Upgrading from Citrix Receiver
3.4 to Receiver 4.2.100

Step by step instructions for upgrading Receiver for Windows

April 2015
Table of Contents

Introduction

Section 1: StoreFront Server

Upgrading with App Shortcuts in a fixed location when using StoreFront ........ 3

- Step 1: Configure GPO to remove Version 3.4 ................................................................. 4
- Step 2: Configure GPO to install Receiver 4.2 ............................................................... 10
- Step 3: Import Citrix Administrative Templates (ADM) .................................................. 16
- Step 4: Configure Storefront policies using Citrix ADM Templates .......................... 18
- Step 5: Configure GPO to add StoreFront to trusted sites ........................................ 24
- Step 6: Run the policy scripts ......................................................................................... 27
- Step 7: Validate the configuration and operation ......................................................... 27

Upgrading with App Shortcuts configured per app when using StoreFront ... 30

- Configuring per app settings using AppCenter in XenApp 6.5 .................................. 31
- Configuring per app settings using Citrix Studio in XenApp or XenDesktop 7.6 ....... 36
- Run the policy scripts .................................................................................................... 40
- Validate the configuration and operation .................................................................... 40

Section 2: Web Interface

Upgrading with Apps Shortcuts in a fixed location when using Web Interface 41

- Pre-requisite check before upgrading ........................................................................ 41
- Configure the GPO to remove 3.4 .............................................................................. 46
- Configure GPO to install Receiver 4.2 ....................................................................... 46
- Import Citrix Administrative Templates (ADM) ......................................................... 53
- Configure Web Interface policies using ADM templates ............................................ 53
- Configure GPO to add the XenApp Services Site as a trusted site ............................ 56
Run the policy scripts ..................................................................................................................................................59
Validate the configuration and operation ..................................................................................................................59

Upgrading with App Shortcuts configured per app when using Web Interface

Configuring per app settings using XenApp 6.5 ........................................................................................................65
Configuring per app settings using XenApp 7.6 Citrix Studio ...............................................................................70

About Citrix

Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

Copyright © 2015 Citrix Systems, Inc. All rights reserved. Citrix, Citrix Receiver, and StoreFront are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.
The upgrade path from Receiver 3.4 for Windows Enterprise to Receiver 4.2.100 for Windows requires the reconfiguration of a number of settings. In-place upgrade by end users is not supported and IT administrators must prepare their environment for users to enjoy a smooth experience after the upgrade. This guide provides IT administrators with step by step instructions for upgrading from Receiver 3.4 for Windows Enterprise to Receiver 4.2.100 for Windows. The guide includes best practices which retain the user experience of pass-through authentication (Single Sign-On) and application shortcuts in the Start menu and desktop.

If you have been using Receiver 3.4 for Windows Enterprise, now is the time to upgrade your desktops and thin clients to Receiver 4.2.100 to enable the best performance for graphics-intensive 3D professional applications, USB redirection with published apps, Microsoft Lync virtualization, local app access, app shortcuts, pass-through authentication, and more.

For information on all the features and system requirements of Receiver 4.2.100 for Windows, and further install and upgrade guidance, see Receiver 4.2 for Windows in Citrix Product Documentation.

Receiver 4.2.100 for Windows enables pass-through authentication in the same way that Receiver 3.4 for Windows Enterprise does. Receiver installs a component called Single Sign-on (SSON). SSON captures the user’s credentials and securely stores them for use in authenticating the users with XenApp and XenDesktop sessions.

Where Receiver 3.4 for Windows Enterprise used to install SSON by default, Receiver 4.2.100 for Windows requires you to enable pass-through authentication using a command line switch (/includeSSON). Typically this is done using a group policy to invoke scripted install of the Receiver. You may also install Receiver on a user device from the command line by executing the installer file with option /includeSSON.

The following sections show how to include SSON in the scripted upgrade to Receiver 4.2.100 for Windows.
Remember to install Receiver 4.2.100 on user devices with local administrative privileges, and add the StoreFront or Web Interface server to the Trusted Zone settings in Internet Explorer to allow connections from Receiver.

