Citrix App Studio 1.0

2014-07-29 11:13:58 UTC

Contents

Citrix App Studio 1.0

Citrix App Studio provides simple unified management of Citrix application and desktop delivery technologies. With App Studio, Citrix Service Providers can:

- Manage multiple farms and provide tenants access to published resources through a single Web-based console
- Offer tenants options for isolating resources, enabling tenants to access shared resources or providing tenants with private access
- Monitor tenants and users and manage resource capacity
- Deploy server or application updates without interrupting service to tenants
- Offer App Studio as a service to customers that are already managed through Citrix CloudPortal Services Manager

About Citrix App Studio 1.0

Known Issues

This section contains:

- Installation Issues
- General issues

Installation Issues

- When running the New-CamFarm, New-CamWIServer, or New-CamSessionHost scripts from the App Studio configuration server, and the configuration server is hosting the XenApp 6.5 installation media, the scripts might fail if the XenAppDVDPath parameter is defined as \\localhost. To resolve this issue, at the XenAppDVDPath prompt, specify the name of the App Studio configuration server when entering the network path. For example, \\ServerName\XenApp\dvd. [#159337]

- When running the New-CamFarm or New-CamSessionHost scripts, the scripts might fail, citing "error -4." This error indicates an issue has occurred when configuring XenApp 6.5 on the target servers. To troubleshoot this issue, check the Temp directory of the target server (typically, C:\Windows\Temp) and review the error logs for complete information relating to Error -4. These logs contain "XenAppConfigConsole" in the file name.

  In the event the error logs indicate a database connectivity issue might be present, perform the following actions:

  1. On the database server, ensure Windows Firewall is configured to allow inbound connections from the other servers in your deployment. Refer to To configure a firewall exception for the App Orchestration database instance for instructions.

  2. Check whether or not the target servers can connect to the XenApp farm database:

     a. On the target server, launch the XenApp Server Role Manager and click Configure.

     b. Proceed through the XenApp Server Configuration Tool until you reach the Database Information page.

     c. Select Existing Microsoft SQL Server Database and specify the database credentials you used when running the App Studio script.

     d. Click Test connection to verify the target server can connect to the database you specified when running the App Studio script.

     e. Close the XenApp Server Configuration Tool. Do not finish the configuration.

  [#268560]

- On servers running the Japanese language version of Windows, the New-CamFarm or New-CamSessionHost scripts might fail during the following events:

  - During reboot of the primary and backup controllers or the session hosts

  - Mapping drives

  - Establishing remote PowerShell connections to servers

  To work around this issue, wait for the affected servers to finish rebooting and then rerun the appropriate scripts with the same parameters. Alternatively, log on to each affected server and rerun the appropriate script. [#291465]

General Issues

- After configuring the App Studio environment and adding servers, changing the license server through the Web console does not change the license server already configured on the servers added to the environment. To change the license server on servers already included in the App Studio environment, choose one of the following methods:

  - **Change the license server manually.**

    On each affected servers, launch the XenApp Server Role Manager and select Edit Licensing.

  - **Change the license server via the command line.**

    On the affected servers, use the XenAppConfigConsole.exe commandwith the /LicenseServerName, /LicenseServerPort, and /LicenseModel options. For more information about these options, refer to the "License options" section of Configuration Command Syntax in Citrix eDocs.

  - **Change the License server host name policy setting for the farm GPO.**

    1. On an affected server in the farm, launch the App Center and click Policies from the tree pane.

    2. Click the Computer tab and then locate the License server host name setting.

    3. Click Add and then enter the new license server name.

  - **Create a new GPO and link it to the root OU.**

    1. On an affected server in the deployment, launch the Group Policy Management Console and create a new GPO.

    2. Edit the GPO and, under Computer Configuration > Policies > Citrix Policies, locate the License server host name policy setting.

    3. Click Add and then enter the new license server name.

    4. Link the GPO to the root OU of the App Studio deployment.

[#263406]

System Requirements for Citrix App Studio

For more information about XenApp and Web Interface server requirements, refer to the topics System Requirements for XenApp 6.5 and System Requirements for the Web Interface in Citrix eDocs.

General Server Requirements

All servers in your App Studio environment must meet the following requirements:

Operating System	Windows Server 2008 R2 SP1
Domain Functional Level	Windows Server 2008 R2. All servers are joined to a single domain. Additionally, all servers, including the database server, are joined to the same domain.
.NET Framework version	4.0.30319. The .NET Framework 4 executable is located in the Support folder of the App Studio installation media.
PowerShell remoting	Enabled. See Create remote administration policies for App Orchestration.
Windows Update Service	Enabled.
Automatic updates	Disabled on all servers designated as XenApp session hosts.
Windows Server Roles	.NET Framework 3.5.1. This Windows server role is required on all XenApp and Web Interface servers in the deployment.

App Studio Configuration Server Requirements

The App Studio configuration server hosts the App Studio configuration service and the App Studio Web console. To install and configure the App Studio configuration server, ensure the following requirements are met, in addition to the general server requirements:

Internet Access	Enabled. App Studio Setup accesses Windows Update to verify the full version of the .NET Framework 4 is installed and to install .NET updates, if required.
Operating system updates	All current Windows updates and patches are installed.
PowerShell version	PowerShell 2.0

Web Browser	Internet Explorer 9. Required on any computer from which the App Studio Web console is accessed.
Database server	SQL Server 2008 R2, configured with SQL Native authentication.

Farm Requirements

To configure the first farm and add infrastructure servers, your environment must include the following items:

- Two servers (physical or virtual), to be prepared and used as primary and backup XenApp controllers.
- One or more servers, to be prepared and used as XenApp session hosts.

  Important: Because these servers will be added to the same workload catalog, these servers must be configured identically, including having the same updates or patches applied. When these servers are added to the App Studio deployment, App Studio registers their capabilities and uses them to evaluate subsequent servers added to the workload catalog. If subsequent servers are not identical to the initial servers' configuration, they are not accepted into the deployment.
- One server, to be prepared and used as the Web Interface server.
- A network file share containing the installation media for XenApp 6.5.
- Microsoft SQL Server 2008 R2 database server, for the farm database.

