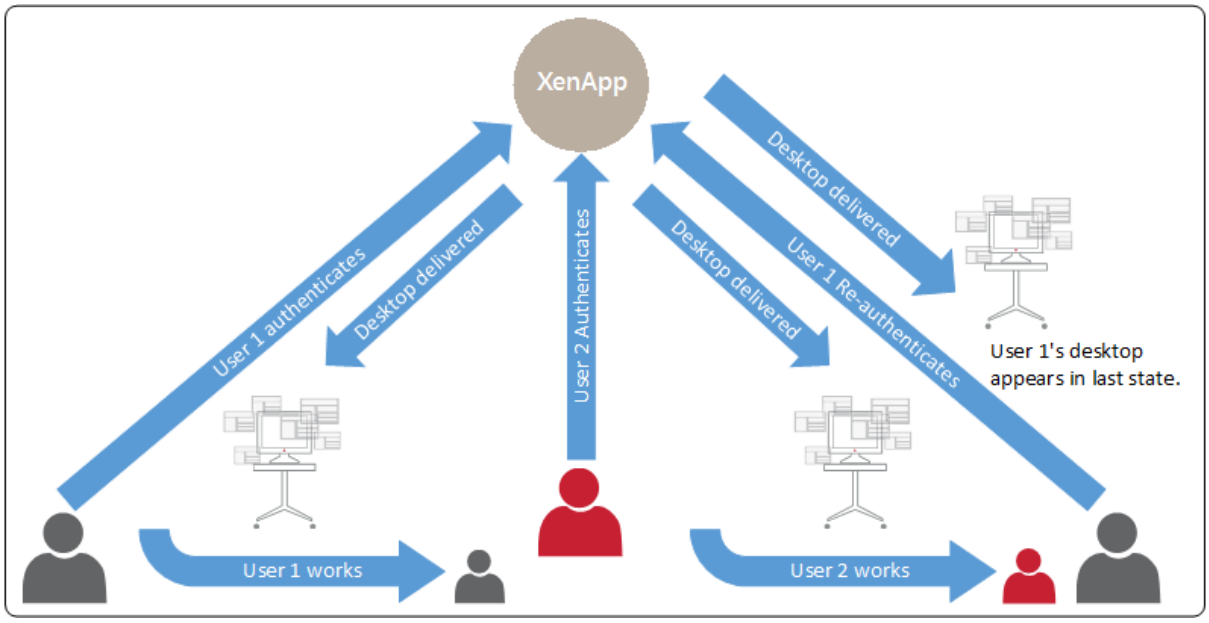
Step 6: Configure Citrix Federated Authentication Service

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.

Review the Expected User Workflow

The following diagram illustrates the expected workflow when the Enterprise Access Management environment is configured to automatically launch a desktop.



Installation Sequence

Step 1: Verify that the Citrix XenApp Environment is Configured Correctly

Before you install the Imprivata agent on endpoint computers, verify that the Citrix XenApp environment is installed and configured correctly:

1. Install the Citrix XenApp Server software.
2. Install the Citrix Web Interface software or Citrix Storefront.
3. Install a supported version of Citrix Workspace app on all endpoint computers where you plan to install the Imprivata agent.
4. Install and configure the XenApp published applications to be used.
5. Verify the Citrix XenApp store settings and note the respective store URLs (Web Site or XenApp Services URL). See the Citrix user documentation for more details.

Step 2: Install the Imprivata Agent on the Citrix Server

To install the Imprivata agent on the Citrix Server, follow the directions for installing a Imprivata Citrix or Terminal Server Agent. See "Deploying the Imprivata Citrix or Terminal Server Agent" in the Imprivata Help.

NOTE:
This step is only required for on-premises deployments. If you are managing your deployment through the Citrix Cloud, you can skip this step.

Step 3: Install the Shared Kiosk Workstation Agent on Endpoint Computers

See "Deploying the Imprivata Agent" in the Online Help for instructions on installing agents. Choose the method that suits your environment.

NOTE: To configure Imprivata for 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 4: Configure the Imprivata Connection to XenApp

Configuring the Imprivata agent connection to XenApp requires:

- One or more Citrix store URLs.
- The names of the desktops and published applications to be available for auto-launch.

