

XenApp Secure Browser

Deployment Guide

Version 1.0

Table of Contents

Introduction.....	1
Architecture.....	2
Deployment.....	2
Machine Catalog.....	3
Delivery Group.....	3
Applications	6
Citrix Policies.....	12
StoreFront.....	15
Validation	19
Advanced Options	20
Active Directory Group Policies	20
Website Shortcuts.....	21
Application Icons	23

Disclaimer

This document is furnished "AS IS". Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix Systems, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc. This document and the software may be used and copied only as agreed upon by the Beta or Technical Preview Agreement

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 2015 of \$3.28 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 © 2016 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.

Introduction

As many applications have been ported to the web, users end up relying on multiple browsers and browser versions in order to achieve compatibility with web-based apps. If the application is an internally hosted application, organizations are also often required to install and configure complex VPN solutions in order to provide secure access to remote users. Typical VPN solutions require a client-side agent that must also be maintained across numerous operating systems and operating system versions.

The challenges with web-based applications explains why web browsers are one of the most heavily deployed applications on Citrix XenApp.

With the latest enhancements to XenApp, users can have a seamless web-based application experience where a hosted web-based application simply appears within the user's preferred local browser. For example, if a user's preferred browser is Mozilla Firefox but the application is only compatible with Microsoft Internet Explorer, XenApp Secure Browser will display the Internet Explorer compatible application as a tab within the Firefox browser.

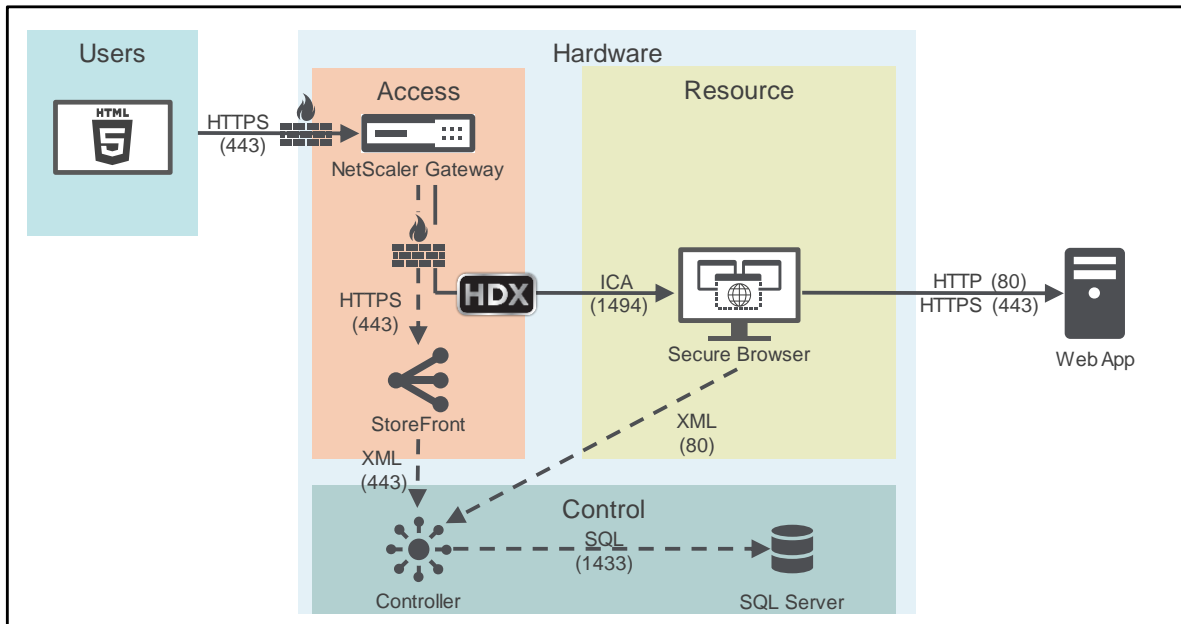
In order to make this a seamless experience, the following must be accomplished:

- **Integrated Experience:** In traditional XenApp deployments, the launching of an application results in a new application icon appearing within the user's task bar. With Secure Browser, the application only appears as a tab within the user's running browser.
- **Browser Bars:** Hosting a browser inside of a browser results in duplicate browser bars, bookmark bars, navigation buttons, etc. The Secure Browser tab must have the same appearance as a traditional browser tab.
- **Authentication:** Most web-based applications include user authentication. In a traditional XenApp deployment, users log in to StoreFront to launch an application only to be required to log on a second time to the web-based application. Secure Browser streamlines the log on experience to mimic that of a traditional PC where the user only authenticates once, to the web-based application.

This document provides instructions for configuring XenApp Secure Browser. Please follow each section in order to ensure a successful installation.

Architecture

The conceptual architecture for XenApp Secure Browser follows the same architecture for any XenApp 7.x and XenDesktop 7.x solution.



- A remote user, securely accessing StoreFront, receives a list of web-based applications, which is generated by the Controller requesting a resource list from SQL Server.
- A remote user selects the web-based application icon displayed within StoreFront.
- The Controller and SQL Server create an appropriate launch command for the user application request.
- The HTML5 Receiver executes the delivered launch command and creates a secure connection, through NetScaler Gateway, to the Secure Browser host.
- The Secure Browser web application launches, using the defined web browser. The web application interface is sent to the user's preferred, local web browser as a new browser tab.
- The user interacts with the Secure Browser application like any other tab in their local browser.

Deployment

Creating a XenApp Secure Browser implementation is accomplished by

- Creating an unauthenticated user delivery group
- Publishing the appropriate browser-based applications
- Enabling HTML5 access with a Citrix Policy
- Integrating an unauthenticated StoreFront Store
- Validating the end-to-end solution

The following sections will guide the admin through the process.

Machine Catalog

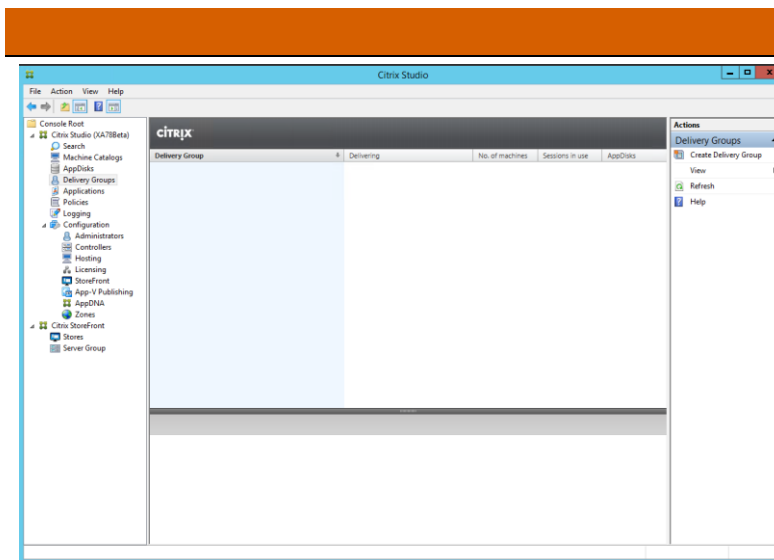
A Citrix XenApp-based machine catalog must already be created within Citrix Studio. The machine catalog must contain at least one XenApp 7.8 server and can utilize Provisioning Services, Machine Creation Services or manual provisioning.

The XenApp Secure Browser hosts must have the appropriate web browsers installed.

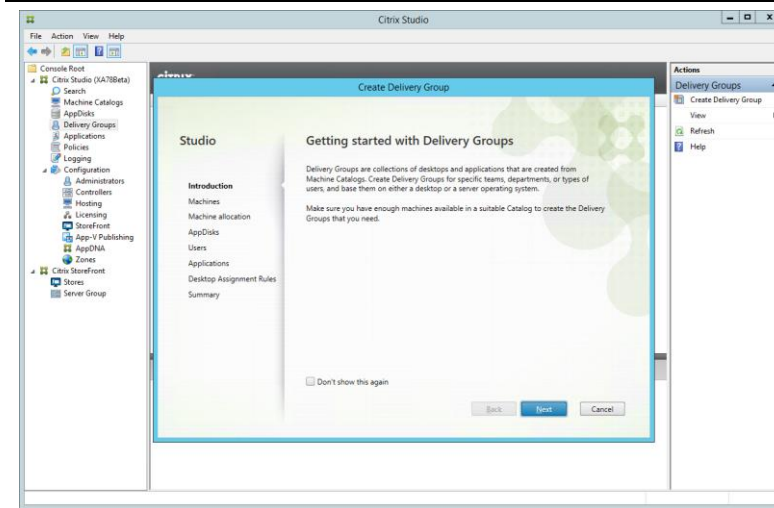
For help on creating and deploying a XenApp Machine Catalog, please refer to the [XenApp Reviewers Guide](#).

Delivery Group

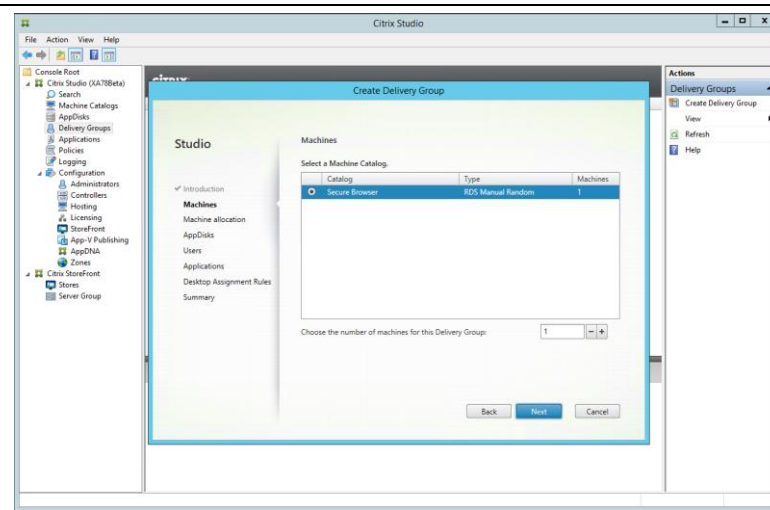
A delivery group defines the available resources and user rights assignments for a particular group of XenApp hosts.



Within **Citrix Studio**, in the navigation tree on the left, select **Delivery Groups**. In the **Actions** pane on the right, select **Create Delivery Group**.

