XenApp Secure Browser Installation with a Citrix Lifecycle Management Blueprint

March 2016

CITRIX®

Table of contents

Overview

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

With the XenApp Secure Browser, 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, a user's preferred browser is Mozilla Firefox but the application is only compatible with Microsoft Internet Explorer. XenApp Secure Browser displays the Internet Explorer-compatible application as a tab within the Firefox browser.

This document describes how to deploy XenApp with Secure Browser using the XenApp Secure Browser blueprint available in Citrix Lifecycle Management.

For more information on Citrix Lifecycle Management, see http://manage-docs.citrix.com/home

What does the blueprint do?

This blueprint includes scripts that perform the following tasks:

1. Install XenApp, including Citrix Licensing Server and StoreFront.
2. Create a XenApp delivery site and StoreFront cluster.
3. Join the provisioned machines to your existing domain.
4. Publish a web application.

Provisioned Machine Configurations

The blueprint includes recommended configurations for each machine that Lifecycle Management provisions to the deployment. The following recommendations are displayed when you configure the VM for each machine tier in the deployment.

For all machines:

- Operating system: Windows Server 2012 R2
- Storage available in the resource location: 50 GB

Machine Type	Recommended vCPUs	Recommended Memory (GB)
Staging Server	2	2
Citrix License Server	2	4
Delivery Controller 1	4	8
Delivery Controller 2	4	8
StoreFront 1	4	8
StoreFront 2	4	8
Browser VDA	4	16

Which browsers are supported?

The blueprint supports publishing to Microsoft Internet Explorer and Google Chrome browsers.

Which resource locations are supported?

You can deploy the blueprint on the following resource location types:

- Citrix XenServer 6.2 and 6.5
- VMware vSphere 5.1 and 5.5

What do I need to use this blueprint?

To use this blueprint, you need the following items:

- An active Subscription Advantage agreement
- Access to Citrix Workspace Cloud. To create an account, visit https://workspace.cloud.com and click **Sign Up and Try It Free**.
- Access to the Lifecycle Management service. To request access, log on to Workspace Cloud and click **Request Trial** from the Workspace Cloud home page. When your request is approved, click **Manage** to access Lifecycle Management.

Prepare for deployment

Before you deploy the XenApp Secure Browser blueprint, use the following tasks to prepare your environment.

Prep Task 1: Identify the domain and disable Group Policy inheritance

Locate the Active Directory domain in your environment where the XenApp deployment will be created. You will need to supply this domain when you configure the blueprint during deployment.

Additionally, Citrix recommends temporarily disabling Group Policy inheritance on the root OU that you will use to deploy these blueprints (specified in the blueprint's OU Path parameter) so that no policies interfere with the deployment process. After the deployment is finished and testing is complete, you can re-enable policy inheritance on the OU.

Prep Task 2: Name your servers (optional)

When you deploy the blueprint, you can supply server names for the machines Lifecycle Management provisions or you can accept the default names that Lifecycle Management assigns. The following table lists the default server names that are assigned:

- Staging server: CTX-Stage
- Delivery Controller 1: CTX-XDC-001
- Delivery Controller 2: CTX-XDC-002
- StoreFront 1: CTX-SFC-001
- StoreFront 2: CTX-SFC-002
- Citrix Licensing: CTX-LIC-001

- Browser VDA: CTX-RDS-001

Prep Task 3: Set up service accounts

The general service account you use must allow you to perform installations, create AD objects, and execute scripts in your deployment. You can use different accounts for different server roles if you wish.

Create a service account in Active Directory under your Organizational Unit (OU) path and delegate control to it. This account needs administrator privileges to be able to join all machines to the domain, install software, and run scripts.

For more information about creating the general service account, refer to https://technet.microsoft.com/en-us/library/cc739458(v=ws.10).aspx on the Microsoft web site.

For more information about the database access permissions required for XenApp, see CTX127998 on the Citrix Support web site.

Important considerations for accounts

This blueprint supports deployment to a single Active Directory domain that you specify. Therefore, the accounts that you specify -- existing accounts as well as accounts that the blueprint creates -- must reside in this domain.

All accounts must be specified in down-level format (*NetBIOSDomainName**UserName*); for example, contoso\BobS. If you are deploying the blueprint in a disjoint NetBIOS environment, provide the NetBIOS domain name which might be different from the DNS domain name. For more information about name requirements, see https://support.microsoft.com/en-us/kb/909264.

