Upgrading from Citrix Receiver 3.X

Enterprise to Receiver 4.X

Step by step guide to maintain app shortcut settings during upgrade, with Windows Group Policies

July 2015
# Table of Contents

- **Upgrading with App Shortcuts in a fixed location when using StoreFront**
  - Step 1: Configure GPO to remove Receiver 3.4
  - Step 2: Configure GPO to install Receiver 4.3
  - Step 3: Import Citrix Administrative Templates (ADMX)
  - Step 4: Configure Storefront policies using Citrix ADMX Templates
  - Step 5: Configure GPO to add StoreFront to trusted sites
  - Step 6: Run the policy scripts
  - Step 7: Validate the configuration and operation
- **Upgrading with App Shortcuts configured per app when using StoreFront**
  - Configuring per app settings using AppCenter in XenApp 6.5
  - Configuring per app settings using Citrix Studio in XenApp or XenDesktop 7.6
  - Run the policy scripts
  - Validate the configuration and operation
- **Upgrading with Apps Shortcuts in a fixed location (Web Interface) – Pre-requisites**
  - Pre-requisite check before upgrading
- **Upgrading with Per-App Shortcuts (Web Interface) – Pre-requisites**
  - Pre-requisite check before upgrading
  - Configuring per app settings using XenApp 6.5
  - Configuring per app settings using XenApp 7.6 Citrix Studio
- **Steps to upgrade Citrix Receiver using GPO with Web Interface**
  - Configure the GPO to remove 3.4
  - Configure GPO to Install Receiver 4.3
  - Import Citrix Administrative Templates (ADMX)
  - Configure Web Interface policies using ADMX templates
  - Configure GPO to add the XenApp Services Site as a trusted site
  - Run the policy scripts
  - Validate the configuration and operation
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 Enterprise for Windows to Receiver 4.3 and above for Windows requires the reconfiguration of a number of settings. In-place upgrade by end users is not supported. 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 Enterprise for Windows to Receiver 4.3 for Windows. The guide includes best practices which retain the user experience of pass-through authentication (Single Sign-On) and shortcuts management in the Start menu and desktop.

If you have been using Receiver 3.4 Enterprise for Windows, now is the time to upgrade your desktops and thin clients to Receiver 4.3 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 4.3 for Windows, and further install and upgrade guidance, see in Citrix Product Documentation.

Receiver 4.3 for Windows enables pass-through authentication in the same way that Receiver 3.4 Enterprise for Windows 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 Enterprise for Windows used to install SSON by default, Receiver 4.3 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 option /includeSSON exists for command line or silent installations. Receiver 4.3 also provides a GUI-based dialog where you can invoke the SSON option when performing a new installation.

The following sections show how to manage app shortcuts on Start Menu and Desktop, and include SSON if required, during the scripted upgrade to Receiver 4.3 for Windows.

Remember to install Receiver 4.3 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. This applies to SSON only.

Section 1: StoreFront Server

This section provides step-by-step guidance for upgrading Receiver 3.4 for Windows to Receiver 4.3 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

1. Configure GPO to uninstall Receiver 3.4
2. Configure GPO to install Version 4.2.100 with SSON enabled
3. Define a StoreFront URL
4. Enable app shortcut settings
5. Add StoreFront as trusted site to Internet Explorer
6. Execute the group policies (GPO)
7. SSON credential saved at first login post-install
8. 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 Receiver 3.4 Enterprise
2. Configure a GPO to install Receiver 4.3 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 Receiver 3.4 Enterprise;
5. Run the GPO to install Receiver 4.3.
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 Receiver 3.4**

Access the domain controller with administrator privileges:
a. Launch the Group Policy Object (GPO) editor:

Launch the GPO editor

b. Locate the organizational unit (OU) where the users are placed:
c. Create a new GPO in this domain:

![Group Policy Management screenshot]

d. In the **New GPO** screen, give a name to this policy. You may leave the Source Starter GPO as default value, click **OK**:

![New GPO dialog box]

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

![Scripts screen](image)

---

g. The **Startup Properties** screen appears. Click **Add**:

![Startup Properties screen](image)
h. 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](image)

i. In the **Browse** screen, locate the remove script that was distributed with the DVD layout of the XenApp or XenDesktop distribution (uninstall/install scripts are typically located in the directory `XenApp_and_XenDesktop7_6\Citrix Receiver and Plugins\Windows\Receiver\Startup_Logon_Scripts`). **Select it, and click Open**:

![Browse](image)