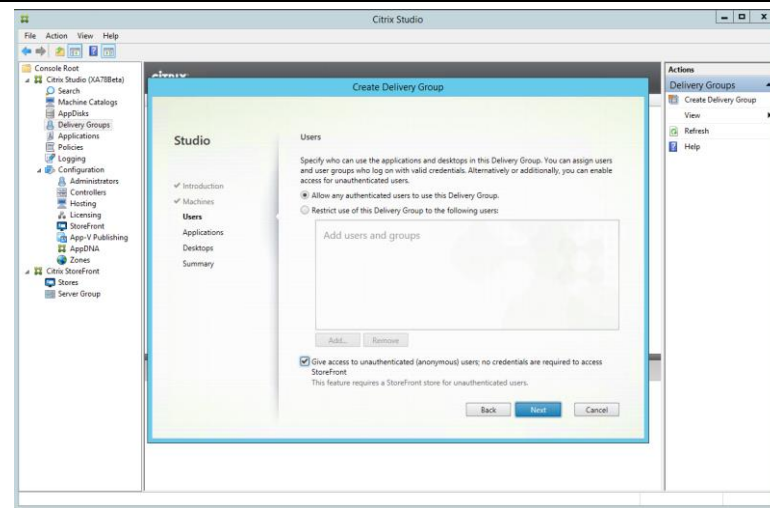


In the **Create Delivery Group** wizard, select **Next** on the **Getting started with Delivery Groups** welcome screen.



Select the appropriate XenApp Machine Catalog within the **Create Delivery Group** wizard.

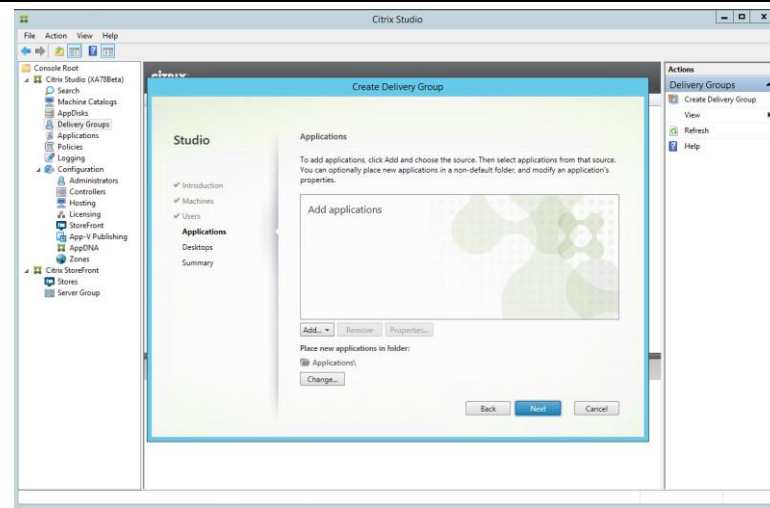
Select the appropriate number of machines to include within this catalog. Select **Next**.



Within the **Users** portion of the **Create Delivery Groups** wizard, select the following:

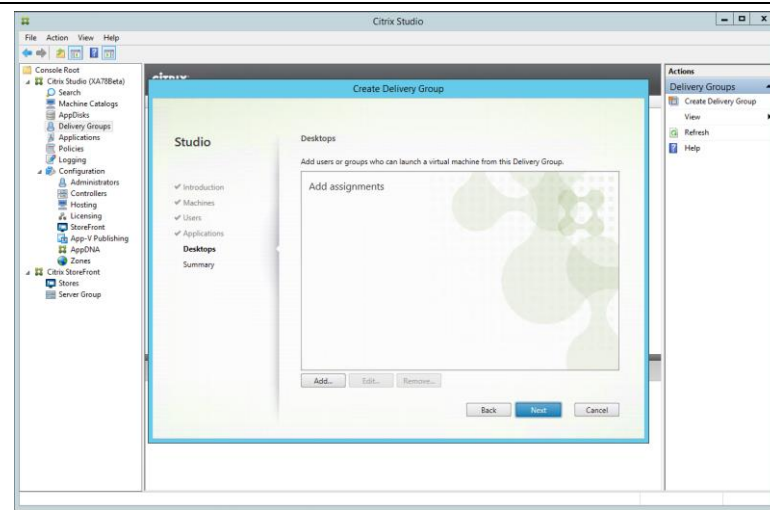
- Allow any authenticated users to use this Delivery Group
- Give access to unauthenticated (anonymous) users

Select **Next**



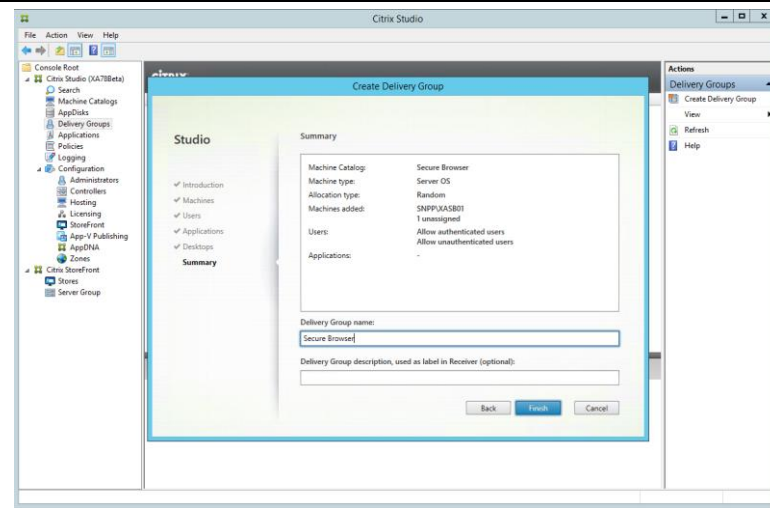
Within the **Applications** portion of the **Create Delivery Groups** wizard, select **Next**.

The appropriate browser-based applications will be created later.

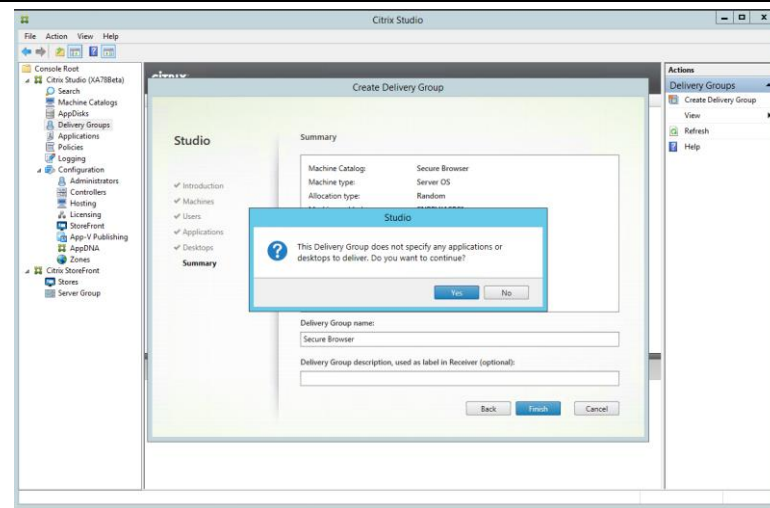


Within the **Desktops** portion of the **Create Delivery Groups** wizard, select **Next**.

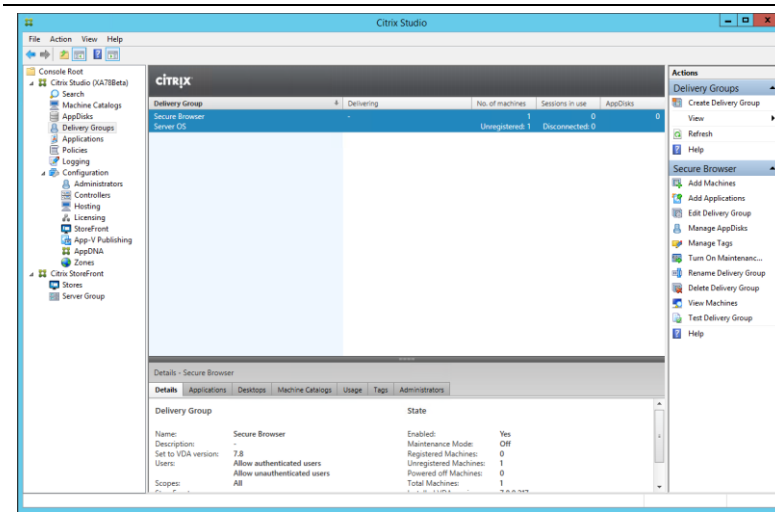
For Secure Browser implementations, users will not require the ability to launch the full desktop interface.



Within the **Summary** portion of the **Create Delivery Groups** wizard, give the delivery group a name that will be referenced by the administrator. Select **Finish**.



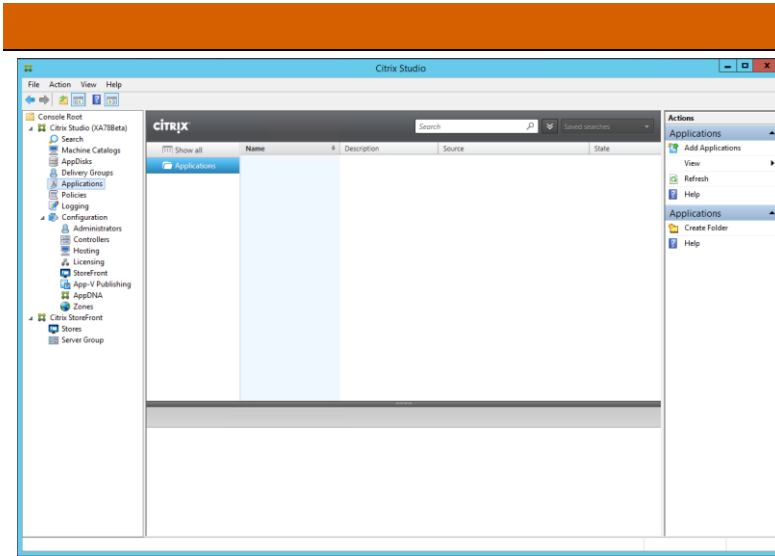
A warning message might appear indicating that the delivery group does not contain any applications or desktops. Select **Yes** to continue.