Prep Task 4: Locate files

When you deploy this blueprint, you will need to supply the location of the XenApp 7.8 ISO that Lifecycle Management will use to install XenApp. During deployment, you will supply this location as a fully qualified UNC path or as a local file path.

Prep Task 5: Prepare a VM template

When you deploy this blueprint, you can allow Lifecycle Management to provision new VMs to your resource location or you can select machines that exist already in your environment. If you elect to provision the new machines that are specified by the blueprint, Lifecycle Management uses a VM template that you prepare which resides in your hypervisor environment. For more information about preparing VM templates for use with XenServer and vSphere resource locations, see Prepare Windows Server templates for deploying blueprints.

You can specify different VM templates for each machine tier that you configure. For example, you can specify a VM template for provisioning the delivery controller and a different VM template for the StoreFront server. The VM templates that you prepare for this blueprint must be running Windows 2012 R2 Datacenter Edition.

To ensure a smooth deployment experience, Citrix recommends installing .NET 3.5 on the VM template you prepare for provisioning the database server. If .NET 3.5 is not present on the template, Lifecycle Management will attempt to download and install it during blueprint deployment. However, if Lifecycle Management cannot complete the download due to connectivity issues with Windows Update, the deployment will fail.

About IP addresses

Citrix recommends deploying this blueprint to your resource location using static IP addresses. You can specify static IP addresses using one of the following methods:

- If you are deploying the blueprints to a VMware vSphere resource location, you can specify static IP addresses when you configure each new VM that Lifecycle Management will provision.
- If you have existing machines that are already configured with static IP addresses, you can specify these machines when you deploy the blueprint.

Important: Existing machines must have the Lifecycle Management Agent installed so that Lifecycle Management can detect them in your resource location. For more information about installing the agent, see Install or remove the Citrix Lifecycle Management Agent.

Prep Task 6: Add your resource location to Lifecycle Management

To deploy this blueprint, you need to add your host environment to Lifecycle Management as a resource location. To do this, you need to have a machine available in your host environment that can act as the connector between your host environment and Lifecycle Management. To be designated as a connector, the machine must have the Citrix Lifecycle Management Agent installed.

For instructions for downloading and installing the Lifecycle Management Agent and adding your resource location, see the following Lifecycle Management topics:

- Add a Citrix XenServer resource location
- Add a VMWare vSphere resource location

Note: You can also add your resource location during the blueprint deployment process. However, adding it beforehand can save you some time and ensure a smoother deployment experience.

Deploy the blueprint

Deploying these blueprints follows the same workflow that you follow for any blueprint in the Blueprint Catalog. For more information about this workflow, refer to the following topics in Deploy blueprints:

- Deploy a blueprint to a Citrix XenServer resource location
- Deploy a blueprint to a VMware vSphere resource location

Save time with configuration settings from the Pre-Deployment Checklist

When you deploy the blueprint, you will need to configure a number of blueprint settings such as service account, and file location. To save time and minimize errors during deployment, consider downloading these settings beforehand as a CSV file that you can update and import to the blueprint. The CSV file contains complete descriptions for each setting so you can enter the right information in the correct format.

The CSV file is available from the blueprint's Pre-deployment Checklist. You can access the checklist by:

- Viewing the blueprint in the Blueprint Designer. On the Overview tab, click **Preview pre-deployment checklist**.
- Deploying the blueprint. The Pre-deployment Checklist displays automatically after you supply the resource location where you want to deploy the blueprint.

On the Pre-deployment Checklist, scroll down to the bottom and click **Export parameter list (.csv)**.

After you have updated the CSV file with the required values, you can import it at the Configuration step in the blueprint deployment process.

Important: When you export the blueprint's CSV file, commas included in parameter entries are automatically converted to semicolons. So, when you update these values in the CSV file, be sure to use semicolons. When you import the CSV file, Lifecycle Management converts all semicolons back to commas. After you import the CSV file, carefully review your entries to ensure they are correctly formatted.

Accessing the Blueprint

The next step is to place the Secure Browser blueprint into your Library.