Database Server Requirements

As part of creating a farm in your environment, App Studio automatically creates the farm database. To ensure the database is created smoothly and can communicate with the other servers in your deployment, the following items are required:

- SQL Server is configured as the default instance.
- SQL PowerShell provider is installed on the database server. This provider is included with SQL Management Studio.
- Windows authentication is configured.
- Windows Firewall is configured to allow inbound connections from the other servers in your deployment. See To configure a firewall exception for the App Orchestration database instance for more information.
- The user account running the scripts has permission to create the database.

If you create the farm database manually, ensure that db_owner permissions for the database are assigned to the user account for IMA. Connections to the database may use either Windows authentication or SQL authentication.

Licensing Requirements

Citrix License Server 11.9 is required for configuring the App Studio server as well as configuring the XenApp and Web Interface servers. If you use an older version of Citrix License Server, App Studio cannot validate the server during configuration of global settings.

Security Requirements

To ensure your deployment is protected from internal and external threats (depending on your network configuration), Citrix strongly recommends you use SSL certificates and enable SSL encryption when deploying App Studio in a production environment. Using SSL ensures the confidentiality, authentication, and integrity of session data.

When using SSL with App Studio, the SSL certificates are used to secure connections to the App Studio configuration service and the App Studio console, which are both hosted on the same server. To use SSL with App Studio, install an SSL certificate on each server you prepare and configure as an App Studio configuration server. The certificate you install must specify the server's common name which matches the server's FQDN. You can specify that App Studio use the installed certificate during the server configuration process described in the topic Installing and Configuring Citrix App Studio.

User Account Requirements

The user account you use to configure your App Studio environment must meet the following requirements:

- Have permission to create databases on the database server.
- Have permissions to connect to the database server using PowerShell remoting. This requirement is met when the database server resides in the same domain as the other servers in the App Studio environment.
- Have access and write permissions to the network file share where the XenApp 6.5 installation media resides.

The user account you designate as the Global Domain Administrator when configuring global settings for your environment must meet the following requirements:

- Be a local administrator on all XenApp servers.
- Have permission to create Active Directory objects and to move machines between Computer folders and organizational units (OUs).

Create remote administration policies for App Orchestration

To facilitate remote administration, create a policy that apply to all machines in your App Orchestration environment and include the following:

- PowerShell execution policy is set to AllSigned or RemoteSigned
- PowerShell remoting is enabled, including auto-configuration of listeners, trusted hosts, and Windows Remote Shell
- Allow inbound remote administration in Windows Firewall

Note: By default, WinRM 2.0 uses the ports 5985 for HTTP traffic and 5986 for HTTPS traffic. If you are using firewalls between the App Orchestration configuration server and the other servers in your deployment, ensure these ports are enabled.

You can create this policy using one of the following methods:

- Manually configure policy settings using the Group Policy Management Console. Use this topic to configure these settings.
- Automatically configure policy settings using the New-CamGPO.ps1 script.

The New-CamGPO script creates a Group Policy Object (GPO) and configures all the required policy settings described in this topic. You can run this script after you prepare the server you want to use as the App Orchestration configuration server, join it to the shared resource domain, and add it to the App Orchestration root OU. This script is located in the %Program Files%\Citrix\CloudAppManagement\InfrastructureTools directory on the App Orchestration configuration server.

After you create this policy, link the GPO to the following objects:

- App Orchestration root OU in the shared resource domain
- All resource OUs in the tenant resource domains that you create

Important: When you deploy machines that reside in these OUs (for example, adding a Delivery Site), App Orchestration issues workflows to complete the deployment tasks. For these workflows to complete successfully, the machines on which they run must have these policy settings applied. App Orchestration does not verify these policy settings are applied before issuing the workflows.

To set the PowerShell execution policy

1. On a server joined to the domain, open the Group Policy Management Console (gpmc.msc) and create a new GPO or edit an existing one.

2. From the Group Policy Management Editor, navigate to Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell.

3. Right-click Turn on Script Execution and select Edit.

4. Select Enabled and then, under Options, select Allow local scripts and remote signed scripts.

To configure PowerShell remoting

To configure PowerShell remoting using Group Policy, use the Group Policy Management Console to enable the WinRM service, configure listeners, set the amount of session memory available, and provide a list of trusted hosts. You will also need to configure the WinRM service to start automatically and ensure Windows Firewall allows traffic through the ports assigned to WinRM.

1. On a server joined to the domain, open the Group Policy Management Console (gpmc.msc) and create a new Group Policy Object (GPO) or edit an existing one.

2. From the Group Policy Management Editor, navigate to Computer Configuration > Policies > Administrative Templates > Windows Components.

3. Use the following table to configure the required policy settings:

Setting Location & Name	Policy Setting	Setting Values
Windows Remote Management (WinRM) > WinRM Service	Allow automatic configuration of listeners	· Enabled. · To configure WinRM to listen on all addresses, type an asterisk (*) in the IPv4 Filter and IPv6 Filter fields.
Windows Remote Management (WinRM) > WinRM Client	Trusted Hosts	· Enabled. · In TrustedHostsList, type an asterisk (*) to indicate all hosts ar trusted.

Windows Remote Shell	Specify maximum amount of memory in MB per Shell	· Enabled. · In MaxMemoryPerShellMB, type `1024`.
	Specify maximum number of remote shells per user	· Enabled. · In MaxShellsPerUser, typing `0` indicates an unlimited number c shells.

4. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > System Services.
5. Double-click the Windows Remote Management service and select the following options:
   - Define this policy setting
   - Automatic
6. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security > Inbound Rules.
7. Right-click Inbound Rules and select New Rule.
8. In the New Inbound Rule Wizard, on the Rule Type page, select Predefined and then select the Windows Remote Management rule. Click Next.
9. On the Predefined Rules page, accept the defaults and click Next.
10. On the Action page, ensure Allow the connection is selected and click Finish.
11. To apply the settings, on each server, open a PowerShell command window and run gpupdate.

To enable remote administration with WMI

As part of maintaining your App Orchestration environment, you might need to update Session Machine Catalogs to deploy patches, upgrade installed applications, or take advantage of new hardware on Session Machines. To ensure the update process occurs smoothly, a firewall exception is required to enable inbound remote administrative connections on TCP ports 135 and 445. If this exception is not present, the update process might fail.

