imprivata®

Product Documentation

Configuring Citrix Workspace App for Imprivata OneSign

Imprivata Enterprise Access Management 24.1

Configuring Citrix Workspace App for Imprivata OneSign

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 document includes information about configuring Citrix Workspace app to support Imprivata OneSign 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:

Before You Begin

Review the following requirements and prerequisite steps before you begin.

Software Requirements and Downloads

Before you begin:

- See the Imprivata OneSign Supported Components to identify supported Citrix Workspace app versions.
- Download the Citrix Workspace app installer from the Citrix Support 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:

1. 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 Imprivata OneSign 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.
3. 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.

OneSign 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 — OneSign 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 — OneSign 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 Citrix documentation.

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 are allowed.

    > **NOTE:**
    > The Imprivata virtual channel must be explicitly allowed in the allowed list. While Citrix has documented that disabling all virtual channels is allowed, Imprivata testing has determined that to be insufficient.

  - 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

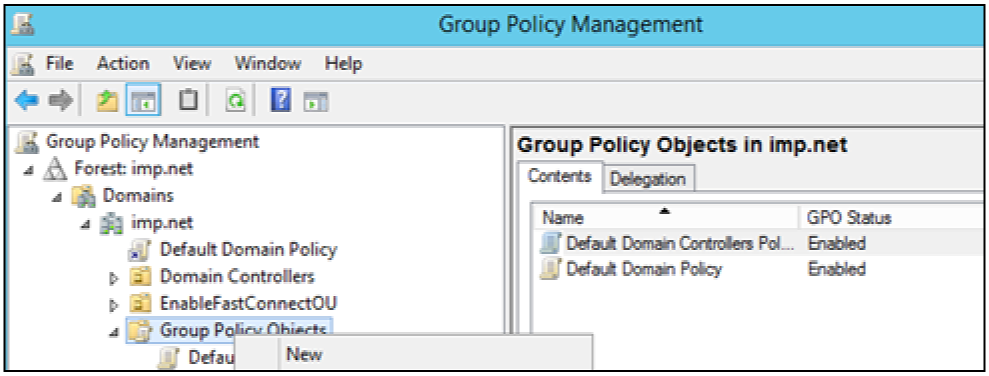
Create an organizational unit (OU), add your endpoint computers to it, and then create a GPO to configure the endpoint computers.

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**.

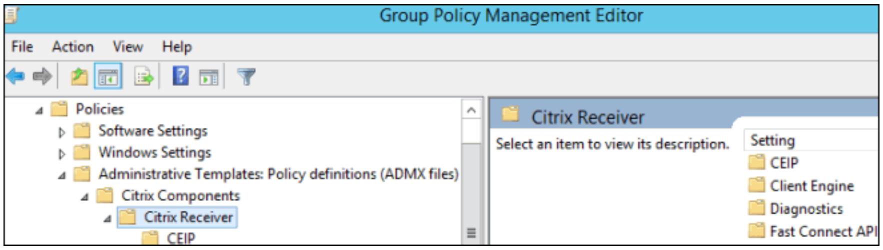


Name	GPO Status
Default Domain Controllers Pol...	Enabled
Default Domain Policy	Enabled

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**.



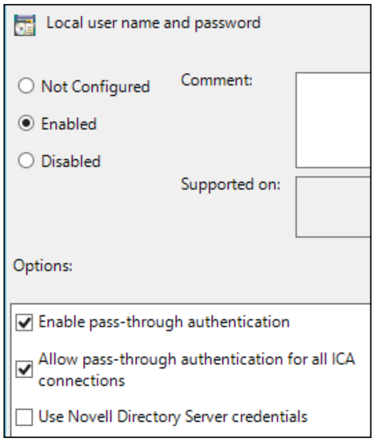
Configure the Group Policy

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

○ Not Configured
● Enabled
○ Disabled

Options:

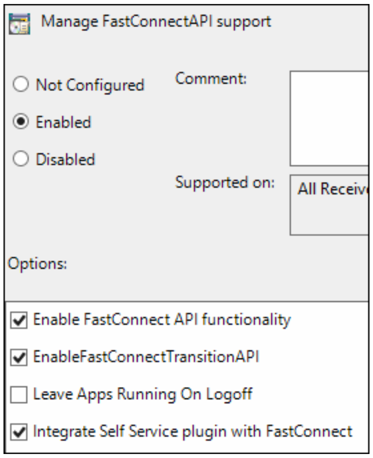
☑ Enable pass-through authentication
☑ Allow pass-through authentication for all ICA connections
☐ Use Novell Directory Server credentials