1. Go to Blueprint Catalog and select the **Secure Browser Service** blueprint to add it to your Library.

2. Go to Design and Deploy to find the blueprint in your Library.
3. Under the Actions column, select **Deploy** to deploy the blueprint.
4. Press **Start Deployment Setup**.
5. Input a Deployment Name. For first time users, there is no Deployment Profile. Once you have completed all the below steps, you can choose to save it as a Deployment Profile so you can redeploy the blueprint to other machines without having to reconfigure.
6. Click **Next**.
7. Select **Resource Location**. You can add a hypervisor at this step if you haven't yet.
8. Once selected, you provide the Resource Location Name, Host, Domain/Server name, Username, Password and Connector for the hypervisor. If you have not created a connector for the hypervisor yet, you may do so here.
9. Select **Prepare a New Connector to download and install the Lifecycle Management Agent**. Follow those instructions to create the connector. If or once you have a connector, click **Next**.
10. A Pre-deployment Checklist with recommended settings will appear. Read all the information that appears in the window. When complete, click **Continue**.

Scaling Options

The next option allows you to choose the scaling options for the deployment. By default, most of the options are preconfigured and not editable. You can change the number of browser VDAs based on memory and space of your resource location. Once completed, click **Next**.

Creating and Configuring VMs

The next option allows for the creation of new VMs or the selection of existing VMs for the deployment. To select an existing VM, select it from the drop-down.

1. To create a new VM, click **Create new VM**.
2. A Parameters window appears with options for Create from Template or Import from XVA, VM Name, Launch Template, Number for vCPUs, Memory Size and Place VM in Host. Default options will appear in the window. The Launch Template should match what your hypervisor has set up already. Click **Next**.
3. The Storage option appears. Default options are shown and additional storage options are available. Click **Next**.
4. The Networking option appears. If you have a static IP you wish to choose, click the checkmark button for Set Static IP and fill in the information for your machine. Click **Next**.
5. The Agent option appears. You can choose to install the Citrix Lifecycle Management Agent on new the VMs. This is recommended, as the agent is required for Lifecycle Management to manage the servers in your deployment. Enter your template credentials.
6. Repeat these steps for all of the VMs you want to configure.

Blueprint Configuration options

In the blueprint deployment process, the Configuration step allows you to enter the parameters that enable Lifecycle Management to provision machines, install software, and create security groups successfully. For this blueprint, configure the following parameters:

- ServiceAccountName: Name, in down-level format, of the general service account used to perform installations, create AD objects, and execute blueprint scripts.
- ServiceAccountPassword: Password for the service account.

