# **D** imprivata<sup>®</sup>

## **Product Documentation**

## Configuring Citrix Workspace App

Imprivata Enterprise Access Management 25.1

© 2025 Imprivata, Inc. All Rights Reserved.

#### 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

© 2025 Imprivata, Inc. All Rights Reserved.

This product is distributed under licenses restricting its use, copying, distribution and decompilation. Imprivata's products may be covered in whole or in part by one or more U.S. pending or issued patents listed at <u>http://www.imprivata.com/patents</u>.

#### Trademark Information

OneSign, Imprivata, and the Imprivata logo are registered trademarks of Imprivata, Inc. ProveID and Imprivata OneSign APG are trademarks of Imprivata, Inc. in the United States and in other countries.

#### Legal Notices

Under international copyright laws, neither the documentation nor software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part without the prior written consent of Imprivata, Inc., except as described in the license agreement.

The names of companies, products, people, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Document revision 25.1

## Configuring Citrix Workspace App for Imprivata Enterprise Access Management

#### NOTE:

 $(\mathbf{i})$ 

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 Citrix Workspace app to support Imprivata Enterprise Access Management SSO and Citrix XenApp.

For more information on how to create a Group Policy to enable Fast Connect, see Citrix Support.

This document contains the following sections:

Configuring Citrix Workspace App for Imprivata Enterprise Access Management	3
Before You Begin	4
Software Requirements and Downloads	4
Citrix Workspace App Installation Requirements	4
Note the Citrix Account URLs	4
Enable Citrix StoreFront for the Citrix FastConnect API	5
Add Citrix Administrative Templates to the Active Directory Domain Controller	5
Locate the Templates	6
Add the Templates to the Central Store on the Domain Controller	6
Enterprise Access Management Workflows and How Citrix Workspace App Reconnects to existing Sessions	6
Enable Imprivata Virtual Channel	7
Create A Group Policy to Manage Fast Connect Configuration	8
Step 1: Create an Organizational Unit for Endpoint Computers	8
Step 2: Create a Group Policy	8
Step 3: Add the Citrix Template Files for the Group Policy	8
Configure the Group Policy	9
Step 1: Configure the Local User Name and Password	9
Step 2: Configure Fast Connect API Support	10
Step 3: Configure Application Shortcuts	11
Step 4: Control Reconnection attempts to Existing Sessions	12
Step 5: Add Accounts	12
Step 6: Create Registry Keys for StoreFront Store Support	13
Step 7: Configure Internet Explorer	14
Step 8: Close the Group Policy Management Editor to Save Your Changes	15
Link The Group Policy Object to the Organizational Unit	15
Configure Security Filtering	15
Verify the Configuration1	16
View Policy Configurations in the Registry	17
Generate a Group Policy Result Report	17

## Before You Begin

Review the following requirements and prerequisite steps before you begin.

#### Software Requirements and Downloads

Before you begin:

- See the Enterprise Access Management with SSO <u>Supported Components</u> to identify supported Citrix Workspace app versions.
- Download the Citrix Workspace app installer from the <u>Citrix Support</u> site.

#### Citrix Workspace App Installation Requirements

Support for Citrix Workspace app requires the following:

- Install Citrix Workspace app with a user that has administrator privileges.
- Single sign-on (pass through) authentication must be enabled during the installation.
- Do not specify an account (Store URL or XenApp Services URL) as part of the installation. This guide details how to configure a GPO to automatically connect endpoint computers to the required account when Citrix Workspace app starts.
- Restart the endpoint computer after the installation.

#### Note the Citrix Account URLs

Configuring the GPO with the Citrix store URLs prevents you from having to:

- Add them when installing Citrix Workspace app
- Provide them to end users to add them manually to Citrix Workspace app.

Before you begin, use Citrix Studio to note the required URLs.

#### Enable Citrix StoreFront for the Citrix FastConnect API

Additional Citrix configuration is required to support the Citrix FastConnect API.