Section 1: StoreFront Server

This section provides step-by-step guidance for upgrading Receiver 3.4 for Windows to Version 4.2.100 using Group Policy Objects (GPOs). The information in this section requires administrative knowledge of GPO policy management, Citrix Studio, and StoreFront server. If your environment uses Web Interface instead of StoreFront, please skip to the instructions provided in the next section.
Upgrading with App Shortcuts in a fixed location when using StoreFront

- Configure GPO to uninstall Receiver 3.4
- Configure GPO to install Version 4.2.100 with SSON enabled
- Define a StoreFront URL
- Enable app short cut settings
- Add StoreFront as trusted site to Internet Explorer
- Execute the group policies (GPO)
- SSON credential saved at first login post-install
- Validate the settings
  - Trusted Sites Zone includes the Storefront URL
  - Validate that SSON is working
  - Apps shortcuts are in the correct location
The basic steps are as follows:

1. Configure a GPO to remove Version 3.4.
2. Configure a GPO to install Version 4.2.100 with SSON, a StoreFront URL, and app short cut settings.
3. Configure a GPO to add trusted sites to Internet Explorer.
4. Run the GPO to remove Version 3.4; this effectively invokes the GPO to execute the changes in the steps above.
5. Run the GPO to install Receiver 4.2.100.
6. Run the GPO to add trusted sites to Internet Explorer.
7. Verify that the Trusted Sites Zone includes the Storefront URL.
8. Validate that SSON is working and that the apps are installed in the correct location.

**Step 1: Configure GPO to remove Version 3.4**

a. Access the domain controller (where Active Directory resides):
b. Launch the Group Policy Object (GPO) editor:

![Launch the GPO]

Launch the GPO

---

c. Locate the organizational unit (OU):

![Locate the organizational unit (OU)]
d. Create a new GPO in this domain:

![Group Policy Management]

e. In the **New GPO** screen, enter the name associated with the GPO and optionally specify a Source Starter GPO, click **OK**:

![New GPO]

f. After creating the new GPO, locate it in the menu tree. Right click to display a context menu, and select **Edit**:
g. In the **Scripts** screen click **Startup**: 

h. The **Startup Properties** screen appears. Click **Add**: 
i. In the Add a Script screen, click Browse to locate the Receiver 3.4 removal script you want to add to the GPO library:

![Add a Script](image1.png)

j. In the Browse screen, locate the remove script that was distributed with the Receiver for Windows 3.4; this script is typically on the server where Receiver was installed. Select it, and click Open:

![Browse](image2.png)

*The name of the script used to remove Receiver for Windows 3.4 is labelled `CheckAndRemoveCitrixReceiverEnterpriseStartupScript.bat`. 
k. The default text editor opens the removal script. Locate the URL path (located on a line labeled **DeployDirectory**) associated with the deployment, and copy it to the clipboard:

```
REM *** (1) PACKAGE LOCATION/DEPLOYMENT DIRECTORY ***
REM ***
REM set DeployDirectory=\10.105.34.198\share\receivers\3.4.300\
REM ***
REM *** (2) SCRIPT LOGGING DIRECTORY ***
REM ***
REM set Logshare=\10.105.34.198\share\receivers\3.4.300\
REM ***
REM *** BEGIN SCRIPT PROCESSING ***
REM ***
REM *** END SCRIPT PROCESSING ***
```

![Image of script file]

The **DeployDirectory** field contains the path for the Receiver deployment package.

l. Return to the **Add a Script** screen and paste the URL path to the **Script Name** field. Click **OK**:
m. You should now see the updated URL path appended to the script. Click OK to return to the GPO Editor screen:

The GPO is now configured to remove Receiver 3.4 for Windows.

Step 2: Configure GPO to install Receiver 4.2

2. Configure a GPO to install Version 4.2.100 with SSON, a StoreFront URL, and app short cut settings:
a. Follow the same process as Step 1 to launch the Group Policy Object (GPO) Editor and locate the Organisation Unit (OU).

b. Create a new GPO in this domain:

c. In the **New GPO** screen, enter the name so you can identify the GPO (for example, *Install_4_2_GPO*); do not specify the Source Starter GPO. Click **OK**:

d. After creating the new GPO, locate it in the menu tree. Right click to display a context menu, and select **Edit**:
In the **Scripts** screen click **Startup**. This will trigger the script to run immediately after the end user device starts-up, and performs the Receiver installation in the background:

The **Startup Properties** screen appears. Click **Add**.
g. In the **Add a Script** screen, click **Browse** to locate the installation script you want to add to the GPO library:

h. In the **Browse** screen, locate the *CheckandDeploy* script that was distributed with the Receiver for Windows 4.2.100 distribution; this script is typically located on the server where Receiver was installed. Select it, and click **Open**:
The name of the script used to install Receiver for Windows 4.2.100 is labelled CheckAndDeployCitrixReceiverPerMachineStartupScript.bat.

i. The default text editor opens the script:

The CheckAndDeployCitrixReceiverPerMachineStartupScript.bat script contains a number of fields containing the current version and path of the citrixreceiver.exe package (the desired version), the location of logs stored to display script run status, and command line options for the installation package.

j. In the deployment script, locate the URL path associated with the deployment, and copy it to the clipboard (this script is typically located on the server where Receiver was installed):
The **DeployDirectory** field contains the path for the Receiver deployment package. This script also contains the option switches to perform silent installation and include single sign-on (SSON).