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 FastConnectAPI support

○ Not Configured
● Enabled
○ Disabled

Supported on: All Receiv

Options:

☑ Enable FastConnect API functionality
☑ EnableFastConnectTransitionAPI
☐ Leave Apps Running On Logoff
☑ Integrate Self Service plugin with FastConnect

Step 3: Configure Application Shortcuts

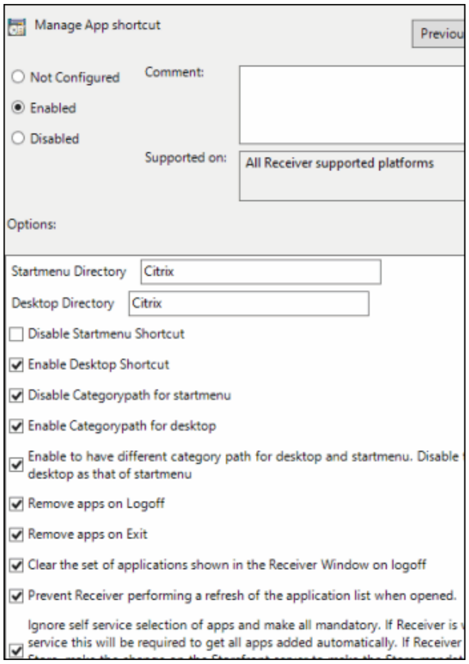
To configure the required settings:

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 shortcut

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: All Receiver supported platforms

Options:

Startmenu Directory: Citrix
Desktop Directory: Citrix

☐ Disable Startmenu Shortcut
☑ Enable Desktop Shortcut
☑ 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:

1. 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:

1. 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:

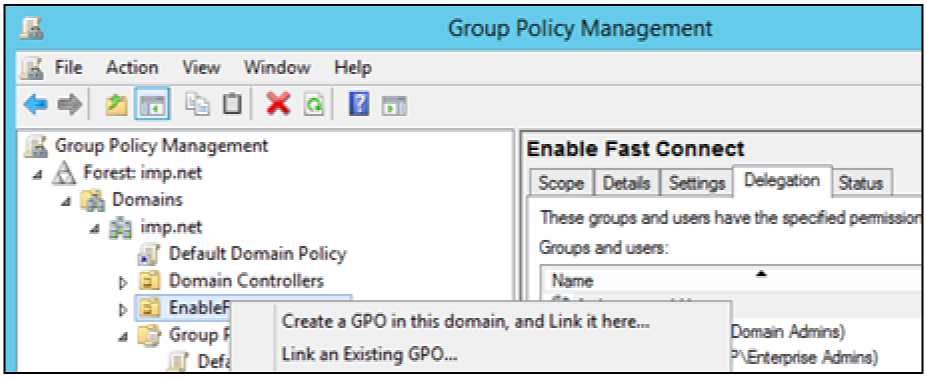
1. In the details pane, open **Trusted Sites Zone**.
2. In the details pane, open **Login options**.
3. In the **Logon options** window, select **Enabled**.
4. From the **Logon options** list, select **Automatic logon with current username and password**.
5. Click **OK**.

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**.