#### **Configure Authentication Methods**

The Citrix store must be configured with the following authentication methods to support the Citrix FastConnect API:

- 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 Receive**r pane, click **Choose Authentication Methods**.
- 5. Click **Add/Remove Methods** and enable the required methods.

#### Verify the Logon Method

The Citrix store logon method (logonMethod) must be configured for single sign-on to support the Citrix FastConnect API.

To verify the logon method:

- From the Citrix StoreFront server, go to the following location: C:\inetpub\wwwroot\Citrix\<name\_of\_store>
- 2. Open the **web** configuration file and find **logonMethod**.
- 3. Verify that the value is set to **sson**. For example:

pnaProtocolResources changePasswordAllowed="Never" logonMethod="sson"

## Add Citrix Administrative Templates to the Active Directory Domain Controller

Configuring Citrix Workspace app with Enterprise Access Management requires the following template files:

- receiver.admx
- receiver.adml

To make these templates available to the Group Policy Management Editor, add them to the Central Store on the domain controller.

#### Locate the Templates

You can locate the templates in the following ways:

- Citrix makes the templates available separately from the Citrix Workspace app installer. Go to the Citrix Workspace app for Windows download page. The ADMX/ADML templates are available in the Admin Tools section.
- The templates are installed with Citrix Workspace app.
  - The ADMX file is located at "C:\Program Files (x86)\Citrix\ICA Client\Configuration".
  - The ADML file is located at "C:\Program Files (x86)\Citrix\ICA Client\Configuration\en-US".

#### Add the Templates to the Central Store on the Domain Controller

Managing Group Policy settings requires that all ADMX/ADML files be added to the Central Store on the domain controller. To add the administrative templates:

- 1. Log into the domain controller.
- 2. Go to C:\Windows\SYSVOL\domain\Policies and create a PolicyDefinitions folder to function as the Central Store.
- Go to C:\Windows\PolicyDefinitions and copy all of the contents, including the en-US folder, to C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions.
- 4. Add receiver.admx to C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions.
- 5. Add receiver.adml to C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions\en-US.
- 6. If the Group Policy Management Editor is open, close the console for the changes to take affect.

#### Enterprise Access Management Workflows and How Citrix Workspace App Reconnects to existing Sessions

The procedures in this guide detail how to configure the GPO to control how Citrix Workspace app reconnects to existing application sessions. Citrix Workspace app **SelfService** must be configured with the **Disabled** option.

The **Disabled** option is required, regardless of the desired end user workflow and application session (roaming) requirements.



**NOTE**: For information about configuring SelfService, see Step 4: Control Reconnection attempts to Existing Sessions.

The following sections detail common end user workflows.

## Session Roaming — Enterprise Access Management does not Launch Applications Automatically

Desired end-user workflow:

- 1. The user authenticates to workstation A.
- 2. The applications to which the user is entitled are loaded automatically to the start menu, desktop, or both.
- 3. The user launches one or more applications manually.
- 4. The workstation becomes locked through user action/inaction or remains active and unlocked.
- 5. The user authenticates to workstation B.
- 6. The applications to which the user is entitled are loaded automatically to the start menu, desktop, or both.
- 7. All applications that remain open from step 4 are launched automatically (roamed).

#### Session Roaming — Enterprise Access Management Launches Applications Automatically

Desired workflow:

- 1. The user authenticates to workstation A.
- 2. The applications to which the user is entitled are loaded automatically to the start menu, desktop, or both.
- 3. The applications that are configured in the user policy automatically launch.
- 4. The workstation either becomes locked through user action/inaction or remains active and unlocked.
- 5. The user authenticates to workstation B.
- 6. The applications to which the user is entitled are loaded automatically to the start menu, desktop, or both.
- 7. The applications that are configured in the user policy automatically launch.

#### Enable Imprivata Virtual Channel

Applies to Citrix 2109 and later.