1. On a server joined to the domain, open the Group Policy Management Console (gpmc.msc) and create a new Group Policy Object (GPO) or edit an existing one. This GPO should be associated with all servers in the App Orchestration environment.
2. From the Group Policy Management Editor, navigate to Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile.
3. Double-click the Windows Firewall: Allow inbound remote administration exception setting and select Enabled.

4. Under Options, in Allow unsolicited incoming messages from these IP addresses, type an asterisk (*).

5. Click OK to save your selection.

To configure a firewall exception for the App Orchestration database instance

To ensure the database server can communicate as required with the other servers in your App Orchestration deployment, create a Windows Firewall exception on the database server that allows connections with other servers.

1. On the database server, click Start > Administrative Tools > Windows Firewall with Advanced Security.
2. In the left pane, click Inbound Rules.
3. Right-click Inbound Rules and then select New Rule. The New Inbound Rule Wizard appears.
4. On the Rule Type page, select Program and then click Next.
5. On the Program page, select This program path and then click Browse.
6. Locate and select the SQL Server executable and then click Open. Typically, the SQL Server executable is located at C:\Program Files\Microsoft SQL Server\MSSQL10_50.*instancename*\MSSQL\Binn\sqlservr.exe.
7. On the Action page, select Allow the connection and then click Next.
8. On the Profile page, select Domain, Private, and Public.
9. On the Name page, enter a name for the rule and click Finish.

Deploying Citrix App Studio

A minimal App Studio deployment consists of the following elements:

- At least one App Studio configuration server, where the App Studio Configuration Service and Web console reside. You use the console to manage farms, workloads, resources, and tenants.
- At least one XenApp farm consisting of two XenApp controllers (a primary controller and a backup controller) to provide data collection.
- At least one XenApp server hosting desktops and applications for tenant access.
- At least one Web Interface server to provide tenants access to hosted desktops and applications.
- At least one server running SQL Server 2008 R2, with both SQL Native authentication and Windows integrated authentication enabled. This server hosts the databases created for the App Studio deployment and for XenApp farms.

New Deployments

Creating a new App Studio deployment consists of the following tasks:

1. Install and configure the App Studio configuration server.
2. Create the deployment's initial farm and workload catalogs.
3. Create the deployment's initial farm and add XenApp controllers to the farm catalog.
4. Add XenApp session hosts to the workload catalog.
5. Add a Web Interface server to the deployment.
6. Make hosted resources available for tenant subscription.
7. Create tenants and subscribe them to services.

You can then use the App Studio dashboard to manage your deployment. The App Studio dashboard displays information at-a-glance about your deployment and provides quick links for performing common administrative tasks. For more information, see the topic Working with the App Studio Console.

Existing Deployments

At some point in the life of your deployment, you might need to add or update services, ensure high availability of resources, or delegate administration. Expanding your deployment might consist of the following tasks:

- Add another App Studio configuration server to increase resiliency of your deployment.
- Create a new version of a workload catalog to update existing session hosts or introduce new services.
- Create additional App Studio administrators to manage your deployment. You can also create helpdesk administrators to enable certain users to monitor assigned tenants and troubleshoot deployment issues using Desktop Director.
- Integrate App Studio with Citrix CloudPortal Services Manager to provision XenApp resources as services to customers and resellers.

Installing and Configuring Citrix App Studio

To install and configure the App Studio configuration server, you perform the following tasks:

- Install the App Studio software on the server designated the configuration server.
- Configure the App Studio configuration server for a new or existing deployment.

To ensure high availability of your deployment, you join additional App Studio configuration servers to your deployment. These servers share the same configuration database, so if any server becomes unavailable, your deployment remains online and tenants can continue accessing their subscriptions.

For optimal availability and resiliency for App Studio, ensure that:

- The App Studio database uses appropriate high availability and resiliency measures, such as regular backups and replication.
- There is more than one App Studio configuration server, none of which share a single point of failure. For example, if two virtual machines act as configuration servers, they should not be on the same hypervisor unless it is configured for high availability (for example, Citrix XenMotion).
- All XenApp farms that App Studio manages use at least two controllers.
- All XenApp farm databases use appropriate high availability and resiliency measures.
- All workloads are sized to at least two workload machines, neither of which share a single point of failure. Ideally, these workload machines are located on a hypervisor with high availability features enabled.

To install the App Studio configuration server

1. On the server designated the App Studio configuration server, double-click Setup.exe from the Citrix App Studio installation media. After a brief initialization period, the Citrix App Studio Setup wizard appears. Click Get Started.
2. Accept the end-user license agreement and click Next.
3. On the Ready to install screen, click Install. The Installing components screen displays the progress of the installation.
4. When the installation process is finished, click Close. The Citrix App Studio Server Configuration wizard appears.

To configure the App Studio configuration server for a new deployment

1. On Welcome screen of the Citrix App Studio Server Configuration wizard, click Get Started.

2. Click Create a new deployment.

3. On the Database Information screen, enter the following information and then click Next:

   - In Database name, type the name of the configuration database.

   - In Database server name, type the name of the database server.

   - In Database user name and Database password, type the SQL Server Authentication credentials of the database user.

   Note: If you specify a database that has not yet been created, App Studio creates the database as part of the configuration process.

   If you do not have sufficient permissions to create databases in your organization, click Display the database initialization script. Your database administrator can use the script that appears to create a database for use with Citrix App Studio.

4. On the SSL information screen, select one of the following options and then click Next:

   - Select Use SSL if you are deploying the App Studio server in a production environment. Click Browse to select the SSL certificate you want to use.

   - Select Don't use SSL if you are deploying the App Studio server in a test environment and do not require SSL to be enabled.

     Note: Choosing this option allows App Studio to transmit sensitive information, including domain administrator credentials, in plain text across the network. Before selecting this option, ensure you are using an isolated test environment with appropriate firewalls in place for your App Studio deployment.

5. On the Update your App Delivery Tools image screen, to replace the original XenApp 6.5 App Delivery Setup Tools files with more recent files from the App Studio installation media, perform the following actions and then click Next:

   a. Leave the Update App Delivery Setup Tools on XenApp installation media option selected.

   b. In Path to XenApp installation media, type the network path to the XenApp installation directory.