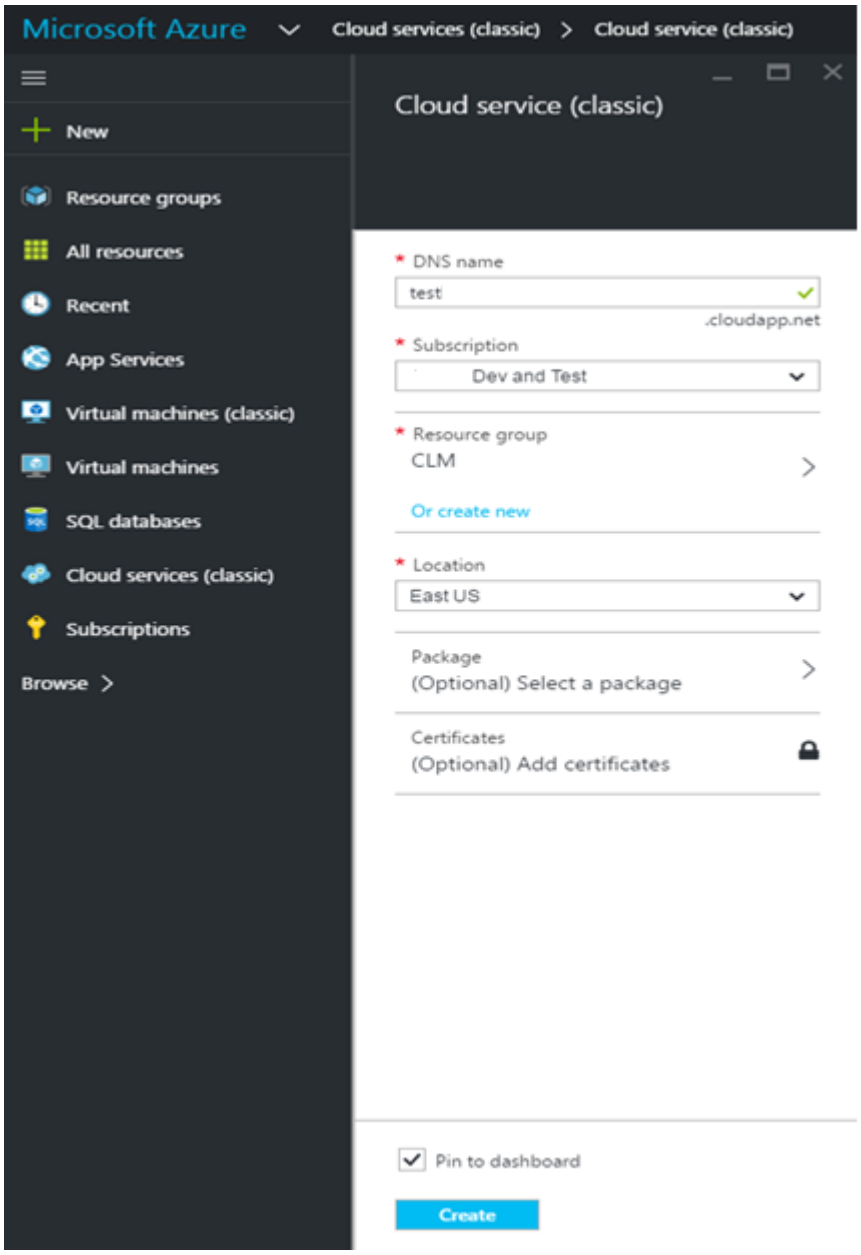
- DNSName: Fully qualified domain name of the Active Directory domain where the deployment will be created.
- OUPath: Full path to the root OU, in distinguished format, where all required AD objects will be deployed.
- MediaLocation: Fully qualified UNC path to a file share containing the XenApp 7.8 installation media.
- SetProductLicenseEdition: For XenApp, choose MPS and then choose the edition: ADV (Advanced), ENT (Enterprise), or PLT (Platinum). For the licensing model for XenApp, choose Concurrent.
- SetLicenseAllocation: Use the free 30 day license trial to configure the site. If you have an AccessCode use the Existing Files option and enter the appropriate value in the AccessCode field. If you choose the **Use Existing Files** option, the blueprint will download and install license files on the license server machine.
- AccessCode: The access code for the purchased product license. The blueprint will download and install the correct license files on the license server. By default, the blueprint will allocate 5 licenses to the deployment. If you need to modify the license allocation, go to the LicenseCount box in Section 2 and modify the value.
- Install Browsers: Choose **Yes** if you want the blueprint to download and install the latest Firefox and Google Chrome versions from the official websites. By default the blueprint will download and install the browsers.
- Install Plugins: Choose **Yes** if you want the blueprint to download and install the latest versions of Flash, Java, and Microsoft Silverlight from the official websites. By default the blueprint will download and install the plugins.

Using Azure

Follow the instructions below to configure the service on Azure using the Lifecycle Management blueprint.

Step 1: Create a cloud service

1. Log on to the Azure portal at https://portal.azure.com.
2. Click **Browse All,** click **Cloud Services,** and then click **Add**. Enter the following information:
    a. In **DNS name**, type the DNS name for the service.
    b. In **Resource group**, select the resource group you want to use for the service.
    c. In **Location**, select the region where you want to deploy the blueprint.
3. Click **Create** and wait for Azure to finish provisioning the cloud service before proceeding to the next step.
4. Once Azure has finished provisioning the cloud service, the portal displays a notification indicating the cloud service was successfully created.