In Citrix 2109 and later, the Virtual channel allow list policy setting is enabled by default. This causes the Imprivata virtual channel to fail. For more information, see the <u>Citrix documentation</u>.

The Virtual channel allow list policy setting enables the use of an allow list that specifies which virtual channels are allowed to be opened in an ICA session. There are two ways to allow the Imprivata virtual channel to run in Citrix 2109 or later:

- When disabled:
  - All virtual channels (including Imprivata virtual channel) are allowed.
  - This is not recommended
- When enabled:
  - Only Citrix virtual channels are allowed
  - ° The Imprivata virtual channel must be added to this allow list.

For example:

IMP1166,C:\Program Files (x86)\Imprivata\OneSign Agent\x64\SSOManHost.exe

To use custom or third-party virtual channels, add the virtual channels to the list.

To add a virtual channel to the list:

- Enter the virtual channel name followed by a comma, and then the path to the process that accesses the virtual channel.
- You can add additional executable paths, separating the paths by commas.

For example: CTXCVC1,C:\VC1\vchost.exe CTXCVC2,C:\VC2\vchost.exe,C:\Program Files\Third Party\vcaccess.exe IMP1166,C:\Program Files (x86)\Imprivata\OneSign Agent\x64\SSOManHost.exe

## Create A Group Policy to Manage Fast Connect Configuration

Create an organizational unit (OU), add your endpoint computers to it, and then create a GPO to configure the endpoint computers.

#### Step 1: Create an Organizational Unit for Endpoint Computers

- 1. From the domain controller, open the Active Directory Users and Computers console.
- 2. In the console tree, create an organizational unit (OU) for your endpoint computers.
- 3. Add or move the required endpoint computers to the OU.

#### Step 2: Create a Group Policy

- 1. From the domain controller, open the Group Policy Management Console.
- 2. In the required domain, select **Group Policy Objects** > **New**.
- 3. In the **New GPO** window, name the GPO and click **OK**.



#### Step 3: Add the Citrix Template Files for the Group Policy

To add the Citrix Administrative templates to the group policy object:

- 1. Right-click the new GPO and select **Edit**. The Group Policy Management Editor opens.
- 2. Go to Computer Configuration > Policies > Administrative Templates Policy Definitions (ADMX files) retrieved from the central store > Citrix Components > Citrix Workspace app.



## Configure the Group Policy Step 1: Configure the Local User Name and Password

To configure the required settings:

- 1. In Group Policy Management Editor tree, select User authentication.
- 2. In the details pane, double-click Local user name and password.
- 3. In the Local user name and password window, select Enabled.
- 4. In the **Options** pane:
  - Select Enable pass-through authentication.
  - Select Allow pass-through authentication for all ICA connections.
  - Deselect Use Novell Directory Server credentials.
- 5. Click **OK**.

The settings should match the following screen capture.

Local user name and password				
O Not Configured	Comment:			
Enabled				
O Disabled				
	Supported on:			
Options:				
Enable pass-through authentication				
Allow pass-through authentication for all ICA connections				
Use Novell Directory Server credentials				

#### Step 2: Configure Fast Connect API Support

To configure the required settings:

- 1. In the Group Policy Management Editor tree, select FastConnect API Support.
- 2. In the details pane, double-click Manage Fast ConnectAPI support.
- 3. In the Manage FastConnectAPI support window, select Enabled.
- 4. In the **Options** pane, select:
  - Select Enable Fast Connect API functionality.
  - Select EnableFastConnectTransisitionAPI.
  - Deselect Leave Apps Running On Logoff.
  - Select Integrate Self Service Plugin with FastConnect.
- 5. Click **OK**.

The settings should match the following screen capture.