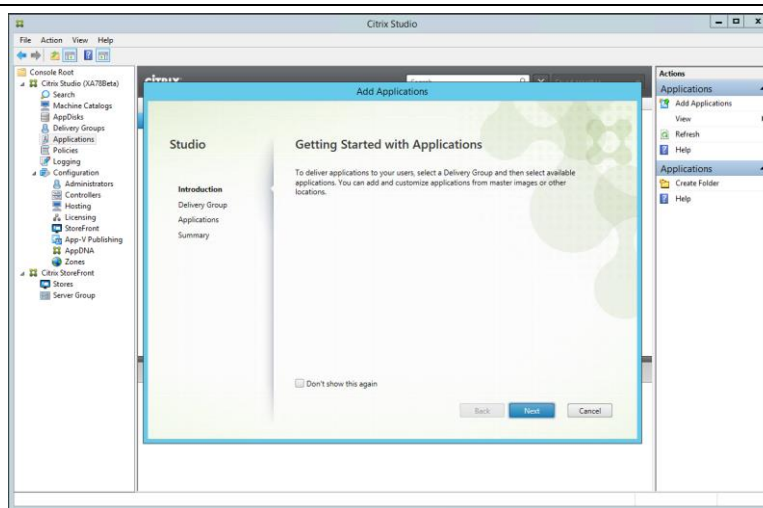
Within Desktop Studio, verify the delivery group appears.

Applications

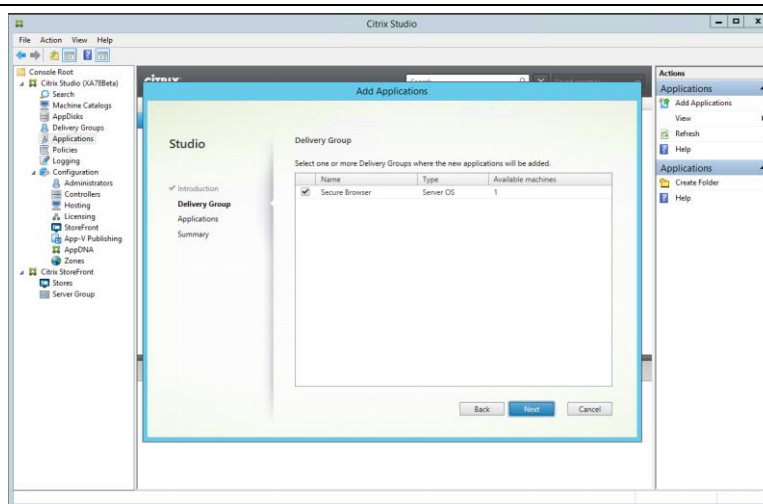
In the previous step, an empty delivery group was created. The next step is to create a set of applications users can access. Although this step could be accomplished in the delivery group portion of the implementation, it is separated as a stand-alone step as admins might wish to add additional applications in the future without being required to recreate the delivery group.



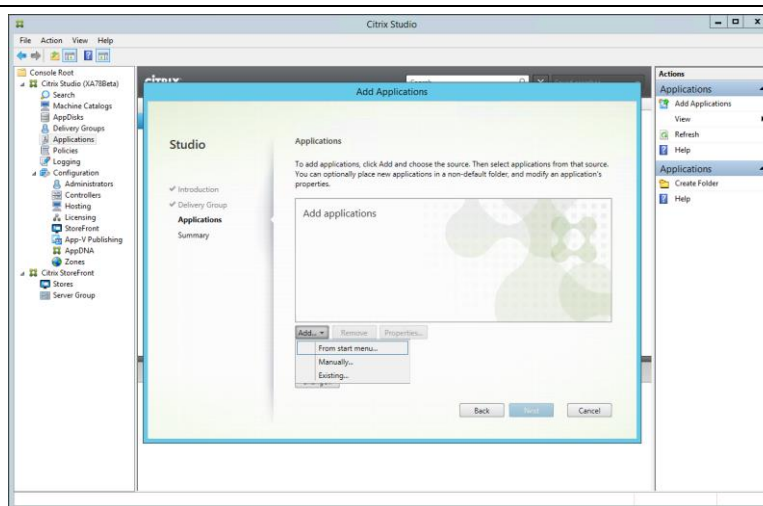
Within Citrix Studio, in the navigation tree on the left, select **Applications**. In the **Actions** pane on the right, select **Add applications**.



Within the **Introduction** portion of the **Add Applications** wizard, select **Next**

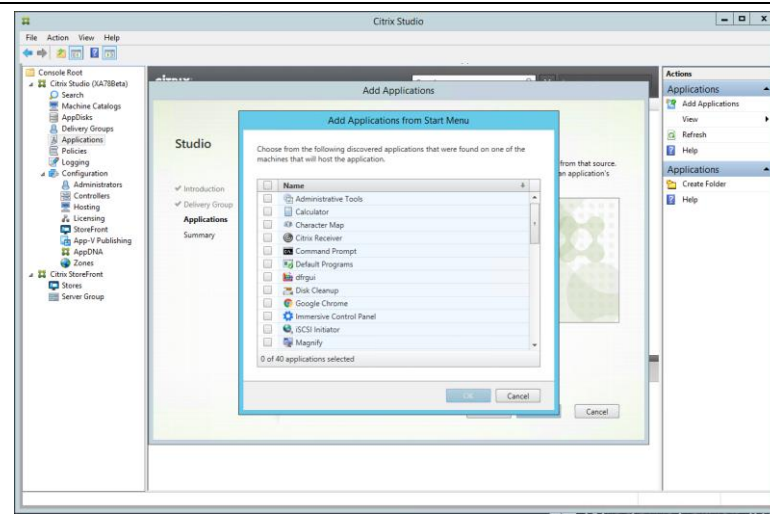


Within the **Delivery Group** portion of the **Add Applications** wizard, select the appropriate delivery group.
Select **Next**

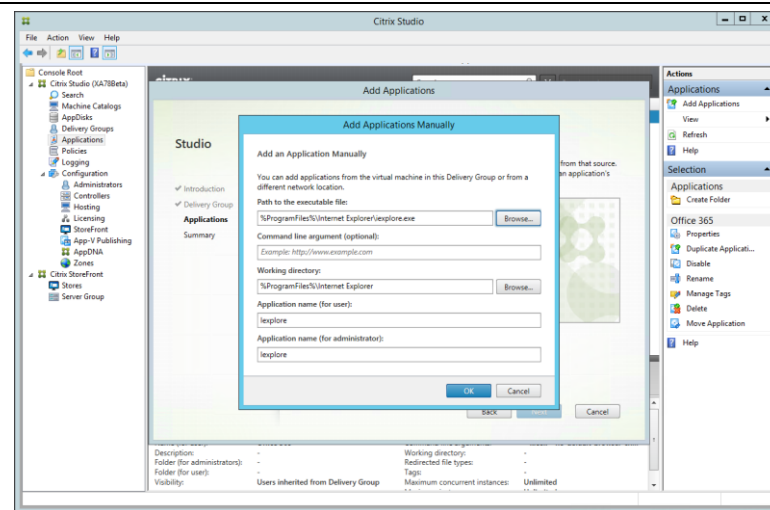


Within the **Applications** portion of the **Add Applications** wizard, do the following:

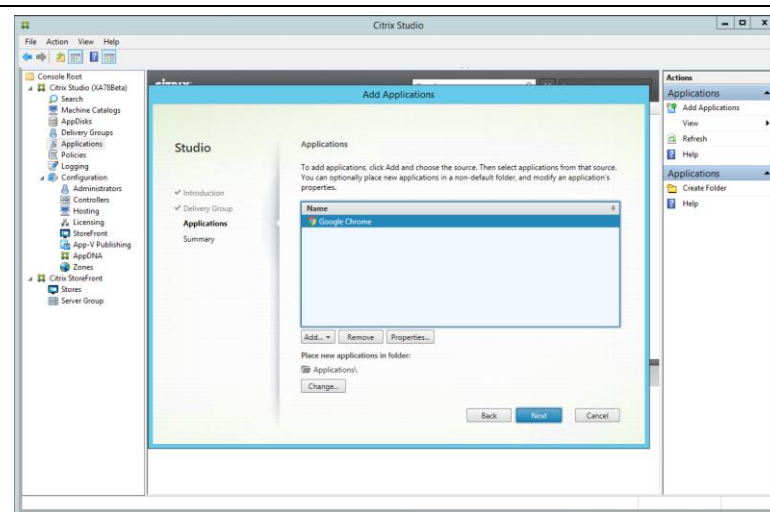
- Google Chrome: Select the **Add...** drop-down item and select **From start menu**
- Microsoft Internet Explorer: Select the **Add...** drop down item and select **Manually...**



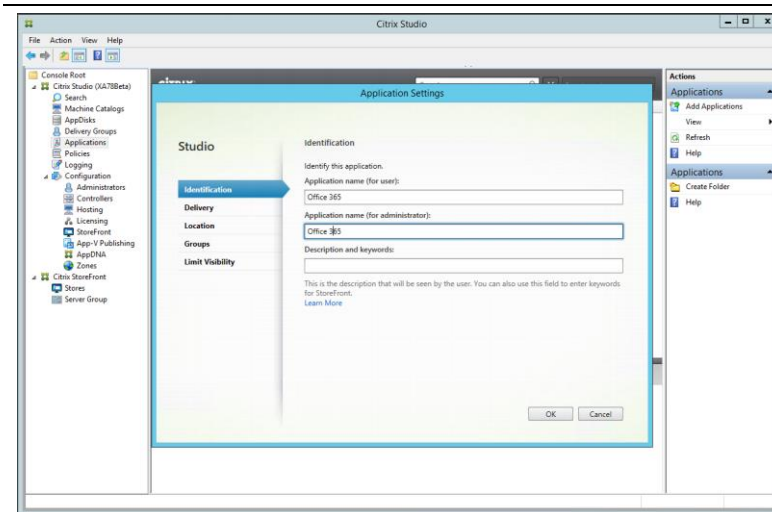
For Google Chrome...
Within the **Add Applications from Start Menu** portion of the **Add Applications** wizard, select **Google Chrome**.
Select **OK**



For Microsoft Internet Explorer...
For the **Patch to the executable file** select **Browse**. Navigate to the installation location for Internet Explorer.
Select **OK**



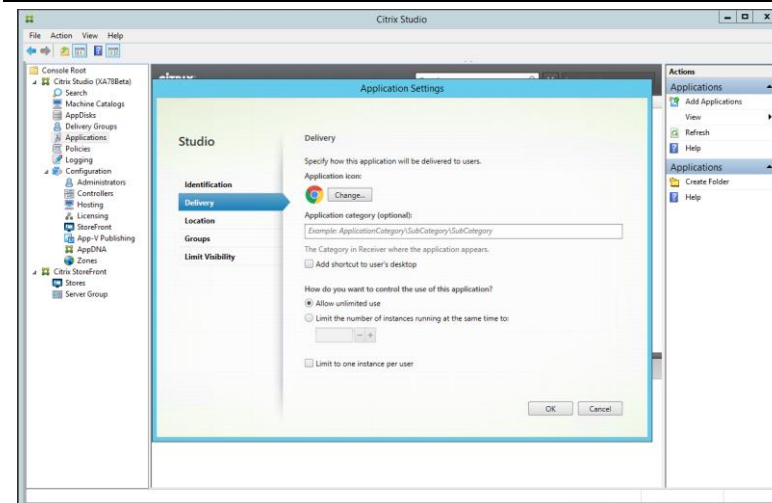
Within the **Applications** portion of the **Add Applications** wizard, select **Google Chrome** or **Internet Explorer**.
Select **Properties**.