To configure the connection:

1. In the Imprivata Admin Console, go to the **Computers** menu > **Virtual Desktops** page > **Citrix XenApp** 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. Enter the exact name of the XenApp published desktop application. Enter the name with the same spelling, spacing, and capitalization as it appears in the Citrix Web Interface or Citrix StoreFront.
5. **Optional**: Click **Add** to configure more published applications. For example, you can add applications to launch on the published desktop.
6. From **Authenticate using**, select the type of credentials that apply to the applications on the specified server.

   BEST PRACTICE: To configure applications to auto-launch and roam, select **Imprivata user credentials** or **External domain credentials**. To auto-launch without application roaming, you can select any credential type.

7. **Optional**: For externally hosted XenApp servers, enter the domain name for external domain credentials (such as **mycompany.com**) .
8. **Optional**: If some XenApp applications are hosted on a second server, click **Add another server** and repeat the steps above.
9. Select **Allow authentication from XenApp-enabled devices**.
10. Click **Save**.

Step 5: Create and Apply User Policies

After you configure the Imprivata connection to Citrix XenApp, create and apply a user policy to auto-launch the published desktop application. You can set up multiple policies to launch different desktops.

Step 5a: 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. Select **Automate access to apps or published desktops**.
8. Select a roaming option:
   - **Roam open applications** — Select this option to roam all applications with an active session. This includes applications that are configured to automatically launch, as well as those that a user has manually launched.
   - **Roam automatically launched applications** — Select this option to roam applications that are configured to automatically launch:
     - If an application session is present, only the automatically launched application is roamed.
     - If an application session is not present, the application is automatically launched again.

   NOTE: Under certain circumstances, applications that users manually launch are also roamed. This typical happens when the session is present, and the application is hosted on the same Citrix server as the applications that are configured to automatically launch.
9. To enable the published desktop application:
   - In the left pane, select only the full desktop application.
   - To enable XenApp applications to launch on the published desktop, select applications in the right pane:
10. Click **Save**.

Step 5b: Apply a User Policy

To apply 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** list without losing your selections. Imprivata keeps track of all the users you have selected and displays 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**.
4. Choose the policy from the drop-down list and click **OK**.

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

Create and apply a computer policy for endpoint computers that are supporting the published desktop application.

Step 6a: Create a Computer Policy for Endpoint Computers

To create the 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 5.
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.
5. Go to the **Virtual Desktops** tab > **Citrix XenApp** section.
6. Select **Automate access to Citrix XenApp** to have Imprivata automatically handle login behavior for Citrix XenApp.
7. 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 XenApp client and user session active** — Preserves the user session. When a user logs back in to this endpoint computer (or another endpoint computer with XenApp enabled), their XenApp applications are preserved just as they were when this endpoint computer was locked.
   - **Shutdown the XenApp client and disconnect the user session** — 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 XenApp enabled), their XenApp applications relaunch.
8. ***Optional*** — For ProveID Embedded devices, select **Enable Published Applications** to enable manually-launched XenApp published applications.

9. Select the Citrix XenApp servers for this computer policy.
10. Click **Save**.

Step 6b: Apply a Computer Policy to Endpoint Computers

Apply the computer policy you just created to endpoint computers.

Manually Assigning 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 apply 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 a 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 (Optional): Disable Automatic Desktop Lock

In this implementation, if the user manually closes every open Citrix XenApp application, the local desktop will lock automatically, even if the user has applications in use on the local endpoint computer. This behavior is dependent on the application state being "disconnected".

To prevent this behavior, create the **DisableLocking** registry key with a **Data Type** of **DWORD** and a **Value** of **1** in the following location:

- **HKLM\Software\SSOProvider\VDI**

NOTE: With the value set to **1**, if the user leaves Workstation 1 without securing the desktop, then logs into Workstation 2, his XenApp published applications will roam with him to Workstation 2, but Workstation 1's desktop will remain open and unsecured.

Troubleshooting

Optimizing Citrix XenApp Session Sharing

In certain network environments, session sharing does not occur when users start multiple XenApp applications at the same time.

To optimize resource consumption, you can minimize this behavior by extending the period Citrix waits for an application to start before it starts the second application in a second session. The default time-out value is 20 seconds.

To extend the time-out period, add the registry key **SucConnTimeout** to **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient** with a **Data Type** of **REG_STRING** and a **Value** of <20 or more seconds>.