Manage FastConr	nectAPI support			
O Not Configured	Comment:			
<ul> <li>Enabled</li> </ul>				
O Disabled				
	Supported on:	All Receive		
Options:				
☑ Enable FastConnect API functionality				
EnableFastConnectTransitionAPI				
Leave Apps Running On Logoff				
✓ Integrate Self Service plugin with FastConnect				

#### Step 3: Configure Application Shortcuts

To configure the required settings:

- 1. In the Group Policy Management Editor tree, select Self Service.
- 2. In the details pane, double-click Manage App shortcut.
- 3. In the Manage App Shortcut window, select Enabled.
- 4. In the **Options** pane, select:
  - In the **Startmenu** field: if you want your Citrix apps in a folder on the Start menu, enter a name for that folder here. If this field is left blank, the apps will appear directly on the Start menu.
  - In the **Desktop Directory** field: if you want your Citrix apps in a folder on the desktop, enter a name for that folder here. If this field is left blank, the apps will appear directly on the desktop.
  - Deselect Disable Startmenu Shortcut.
  - Select Enable Desktop Shortcut.
  - Select Disable Categorypath for startmenu.



BEST PRACTICE: Use Citrix StoreFront categories in the Start menu instead.

- Select Enable Categorypath for desktop and Enable to have different category path startmenu.
- Select Remove apps on Logoff.
- Select Remove apps on Exit.
- Select Clear the set of applications shown in the Receiver Window on logoff.
- Select Prevent Receiver performing a refresh of the application list when opened.

- Select Ignore self service selection of apps and make all mandatory.
- 5. Click **OK**.

The settings should match the following screen capture.

Manage App sh	ortcut	Previou		
O Not Configured	Comment:			
Enabled				
O Disabled				
	Supported on:	All Receiver supported platforms		
Options:				
Startmenu Directory	Citrix			
Desktop Directory	Citrix			
Disable Startment	u Shortcut			
Enable Desktop S	hortcut			
✓ Disable Categorypath for startmenu				
✓ Enable Categorypath for desktop				
Enable to have different category path for desktop and startmenu. Disable desktop as that of startmenu				
Remove apps on Logoff				
Remove apps on Exit				
Clear the set of applications shown in the Receiver Window on logoff				
Prevent Receiver performing a refresh of the application list when opened.				
Ignore self service selection of apps and make all mandatory. If Receiver is service this will be required to get all apps added automatically. If Receiver				

#### Step 4: Control Reconnection attempts to Existing Sessions

To configure the required settings:

- 1. In the Group Policy Management Editor tree, select **Self Service**.
- 2. In the details pane, double-click **Control When Receiver Attempts to Reconnect to Existing Sessions**.
- 3. In the Control when Receiver attempts to reconnect to existing sessions window, select Enabled.
- 4. In the **Options** pane, open **Choose the appropriate combination of reconnect conditions**, and select **Disabled**.
- 5. Click **OK**.

#### Step 5: Add Accounts

To configure the required settings:

- 1. In the Group Policy Management Editor tree, select **Storefront**.
- 2. In the details pane, double-click StorefrontAccounts List.
- 3. In the Storefront Account List window, select Enabled.
- 4. Click **Show**.
- 5. In the **Show Contents** window, enter the store account (Store URL or XenApp Services URL) details using the following syntax:

store\_name;store\_url;store\_enabled\_state;store\_description

- *store\_name* is the name users see for the store.
- *store\_url* is the Services URL for the store.
- store\_enabled\_state specifies if the store is available to users. Set to On or Off.
- *store\_description* is the description users see for the store.

#### XenApp Services example:

SalesStore;https://example.com/Citrix/SalesStore/PNAgent/config.xml;On;Store for Sales Staff **Store example**: SalesStore;https//example.com/Citrix/SalesStore/;On;Store for Sales Staff



**NOTE**: The **store\_enabled\_state** syntax is case-sensitive.

#### Step 6: Create Registry Keys for StoreFront Store Support

(Optional) This step is required only if your Citrix environment is using Store URLs. Configuring the registry keys requires that you:

- Add the ConnectionSecurityMode and the ProtocolOrder values to the Citrix AuthManager registry key.
- Create the **Protocols** registry key with a **httpbasic** subkey, which has a value of **Enable**.