Within the **Identification** portion of the **Application Settings** wizard, provide the following details:

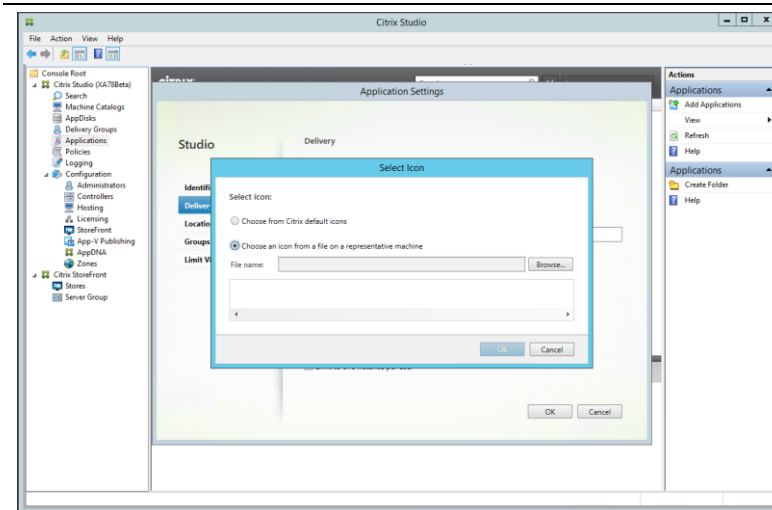
- **Application name (for users):** This will be the application name users see within StoreFront.
- **Application name (for administrator):** This will be the application name administrators see in Studio.

Select **Delivery**.



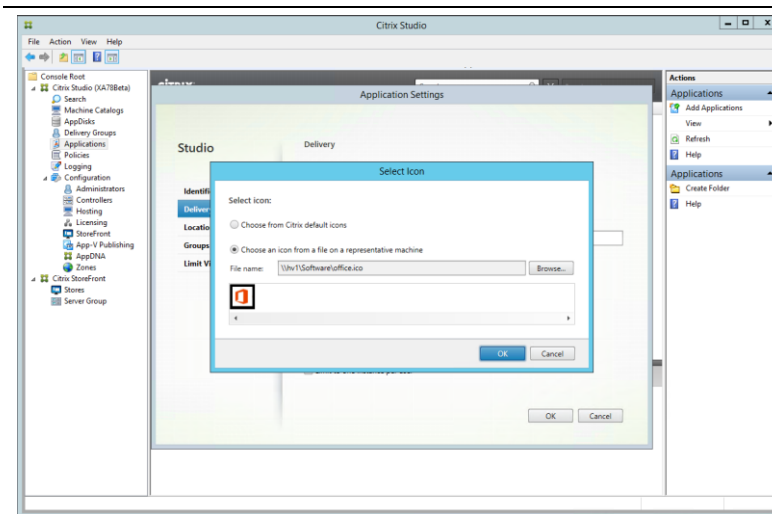
Users will want to see a unique icon for the application instead of the default Chrome or Internet Explorer icon.

Within the **Delivery** portion of the **Application Settings** wizard, select **Change** next to the application icon.

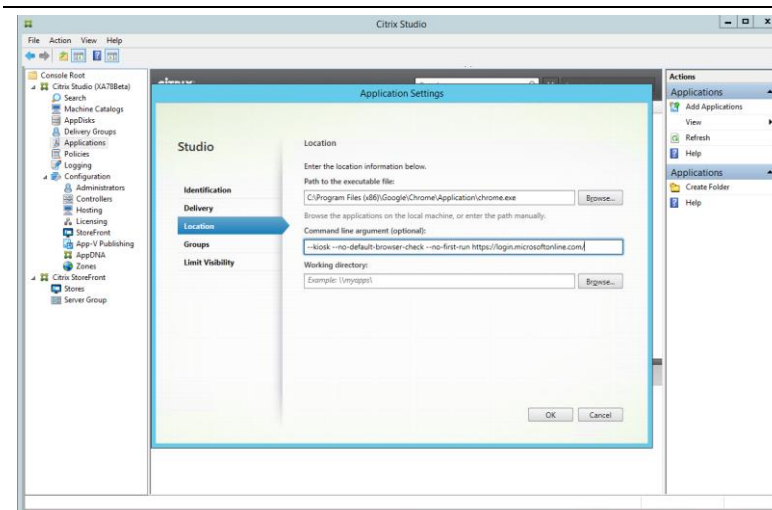


In the **Select Icon** screen, select **Choose an icon from a file on a representative machine** and select **Browse**.

Select **Yes** to the warning message **Unable to browser machines in delivery group. Do you want to browser the local machine?**



Navigate to the file containing the icon. Within the **Select Icon** screen, select the icon. Select **OK**.



Select **Location** within the **Application Settings** wizard. Add the following in the **Command line argument** box
For Google Chrome:

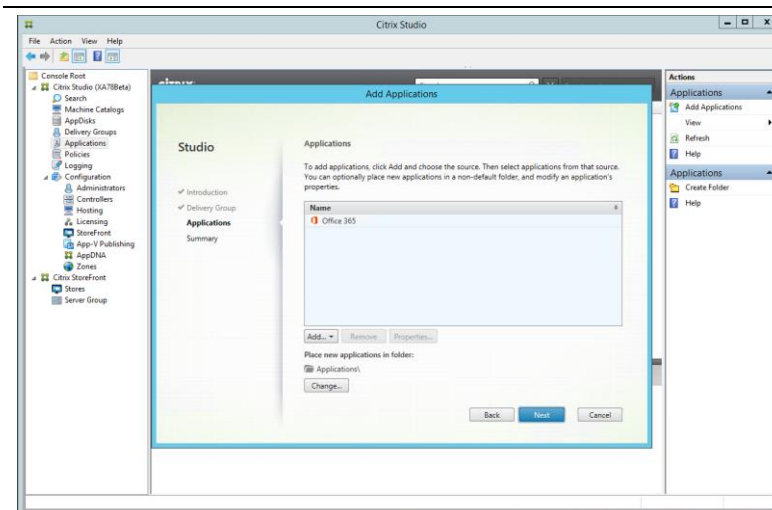
```
--kiosk --no-default-browser-check --no-first-run URL
```

For Microsoft Internet Explorer:

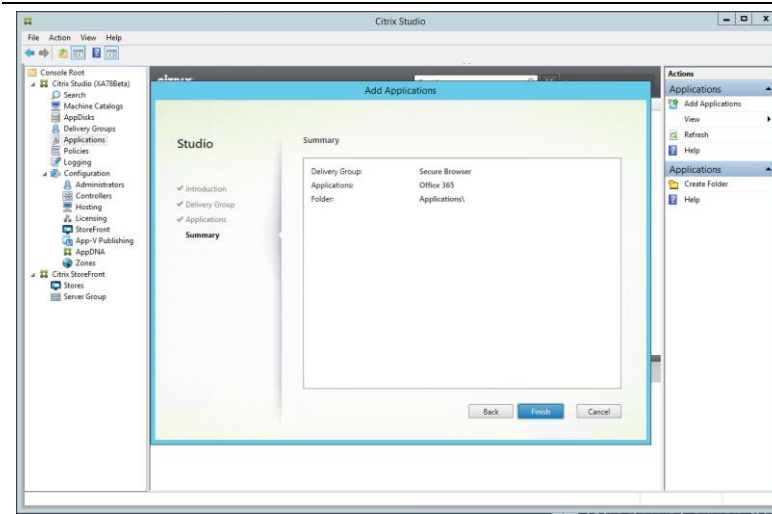
```
-k URL
```

Select **OK**.

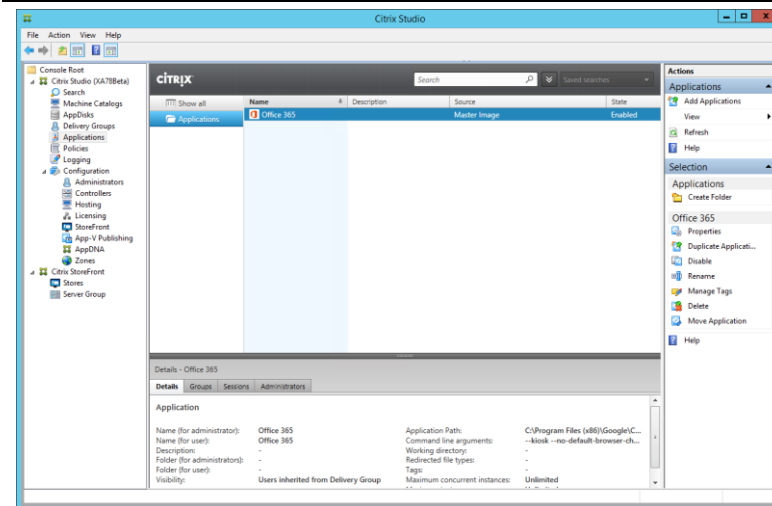
Note: For URL, enter in the `http://` URL for the application:



Within the **Applications** section of the **Add Applications** wizard, select **Next**.