The name of the script used to remove Receiver for Windows 3.4 is labelled `CheckAndRemoveCitrixReceiverEnterpriseStartupScript.bat`. 
j. The default text editor opens the removal script; download the 3.4 Receiver installer from citrix.com if you do not have access to the removal script. Locate the URL path (located on a line labeled `DeployDirectory`) associated with the deployment, and copy it to the clipboard:

![Image of text editor with removal script]

The `DeployDirectory` field contains the path for the Receiver deployment package. This script is accessible in the 3.4 Receiver installer (citrixreceiverenterprise.exe).

k. Return to the Add a Script screen and paste the URL path to the Script Name field. Click OK:
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 4.3**

1. Configure a GPO to install Receiver 4.3 with SSON, a StoreFront URL, and app shortcut 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, name the policy (for example, *Install_4_3_GPO*); leave the Source Starter GPO as default (none). Click **OK**:

![New GPO window](image)

**New GPO**

Name:

*Install_Receiver_4_3_GPO*

Source Starter GPO:

*none*

[OK] [Cancel]

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

![Group Policy Management window](image)
e. 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:
f. The **Startup Properties** screen appears. Click **Add**: 

![Startup Properties Screen](image)

g. 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](image)

h. In the **Browse** screen, locate the **CheckandDeploy** script that was distributed with the Receiver 4.3 for Windows distribution (this script is provided with the XenApp/XenDesktop download); Select it, and click **Open**: 

![Browse Screen](image)
The name of the script used to install Receiver 4.3 for Windows is labelled `CheckAndDeployCitrixReceiverPerMachineStartupScript.bat`.

i. The default text editor opens the script:

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

The `CheckAndDeployCitrixReceiverPerMachineStartupScript.bat` script contains a number of fields containing the current Receiver 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 (for example, set `DeployDirectory=\\10.105.34.108\share\4.2CU1\`), 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**:

![Add a Script](image)

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 4.3.

Close the GPO editor.

**Step 2.1: Import Citrix Administrative Templates (ADMX)**

With release 4.3 onwards, Receiver uses ADMX files instead of ADM files, renamed as follows:

- icaclient.adm to *receiver.admx*
- icaclient_usb.adm to *receiver_usb.admx*
- ica-file-signing.adm to *ica-file-signing.admx*
- HdxFlash-Client.adm to *HdxFlash-Client.admx*

**ADMX/ADML location**

*receiver.admx*, *receiver.adml*, *ica-file-signing.admx*, *HdxFlash-Client.admx* are typically found in “C:\Program Files\Citrix\ICA Client\Configuration”

*receiver_usb.admx*, *receiver_usb.adml* are typically found in “C:\Program Files\Citrix\ICA Client\Configuration\en”

*HdxFlash-Client.adml* is typically found in “C:\Program Files\Citrix\ICA Client\Configuration\en-US”

A pre-requisite to this step is having access to these ADMX templates from the domain controller. As a best practice, copy the ADMX/ ADML files from the Receiver folder to a network share before continuing.

Citrix recommends using the Group Policy Object template file to configure rules for CEIP, Client Engine, Diagnostics, Fast Connect API Support, multi-Stream ICA, Network routing, Remoting client devices, Self-service, Storefront, User
authentication, User experience, Generic USB Remoting, ica-file-Signing, HDX Media Stream Flash Redirection - Client.

You can use the template file with domain policies and local computer policies.

For local computer policies, import the template file as follows:

<table>
<thead>
<tr>
<th>File Type</th>
<th>File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMX language neutral(.admx)</td>
<td>%systemroot%\policyDefinitions</td>
</tr>
<tr>
<td>ADML language specific (.adml)</td>
<td>%systemroot%\policyDefinitions[MUIculture]</td>
</tr>
<tr>
<td></td>
<td>E.g.: %systemroot%\policyDefinitions\en-us</td>
</tr>
</tbody>
</table>

For domain policies, import the template file as follows:

<table>
<thead>
<tr>
<th>File Type</th>
<th>File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMX language neutral(.admx)</td>
<td>%systemroot%\sysvol\domain\policies\PolicyDefinition</td>
</tr>
<tr>
<td>ADML language specific (.adml)</td>
<td>%systemroot%\sysvol\domain\policies\PolicyDefinition [MUIculture]</td>
</tr>
<tr>
<td></td>
<td>e.g.: %systemroot%%\sysvol\domain\policies\PolicyDefinition \en-us</td>
</tr>
</tbody>
</table>

After the files have been copied to the respective locations, open the Group Policy Management Editor, select Policies, to see the following policies:
Step 2.2: Configure Storefront policies using Citrix ADMX Templates