#### Add the ConnectionSecurityMode Value

To add the value:

- In the Group Policy Management Editor tree, go to Computer Configuration > Preferences > Windows Settings.
- 2. Right–click **Registry** and select **New > Registry item**.
- 3. In the New Registry Properties window, select Create from the Action list.
- 4. From the **Hive** list, select **HKEY\_LOCAL\_Machine**.
- 5. Enter the following in the Key Path field:
  - 64-bit Software\Wow6432Node\Citrix\AuthManager\
- 6. In the Value name field, enter ConnectionSecurityMode.
- 7. From the Value type list, select REG\_SZ.
- 8. In the Value data field, enter Any. Click OK.

#### Add the Protocol Order Value

To add the value:

- In the Group Policy Management Editor tree, go to Computer Configuration > Preferences > Windows Settings.
- 2. Right–click **Registry** and select **New > Registry item**.
- 3. In the New Registry Properties window, select Create from the Action list.
- 4. From the **Hive** list, select **HKEY\_LOCAL\_Machine**.
- 5. Enter the following in the Key Path field:
  - 64-bit Software\Wow6432Node\Citrix\AuthManager\
- 6. In the Value name field, enter ProtocolOrder.
- 7. From the Value type list, select REG\_MULTI\_SZ.
- 8. In the Value data field, enter httpbasic. Click OK.

#### Create the Protocols registry key

To create the key:

- 1. In the New Registry Properties window, select Create from the Action list.
- 2. From the Hive list, select HKEY\_LOCAL\_Machine.
- 3. Enter one of the following in **Key Path**:
  - 64-bit Software\Wow6432Node\Citrix\AuthManager\Protocols\httpbasic
- 4. In the Value name field, enter Enabled.
- 5. From the Value type list, select REG\_SZ.
- 6. In Value data field, enter true. Click OK.

#### Step 7: Configure Internet Explorer

Configuring Internet Explorer requires that you:

- Add the domain of the Services URL as a trusted site.
- Configure user authentication for automatic logon.

#### Add a Trusted Site

To add a trusted site:

- 1. In the Group Policy Management Editor tree, go to Windows Components > Internet Explorer > Internet Control Panel > Security Page.
- 2. In the details pane, open Site to Zone Assignment List.
- 3. In the Site to Zone Assignment List window, select Enabled.
- 4. In the **Options** section, click **Show**.
- 5. In the Value name field, type the scheme and domain of the Services URL.

**Example**: If the URL is https://example.com/Citrix/SalesStore/PNAgent/config.xml, then enter https://example.com.

- 6. In the Value field, type 2 and click OK.
- 7. Apply the changes to the Site to Zone Assignment List.

#### Configure User Authentication

To configure user authentication:

- 1. In the details pane, open Trusted Sites Zone.
- 2. In the details pane, open Login options.
- 3. In the Logon options window, select Enabled.
- 4. From the Logon options list, select Automatic logon with current username and password.
- 5. Click **OK**.

## Step 8: Close the Group Policy Management Editor to Save Your Changes

Closing the Group Policy Management Editor saves the changes to the GPO. The Group Policy Management utility opens. Your GPO appears in **Group Policy Objects** in the Group Policy Management tree.

# Link The Group Policy Object to the Organizational Unit

- 1. In the Group Policy Management window, right-click the new OU you created and select Link an Existing GPO.
- 2. In the Select GPO window, select the new GPO and click OK.



### **Configure Security Filtering**

1. In the Group Policy Management window, navigate to your new OU, select your new GPO, and click the **Scope** tab.

2. In the **Scope** tab > **Security Filtering** section, set the filter as necessary. In this example, the filter is set to **Everyone** to make this policy accessible to everyone.