**k.** Return to the **Add a Script** screen and paste the URL path to the **Script Name**. Click **OK**:

**l.** The **Startup Properties** screen appears, with the updated URL path appended to the script. Click **Apply**, then **OK** to return to the GPO Editor screen:
The GPO is now configured to install Receiver for Windows 4.2.100.

Close the GPO editor.

**Step 3: Import Citrix Administrative Templates (ADM)**

A pre-requisite to this step is having access to the ADM templates available in the folder where you install Citrix Receiver. This is typically `%ProgramFiles% → Citrix → ICA Client → Configuration`. As a best practice, copy the ADM files in this folder to a network share before continuing. The alternative is to install Receiver on the domain controller, where you create the GPO policies.

a. In the Group Policy Management Editor, select **Policies:**
b. Select **Administrative Templates**, right click to display a context menu. Select **Add\Remove Templates**:

![Administrative Templates context menu](image)

![Add/Remove Template screen](image)

c. In the Add/Remove Template screen, click **Add**:

![Add button](image)

d. In the Policy Templates screen, browse to the network share where you copied ADM templates, from the Receiver installation folder earlier. Select the file **icaclient.adm**. Click **Open**:

![Open button](image)
After opening the file, it appears in the **Add/Remove Templates** screen:

![Add/Remove Templates](image)

Click **Close**.

**Step 4: Configure Storefront policies using Citrix ADM Templates**

Now that the script has been configured to deploy Receiver for Windows 4.2.100, and the policies templates have been imported, access policies to configure the StoreFront URL associated with Receiver.

e. In the Group Policy Management Editor screen, select the **Storefront** folder under **Policies** → **Classic Administrative Template** → **Citrix Components** → **Citrix Receiver**:
f. Select **Storefront Accounts List**:

g. In the Storefront Accounts List screen, select **Enabled**. Click **Show** to enter Storefront account details:
The **Show Contents** screen allows you to configure account details. Click the icon to specify Storefront account details:

Enter the Storefront URL and other details. Remember to follow the syntax exactly as shown in the HELP text above, separated by semi-colons (;) Click **OK**:
h. In the Policies → Classic Administrative Template section of the Group Policy Management Editor, select **SelfService** to configure app shortcut settings:

In the SelfService screen, select **Manage SelfServiceMode**: 

![Image of SelfService screen]
In the **Manage SelfServiceMode** screen, the default setting is “Not Configured” which allows self-service mode to be used. To activate the “shortcuts only mode” that we want here, select **Disabled**. Click **Apply**, then **OK**:

![Manage SelfServiceMode Screen](image)

In the SelfService screen, select **Manage App shortcut**:

![Manage App shortcut Screen](image)

In the Manage App shortcut screen, select **Enabled**. In the options portion of the screen, enter the names for the **Startmenu Directory** and the
Desktop Directory (for example, Citrix Apps) or leave it blank to use the default folder name “Citrix”. Select Enable Desktop Shortcut. Click Apply, then OK:

i. Next, still within the Policies→Classic Administrative Template section of the Group Policy Management Editor, select User Authentication to configure Single Sign-on (SSON) settings:
In the **User authentication** screen, select **Local user name and password**:  

![User authentication screen](image1)

In the Local user name and password screen, click **Enabled**. In the options portion of the screen, select **Enable pass-through authentication** and **Allow pass-through authentication for all ICA connections**. Click **Apply**, then **OK** to commit the changes:

![Local user name and password screen](image2)

**Step 5: Configure GPO to add StoreFront to trusted sites**

3. **Configure a GPO to add trusted sites to Internet Explorer.**
   
a. In the **Policies** section of the Group Policy Management Editor, select **Windows Components**:
Expand the **Windows Components** folder. Select **Internet Explorer**:

Expand the **Internet Explorer** folder and select **Internet Control Panel**:

Expand the **Internet Control folder**, and select **Security Page**. In the Security Page portion of the screen, select **Site to Zone Assignment List**:
b. In the Site to Zone Assignment screen, select **Enabled**. Click **Show** to locate the Storefront URL:

The **Show Contents** screen allows you to configure the URL and set the value for the Internet zone. Click the edit icon to enter the *Storefront URL* under
Value Name. In the Value field, enter 1; this value associates the Storefront URL with the Intranet zone. Click OK to apply the changes:

![Value Name](image)

In the Site to Zone Assignment screen, select Apply, then OK.