Now that the script has been configured to deploy Receiver for Windows 4.3, and the policies templates have been imported, access policies to configure the StoreFront URL associated with Receiver.
a. In the Group Policy Management Editor screen, select the Storefront folder under Policies → Classic Administrative Template → Citrix Components → Citrix Receiver:

b. Select Storefront Accounts List:

c. 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, separated by semi-colons (;) Click **OK**:
d. In the **Policies**→**Administrative Template**→**Citrix Receiver** section of the Group Policy Management Editor, select **SelfService** to configure app shortcut settings:

In the **Manage SelfServiceMode** screen, the default setting is “Not Configured” which allows self-service mode to be used. We select **DISABLED** to turn off self-service mode and activate the “shortcuts mode”. Click **Apply**, then **OK**.
In the SelfService screen, select **Manage App shortcut**: 

![Manage App shortcut](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**.
e. Next, still within the Policies→ 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:
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:

---

**Step 3: Configure GPO to add StoreFront to trusted sites**

1. **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:
In the Site to Zone Assignment screen, select **Apply**, then **OK**.

**Step 4: 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.

1. **Runs the GPO to remove Receiver 3.4;** the invoked script removes the previously installed Receiver Enterprise 3.4 software from the client machine referenced in the group policy.
2. **Runs the GPO to install Receiver 4.3;** the invoked script installs Receiver for Windows 4.3 and configures the client for SSON, adds the Storefront URL, and places app short cut settings on the client machine Start Menu and Desktop.
3. **Runs the GPO to add trusted sites to Internet Explorer.** The client is automatically configured upon startup and user login.

**Step 5: Validate the configuration and operation**

4. 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:
Once the machine runs the GPO and installs Receiver 4.3, 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.

5. 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:

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

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**: 

![](image1.png)

d. After adding a local computer, the **Servers** field is automatically populated with the appropriate server. Click **Next**: 

![](image2.png)
The **Preview Discovery** screen appears. Verify that the correct XenApp server appears. **Click Next:**

After the **Discovery Progress** is completed, click **Finish:**
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**:

![Image of Citrix Studio with Properties dialog open]

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). Leaving this field blank automatically sets the folder to the default name ‘Citrix’. Click **Apply**, then **OK** to commit the changes:
e. On the domain controller machine, import ADMX/ADML templates in order to configure Receiver settings using GPO. See Step 3: Import Citrix Administrative Templates (ADMX).

⚠️ 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:

![PowerShell window]

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 4: Run the policy scripts.](#)

**Validate the configuration and operation**

Follow the instructions in [Step 5: Validate the configuration and operation.](#)
Section 2: Web Interface

Upgrading with Apps Shortcuts in a fixed location (Web Interface) – Pre-requisites

The previous section talked about upgrading to Receiver 4.3 when the environment is running StoreFront, which is the recommended front-end for all deployments with XenApp and XenDesktop 7.x. This section provides step-by-step guidance if your environment continues to leverage Receiver with 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 Enterprise to Receiver 4.3. App shortcuts may be defined for all apps, or on a per-app basis. This module looks at the first use case, and the next module will look at the per-app settings.

Pre-requisite check before upgrading

With Receiver 3.4 Enterprise, 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 4.3. 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*.
vi. Validate or configure the settings under Start Menu Shortcuts as illustrated in the following screen:
   a. *Control* → Use site settings (defined on this page)
   b. *Display* → Always (place resource shortcuts on the Start menu)
vii. Validate or configure the settings under **Desktop Shortcuts** as illustrated in the following screen:
   a. Control → Use site settings (defined on this page)
   b. Display → Always (place resource shortcuts folder on desktop)

viii. Validate or configure the options for Shortcut Removal as illustrated in the following screen:
   a. Select **Remove Citrix online plug-in shortcuts**
   b. Under Settings, select
i. Remove Shortcuts → When the Citrix online plug-in closes

ii. Types of shortcuts to remove → Citrix online plug-in and user-created shortcuts

ix. Click **OK** to save and exit

Back on the Citrix Web Interface Management screen, validate or configure the PNAgent site settings for Single Sign On (SSON):

i. Click **XenApp Services Sites**.

ii. Right click **PNAgent** site and select **Authentication Methods** in the context menu.
iii. In the Configure Authentication Methods – PNAgent screen, select **Pass-through (default)**.

iv. Click **OK**.

Now we are ready to perform the upgrade to Receiver 4.3. The flow of steps is as follows:

1. Configure a GPO to remove Receiver 3.4.
2. Configure a GPO to install Receiver 4.3 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 Receiver 3.4.
5. Run the GPO to install Receiver 4.3 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.

If you don’t need to define per app settings, skip the next module and jump to Steps to upgrade Citrix Receiver using GPO with Web Interface.