📓 Group I	Policy Management	_ <b>D</b> X
Image: File Action View Window Help       ◆ ➡       2       Image: Open Define Management		- 8 ×
Group Policy Management  Group Policy Management  Group Policy Management  Group Policy Default Domain Policy  Default Domain Policy  EnableFastConnectOU  Group Policy Objects  Default Domain Controllers Policy  Default Domain Controllers Policy  Default Domain Policy  Default Domain Policy  Starter GPOs  Sites  Group Policy Modeling  Group Policy Results  Administrator on THIRTYTWO	Enable Fast Connect         Scope       Details       Settings       Delegation         Links       Display links in this location:       Imp.net         The following stes, domains, and OUs are linked to this GPO:       Location       Enforced         Image: Location       Image: Location       Enforced         Image: Location       Image: Location       Enforced         Image: Location       Image: Location       No         Image: Location       Image: Location       Image: Location         Security Filtering       Image: Location       Image: Location         Image: Location       Image: Location       Image: Location       Image: Location         Image: Location	V Unk Enablec Yes
	Add     Remove     Properti	es

## Verify the Configuration

All endpoint computers in the OU receive the new GPO settings at the next Group Policy refresh interval. The default interval is 90 minutes. You can verify the configuration with the following methods.

#### View Policy Configurations in the Registry

On an endpoint computer in the OU, you can verify the GPO settings are applied by viewing the settings in the registry:

- 1. Go to:
  - 64—bit HKEY\_LOCAL\_MACHINE > SOFTWARE > Wow6432Node > Policies > Citrix > Dazzle
  - 32—bit HKEY\_LOCAL\_MACHINE > SOFTWARE > Policies > Citrix > Dazzle
- 2. Review the settings as configured in <u>Configure Group Policy</u>.

📸 Registry Editor				
File Edit View Favorites Help				
D - 📕 ODBC	*	Name	Туре	Data
▷ → Policies		ab (Default)	REG_SZ	(value
RegisteredApplications		ab AllAppsAreMandatory	REG_SZ	false
Sonic		ab ClearAppListOnLogoff	REG_SZ	true
		💩 DesktopDir	REG_SZ	Citrix
Wow6432Node		EnableFastConnectTransitionAPI	REG_SZ	true
		FastConnectAPISupportEnabled	REG_SZ	true
	ab FastConnectUsingSSP	REG_SZ	true	
Dients		ab LeaveAppsRuningOnLogoff	REG_SZ	false
⊳		ab PutShortcutsInstartmenu	REG_SZ	false
Microsoft		ab PutShortcutsOnDesktop	REG_SZ	true
MozillaPlugins		ab RemoveAppsOnExit	REG_SZ	true
P - 🌺 ODBC		ab RemoveAppsOnLogoff	REG_SZ	true
A bolicies	=	ab StartMenuDir	REG_SZ	Citrix
⊿ · 🎍 Citrix		ab SuppressRefreshOnStartup	REG_SZ	true
		ab UseCategoryAsStartMenuPath	REG_SZ	false
▷ - 🎳 ICA Client		ab WSCReconnectMode	REG_SZ	2

#### Generate a Group Policy Result Report

By generating a Group Policy Result Report, you can select a specific endpoint computer to query; the report indicates which GPOs are applied.

- 1. In the Group Policy Management window, right-click Group Policy Results > Group Policy Results Wizard...
- 2. In the **Computer Selection** page, select the computer for which you want to display policy settings, and click **Next**.
- 3. In the User Selection page, enter a domain administrator and click Next.
- 4. Click **Finish** to close the wizard.

 The report is not actually run yet; in the Group Policy Management window > Group Policy Results section, right-click the report you just created and click Rerun Query.



**NOTE**: If the Windows WMI service is disabled or restricted on the endpoint computer, the report will not work.

- 6. After the report is generated, select the report from the left navigation. In the example below it is named after the endpoint computer **THIRTYTWO**.
- 7. In the details pane, select the **Details** tab. Your GPO is listed in the section **Applied GPOs**.