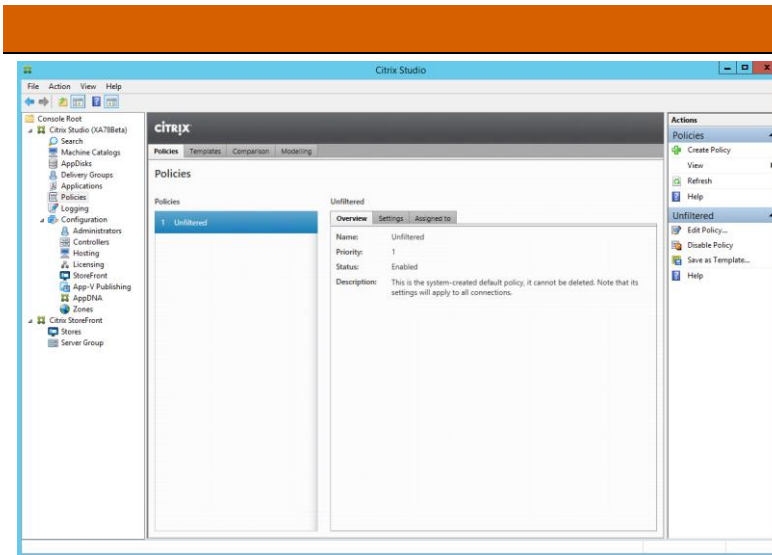
Select Finish



The application should now appear within Studio.

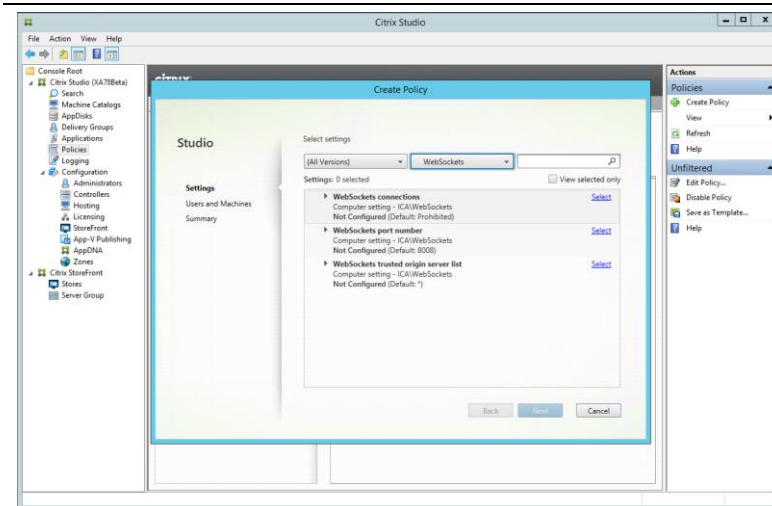
Citrix Policies

In order to allow HTML5 access to the available resources, the system must allow web socket connections. The following steps shows how to use a Citrix policy to provide this functionality.



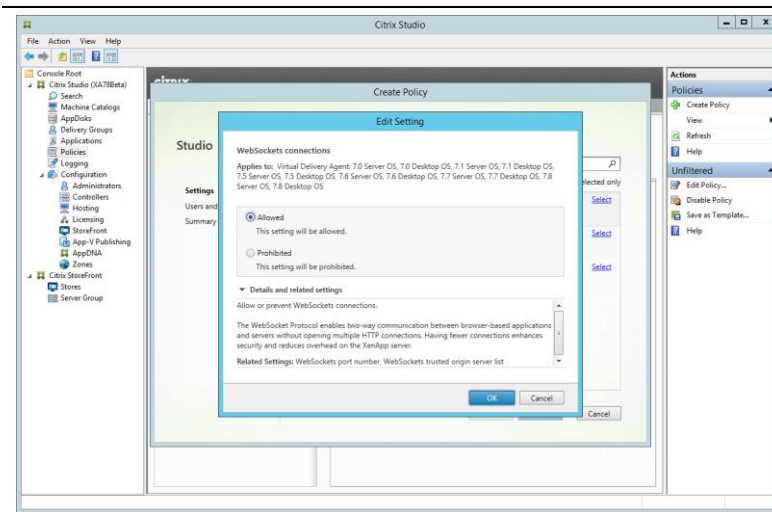
Within **Citrix Studio**, in the navigation tree on the left, select **Policies**.

In the **Actions** pane on the right, select **Create Policy**.

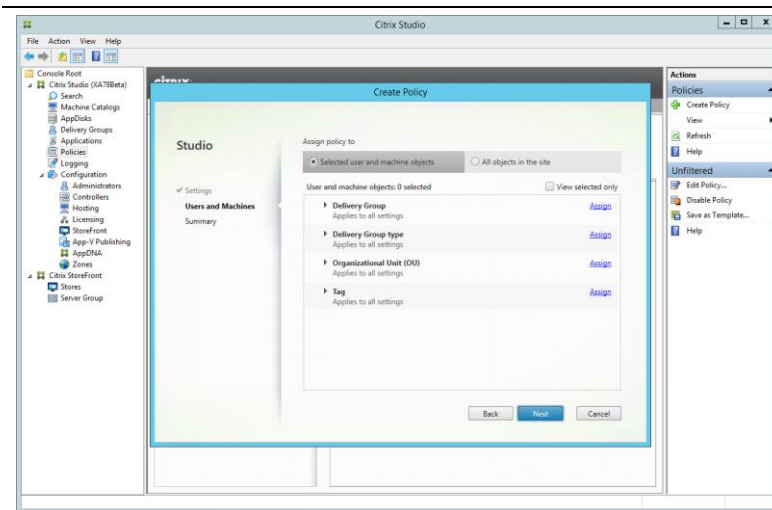


Within the **Settings** screen of the **Create Policy** wizard, select **Web Sockets** in the **All Settings** drop down box.

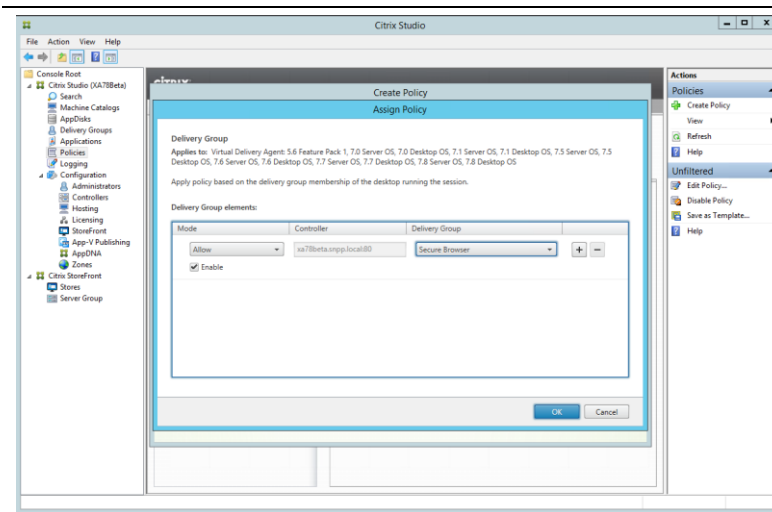
In the settings portion of the dialog box, highlight **WebSockets connections** and click **Select**.



Within the **Edit Settings** screen, select **Allowed**.
 Select **OK**.
 Select **Next**



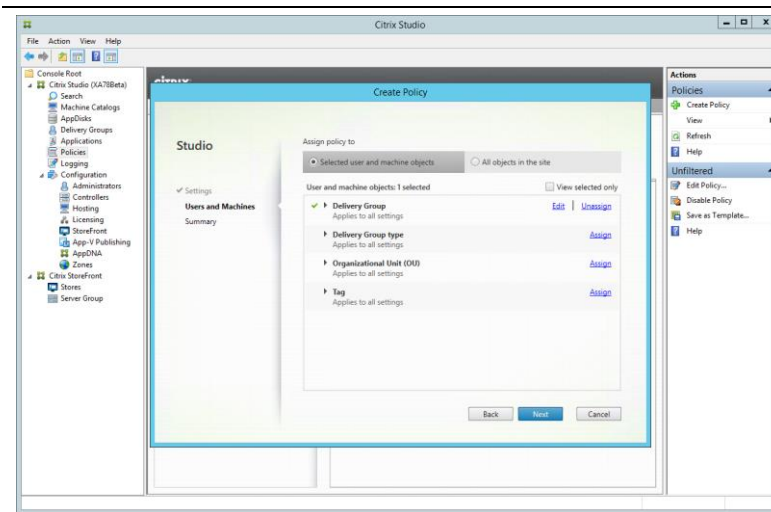
Within the **Users and Machines** screen of the **Create Policy** wizard, select **Delivery Group** and select **Assign**



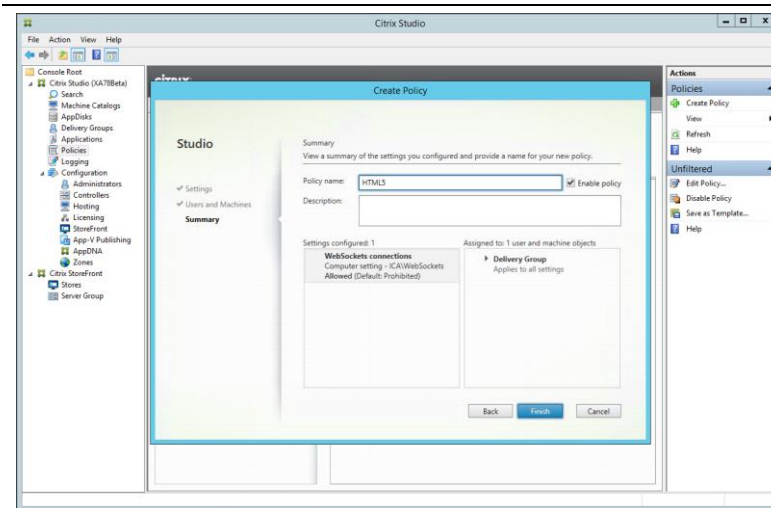
In the **Assign Policy** screen, set the following:

- Mode: Allow
- Delivery Group: Delivery group name for Secure Browser apps

Select **OK**



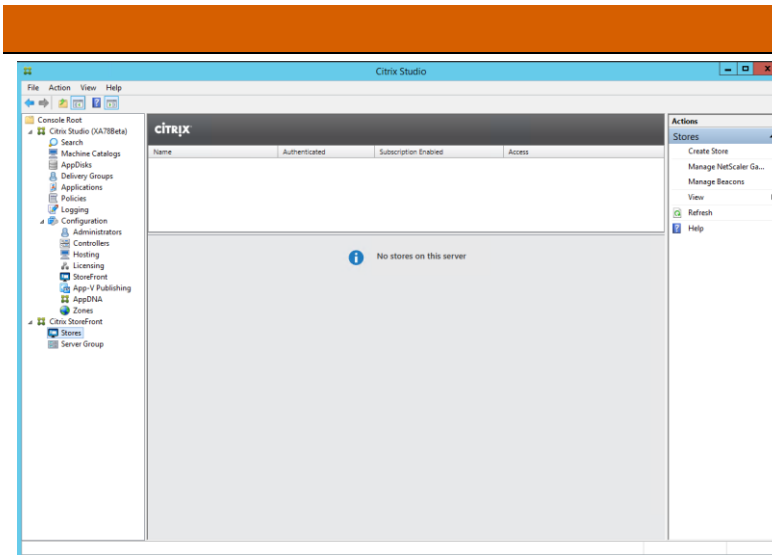
In the **Users and Machines** screen of the **Create Policy** wizard, select **Next**.