**Step 6: Run the policy scripts**

From the command prompt (with domain administrator privileges) of the domain controller CLI, run `gpupdate /force` to cumulatively execute all the policy scripts. They will run the next time the client machines start-up.

4. **Run the GPO to remove Version 3.4.** The invoked script removes the previously installed Receiver Enterprise 3.4 software from the client machine referenced in the group policy.

5. **Run the GPO to install Receiver 4.2 with Single Sign-on (SSON), a StoreFront URL, and app short cut settings.** The invoked script installs Receiver for Windows 4.2.100 and configures the client for SSON, the Storefront URL, and app short cut settings on the client machine referenced in the group policy.

6. **Run the GPO to add trusted sites to Internet Explorer.** The client is automatically configured upon startup and user login.

**Step 7: Validate the configuration and operation**

7. In Internet Explorer, verify that the Trusted Sites Zone includes the Storefront URL:
Select **Local intranet**, and click **Sites**:

Click **Advanced** to display the Local intranet trusted site screen:
In the example above the StoreFront server name is added in intranet zone.

Once the machine runs the GPO and installs Receiver 4.2.100, the machine has to be logged off once. When the user logs in again the single sign-on process ssonsvr.exe will start running and captures the logged in user credentials. The credentials will be passed to Receiver for passthrough authentication in subsequent logins.

8. Validate that SSON is working and that the apps shortcuts are installed in the correct location.
Upgrading with App Shortcuts configured per app when using StoreFront

In the previous section, we set up to publish app shortcuts for all published apps. If instead you wish to configure custom app-shortcut settings per app, use the instructions in this section. The steps require configuration of each app in the XenApp Console to place them in the desired location. Then follow the GPO configuration as described in the previous section to complete the deployment.
The steps are different depending on whether your environment is on XenApp 6.5 or the newer XenApp/XenDesktop 7.6. Both methods are provided below.

**Configuring per app settings using AppCenter in XenApp 6.5**

a. From the Remote Desktop Connection Manager, launch **Citrix AppCenter**:

![Citrix AppCenter](image1.png)

A .NET Authenticode message may appear; click **Ask me later** to continue:

![Ask me later](image2.png)

b. In the **Select Products or Components** screen, expand the Citrix Resources folder. Select **XenApp** and **deselect Single Sign-On** (if password...
manager component is *not* installed on XenApp Server machine), else leave as default. Click **Next**.

c. In the **Select Servers** screen, click **Add Local Computer**.
d. After adding a local computer, the **Servers** field is automatically populated with the appropriate server. Click **Next**:

The **Preview Discovery** screen appears. Verify that the correct XenApp server appears. Click **Next**:
After the **Discovery Progress** is completed, click **Finish**:

```
<table>
<thead>
<tr>
<th>Step</th>
<th>Discovery Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome</td>
<td>Discovery completed</td>
</tr>
<tr>
<td>Select Product or Components</td>
<td></td>
</tr>
<tr>
<td>Configure Discovery</td>
<td></td>
</tr>
<tr>
<td>XenApp</td>
<td></td>
</tr>
<tr>
<td>Select Servers</td>
<td></td>
</tr>
<tr>
<td>Preview/Discovery</td>
<td></td>
</tr>
<tr>
<td>Discovery Progress</td>
<td></td>
</tr>
</tbody>
</table>
```

e. In **Citrix AppCenter**, expand the **Applications** folder:
f. In the **Applications** folder, select the app for which you wish to create a short-cut (for example, PowerPoint):

Right-click the application name (PowerPoint, in this example) to display a context menu. Select **Application properties**:

In the **Application Properties** screen, select **Shortcut presentation**.

In the Shortcut presentation portion of the screen:
- Select **Add to the client’s Start menu**. Enter a name for the folder, for example, *MS Office 2010 Apps*. By default, the folder is named Citrix.
- Select **Add shortcut to the client’s desktop**.

After configuring options for the shortcut presentation, click **Apply**, then **OK** to commit the changes.

