imprivata®

Product Documentation

Configuring Citrix XenApp Published Desktops and Fast User Switching on Linux Thin Clients

Imprivata Enterprise Access Management 24.1

NOTE:
Beginning with 24.1, 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 guide includes information about configuring Imprivata OneSign® and Citrix XenApp published desktops for fast user switching (Citrix FUS) on ProveID Embedded-enabled Linux thin clients.

This document contains the following sections:

About Citrix Fast User Switching

Fast user switching lets multiple users share a workstation (kiosk workstation) and use the same applications under the correct credentials.

In a Citrix environment with FUS:

- A Citrix session is launched on a thin client that is logged in with generic credentials.
- While the Citrix Virtual Apps published desktop is already running and logged in with generic credentials, users authenticate to the Imprivata agent.
- When the Imprivata agent detects a user switch, Imprivata OneSign either shuts down the open applications on the Citrix desktop from the previous user, or keep the applications open but switches the logged in user in that application.

Before You Begin

Thin Client and License Requirements

Before you begin:

- Review the *Imprivata OneSign Supported Components* in the Imprivata Environment Reference to confirm that your thin client models and firmware versions are supported.
- An Imprivata OneSign Authentication Management (AM) or Imprivata OneSign AM/Single Sign–On (SSO) license is required for this workflow.

Requirements

This workflow is designed to be persistent and requires Citrix Sessions to be configured to Logout on disconnect in your Citrix Environment. Reconnecting to existing Fast User Switching sessions can result in PHI exposure.

Note the Citrix Connection Information

The URL required to configure the thin client connection to Citrix depends on how users are to access the Citrix store:

- **Storefront Web Site URL** – If the store is configured with a Web Site Store URL, the thin client communicates with Citrix using the respective URL.

  Example: If the store is configured with `https//example.com/Citrix/SalesStore`, then configure the thin client connection with `https//example.com/Citrix/SalesStoreWeb`.
- **XenApp Services URL** – If the store is configured with a XenApp Services URL, the thin client communicates with Citrix using the respective URL.

  Example: If store is configured with `https://example.com/Citrix/SalesStore/PNAgent/config.xml`, then configure the thin client connection with `https://example.com/Citrix/SalesStore/PNAgent/config.xml`.

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.

Citrix License Usage and Expected End User Workflow

A Citrix license is consumed when the thin client establishes a Citrix session and launches the resource. The procedures in this guide detail how to configure the computer policy to determine when the thin client establishes the session, thereby controlling license usage, but affecting the end user workflow.

You can configure the computer policy to enforce one of the following:

- Automatically reconnect to a session when a session ends.
- Wait for a user to manually start a session.

The **Automatically reconnect on session end** setting, which is located on the **Shared Workstation tab** of the computer policy, controls this behavior. Review the following and identify which workflow best fits the needs of your organization. Use this information when configuring the computer policy.

The Thin Client Automatically Establishes a Citrix Session

If **Automatically reconnect on session end** is enabled, the thin client keeps a Citrix session established, even when the endpoint is not in use. For example, the thin client automatically establishes a Citrix session and launches the published desktop when the thin client starts, a user logs off, or the Citrix session times out.

Although keeping a session established streamlines the end user workflow, the thin client always consumes a Citrix license, as detailed by the following:

1. The kiosk workstation starts.
   - The thin client establishes a Citrix session using generic user credentials and launches the published desktop.
   - The desktop runs under the generic credentials. Establishing a Citrix session consumes a license.
2. The Imprivata OneSign login window appears. While the published desktop remains running under the generic credentials, a Citrix license remains consumed.
3. User 1 (Nurse) authenticates to Imprivata OneSign.
   - The kiosk workstation is unlocked.
   - The same Citrix license remains consumed.
4. User 1 clicks icons on the desktop to open applications:
   - **Application A** has been configured to remain open after a user logs off.

     Epic Hyperspace configured with the Imprivata Connector for Epic Hyperdriveis an example of this configuration.

- **Application B** has been profiled with the Imprivata OneSign 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.

5. User 1 also opens **Application C**, which has not been profiled with the APG.
6. User 1 completes their work. The workstation becomes locked through their action/inaction.