In the **Summary** screen of the **Create Policy** wizard, give the policy a name and select **Finish**.

StoreFront

To get access to the available resources, users use their local web browser and connect to the StoreFront site. The following steps outlines how to setup a new StoreFront site for unauthenticated user access.

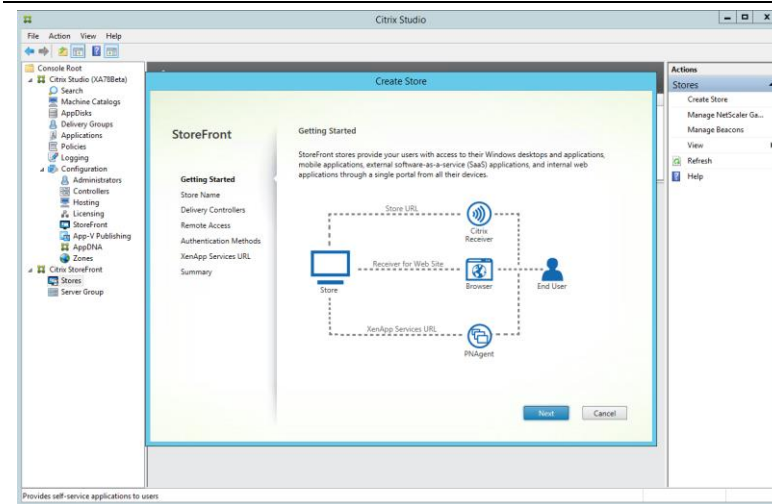


For implementations where StoreFront is installed on the delivery controller:

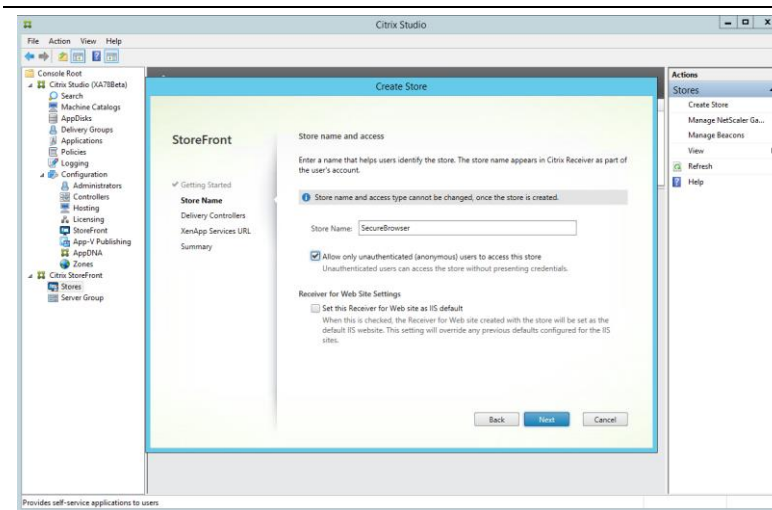
- Within **Citrix Studio**, in the navigation tree on the left, select **Citrix StoreFront - Stores**.
- In the **Actions** pane on the right, select **Create Store**.

For implementations where StoreFront is installed on a dedicated host:

- Within **Citrix StoreFront**, in the navigation tree on the left, select **Stores**.
- In the **Actions** pane on the right, select **Create Store**.



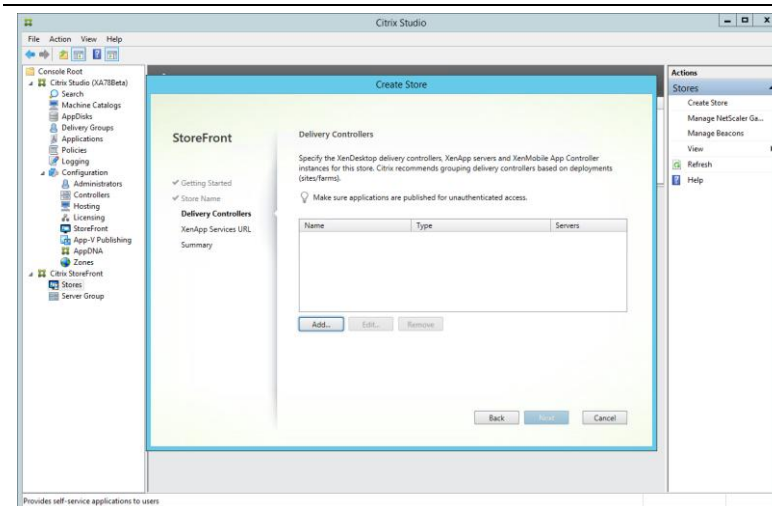
In the **Getting Started** screen of the **Create Store** wizard, select **Next**.



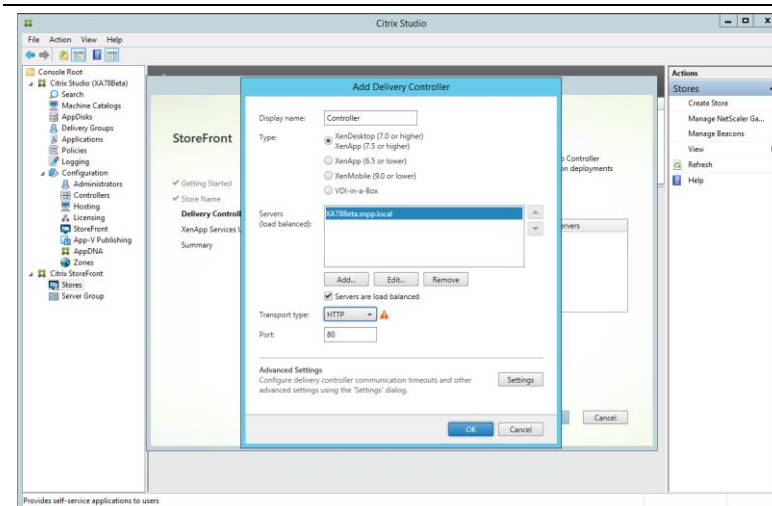
In the **Store Name** screen of the **Create Store** wizard, do the following:

- Provide a store name to be used to uniquely identify this store
- **Enable** the Allow only unauthenticated users to access this store

Select **Next**



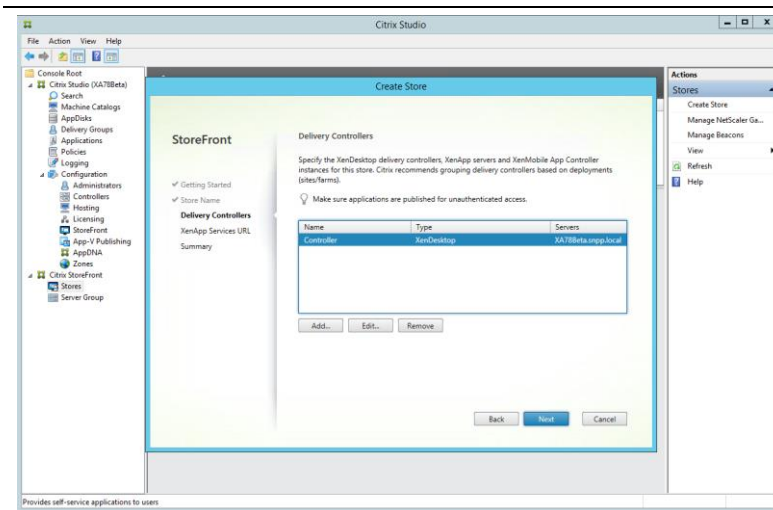
In the **Delivery Controllers** screen of the **Create Store** wizard, select **Add**.



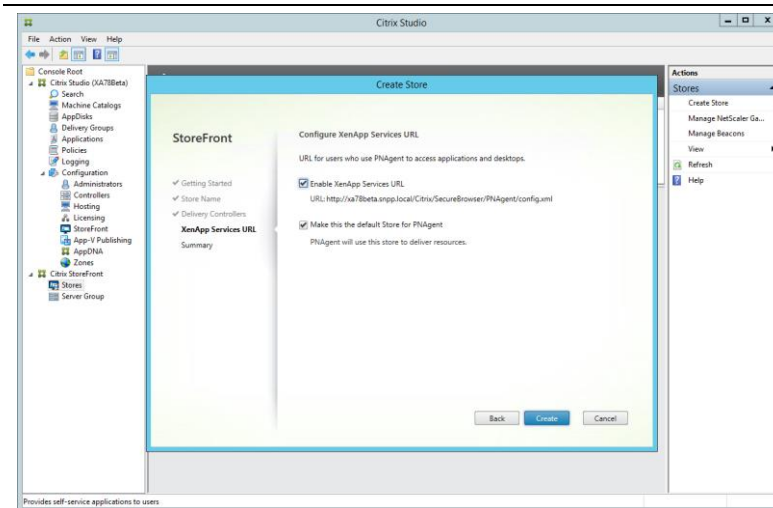
In the **Add Delivery Controller** screen, do the following:

- Provide a Display Name
- Select XenDesktop 7.0 or higher and XenApp 7.5 or higher configuration type
- Add the respective delivery controllers fully qualified domain names
- Specify the appropriate transport type: HTTP or HTTPS. If using HTTPS, appropriate server and root certificates must be installed and configured.