**Configuring per app settings using Citrix Studio in XenApp or XenDesktop 7.6**

a. From the Remote Desktop Connection Manager, launch Citrix Studio:
b. In Citrix Studio, select **Delivery Groups** in the navigation tree. Click the **Applications** tab:

c. Select the application and right click to display a context menu. Click **Properties**:
d. In the **Application Settings** screen, select **Delivery**. Select **Add shortcut to user’s desktop**. Optionally, enter a name for the **app category** (for example, MS Office 2013 Apps); by default, the folder is named Citrix. Leaving this field blank automatically sets the folder to the default name. Click **Apply**, then **OK** to commit the changes:

![Application Settings](image1)

e. On the domain controller machine, import ADM templates in order to configure Receiver settings using GPO. See Step 3: Import Citrix Administrative Templates (ADM).
The GUI only configures app shortcuts to the desktop. If you want the application shortcuts to show up in the Start menu on the client machine, run the Powershell commands below.

f. Run PowerShell from the Windows Start menu on the Delivery Controller machine using administrator privileges; this task must be performed before running the GPOs:

```
g. In PowerShell type “$asnp Citrix.*”.

h. In PowerShell set the application property “-ShortcutAddedToStartMenu” to “$true” as illustrated below. For example:
```

```powershell
Set -BrokerApplication -Name “word2013” -ShortcutAddedToStartMenu $true
```
Ensure the application name (for example, word 2013) in the PowerShell cmdlet matches the application name in the GUI. Do this for all applications where you want a Start menu shortcut.

**Run the policy scripts**

Follow the instructions in Step 6: Run the policy scripts.

**Validate the configuration and operation**

Follow the instructions in Step 7: Validate the configuration and operation.
Section 2: Web Interface

Upgrading with Apps Shortcuts in a fixed location when using Web Interface

The previous section talked about upgrading to Receiver 4.2.100 when the environment is running StoreFront, which is the recommended front-end for latest deployments. This section provides step-by-step guidance if your environment continues to leverage the older Web Interface (WI) server. The steps are different when running XenApp 6.5 at the back-end and when running XenApp or XenDesktop 7.6, so we will cover both methods here.

The information in this section requires administrative knowledge of Group Policy Object (GPO) management and Citrix Studio.

The plan is to upgrade a running Web Interface server already using app shortcuts and pass-through authentication, without losing any settings during the upgrade from Receiver 3.4 to Receiver 4.2.100.

Pre-requisite check before upgrading

With Receiver 3.4, validate the following Web Interface Machine Settings or make these changes now to prepare for app shortcuts and single sign-on after upgrading to Receiver 4.2.100. This is the expected configuration in the PNAgent site settings for Start Menu and Desktop Shortcuts:

i. Open the Citrix Web Interface Management Console.
ii. Select **XenApp Services Sites**.
iii. Select the PNAgent.
iv. Right click the PNAgent; select **Shortcuts**.
v. In the **Manage Shortcuts** screen, expand **Shortcut Creation**. Validate or configure the settings for **Control** (Use site settings (defined on this page)) and **Display** (always place resource shortcuts on the Start menu) as illustrated in the following screen:
Select Desktop Shortcuts. Validate or configure the settings for Control (Use site settings (defined on this page) and Display (always place resource shortcuts on the Start menu) as illustrated in the following screen:
Select **Shortcut Removal**. Validate or configure the options for **Shortcut Removal** (select the Remove Citrix online plug-in shortcuts) and **Settings** (When the Citrix online plug-in closes) and select the Types of shortcuts to remove (Citrix online plug-in and user-created shortcuts) as illustrated in the following screen:
1. In the Citrix Web Interface Management screen, configure the PNAgent site settings for Single Sign On (SSON):
   vi. Open the **Citrix Web Interface** Management Console.
   vii. Click **XenApp Services Sites**.
   viii. Right Click **PNAgent** site and select **Authentication Methods** in the context menu.
   ix. In the Configure Authentication Methods – PNAgent screen, select **Pass-through (default)**.
   x. Click **OK**.
Now we are ready to perform the upgrade to Receiver 4.2.100. The basic steps are as follows:

1. Configure a GPO to remove Receiver 3.4.
2. Configure a GPO to install Receiver 4.2.100 with SSON, a XenApp Services Site(PNAgent) URL, and app short cut settings.
3. Configure a GPO to add trusted sites to Internet Explorer.
4. Run the GPO to remove version 3.4.
5. Run the GPO to install version 4.2.100 with SSON, a XenApp Services Site(PNAgent) URL, and app short cut settings.
6. Run the GPO to add trusted sites to Internet Explorer.
7. Verify that the Trusted Sites Zone includes the Storefront URL.
8. Validate that SSON is working and that the apps are installed in the correct location.
Configure the GPO to remove 3.4

Follow the instructions in Step 1: Configure GPO to remove Version 3.4 to create an Uninstall Policy that will remove Receiver 3.4 from client machines upon start-up.