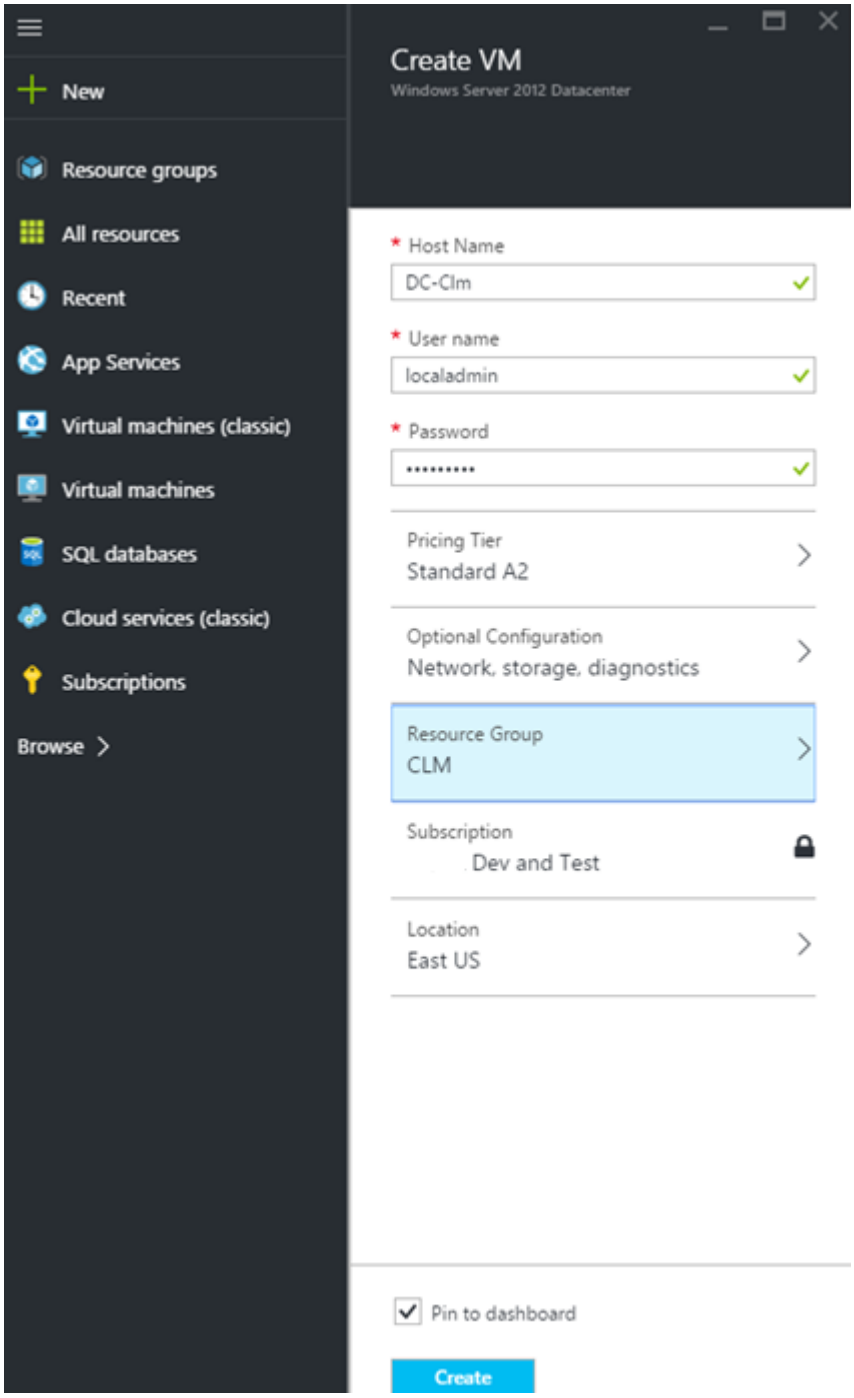


Step 2: Create a domain controller

1. In the Azure console click **Browse All** > **Virtual machines** > **Add.**
2. Select Windows 2012 R2 Data Center and click **Create**. Enter the following information:
    a. In **Host name**, type the computer name for the domain controller.
    b. In **User name and Password,** type the user name and password.
    c. In **Optional Configuration,** select the cloud service you created in “Step 1: Create a cloud service.”
    d. In **Storage,** choose the existing storage or create new one.

3. Click **Create** and wait for Azure to finish provisioning the cloud service before proceeding to the next step
4. Once the virtual machine deploys successfully, log in to the VM and configure it to be a domain controller for the deployment.

Important: The domain controller should reside in the same cloud service and storage as the other servers that will be deployed throughout the blueprint.