   For example, a proximity card tap-out or an Imprivata OneSign inactivity timeout. The user does not shut down any of their applications.

   - The Citrix session remains open.
   - User 1's Imprivata OneSign session is locked but **not** logged off.
7. User 2 (Doctor) authenticates to the kiosk workstation.
   - **Application A**: The Imprivata OneSign Citrix or Terminal Server agent executes the logoff sequence to switch users within Application A.

     User 2 is logged into Imprivata OneSign. Depending on the application settings, the same screen User 1 was viewing opens. For example, the same patient chart is revealed.
   - **Application B** shuts down.
   - **Application C** remains open in the exact same state as User 1 left it.

   > **NOTE**: Some applications offer configuration options to control whether the same application screen opens after Citrix FUS. Other applications' login and logout behavior is not configurable.
8. User 2 completes their work. The workstation becomes locked through their action/inaction.

   For example, a proximity card tap-out or an Imprivata OneSign inactivity timeout.
9. If the user logs out of the desktop, or a Citrix inactivity timeout causes the desktop to log off, the Citrix license is released.
10. The thin client automatically establishes another Citrix session using the generic user credentials and launches the published desktop.

    A Citrix license is consumed, while the published desktop remains running under the generic user credentials.

The Thin Client does not Automatically Establish a Citrix Session

If **Automatically reconnect on session end** is disabled, the thin client does not establish a Citrix session when it starts or the user session ends. Instead, the endpoint prompts the user to start the session.

Although re-establishing the Citrix session to launch the published desktop can take longer than launching it from an established connection, a Citrix license is only consumed when the endpoint is in use, as detailed by the following:

1. The kiosk workstation starts.
   - The thin client prompts users to start a session.
   - A Citrix license is not consumed while the workstation remains unused.

2. User 1 (Nurse) clicks **OK**. The thin client establishes a Citrix session using generic user credentials and launches the published desktop.
   - The desktop runs under the generic credentials.
   - Establishing a Citrix session consumes a license.
3. The Imprivata OneSign login window appears. While the published desktop remains running under the generic credentials, a Citrix license remains consumed.
4. User 1 authenticates to Imprivata OneSign.
   - The kiosk workstation is unlocked.
   - The same Citrix license remains consumed.
5. User 1 clicks icons on the desktop to open the following applications:
   - **Application A** has been configured to remain open after a user logs off.

     Epic Hyperspace configured with the Imprivata Connector for Epic Hyperdriveis an example of this configuration.
   - **Application B** has been profiled with the APG to shut down automatically after a user logs off.

   The Imprivata Citrix or Terminal Server agent manages SSO for these applications.
6. User 1 also opens **Application C**, which has not been profiled with the APG.
7. User 1 completes their work. The workstation becomes locked through their action/inaction.

   For example, a proximity card tap-out or an Imprivata OneSign inactivity timeout. She does not shut down any of her applications.
   - The Citrix session remains open.
   - User 1's Imprivata OneSign session is locked but **not** logged off.
8. User 2 (Doctor) authenticates to the kiosk workstation.
   - **Application A**: The Imprivata OneSign Citrix or Terminal Server agent executes the logoff sequence to switch users within Application A.

     User 2 is logged into Imprivata OneSign. Depending on the application settings, the same screen User 1 was viewing opens. For example, the same patient chart is revealed.
   - **Application B** shuts down.
   - **Application C** remains open in the exact same state as User 1 left it.

   > **NOTE**: Some applications offer configuration options to control whether the same application screen opens after Citrix FUS. Other applications' login and logout behavior is not configurable.
9. User 2 completes their work. The workstation becomes locked through their action/inaction.

   For example, a proximity card tap-out or an Imprivata OneSign inactivity timeout.
10. If the user logs out of the desktop, or a Citrix inactivity timeout causes the desktop to log off, the Citrix license is released.
11. The thin client prompts users to start a session.

    A Citrix license is not consumed while the workstation remains unused.

Thin Client Configuration

In this section, you configure your thin clients to automatically connect to the published desktop with generic workstation–based credentials.

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 workstation in the environment.
- Disable session roaming in Citrix workspace control.