   Note: This update is required only once for your deployment. Clear this option if this update has already occurred.

6. On the Ready to configure screen, click Configure.

After configuration finishes, click Close. Continue configuring your new deployment by launching the App Studio Web console and configuring the global settings.

To configure the App Studio configuration server for an existing deployment

Before joining additional App Studio configuration servers to a deployment, ensure you have configured the global settings using the primary configuration server with which you created the deployment. If you attempt to join additional configuration servers without first configuring the new deployment's global settings, the servers will fail to join the deployment.

Additionally, ensure at least one configuration server in the deployment is online before joining additional servers. This ensures the server can acquire the information necessary to join the deployment.

1. On the server designated the App Studio configuration server, install the App Studio software as instructed in To install the App Studio configuration server. When the installation finishes, the App Studio Server Configuration wizard appears.

2. On Welcome screen of the Citrix App Studio Server Configuration wizard, click Get Started.

3. Select Join an existing deployment.

4. On the Database Information screen, enter the following information and then click Next:

   - In Database name, type the name of the configuration database for the deployment you want to join.

   - In Database server name, type the name of the database server.

   - In Database user name and Database password, type the SQL Server Authentication credentials of the database user.

5. On the SSL information screen, select one of the following options and then click Next.

   Note: You must select the same SSL option that you selected when the deployment was originally created. App Studio does not support environments in which some servers employ SSL while others do not.

   - Select Use SSL if the existing environment has been configured to use SSL. Click Browse to select the SSL certificate you want to use.

   - Select Don't use SSL if the existing environment has been configured for unencrypted data transmission.

6. On the Ready to configure page, click Configure.

After configuration finishes, click Close. When you log on to the App Studio Web console, the dashboard for the deployment appears.

To configure App Studio global settings

You configure global settings after installing the initial App Studio configuration server in your deployment. These settings include the name of the Citrix License Server, the credentials for the global administrator account, and the paths to the Active Directory organizational units (OUs) where shared Web Interface servers and decommissioned server reside. During this process, you also create the initial farm and workload catalogs where App Studio places the XenApp controllers and session hosts that are added to the deployment.

When creating the farm and workload catalogs, you specify the import OUs where you want App Studio to place the farm servers and session hosts that you add to your deployment.

Important: When specifying these OUs, ensure they do not reside within another import OU. Otherwise, App Studio will not register the imported servers appropriately. For example, if the farm import OU resides within the workload machine import OU, and you add farm servers to your deployment, App Studio registers the servers as workload machines instead. However, if the farm import OU and workload machine import OU reside as peers within the shared allocation OU, then App Studio correctly registers any farm servers you add to the deployment.

After setting up your deployment, you can access the global settings at any time from the App Studio Home page or from the Infrastructure page. From the Home page, under Actions, click Global configuration settings. From the App Studio menu bar, click System > Infrastructure > Edit Global Settings.

Before configuring the global settings, ensure you have created the shared allocation OU in Active Directory. If this OU is not present when you configure the global settings, App Studio cannot validate its location and returns an error.

1. Launch the App Studio Web console by clicking Start > All Programs > Citrix > Citrix App Studio and enter the credentials of the domain administrator used to install the configuration server.

2. From the Home page, click Configure Citrix App Studio.

3. On the Global Settings page, enter the following information and then click Next:

    - License Server: The name of the Citrix License Server you want to use.

    - Shared allocation domain: The Active Directory domain to which all servers in the deployment belong.

    - Shared allocation OU: The Active Directory OU that acts as the root OU of your App Studio deployment.

    - Shared infrastructure import OU: The Active Directory OU where App Studio places shared Web Interface servers that you add to the deployment. This field is populated automatically based on the shared allocation OU; however, you can modify this entry to reflect any OU in the shared allocation domain.

- Decommisioned Server OU: The Active Directory OU where servers removed from App Studio allocation reside. This field is populated automatically based on the shared allocation OU; however, you can modify this entry to reflect any OU in the shared allocation domain.

- Global Domain Administrator: Credentials for the domain administrator account you want to use. This account must have permission to use PowerShell remoting to access all computers in the shared allocation domain you specified, add Active Directory objects, and move computers between OUs. User names are specified in "Domain\Username" format.

4. On the Create Farm Catalog page, enter the following information and then click Next:

   - In Name, enter a name for the farm catalog.

   - In Description, enter a brief description of the farm catalog.

   - In Tags, type labels, separated by commas, by which you can identify the purpose of the farm catalog. You can use these tags later on to allocate resources.

   - In Maximum workload machines per farm, enter the maximum number of XenApp session hosts allowed in each farm in the catalog.

   - In Farm Import OU (relative to shared domain), enter the path to the Active Directory OU where you place the XenApp controllers that Citrix App Studio will add to the farm catalog. Although this field populates automatically based on the shared allocation OU and the catalog name, you can modify this field to reflect any OU in the shared allocation domain.
5. On the Farm Catalog Database Credentials page, select the authentication type for the farm database, enter the appropriate credentials and click Next.

   Note: For this release, only Windows Authentication is supported. Citrix App Studio uses these credentials to join XenApp session hosts to a farm from this farm catalog. Therefore, all farms in the catalog must use these credentials, even if they use different database servers or instances. Additionally, ensure the credentials entered are valid as App Studio cannot validate them until farms and workload machines are imported.

6. On the Create Workload Catalog page, enter the following information and then click Next:

   - In Name, type the name of the catalog.

   - In Description, enter a brief description of the workload catalog.

   - In Tags, type labels, separated by commas, by which you can identify the purpose of the workload catalog. You can use these tags later on to allocate resources.

   - In Workload Machine Import OU (relative to shared domain), enter the path to the Active Directory OU where you place the XenApp session hosts that Citrix App Studio will add to the workload catalog. Although this field populates automatically based on the shared allocation OU and the catalog name, you can modify this field to reflect any OU in the shared allocation domain.
7. Click Finish. Citrix App Studio completes the configuration and returns you to the Welcome page.

After configuring global settings, App Studio initiates workflows that create the OUs you specified. You can view these workflows by clicking Workflows from the console menu bar. After these workflows finish, continue setting up your App Studio deployment by adding farms, XenApp session hosts, and Web Interface servers.