**Upgrading with Per-App Shortcuts (Web Interface) – Pre-requisites**

The previous module validated the pre-requisites to enable shortcuts for all apps. This module provides step-by-step guidance to validate the pre-requisites to define app shortcuts per app, using Group Policy Objects and Web Interface. The information in this section requires administrative knowledge of Group Policy Object (GPO) policy and Citrix Studio.
Pre-requisite check before upgrading

With Receiver 3.4 Enterprise, validate the following Web Interface Machine Settings or make these changes now to prepare for shortcuts per app and single sign-on after upgrading to Receiver 4.3. 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**.
vi. Validate or configure the settings under Start Menu Shortcuts as illustrated in the following screen:
   a. **Control** → Use server farm settings (defined in resource)
   b. **Display** is greyed out, not applicable for this setting
vii. Validate or configure the settings under **Desktop Shortcuts** as illustrated in the following screen:
   a. **Control** → Use server farm settings (defined in resource)
   b. **Display** is greyed out, not applicable for this setting
viii. Validate or configure the options for Shortcut Removal as illustrated in the following screen:
   a. Select **Remove Citrix online plug-in shortcuts**
   b. Under Settings, select
      i. Remove Shortcuts → When the Citrix online plug-in closes
      ii. Types of shortcuts to remove → Citrix online plug-in and user-created shortcuts
ix. Click **OK** to save and exit

Back on the Citrix Web Interface Management screen, validate or configure the PNAgent site settings for Single Sign On (SSON):

i. Click **XenApp Services Sites**.

ii. Right Click **PNAgent** site and select **Authentication Methods** in the context menu.

iii. In the Configure Authentication Methods – PNAgent screen, select **Pass-through (default)**.

iv. Click **OK**.

You are now ready to perform the upgrade to Receiver 4.3. The steps include:

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 Receiver 3.4 Enterprise.
3. Configure a GPO to install Receiver 4.3 with SSON, a XenApp Services Site URL, set the SelfServiceMode=False and Disable Startmenu shortcut.
4. Configure a GPO to add trusted sites to Internet Explorer.
5. Run the GPO to remove Receiver 3.4.
6. Run the GPO to install Receiver 4.3.
7. Run the GPO to add trusted sites to Internet Explorer.
8. Verify that the Trusted Sites Zone includes the Web Interface URL.
9. Validate that SSON is working, and that apps are in the desired location.
Configuring per app settings using XenApp 6.5

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

The following procedure is for administrators running XenApp 6.5.

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

```
1. From the Remote Desktop Connection Manager, launch Citrix AppCenter:
```

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

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

c. 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.
d. In the **Select Servers** screen, click **Add Local Computer**: 

![Screen showing Select Servers with Add Local Computer button]

e. After adding a local computer, the Servers field is automatically populated with the appropriate server. Click **Next**:

![Screen showing Select Servers with populated Servers field]
f. The **Preview Discovery** screen appears. Verify that the correct XenApp server appears. Click **Next**:

g. In the **Discovery Progress** screen, click **Finish**:
h. In Citrix AppCenter, expand the Applications folder:

i. In the Applications folder, select the app to configure (in this example, PowerPoint) and right click to bring up context menu:
j. Select **Application properties** from the context menu of the app:

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

Configuring per app settings using XenApp 7.6

> The following procedure is for administrators running XenApp 7.6 or later

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. Enter the name of the app category, in this example, MS Office 2013 Apps. Select Add shortcut to user’s desktop. Click Apply, then OK to commit the changes:
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.

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

```
> asnp Citrix.*
```

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

```
Set-BrokerApplication -Name "word2013" -ShortcutAddedToStartMenu $true
```
Ensure the application name (in this 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.

We are now ready to complete the group policy set up and upgrade to Receiver 4.3 with shortcuts defined per-app with Web Interface. Follow the instructions in the next module: Steps to upgrade Citrix Receiver using GPO with Web Interface.

**Steps to upgrade Citrix Receiver using GPO with Web Interface**

**Configure the GPO to remove 3.4**

Follow the instructions in Step 1: Configure GPO to remove Receiver 3.4 to create an Uninstall Policy that will remove Receiver 3.4 from client machines upon start-up. Return here to continue with the procedure using Web Interface settings.