Configure GPO to Install Receiver 4.2

Follow these instructions to create an Install Policy that will deploy Receiver 4.2.100 to client machines with necessary PNAgent settings, upon start-up:

1. Configure a GPO to install Version 4.2.100 with SSON, a XenApp Services Site(PNAgent) URL, and app short cut settings:
   a. Access the domain controller (where Active Directory resides):
   b. Launch the GPO editor:
c. Locate the organizational unit (OU):

![Image of organizational unit (OU)](image1)

d. Create a new GPO in this domain:

![Image of creating a new GPO](image2)

e. In the **New GPO** screen, enter the name associated with the GPO (for example, *Install_4_2_GPO*) and optionally specify a Source Starter GPO, click **OK**:

![Image of creating a GPO](image3)
f. After creating the new GPO, locate it in the menu tree. Right click to display a context menu, and select **Edit**:

![New GPO dialog box](image1)

![Group Policy Management](image2)

  - **g.** In the **Scripts** screen click **Startup**:

![Scripts screen](image3)

  - **h.** The **Startup Properties** screen appears. Click **Add**:
i. In the **Add a Script** screen, click **Browse** to locate the installation script you want to add to the GPO library:

![Add a Script](image1)

j. In the **Browse** screen, locate the remove script that was distributed with the Receiver 3.4 for Windows. Select it, and click **Open**:

![Browse](image2)
The name of the script used to install Receiver 4.2.100 for Windows is labelled `CheckAndDeployCitrixReceiverPerMachineStartupScript.bat`.

**k. The default text editor opens the script:**

```
REM ******** DATE: May 9, 2011
REM ******** DESCRIPTION:
REM Check and Deploy Citrix Receiver PM
REM Via Active Directory Startup Script
REM ******** INPUTS: (1) Current version of package
REM (2) Package Location/Deployment Directory
REM (3) Script Logging Directory
REM (4) Package Installer Command Line options
REM ******** OUTPUTS: Installs the Citrix Receiver PM
REM Reports an error if the package is already installed
```

The `CheckAndDeployCitrixReceiverPerMachineStartupScript.bat` script contains a number of fields that containing the version of the citrixreceiver.exe package, the path location of the citrixreceiver.exe package, the path location for storing logs of script run status, and command line options for citrixreceiver.exe package installation.

**l. Locate the URL path associated with the deployment, and copy it to the clipboard:**
In the deployment script (above) include the following command line parameter:

/silent /includeSSON /STORE0=“PNAgent;https://BLR4XAB-SQ915GE.blricat.com/citrix/PNAgent/config.xml;On;My PNAgent Site”

In addition, edit the line which starts with “start /wait” to include the variable “%CommandLineOptions%”. After editing the deployment script, it resembles the screens depicted below:

The DeployDirectory field contains the path for the Receiver deployment package.

m. Return to the Add a Script screen and paste the URL path to the Script Name. Click OK:
n. The **Startup Properties** screen appears, with the updated URL path appended to the script. Click **Apply**, then **OK** to return to the GPO Editor screen:

![Startup Properties screen](image)

The GPO is now configured to install Receiver for Windows 4.2.100.

Close the GPO editor.
**Import Citrix Administrative Templates (ADM)**

Follow the instructions in Step 3: Import Citrix Administrative Templates (ADM) to import Citrix Administrative Templates (ADM) into the Group Policy Management Editor.

**Configure Web Interface policies using ADM templates**

Now that the script has been configured to deploy Receiver for Windows 4.2.100, and the policy templates have been imported, access policies to configure the StoreFront URL associated with Receiver:

j. In the Group Policy Management Editor screen, select the **SelfService** folder under **Policies** → **Classic Administrative Template** → **Citrix Components** → **Citrix Receiver** to configure the app shortcut settings:

In the SelfService screen, select **Manage SelfServiceMode**: 
In the Manage SelfServiceMode screen, select **Disabled**. Click **Apply**, then **OK**:

![Manage SelfServiceMode Screen]

In the SelfService screen, select **Manage App shortcut**:

![SelfService Screen]

In the Manage App shortcut screen, select **Enabled**. In the options portion of the screen, enter the names for the **Startmenu Directory** and the **Desktop Directory** (for example, **Citrix_Apps**). Select Enable Desktop Shortcut. Click **Apply**, then **OK**:
o. In the **Policies** section of the Group Policy Management Editor, select **User Authentication** to configure Single Sign-on (SSON) settings:

In the **User authentication** screen, select **Local user name and password**:
In the Local user name and password screen, click **Enabled**. In the options portion of the screen, select **Enable pass-through authentication** and **Allow pass-through authentication for all ICA connections**. Click **Apply**, then **OK** to commit the changes:

**Configure GPO to add the XenApp Services Site as a trusted site**

2. **Configure a GPO to add trusted sites to Internet Explorer.**
   a. In the **Policies** section of the Group Policy Management Editor, select **Windows Components**: 
Expand the **Windows Components** folder. Select **Internet Explorer**:

Expand the **Internet Explorer** folder and select **Internet Control Panel**:

Expand the **Internet Control folder**, and select **Security Page**. In the Security Page portion of the screen, select **Site to Zone Assignment List**.
b. In the Site to Zone Assignment screen, select **Enabled**. Click **Show** to locate the Storefront URL:

The **Show Contents** screen allows you to configure the URL and set the value for the Internet zone. Click the edit icon to change the Storefront URL. In the
Value field, enter 1; this value associates the Storefront URL with the Internet Intranet zone. Click OK to apply the changes:

In the Site to Zone Assignment screen, select Apply, then OK.

Run the policy scripts

Follow the instructions in Step 6: Run the policy scripts.

Validate the configuration and operation

Follow the instructions in Step 7: Validate the configuration and operation.
Upgrading with App Shortcuts configured per app when using Web Interface

This section provides step-by-step guidance for upgrading Receiver 3.4 for Windows to Receiver 4.2.100 using Group Policy Objects. The information in this section requires administrative knowledge of Group Policy Object (GPO) policy and Citrix Studio.

Web Interface Machine Settings:

1. The Web Interface has the following PNAgent site settings configured for Start Menu and Desktop Shortcuts:
   
   I. Open the Citrix Web Interface Management Console.
   
   II. Click XenApp Services Sites. Right click to display a context menu. In the context menu, select Manage Shortcuts. The Manage Shortcuts – PNAgent screen appears.
   
   III. Expand Shortcut Creation. Select Start Menu Shortcuts; in the Control portion of the screen, select Use server farm settings (defined in resources). Click OK:
IV. Select Desktop Shortcuts. In the Control portion of the screen, select Use server farm settings (defined in resource). Click OK:
Select **Shortcut Removal**. Select the **Remove Citrix online plug-in shortcuts** checkbox. In the Settings area of the screen, select **When the Citrix online plug-in closes**. Click **OK**.
2. The Web Interface has the following PNAgent site settings configured for Single Sign ON(SSON):
   xi. Open the **Citrix Web Interface** Management Console.
   xii. Click **XenApp Services Sites**.
   xiii. Right Click PNAgent site and select **Authentication Methods**. In the Configure Authentication Methods – PNAgent screen, select **Pass-through (default)**. Click OK:
The steps are as follows:

1. Configure each app in the XenApp Console to place them in the desired location using the Remote Desktop Connection Manager.
2. Configure a GPO to remove version 3.4 as per the previous section.
3. Configure a GPO to install version 4.2.100 with SSON, a XenApp Services Site URL, and set the SelfServiceMode=False and Disable Startmenu shortcut.
4. Configure a GPO to add trusted sites to Internet Explorer as per the previous section.
5. Run the GPO to remove version 3.4 as per the previous section.
6. Run the GPO to install Receiver 4.2.100 as per the previous section.
7. Run the GPO to add trusted sites to Internet Explorer as per the previous section.
8. Verify that the Trusted Sites Zone includes the Storefront URL as per the previous section.
9. Validate that SSON is working, and that apps are in the desired location as per the previous section.
Configuring per app settings using XenApp 6.5

Use the information in this section to configure apps using per-app settings.

The following procedure is for administrators running XenApp 6.5.

a. From the Remote Desktop Connection Manager, launch **Citrix AppCenter**:

   ![Citrix AppCenter](image)

   A .NET Authenticode message may appear; click **Ask me later** to continue:

   ![Ask me later](image)

   b. In the **Select Products or Components** screen, expand the Citrix Resources folder. Select **XenApp**; do not select **Single Sign-On if password**
manager component is not installed in XenApp Server machine. Click Next.

c. In the Select Servers screen, click Add Local Computer:
d. After adding a local computer, the Servers field is automatically populated with the appropriate server. Click **Next**:

The **Preview Discovery** screen appears. Verify that the correct XenApp server appears. Click **Next**:
In the **Discovery Progress** screen, click **Finish**:

![Discovery Progress Screen](image)

e. In **Citrix AppCenter**, expand the **Applications** folder:

![Citrix AppCenter](image)

f. In the **Applications** folder, select an app (for example, PowerPoint):
Select **PowerPoint** and right click to display a context menu. Select **Application properties**:

In the **Application Properties** screen, select **Shortcut presentation**. In the Shortcut presentation portion of the screen:

- Select **Add to the client’s Start menu**. Enter a **name** for the shortcut, for example, *MS Office 2010 Apps*.
- Select **Add shortcut to the client’s desktop**.
After configuring options for the shortcut presentation, click **Apply**, then **OK** to commit the changes.