> **NOTE**: For more information about disabling session roaming in workspace control, see the Citrix documentation.

Step 1: Create a Generic User Account in Your User Directory

A generic user account is required to log into the thin client and establish a session with the published desktop. When adding the generic user to your user directory, consider the following:

- These credentials are only used to automatically log in and deliver the published desktop.
- The generic user account must have access to the Citrix Delivery group that references the machine catalog of the desktop.
- To support Citrix SAML connections for fast user switching, the generic user account must be enrolled in Imprivata OneSign.

Step 2: Configure the Thin Client Connection to the Published Desktop

Configure the thin client to connect to the published desktop using the generic user credentials.

> **NOTE**: Unlike previous Imprivata OneSign versions, the following procedure applies to all supported thin/zero clients. It is not necessary to configure the connection using the native administrative utilities of the device.

To configure the connection:

1. Connect to the device through an SSH session.
2. Type the following command:

   ```
   /usr/lib/imprivata/bin/python /usr/lib/imprivata/runtime/bin/fus-storage citrix -u <GenericUser> -d <GenericUserDomain> -p '<GenericUserPassword>' -s https://<CitrixStoreURL> -r PublishedDesktopName [--saml]
   ```

   Note regarding the optional `--saml` argument:

   - To enable SAML connections for fast user switching (FUS) for this thin client, include the `--saml` argument. Otherwise, omit that argument.
   - Citrix SAML connections for fast user switching for a thin client can also be enabled in the Agent VDI section of the ProveID Embedded configuration for that thin client.

   Examples:

   - Storefront Website URL

     ```
     /usr/lib/imprivata/bin/python /usr/lib/imprivata/runtime/bin/fus-storage citrix -u exampleuser -d imprivatainc -p 'Pa$$word' -s https//example.com/Citrix/SalesStoreWeb -r desktop
     ```

   - XenApp Services URL

     ```
     /usr/lib/imprivata/bin/python /usr/lib/imprivata/runtime/bin/fus-storage citrix -u exampleuser -d imprivatainc -p 'Pa$$word' -s https://example.com/Citrix/SalesStore/PNAgent/config.xml -r desktop
     ```

3. Press **Enter**.

Citrix Configuration

In this section, you:

- Install the Imprivata agent on the Citrix server that is delivering the published desktop.
- Configure a series of registry keys to enable the Citrix server for FUS.

Step 1: Install the Imprivata Agent

Install the Imprivata Citrix or Terminal Server agent (type 3) on the Citrix server that is delivering the published desktop.

For more information on installing the Imprivata agent, see "Deploying the Imprivata Agent" in the Imprivata Online Help.

Step 2: Enable the Citrix Server for FUS

On the published desktop, configure the following registry keys:

Name/Type	Location	Value
DisableCAD DWORD	32-bit HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System 64-bit HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\System	Default "0" Set to "1"
DisableCAD DWORD	32-bit HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon 64-bit HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	Default "0" Set to "1"
LockRemoteSessionWithAgentOnClient DWORD	64-bit HKLM\SOFTWARE\SSOProvider\ISXAgent	Default "0" Set to "1"
LockVirtualSessionWithHotKey DWORD	64-bit HKLM\SOFTWARESSOProvider\ISXAgent	Default "0" Set to "1"
RedirectionSupported DWORD	64-bit HKLM\SOFTWARE\SSOProvider\DeviceManager	Default "0" Set to "1"

Name/Type	Location	Value
RemoteOnly DWORD	64-bit HKLM\SOFTWARE\SSOProvider\DeviceManager	Default "0" Set to "1"

Imprivata OneSign Configuration

In this section you configure:

- A user policy.
- Two computer policies.

  One for your thin client workstations, and another for the Citrix server that is delivering the published desktop.

Step 1: Create and Assign a User Policy

Create the User Policy

To create the user policy:

1. In the Imprivata Admin Console, click **Users** > **User policies**.
2. Click **Add**, and enter a policy name.
3. Go to the **Desktop Authentication** section, and select the allowed authentication methods.

   > **NOTE**: The additional Imprivata ID settings that are available in the **Authentication method options** section do not apply to Secure Walk Away.