Step 3: Deploy the XenApp Secure Browser blueprint

1. Log on to Citrix Lifecycle Management at https://lifecycle.cloud.com.
2. From the menu bar, click **Blueprint Catalog** and add the XenApp Secure Browser blueprint to your account.
3. Click **Design & Deploy**, point to the blueprint and click **Actions > Deploy**, then click **Start deployment setup**.
4. On the **Profile** page, enter a **Deployment Name** and click **Next**.
5. On the **Resource Location** page, enter the following information and then click **Next**:
    a. In **Resource Location**, select your Azure resource location.
6. On the Pre-deployment Checklist, click **Continue**.
7. On the **Size** page, ensure **Create new VMs** is selected and then perform the following actions for each machine tier:
    a. Select your Azure resource location to configure the VM that Lifecycle Management will provision. The Configure VM dialog box appears.
    b. Click the **Windows** tab and select the **Windows Server 2012 R2 Datacenter** machine image.
8. On the **Instance Details** page, select the following settings and then click **Next**.
9. In **Machine Size**, select the appropriate machine configuration. By default, the machine size listed in the Recommended Configuration box is selected.
10. In **Choose Cloud Service**, select the cloud service you created in “Step 1: Create a cloud service.” The region associated with the service is automatically selected.
11. In **Virtual Network**, select **Do not use virtual network**.
12. In **Storage Account**, if you have an existing Azure storage account associated with the region of your cloud service, it will be automatically selected. If you want to create a new storage account for the cloud service or you don't have an existing storage account, leave the default value **Auto Generate Store Account**. Auto-generated storage account names begin with "random" and are followed by a randomly generated alphanumeric string.
13. On the **Security and Network** page, enter the **Username** and **Password** you want to use for the Administrator account and then click **Next**.
14. The credentials you enter are used for the local administrator account on these servers.

    Important: Do not use "Administrator" or "Admin" as the username for these VMs. As a security best practice, Azure requires distinct usernames for administrator accounts. Therefore, enter a different username for the VMs in each tier. For example, you might enter "domainadmin" for the Domain Controller VM tier and "localadmin" for the Delivery Controller and Server VDA VM tiers.
15. On the **Summary** page, click **Finish** to close the Configure VM dialog box and return to the blueprint deployment.
16. After you have configured the VM for each machine tier, click **Next** to continue the deployment.

Perform post-deployment tasks

This section describes the tasks you should perform after deploying the XenApp Secure Browser blueprint.

Secure your deployment

Securing your XenApp deployment is important. If you choose to do so using the Secure Sockets Layer (SSL) security protocol, you must generate, distribute, and install SSL certificates to secure the communication within the deployment. This may include the following tasks, none of which is implemented by the blueprint.

Secure this component...	By establishing...
XML	SSL communication between StoreFront servers and delivery controllers
Virtualization infrastructure	SSL communication between the virtualization infrastructure and the delivery controllers
Virtual desktops	SSL communication between users' endpoints and the Virtual Delivery Agent on virtual desktops
StoreFront	SSL communication between users' endpoints and StoreFront servers
Database	SSL communication between the servers running the XenApp and XenDesktop databases and the delivery controllers

Remove temporary objects

For security and good housekeeping, consider removing any objects such as media locations and reverting any temporary changes (for example, GPO policies and database permissions) that you created or put in place during blueprint design and deployment. Also, consider disabling the general service account for a period of time (for example, 1-2 weeks) before deleting. If no issues arise in your deployment during that time, you can delete the account. Additionally, if you disabled Group Policy inheritance to ensure unimpaired blueprint deployment, re-enable it after you have completed testing of the deployment. Finally, be sure to remove the Staging VM.

Add users to Active Directory security groups for the deployment

Before you can use Studio or Citrix License Server to administer your new delivery site, add the appropriate users to the XenApp and Licensing groups that the blueprint creates during deployment. When you deploy the blueprint, you can specify these group names or you can allow the blueprint to use the default group name. The following table shows the blueprint input parameters and the default names for each group.

Group Type	Blueprint input parameter for specifying the group name	Default group name created by blueprint
XenApp	XA-XD-AdminGroup	CTX_RES_XDC_Admins
Citrix Licensing	LicenseServerAdminGroup	CTX_RES_LIC_Admins

Refine application access behavior

After deploying the blueprint, you can log on to the machines Lifecycle Management deployed and verify the browsers. You should see VDA(s) created with the browsers and plugins installed and a Delivery Catalog created on the delivery controller. Within Citrix StoreFront, in the navigation tree on the left, select Stores and you will see the stores created by the blueprint.

At this stage, you can configure XenApp to refine the access, scope, and behavior of the applications using machine catalogs and delivery groups. You can use machine catalogs to power manage the machines and control users' application experience. With delivery groups, you can control who can access the applications you make available.

For more information about machine catalogs and delivery groups, see http://docs.citrix.com. For additional configuration guidance for XenApp Secure Browser, see http://docs.citrix.com/content/dam/docs/en-us/workspace-cloud/downloads/Secure%20Browser%20-%20Deployment%20Guide.pdf

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