**Configure GPO to Install Receiver 4.3**

Follow these instructions to create an Install Policy that will deploy Receiver 4.3 to client machines with necessary PNAgent settings, upon start-up:

1. Configure a GPO to install Receiver 4.3 with SSON, a XenApp Services Site(PNAgent) URL, and app shortcut settings:
   a. Access the domain controller (or where you execute domain policies):
   b. Launch the GPO editor, Administrative Tools → Group Policy Management:
c. Locate the organizational unit (OU) which hosts the Citrix Receiver users:

![GPO Editor Image]

Launch the GPO editor

d. Right click the OU name, to Create a GPO in this domain:
e. In the **New GPO** screen, name the GPO (for example, `Install_4_X_GPO`) and leave Source Starter GPO as none (default), click **OK**:

![New GPO screenshot]

f. After creating the new GPO, locate it in the menu tree. Right click to display a context menu, and select **Edit**:
g. Under Computer Configuration → Policies → Windows Settings → Scripts, select **Startup**: 

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 screen]

j. In the **Browse** screen, locate the install script distributed with Receiver 4.3 (uninstall/install scripts are typically located in the directory `XenApp_and_XenDesktop7_6\Citrix Receiver and Plugins\Windows\Receiver\Startup_Logon_Scripts\`). Click **Open**:
The name of the script used to install Receiver 4.3 for Windows is labelled CheckAndDeployCitrixReceiverPerMachineStartupScript.bat.

k. The default text editor opens the script:

```
REM *** DATE: May 9, 2011
REM *** DESCRIPTION: Check and deploy Citrix Receiver PM 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 containing the path location of the citrixreceiver.exe package, the path location for storing logs of script run status, and command line options for the citrixreceiver.exe package installation.

l. Locate the URL path associated with the deployment (for example, set DeployDirectory=\10.105.34.108\share\4.2CU1\), and copy it to the clipboard (note that this path indicates the location of the installer (citrixreceiver.exe)): 
m. In the deployment script (above) include the following command line parameter:

```
/silent /includeSSON /STORE0="PNAgent;https://<CONTROLLER-FQDN>/citrix/PNAgent/config.xml;On;My PNAgent Site"
```

n. In addition, edit the line which starts with “start /wait” to include the variable “%CommandLineOptions%”.

```
start /wait %DeployDirectory%\CitrixReceiver.exe "%CommandLineOptions%"
```

The **DeployDirectory** field contains the path for the Receiver deployment package (for example, set DeployDirectory=\10.105.34.108\share\4.2CU1\); this path indicates the location of the installer (citrixreceiver.exe).

o. Return to the **Add a Script** screen and paste the URL path to the **Script Name**. Click **OK**: 
p. The updated URL path is now visible on the **Startup Properties** screen. Click **OK** to return to the GPO Editor screen:

q. Close the GPO editor.

The GPO is now configured to install Receiver for Windows 4.3.

**Import Citrix Administrative Templates (ADMX)**

Follow the instructions in **Step 3: Import Citrix Administrative Templates (ADMX)** to import Citrix Administrative Templates (ADMX\ ADML) into the Group Policy Management Editor. Return here to continue with the procedure using Web Interface settings.
Configure Web Interface policies using ADMX templates

Now that the script has been configured to deploy Receiver for Windows 4.3, and the policy templates have been imported, access policies to configure the app shortcuts for Citrix Receiver:

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

b. Select Manage SelfServiceMode under SelfService:

c. In Manage SelfServiceMode, select Disabled. This activates shortcuts mode. Click OK.
d. Select **Manage App shortcut** under SelfService:

![Manage App shortcut screenshot]

- 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** (default ‘Citrix’ will be used if left blank). Select Enable Desktop Shortcut. Click **Apply**, then **OK**.
f. Select **User Authentication** to configure Single Sign-on (SSON) settings, from the **Policies** in Group Policy Management Editor:

![Group Policy Management Editor](image)

**User authentication** screen, edit **Local user name and password**:

![User authentication](image)
h. In the Local user name and password policy setting, 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**:

When this policy is run, app shortcuts and single-sign on (SSON) will be enabled.

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

a. In the Policies section of the Group Policy Management Editor, select Windows Components:
b. Expand the Windows Components folder. Select **Internet Explorer**:

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

d. Expand the Internet Control Panel node and select **Security Page**. In the Security Page policy settings, select **Site to Zone Assignment List**:
e. In the Site to Zone Assignment screen, select **Enabled**. Click Show to locate the Web Interface URL:

f. 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 Web Interface URL. In the **Value** field, **enter 1**; this value associates the Web Interface URL with the Intranet zone. Click **OK** to apply the changes:
g. In the Site to Zone Assignment screen, select **Apply**, then **OK**.

When this policy is run, the Web Interface site URL will be added as a trusted site in Internet Explorer

**Run the policy scripts**

Follow the instructions in **Step 4: Run the policy scripts**.

**Validate the configuration and operation**

Follow the instructions in **Step 5: Validate the configuration** and operation.