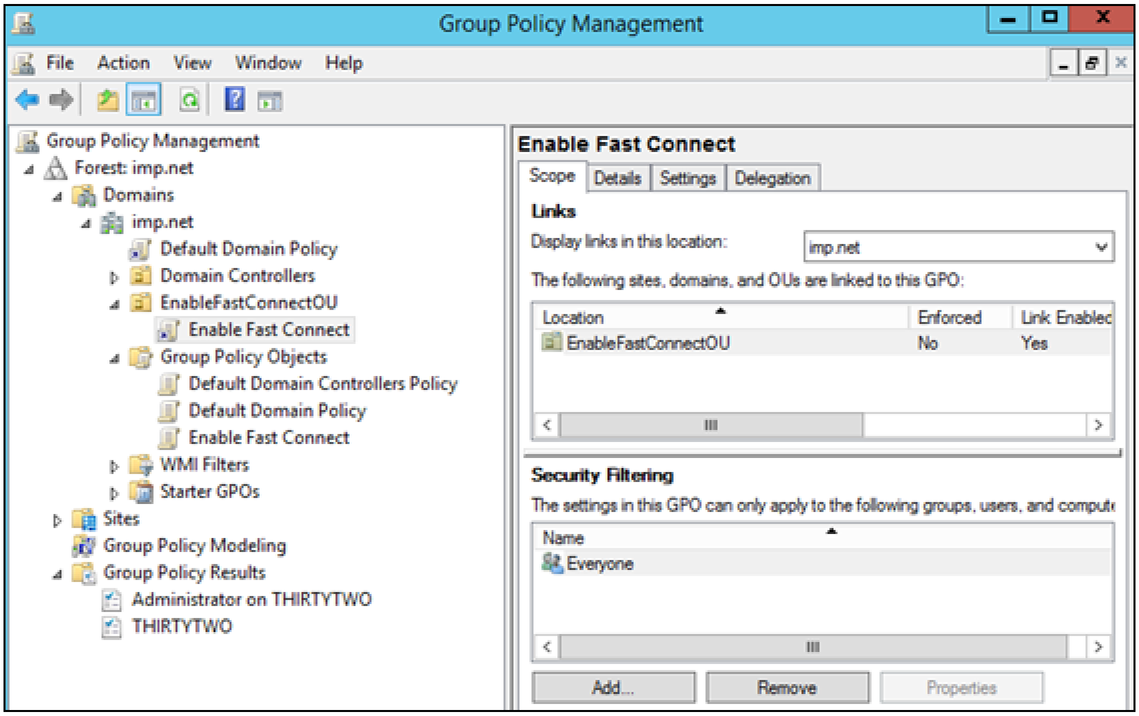
These groups and users have the specified permission

Groups and users:

Domain Admins)
P\Enterprise Admins)

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.



Display links in this location: imp.net

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled
EnableFastConnectOU	No	Yes

The settings in this GPO can only apply to the following groups, users, and comput