Creating and Modifying Farm Catalogs

A farm catalog consists of XenApp controllers that are configured identically, including having the same patches or updates applied. If you attempt to create a farm using controllers that are not identical to all others in the farm catalog, App Studio will not accept them into your deployment.

Before you create a farm, consider whether you want to use an existing farm catalog or need to create a new farm catalog. If you need to add a farm that includes features that you want to use to differentiate services, then you must create a new farm catalog. For example, you want to add a farm that provides a high degree of availability to tenants.

To add a new farm catalog

1. From the App Studio Home page, under Actions, click Create a new farm catalog. The Farm Catalog wizard appears.

2. On the Create Farm Catalog screen, enter the following information and then click Next:

   - In Name, enter a name for the farm catalog.

   - In Tags, type labels, separated by commas, by which you can identify the purpose of the farm catalog.

   - In Maximum workload machines per farm, enter the maximum number of XenApp servers allowed in each farm in the catalog.

   - In Farm Import OU (relative to shared domain), enter the path to the Active Directory OU where you place the XenApp controllers that Citrix App Studio will add to the farm catalog.

3. On the Farm Catalog Database Credentials screen, select the authentication type for the farm database, enter the appropriate credentials and click Next.

4. On the Summary screen, click Finish. The new farm catalog appears on the Farm Catalogs page.

To modify farm catalog information

1. From the menu bar of the App Studio console, click Provisioning > Farm Catalogs. The Farm Catalogs page appears.
2. Click the name of the farm catalog you want to modify. The farm catalog page appears.
3. Click Edit. The Edit Farm Catalog screen appears.
4. Modify the information in each field as desired.
5. Click Save Farm Catalog to save your changes.

To remove a farm catalog from the App Studio deployment

You can remove farm catalogs in the following ways:

- Delete: App Studio executes workflows to remove the selected farm catalog and any associated farms from the deployment. The Farm Catalogs console page continues to display the farm catalog, indicating it is being deleted. When the workflows are completed, the Farm Catalogs page displays only the remaining catalogs.
- Force Delete: If deletion is unsuccessful, you can forcibly delete the farm catalog. The deletion workflows that App Studio executes might be unsuccessful if, for example, any of the farms in a farm catalog is unreachable over the network. Also, deletion might be unsuccessful if any of the farms in a catalog have a corrupt IMA database that App Studio cannot remove appropriately. Forcibly deleting the farm catalog removes the catalog and all associated farms from the deployment without attempting any further cleanup of the deployed farms. Use this option only if the XenApp controllers are unresponsive or otherwise cannot complete the deletion process.

To monitor the deletion workflows, from the App Studio menu bar, click System > Workflows.

1. From the menu bar of the App Studio console, click Provisioning > Farm Catalogs. The Farm Catalogs page appears.
2. Click the name of the farm catalog you want to remove. The farm catalog page appears.
3. To delete the farm catalog, perform the following actions:
    a. Click Delete. The Delete Farm Catalog screen appears, confirming you want to delete the farm catalog.
    b. Click Delete Farm Catalog to remove the catalog from the App Studio deployment. App Studio removes the farm catalog and any farms it contains from the deployment. Afterward, the Farm Catalogs console page displays only the remaining catalogs.
4. If deleting the farm catalog results in an error, perform the following actions:

a. Click Force Delete. A message appears, confirming you want to forcibly delete the farm catalog.

b. Click Forcibly Delete Farm Catalog. App Studio removes the farm catalog and any farms it contains from the deployment. Afterward, the Farm Catalogs console page displays only the remaining catalogs.

To add farms to a farm catalog

After completing initial setup of the Citrix App Studio configuration server, you can add farms to the farm catalog. This includes configuring XenApp controllers and setting up the farm database. To create a farm, you use the App Delivery Setup Tools to run the New-CamFarm script. After the farm is added to the farm catalog, you can create additional farms for other tenants using the App Delivery Tools or by using a XenServer snapshot of the servers in the first farm.

Important: When using the App Delivery Setup Tools to deploy additional farms, you must ensure that the XenApp controllers are configured identically to the first controllers added to the farm catalog. This includes hardware, software, operating system version, and operating system updates and patches. If machine configurations differ, importing to the farm catalog might fail.

When executed, the New-CamFarm script prompts you for specific information related to your deployment, such as farm catalog OU path, configuration server address, and Citrix Licensing server. As a deployment aid, App Studio can show you the actual information needed for each prompt, based on the farm catalog you select and the details you provided when you configured App Studio. To view this information, you can perform either of the following actions:

- For a new deployment, from the App Studio Home page, in the Add farms section, click How do I do this?
- For an existing deployment, from the App Studio console menu bar, click Provisioning > Farm Catalogs, and then click the name of the farm catalog where you want to add the farm. From the farm catalog console page, click How do I add farms to this farm catalog?

When you click either of these links, a new browser tab (or window) opens and displays the deployment-specific information you can supply at each script prompt.

1. On the App Studio configuration server, click Start > Citrix > App Delivery Setup Tools > App Delivery Setup Tools PowerShell (x64).
2. Type the command .\New-CamFarm.
3. When prompted, provide the following information. Where applicable, default selections are highlighted in yellow. You can accept these defaults by pressing ENTER.
    - ConfigServiceAddress: Enter the name of the server hosting the App Studio configuration service.
    - CanonicalOUPath: Enter the farm import OU that you specified when you configured the App Studio global settings and created the initial farm catalog for your deployment.
    - Enter the network share where the XenApp DVD is located: Enter the network path where the XenApp installation media is located. Example: \\path\to\XenApp\dvd.