Select **OK**



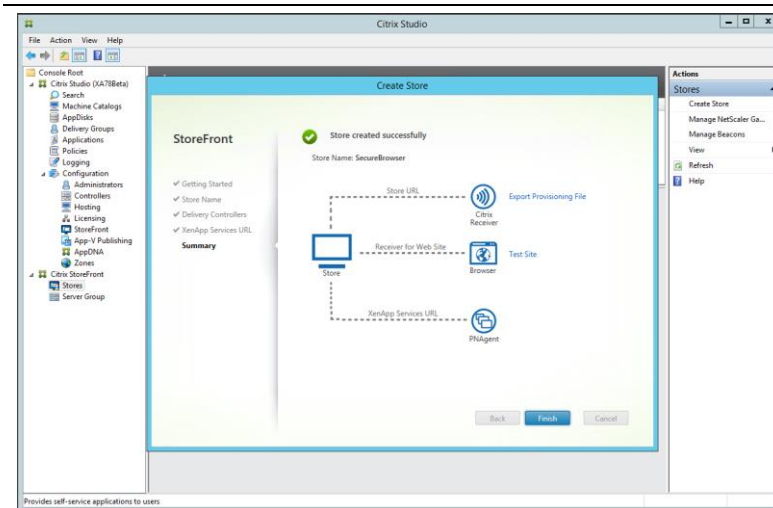
In the **Delivery Controllers** screen of the **Create Store** wizard, select **Next**.



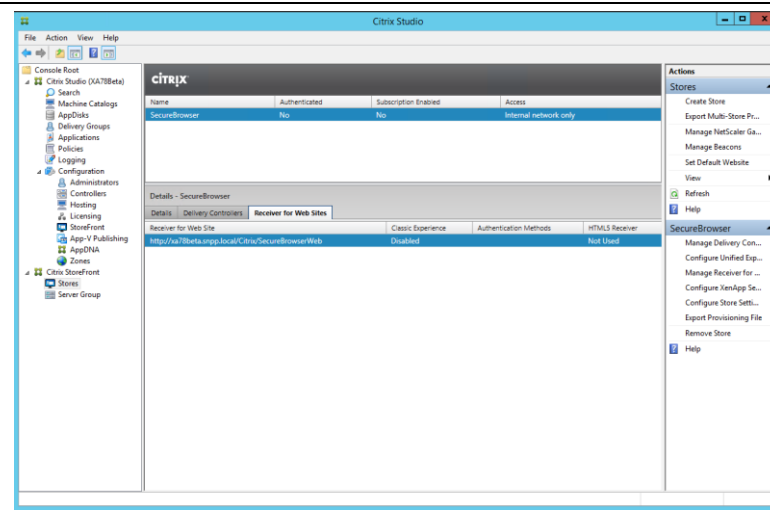
In the **XenApp services URL** screen of the **Create Store** wizard, select the following

- Enable XenApp Services URL
- Make this the default Store for PNAgent

Select **Next**.

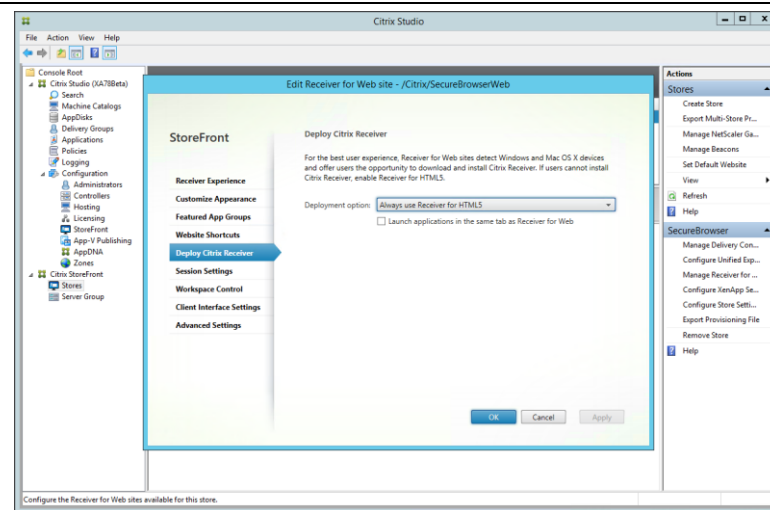


In the **Summary** screen of the **Create Store** wizard, select **Finish**.



The new store should be visible in Citrix Studio.

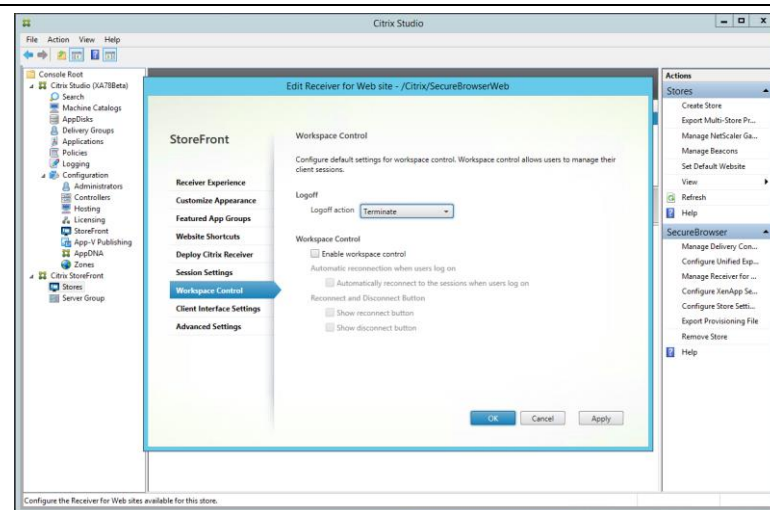
Select **Receiver for Web Sites** in the middle of the screen. Remember this URL as it is used by end users to access the store.



Within Citrix Studio, select **Manage Receiver for Web Sites** on the right side of the console.

Select **Deploy Citrix Receiver** tab.

Select **Always use Receiver for HTML5** in the Deployment options section.



Select **Workspace Control**.

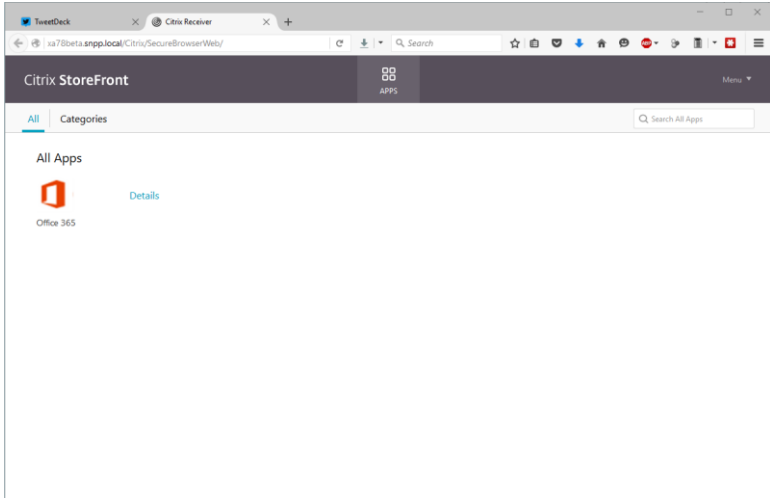
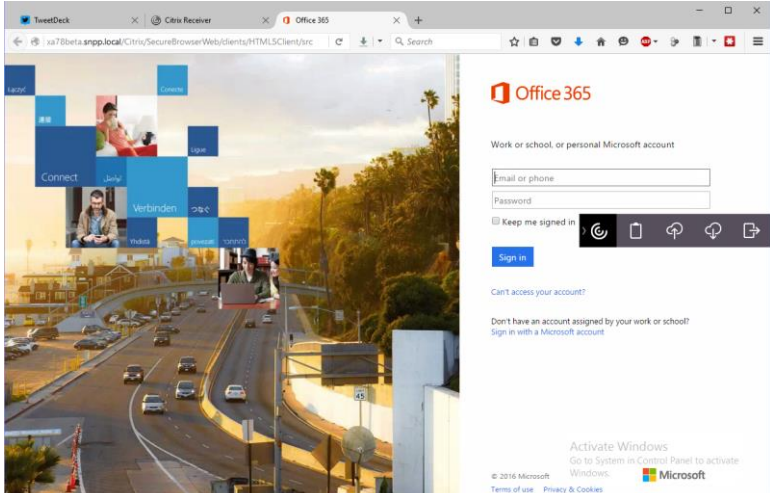
Set Logoff action to **Terminate**

Unselect Enable workspace control

Select **OK**

Validation

At this point, it is advisable to test the configuration to validate all components are working together, properly.

 <p>The screenshot shows the Citrix StoreFront web application. The browser address bar indicates the URL is <code>sa78beta.snpp.local/Citrix/SecureBrowserWeb/</code>. The page title is 'Citrix StoreFront'. Under the 'All Apps' section, the 'Office 365' application is highlighted with a red box.</p>	<p>On an end point device, launch a web browser and navigate to the StoreFront address for websites.</p> <p>Validation: StoreFront should not request the user to log in. Select the web app.</p>
 <p>The screenshot shows the Office 365 sign-in page. The browser address bar shows <code>sa78beta.snpp.local/Citrix/SecureBrowserWeb/Clients/HTML5Client/src</code>. The page features a large background image of a highway and a sign-in form with fields for 'Email or phone' and 'Password', a 'Keep me signed in' checkbox, and a 'Sign in' button. There are also links for account recovery and activation.</p>	<p>Validation: XenApp Secure Browser should create a new tab within the user's running browser.</p> <p>Validation: The XenApp Secure Browser tab should only contain a single set of navigation buttons and bars. The experience should mimic that of the traditional PC experience.</p>

Advanced Options

Additional items can be done to augment a XenApp Secure Browser implementation. These items include

- Active Directory Group Policies
- Website Shortcuts
- Application Icons

Active Directory Group Policies

Microsoft Active Directory Group Policies can be used to configure Internet Explorer and Google Chrome. Internet Explorer settings are already incorporated into Active Directory while Google Chrome requires downloading and installing the appropriate policy templates.

The policies for Internet Explorer and Google Chrome should be applied to the Active Directory Organizational Unit (OU) containing the computer accounts for the XenApp Secure Browser servers.