Name
Everyone

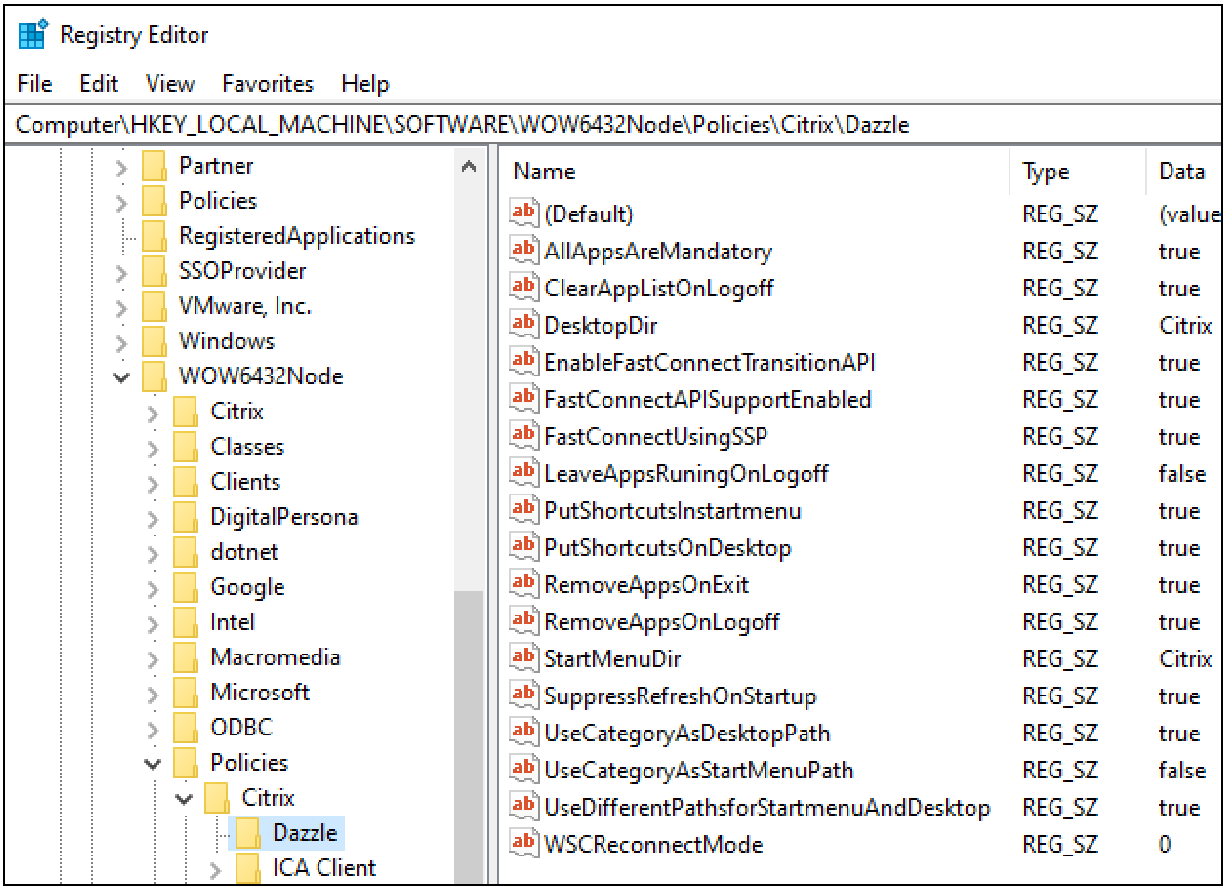
Verify the Configuration

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 Configure Group Policy.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\Dazzle

Name	Type	Data
(Default)	REG_SZ	(value
AllAppsAreMandatory	REG_SZ	true
ClearAppListOnLogoff	REG_SZ	true
DesktopDir	REG_SZ	Citrix
EnableFastConnectTransitionAPI	REG_SZ	true
FastConnectAPISupportEnabled	REG_SZ	true
FastConnectUsingSSP	REG_SZ	true
LeaveAppsRuningOnLogoff	REG_SZ	false
PutShortcutsInstartmenu	REG_SZ	true
PutShortcutsOnDesktop	REG_SZ	true
RemoveAppsOnExit	REG_SZ	true
RemoveAppsOnLogoff	REG_SZ	true
StartMenuDir	REG_SZ	Citrix
SuppressRefreshOnStartup	REG_SZ	true
UseCategoryAsDesktopPath	REG_SZ	true
UseCategoryAsStartMenuPath	REG_SZ	false
UseDifferentPathsforStartmenuAndDesktop	REG_SZ	true
WSCReconnectMode	REG_SZ	0

Generate a Group Policy Result Report

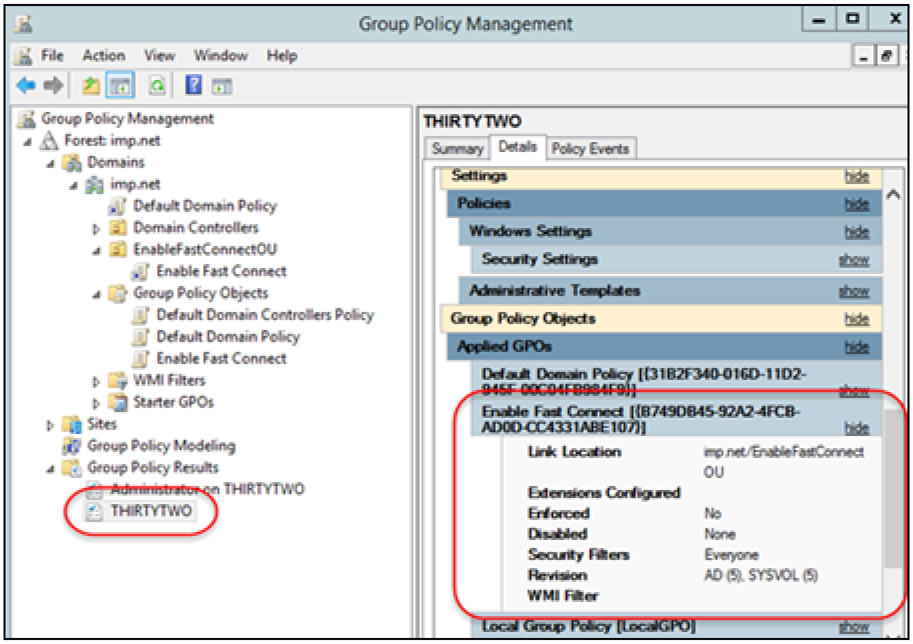
By generating a Group Policy Result Report, you can select a specific endpoint computer to query; the report indicates which GPOs are applied.

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.

5. 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**.



Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}] show

Enable Fast Connect [{B749DB45-92A2-4FCB-AD0D-CC4331ABE107}] hide

Link Location	imp.net/EnableFastConnect OU
Extensions Configured	
Enforced	No
Disabled	None
Security Filters	Everyone
Revision	AD (5), SYSVOL (5)
WMI Filter	

Local Group Policy [LocalGPO] show