- XenApp Edition: Select P for XenApp Premium Edition (default) as this is the only supported edition of XenApp.
- Enter the name of the farm to be created: Enter the name of the XenApp farm you want to create.
- Enter the name of the Windows Active Directory Domain to which these servers belong: Enter domain where the farm servers are located.
- Enter the name of the server where the SQL DB is hosted: Enter the name of the SQL database server.
- Database Authentication: Select Windows (default) or SQL authentication.
- Database Creation: Specify whether or not you want to create the database during farm setup and the database user account you want to use. (default is Y)
- Enter the name of the server designated as the primary data collector for the farm: Enter the name of the server to be configured as the primary XenApp controller.
- Enter the name of the server designated as the backup data collector for the farm: Enter the name of the server to be configured as the backup XenApp controller.
- Install and Configure a Web Interface Server: Specify whether or not you want to configure a unique Web Interface server during farm setup. Select N (default) to use shared Web Interface infrastructure servers in your environment.
- Install and Configure a separate XML Server: Specify whether or not you want to configure a separate instance of the XML Service for the farm. Select N (default) unless you know the volume of application launch requests will require a dedicated server to handle the load.
- Enter the name of the Licensing Server to be used with the farm: Enter the name of the Citrix License Server.
- Change ACLs of XenApp Tools: Specify whether or not you want to change the access control lists (ACLs) of the XenApp command line tools to restrict tenant access. Select Y (default) if you intend to provision services to tenants using shared servers.

The script installs XenApp 6.5 with App Studio extensions on the servers you specified, and then moves the servers to the farm catalog's import OU.

After you add the farm, workflows are initiated that evaluate the XenApp controllers and add them to the appropriate farm catalog. These workflows might take several minutes to complete. You can monitor them by clicking System > Workflows.

If you add the farm to a new deployment, the App Studio Home page refreshes and indicates the XenApp controllers are part of the deployment. Continue setting up your deployment by adding Web Interface servers and XenApp session hosts. When all required components have been added, click Setup complete! Go to the Dashboard to view the App Studio dashboard and manage your deployment.

If you add the farm to an existing deployment, the XenApp controllers appear on the Farms tab of the farm console page.

Creating and Modifying Workload Catalogs

A workload catalog consists of a group of XenApp session hosts, all with the same configuration and the same installed applications. This ensures there are no variations among session hosts when provisioning services, enabling tenants' users to launch advertised applications and desktops when needed.

Workload catalogs are not bound to any specific farm in the App Studio deployment. App Studio moves session hosts to any farm as needed to satisfy the allocation requirements of the workloads created.

To add a new workload catalog

After you set up the first workload catalog in your App Studio deployment, you can create additional workload catalogs. You might set up these catalogs for servers that host different applications or that have been configured differently than servers in the first workload catalog.

1. From the App Studio Home page, under Actions, click Create a new workload catalog. The Workload Catalog wizard appears.
2. On the New Workload Catalog screen, enter the following information:
   - In Name, type the name of the catalog.
   - In Tags, type labels, separated by commas, by which you can identify the purpose of the workload catalog.
   - In Workload Machine Import OU (relative to shared domain), enter the path to the Active Directory OU where you place the XenApp session hosts that Citrix App Studio will add to the workload catalog.
3. Click Create Workload Catalog. The Workload Catalogs console page refreshes and displays the new catalog in the list.

To modify workload catalog information

1. From the menu bar of the App Studio console, click Provisioning > Workload Catalogs. The Workload Catalogs page appears.
2. Click the name of the workload catalog you want to modify. The Edit Workload Catalog screen appears.
3. Modify the information in each field as desired.
4. Click Save Workload Catalog to save your changes.

To remove a workload catalog from the App Studio deployment

You can remove workload catalogs in the following ways:

- Delete: App Studio executes workflows to remove the selected workload catalog and all associated session hosts, including workloads and advertisements. This includes moving associated session hosts to the Decommissioned Servers OU. The Workload Catalogs console page continues to display the workload catalog, indicating it is being deleted. When the workflows are completed, the Workload Catalogs page displays only the remaining catalogs.

- Force Delete: If deletion is unsuccessful, you can forcibly delete the workload catalog. The deletion workflows that App Studio executes might be unsuccessful if, for example, any of the session hosts in a workload catalog are unreachable over the network. This might occur if a session host is taken offline prior to deleting the workload catalog. Forcibly deleting the workload catalog removes the catalog and all associated session hosts from the deployment without any further cleanup activity. Use this option only if the associated session hosts are unresponsive or otherwise cannot complete the deletion process.

To monitor the deletion workflows, from the App Studio menu bar, click System > Workflows.

1. From the menu bar of the App Studio console, click Provisioning > Workload Catalogs. The Workload Catalogs page appears.

2. Click the name of the workload catalog you want to remove. The workload catalog page appears.

3. To remove the workload catalog, perform the following actions:

    a. Click Delete. A message appears, confirming you want to remove the catalog.

    b. Click Delete Workload Catalog. App Studio removes the catalog from the App Studio database and the workload machine page no longer lists the catalog.
4. If deleting the workload catalog results in an error, perform the following actions:

    a. Click the Workflows tab and cancel any deletion workflows for the catalog that are in Pending or Ready states.

    b. Click Force Delete. A message appears, confirming you want to forcibly delete the workload catalog.

    c. Click Forcibly Delete Workload Catalog. App Studio removes the workload catalog and any session hosts it contains from the deployment. Afterward, the Workload Catalogs console page displays only the remaining workload catalogs.

Adding and Removing Session Hosts

After you add farms to the farm catalog, you can add XenApp session hosts to the workload catalog using the New-CamSessionHost script included in the App Delivery Setup Tools. When you add session hosts, you specify the workload catalog to which the servers belong. All session hosts in a workload catalog must be configured identically, including having the same updates or patches applied.

Important: If you attempt to add session hosts that are not identical to all others in the workload catalog, App Studio will not accept them into your environment. If you need to add session hosts that have differing capabilities or applications, you must create a separate workload catalog for them.

When executed, the New-CamSessionHost script prompts you for specific information related to your deployment, such as the workload catalog OU path. As a deployment aid, App Studio can show you the actual information needed for each prompt, based on the workload catalog you select. To view this information, perform either of the following actions:

- For a new deployment, from the App Studio Home page, in the Add machines section, click How do I do this?
- For an existing deployment, from the menu bar of the App Studio console, click Provisioning > Workload Catalogs and then click the name of the workload catalog where you want to add the session host. From the workload catalog console page, click How do I add machines to this workload catalog?

When you click either of these links, a new browser tab (or window) opens and displays the deployment-specific information you can supply at each script prompt.

To add XenApp session hosts

1. Click Start > Citrix > App Delivery Setup Tools > App Delivery Setup Tools PowerShell (x64).

2. Type the command .\New-CamSessionHost.

3. When prompted, provide the following information:

   - SessionHosts[0], SessionHost[1], etc.: Enter the name of the XenApp session host. When you press ENTER after each entry, you are prompted to enter another session host. To progress to the next part of the script, leave the prompt empty and press ENTER.