### Configuring per app settings using XenApp 7.6 Citrix Studio

- The following procedure is for administrators running XenApp 7.6.
  - From the Remote Desktop Connection Manager, launch Citrix Studio:
h. In Citrix Studio, select **Delivery Groups** in the navigation tree. Click the **Applications** tab:

i. Select the application and right click to display a context menu. Click **Properties**: 
If you want the application to have a Start menu shortcut created on the client machine, first set the application property “-ShortcutAddedToStartMenu” to “$true” using the PowerShell cmdlet as illustrated below:

```
PS C:\Windows\system32> Set-BrokerApplication -Name "Word2013" -ShortcutAddedToStartMenu $true
```

j. In the **Application Settings** screen, select Delivery. Enter the name of the **app category**, for example, MS Office 2013 Apps. Select **Add shortcut to user’s desktop**. Click **Apply**, then **OK** to commit the changes:
Access the domain controller (where Active Directory resides):

a. Launch the GPO editor:
b. Locate the organizational unit (OU):

c. Create a new GPO in this domain:
d. In the **New GPO** screen, enter the name associated with the GPO (for example, *Install_4_2_GPO*) and optionally specify a Source Starter GPO, click **OK**:

![New GPO screen](image)


e. After creating the new GPO, locate it in the menu tree. Right click to display a context menu, and select **Edit**:

![Edit GPO](image)
f. In the **Scripts** screen click **Startup**:  

![Scripts screen](image)

```
g. The **Startup Properties** screen appears. Click **Add**:  
```
h. In the **Add a Script** screen, click **Browse** to locate the installation script you want to add to the GPO library:

![Add a Script screen]

i. In the **Browse** screen, locate the remove script that was distributed with the Receiver 3.4 for Windows. Select it, and click **Open**:

![Browse screen]
The name of the script used to install Receiver 4.2.100 for Windows is labelled **CheckAndDeployCitrixReceiverPerMachineStartupScript.bat**.

j. The default text editor opens the script:

![Screenshot of Notepad showing the script](image)

The **CheckAndDeployCitrixReceiverPerMachineStartupScript.bat** script contains a number of fields containing the version of the citrixreceiver.exe package, the path location of the citrixreceiver.exe package, the path location for storing logs of script run status, and command line options for citrixreceiver.exe package installation.

k. Locate the URL path associated with the deployment, and copy it to the clipboard:
In the deployment script (above) include the following command line parameter and also edit the line which start with “start /wait” to include variable “%CommandLineOptions%”. After editing the script, it resembles the screen captures illustrated below:

```
/silent /includeSSON /STORE0="PNAgent;https://BLR4XAB-SQ915GE.blricat.com/citrix/PNAgent/config.xml;On;My PNAgent Site"
```

The `DeployDirectory` field contains the path for the Receiver deployment package. This script also contains an action to perform silent installation.
l. Return to the Add a Script screen and paste the URL path to the Script Name. Click OK:

m. The Startup Properties screen appears, with the updated URL path appended to the script. Click Apply, then OK to return to the GPO Editor screen:

The GPO is now configured to install Receiver for Windows 4.2.100.

Close the GPO editor.
The steps to disable Start menu shortcuts are the same in the previously section. Choose the Manage App Shortcut setting by selecting **Enabled**; in the Options section of the screen, select **Disable Startmenu Shortcut**. Click **OK**:

2. Run the GPO to remove Receiver 3.4 for Windows.
3. Run the GPO to install Receiver 4.2.100 for Windows with SSON, a XenApp Services Site URL, SelfServiceMode=False and Disable Startmenu shortcut
4. Run the GPO to add trusted sites to Internet Explorer.
5. Once machine has ran the GPO and installed 4.2 receiver, the machine has to be logged off once. So now when the user log-ins back the single sign-on process `ssonsvr.exe` will start running and capture the logged in user credentials, so that the credentials will be passed to receiver for passthrough authentication.

Validate that SSON is working, and that apps are in the desired location.