Note: Active Directory User Configuration policies will not function with unauthenticated users, which are used as part of this deployment guide. Unauthenticated users are based on local user accounts and not domain accounts. In order to implement User configuration policies, local policies must be used.

Internet Explorer Policy

The following settings are recommended for XenApp Secure Browser applications delivered through Internet Explorer:

Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer	
Prevent running first run wizard	Enabled - go directory to homes page
Turn off Automatic Crash Recovery	Enabled
Turn off Reopen Last Browsing Session	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone	
Turn off first run prompt	Enabled First run opt in: Enabled

The following requires a local policy on the XenApp Secure Browser server.

User Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Browser Menus	
Turn off Shortcut Menu	Enabled

Google Chrome Policy

The following settings are recommended for Secure Browser applications delivered through Google Chrome:

Note: The ADMX file for Google Chrome can be obtained from:

<https://support.google.com/chrome/a/answer/187202?hl=en>.

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome

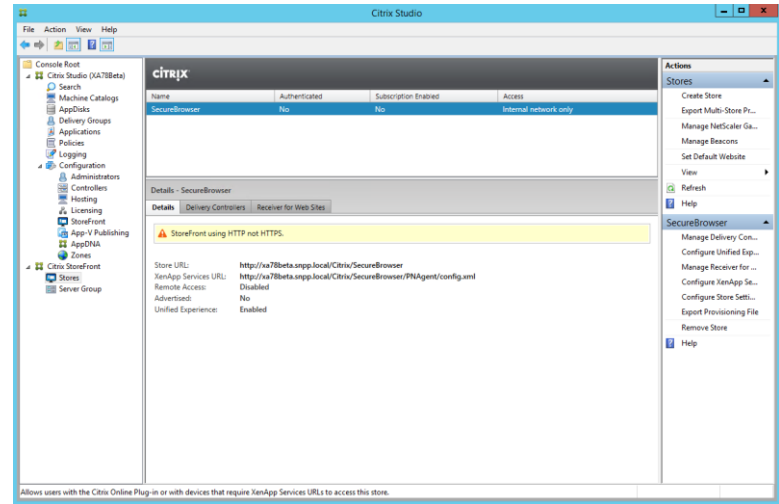
Continue running background apps when Google Chrome is closed	Disabled
Disable saving browser history	Enabled
Specify a list of enabled plugins	Enabled

Computer Configuration\Policies\Administrative Templates\Google\Google Chrome\Password manager

Allow users to show passwords in Password Manager	Disabled
Enable the password manager	Disabled

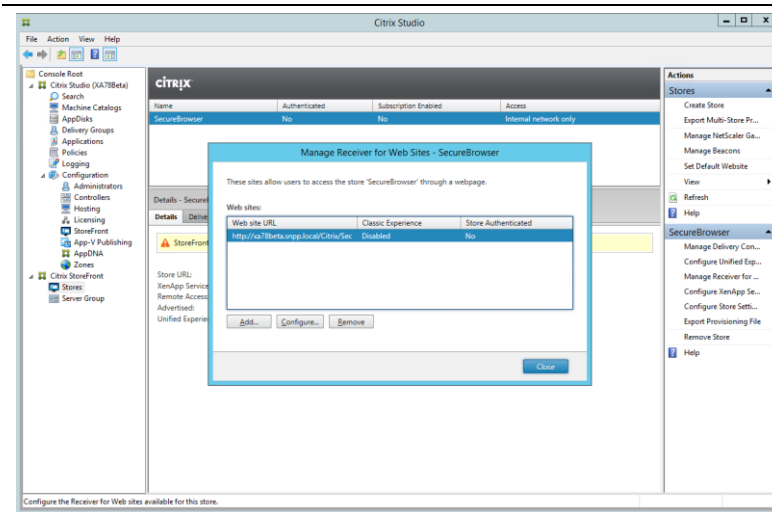
Website Shortcuts

The deployment guide assumes an organization wishes to have users access StoreFront to get to their applications. However, certain user and business requirements dictate the need to have an application icon hosted on a non-StoreFront website in order to provide a more seamless experience. The following steps enables this functionality:

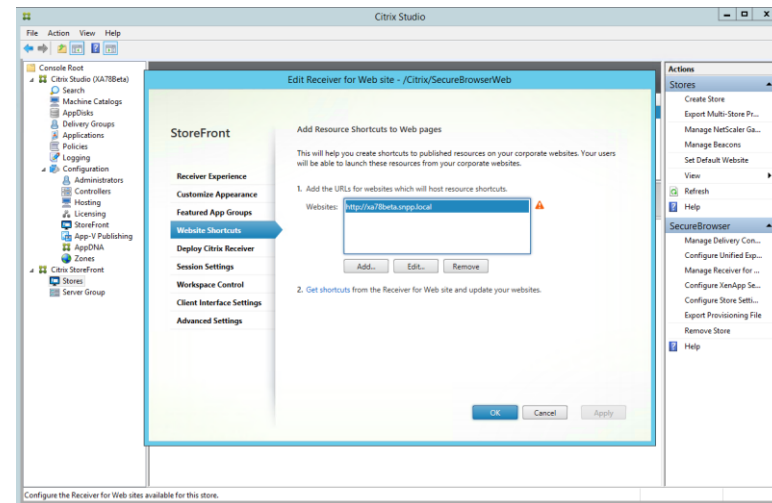


Within Citrix Studio or Citrix StoreFront, select the appropriate store.

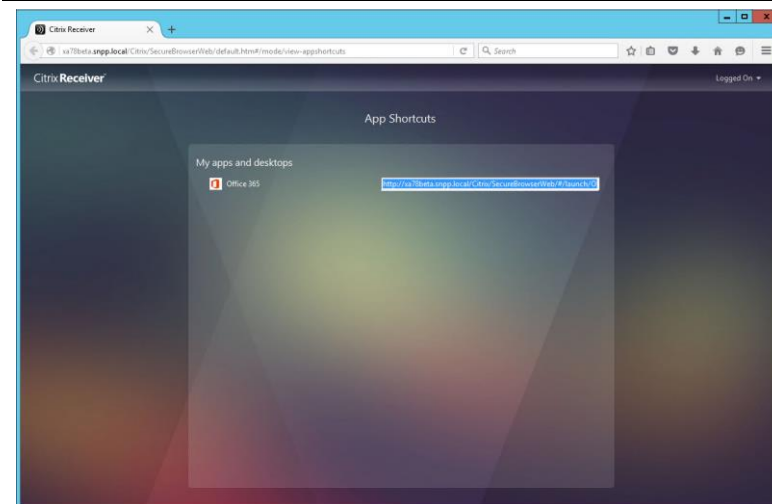
In the **Actions** pane on the right, select **Manage Receiver for Web Sites**



Within the Manage Receiver for Web Sites screen, select **Configure**



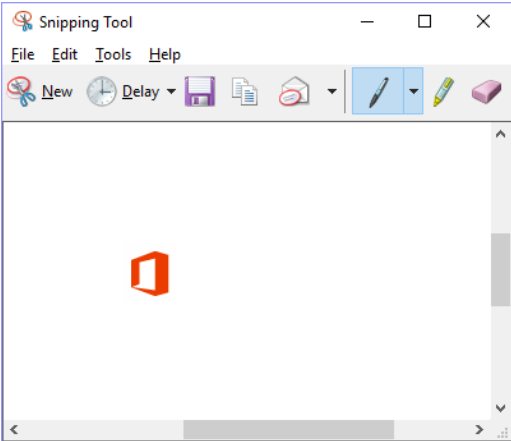
Select **Website Shortcuts**
Select **Add**
Enter in the URL for the website that will host the links to the published resources.
Select the link **Get Shortcuts**

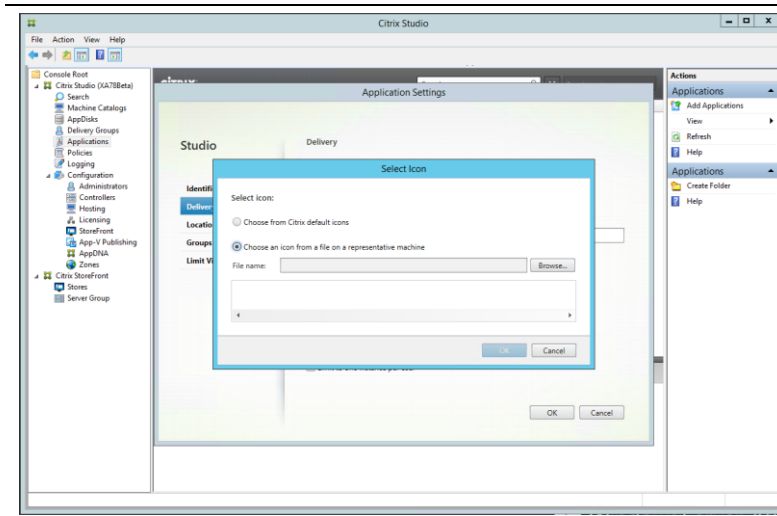


The **Get Shortcuts** website provides a list of each published resource and the corresponding URL.
This URL should be used as the link on the corporate website to access the published resource. When a user selects the link from the corporate website, the app automatically launches.
If the link is used on any other website that was not defined in the previous step, users are asked if they wish to launch the resource.

Application Icons

Publishing a web-based app through Internet Explorer or Chrome results in the icon for the application being either the Internet Explorer icon or the Chrome icon. XenApp allows for the use of custom images, but those images must be in an .ICO file (as well as others standards). The following allows an administrator to easily create custom icon files for XenApp Secure Browser.

	<p>Use the Snipping Tool, within Windows, to create a screen capture of an image to be used as an icon. Save the file as a .PNG file type.</p>
	<p>Numerous graphical processing tools allows for the creation of ICO files. There are also free tools online that converts PNG files to ICO files.</p> <p>For example,</p> <ul style="list-style-type: none"> • http://convertico.com/ will convert the PNG file into an ICO file. • http://www.favicon.cc/ will convert the PNG file into an ICO file and allow modifications to the image. <p>Save the file</p>



Within **Citrix Studio**, launch the properties of the published resource and select **Delivery**.

Select **Change** for the icon.

Select **Choose an icon from a file or a representative machine** and select **Browse**

Select the previously saved ICO file.

In the **Select Icon** screen, verify the icon is selected and hit **OK**.