   - XenAppDVDPath: Enter the network path where the XenApp installation media is located. Example: \\path\to\XenApp\dvd

   - CanonicalOUPath: Enter the path in Active Directory to the workload machine import OU where you want to add the session hosts. Example: my-domain.com/CloudAppManagement/Workload Catalogs/Office Apps

   The script installs XenApp 6.5 with App Studio extensions on the servers you specified and then moves the servers to the workload machine import OU.

After you add new session hosts to your deployment, workflows are initiated that evaluate the session hosts and add them to the workload catalog. If the workload catalog is overallocated, the session hosts are moved to the appropriate workload OU. These workflows might take several minutes to complete. You can monitor them by clicking System > Workflows.

If you add the session hosts to a new deployment, the App Studio home page refreshes and indicates the session hosts are part of the deployment. Continue setting up your deployment by adding Web Interface servers and XenApp farms. When all required components have been added, click Setup complete! Go to the Dashboard to view the App Studio dashboard and manage your deployment.

If you add the session hosts to an existing deployment, the servers appear on the Workload Machines tab of the workload catalog's console page.

To remove XenApp session hosts from the App Studio deployment

You can remove XenApp session hosts from your App Studio deployment in the following ways:

- Drain: Session hosts that are allocated to a workload are drained before removal. New connections are refused and users can reconnect to their existing sessions and terminate them when finished. When all user sessions have ended, App Studio moves the session host to the Decommissioned Servers OU and removed its entry from the App Studio database.

- Delete: Session hosts that are not allocated to any workloads are deleted. App Studio moves the session host to the Decommissioned Servers OU and removes its entry from

the App Studio database.

- Force Delete: If deletion is unsuccessful, you can forcibly delete the session host. By doing this, you remove any associated workflows that have not yet completed. Therefore, you should use this option only if the session host is unresponsive or otherwise cannot complete the deletion process.

1. From the menu bar of the App Studio console, click Provisioning > Workload Catalogs. The Workload Catalogs page appears.

2. Click the name of the workload catalog containing the session host you want to remove. The workload catalog page displays the workload machines assigned to the selected catalog.

3. If the session host you want to remove is allocated to a workload, perform the following actions:

   a. Click Drain. A message appears, confirming you want to drain the selected session host.

   b. Click Drain Workload Machine. The workload machine page refreshes and notes the selected session host is being drained. Afterward, App Studio deletes the session host.

4. If the session host you want to remove is unallocated, perform the following actions:

   a. Click Delete. A message appears, confirming you want to delete the selected session host.

   b. Click Delete Workload Machine.

   The workload machine page refreshes and notes the selected session host is being deleted.

5. If the session host is unresponsive or deleting the session host results in an error, perform the following actions:

   a. Click the Workflows tab and cancel any deletion workflows for the session host that are in Pending or Ready states.

   b. Click Force Delete. A message appears, confirming you want to forcibly delete the session host.

   c. Click Forcibly Delete Workload Machine. The workload machine page refreshes and displays only the remaining session hosts.

Adding and Removing Web Interface Servers

In your App Studio deployment, Web Interface servers are considered *infrastructure resources* that can be shared among several tenants or dedicated to a specific tenant. To add Web Interface servers to your deployment, you use the App Delivery Setup Tools to run the New-CamWIServer script.

Important: Before adding Web Interface servers to your deployment, ensure the servers have the .NET Framework 3.5.1 Windows server role installed, as noted in System Requirements for Citrix App Studio. If this server role is not installed, the New-CamWIServer script fails.

When executed, the New-CamWIServer script prompts you for specific information related to your deployment, such as infrastructure import OU path and configuration server address. As a deployment aid, App Studio can show you the actual information needed for each prompt, to add shared Web Interface servers to your deployment. To view this information, perform either of the following actions:

- For a new deployment, from the App Studio Home page, in the Add Web Interface servers section, click How do I do this?
- For an existing deployment, from the menu bar of the App Studio console, click System > Infrastructure and then click How do I add shared infrastructure machines?

When you click either of these links, a new browser tab (or window) opens and displays the deployment-specific information you can supply at each script prompt.

To add Web Interface servers to the App Studio deployment

Adding shared or private Web Interface servers depends on the infrastructure import OU that you specify when you run the New-CamWIServer script included in the App Delivery Setup Tools. If you specify the shared infrastructure import OU, the Web Interface server is available to all tenants provisioned with shared or private sites. If you specify the infrastructure import OU of a specific tenant, the Web Interface server is available only to that tenant.

1. From the App Studio configuration server, click Start > Citrix > App Delivery Setup Tools > App Delivery Setup Tools PowerShell (x64).
2. Type the command .\New-CamWIServer.
3. When prompted, enter the following values:
    - WIServerName: Enter the name of the server on which you want to install Web Interface.

- XenAppDVDPath: Enter the network path to the share containing the XenApp DVD installation media. This path must be accessible using the name you specify from a session on the target machine. Example: \\path\to\XenApp\dvd

- ConfigSvcAddress: Enter the name of the server hosting the App Studio configuration service.

- CanonicalOUPath: To add the server as a shared Web Interface server, enter the shared infrastructure import OU that you specified when you configured the App Studio global settings for your deployment. To add the server as a private Web Interface server, enter the tenant's infrastructure import OU that you specified when you created the tenant.

The script installs Web Interface with App Studio extensions and moves the machine to the appropriate infrastructure import OU. This process can take several minutes to complete. You can monitor the status by clicking System > Workflows.

Shared Web Interface servers appear on the Infrastructure page of the App Studio console. Private Web Interface servers appear on the Private Infrastructure Machines tab of the tenant's console page.

If you intend to offer hosted desktops to tenants, continue configuring the Web Interface server by enabling the Desktop Viewer. The Desktop Viewer is required for displaying the hosted desktops to which tenants are subscribed. By default, the Desktop Viewer is not enabled when Web Interface is installed.