4. Save the policy.

Assign the User Policy

To assign users to the policy:

1. In the Imprivata Admin Console, click **Users** > **Users**.
2. Do one of the following:
   - Manually select users, and then click **Apply Policy**.
   - Click **Bulk Actions** > **Assign User Policies** to download a sample CSV file.
3. Modify this file to map multiple users to the policy, and then import it.

Step 2: Create and Assign a Computer Policy for Thin Clients

Create the Computer Policy

To create a computer policy:

1. In the Imprivata Admin Console, go to the **Computers** menu > **Computer Policies** page.
2. Click **Add**, and then enter a name for the computer policy.
3. On the **Shared Workstation** tab, go to the **Kiosk Workstations** section.
4. Select **Allow Fast User Switching with Citrix or Terminal Servers**.
5. Do one of the following:
   - If the desired end user workflow is The Thin Client Automatically Establishes a Citrix Session, select **Automatically reconnect on session end**.
   - If the desired end user workflow is The Thin Client does not Automatically Establish a Citrix Session, deselect **Automatically reconnect on session end**.

6. Select one of the following in the **Windows Authentication** section:
   - Authenticate using Windows
   - Authenticate using Imprivata

     This setting skips Windows authentication, and is useful if the kiosk workstation is not in a trusted domain.
7. Click **Save**.

Assign the Computer Policy

There are a number of different ways to assign a computer policy. Computer policy assignment rules are an efficient method. They let you assign the policy to multiple workstations at once, and are automatically applied to computers that are added to the enterprise later.

To assign the computer policy:

1. In the Imprivata Admin Console, click **Computers** > **Computer policy assignment**.
2. At the top of the assignment pane, select a **Site** location and **Schedule** the frequency at which the rule runs. This setting applies to all assignment rules.
3. Click **Add New Rule**, and name it.
4. Select one of the following options:
   a. **Active directory groups** — Select one or more groups to add. When you close the group selection window the rule displays the number of groups you chose.
   b. **Active directory OUs (Organizational Units)** — Select one or more OUs to add. When you close the group selection window the rule displays the number of OUs you chose.
   c. **Computer IP address** — Enter the range of IP addresses to include in this computer policy
   d. **Computer host name** — A computer matches if its host name contains the text entered in this field
   e. **Imprivata agent type** — Choose an agent type from the list
5. Select a policy from **Apply this computer policy**.
6. Click **Save**.

Step 3: Create and Assign a Computer Policy for the Citrix Server

To create the computer policy:

1. In the Imprivata Admin Console, go to the **Computers** menu > **Computer policies** page.
2. Click **Add** and name the policy.
3. On the **Citrix or Terminal Server** tab, go to the **Fast User Switching** section.

NOTE: The settings in the section **Authenticating generic user or anonymous Citrix XenApp or Terminal Server sessions** are not used in a ProveID Embedded environment.

4. Under **Endpoints with an installed ProveID Embedded agent**, select **Allow Fast User Switching with the remote server if allowed in computer policy**.
5. Save the policy and assign it to the Citrix server.

Next Steps

The following sections detail additional areas of configuration and reference the respective Imprivata OneSign documentation.

Install ProveID Embedded

If you have not already, install Imprivata ProveID Embedded on your thin client devices.

To install and configure ProveID Embedded, see "Configuring ProveID Embedded on Linux Thin Clients" in the Imprivata Help.

Configure Application Profiles

You can configure one or more Imprivata APG profiles to manage the application SSO and logoff sequences that are detailed in Citrix License Usage and Expected End User Workflow.

Consider the following:

- If you are configuring Imprivata OneSign with Epic Hyperspace, an application profile is not required. The Imprivata Connector for Epic Hyperspace manages the logout behavior.
- For complete details on how to profile an application, see "Generating an Application Profile" in the Imprivata help.

When configuring a logoff sequence, be sure to set the values under **Execute the logoff sequence** as follows:

- Select **During fast user switching on a kiosk workstation**.
- Deselect **Shut down the application during fast user switching on a kiosk workstation?**.
- Deselect **Before the application is shut down by OneSign**.