To enable the Desktop Viewer

When tenants access hosted desktops, the Desktop Viewer displays the desktop and enables tenants to access any installed or hosted applications. However, when App Studio creates XenApp Web and XenApp Services sites for a tenant, the Desktop Viewer is not enabled by default. Use this procedure to enable the Desktop Viewer on each Web Interface server in your deployment.

1. Locate the webinterface.conf file and open it in a text editor. Typically, this file is stored in the following locations:

   - XenApp Web sites: C:\inetpub\wwwroot\Citrix\WI*SiteName*\conf

   - XenApp Services sites: C:\inetpub\wwwroot\Citrix\PNA*SiteName*\conf

   where *SiteName* is the name of the tenant's Web Interface site.
2. Locate the ShowDesktopViewer setting and delete the prepended number sign (#). Configure the setting as follows:

   ShowDesktopViewer=On

To remove a Web Interface server from the App Studio deployment

When you remove a Web Interface server from your deployment, App Studio moves the server to the Decommissioned Servers OU in Active Directory and removes the server's entry from the App Studio database.

If your initial attempt to remove a Web Interface server is unsuccessful, you can forcibly delete it. By doing this, you also remove any associated workflows that have not yet completed. Use this option only if the Web Interface server is unresponsive or otherwise cannot complete the deletion process.

To restore a deleted server, move the server from the Decommissioned Servers OU to the Shared Infrastructure Import OU. App Studio detects the addition to the OU and adds the server to the Infrastructure page of the console.

1. From the menu bar of the App Studio console, perform one of the following actions:

   - To remove a shared Web Interface server, click System > Infrastructure.

   - To remove a private Web Interface server, click Tenants, select the appropriate tenant, and then click the Private Infrastructure Machines tab on the tenant's console page.

   The Infrastructure page appears, listing all the Web Interface servers in the deployment.

2. To delete a Web Interface server, perform the following actions:

   a. For the Web Interface server you want to remove, click Delete. A message appears, confirming you want to remove the Web Interface server.

   b. Click Delete Infrastructure Machine. The console page refreshes and notes the selected Web Interface server is being deleted.

3. If the Web Interface server is unresponsive to the deletion workflows or if deleting the Web Interface server results in an error, perform the following actions:

   a. Click the Workflows tab and cancel any deletion workflows for the Web Interface server that are in Pending or Ready states.

   b. Click Force Delete. A message appears, confirming you want to forcibly delete the Web Interface server.

   c. Click Forcibly Delete Infrastructure Machine. The console page refreshes and no longer lists the selected Web Interface server.

When the deletion workflow is complete, the console page no longer lists the Web Interface server.

Configuring Hosted Desktops for Tenant Access

To manage and configure restrictions within published desktops, run the New-CtxManagedDesktopGPO script from an App Studio configuration server in your deployment. This script is typically located at C:\Program Files (x86)\Citrix\App Delivery Setup Tools.

When executed, the New-CtxManagedDesktopGPO script creates the following Group Policy objects (GPOs):

Name	Type	Description
CtxStartMenuTaskbarUser	User	Changes the pinned shortcuts on the Taskbar and configures the Start menu to match a Windows 7 environment. Requires the Enhanced Desktop Experience feature of XenApp 6.5 (installed by default when XenApp is installed on session hosts).
CtxPersonalizableUser	User	Enables users to change the desktop wallpaper. Prevents users from installing programs, viewing properties, scheduling tasks, or shutting down the server. Requires the Enhanced Desktop Experience feature of XenApp 6.5 (installed by default when XenApp is installed on session hosts). Used with the CtxRestrictedComputer GPO.
CtxRestrictedUser	User	Includes the restrictions in the CtxPersonalizableUser GPO and prevents users from modifying desktop wallpaper and Start menu and Taskbar settings. Used with the CtxRestrictedComputer GPO.
CtxRestrictedComputer	Computer	Prevents users from accessing the Task Manager, Administrative Tools, Windows Update, Help and Support, and removable drives. Used with either the CtxPersonalizableUser or CtxRestrictedUser GPOs.

The OUs to which you apply these GPOs depend on the OU structure of your App Studio deployment in Active Directory. If your deployment's XenApp servers and tenants reside within the Shared Allocation OU, apply these GPOs to the Shared Allocation OU. If your deployment's XenApp servers and tenants reside elsewhere within the shared allocation domain, perform the following actions:

- Apply the CtxRestrictedComputer GPO to the OU containing your deployment's XenApp servers.
- Apply the CtxStartMenuTaskbarUser, CtxPersonalizableUser, or CtxRestrictedUser GPOs to the OU containing your deployment's tenant OUs.

To restrict user access to XenApp servers and control desktop personalization

1. Launch the Group Policy Management Console (Click Run, then type gpmc.msc).
2. In the left pane, locate the Shared Allocation OU for your App Studio deployment and perform the following actions:
   a. Right-click the OU and select Link an Existing GPO.
   b. Select CtxRestrictedComputer.
   c. Depending on the level of desktop personalization you want to allow, select either CtxPersonalizableUser or CtxRestrictedUser.
   d. Click OK.
3. To view the configured settings for each GPO, select the linked GPO and, in the right pane, click the Settings tab.

To enable the Windows 7 look and feel for hosted desktops

1. Launch the Group Policy Management Console (Click Run, then type gpmc.msc).
2. In the left pane, locate the Shared Allocation OU for your App Studio deployment and perform the following actions:
   a. Right-click the OU and select Link an Existing GPO.
   b. Select CtxStartMenuTaskbarUser and click OK.
3. To view the GPO's configured settings, select the linked GPO and, in the right pane, click the Settings tab.

Managing Your App Studio Deployment

After your App Studio deployment is complete, you can manage tenants, services, and subscriptions. Managing your deployment includes the following tasks:

- Get acquainted with the App Studio console for managing your deployment.
- Learn how to use workflows to monitor the processes in your deployment.
- Make hosted resources available for tenant subscription.
- Create tenants and subscribe them to services.
- Create a new version of a workload catalog to update existing session hosts or introduce new services.
- Create additional App Studio administrators to manage your deployment. You can also create helpdesk administrators to enable certain users to monitor assigned tenants and troubleshoot issues using Desktop Director.
- Add more App Studio configuration servers to increase the availability and resiliency of your deployment.

If you use Citrix CloudPortal Services Manager to provide services to customers and resellers, you can enable App Studio to provide hosted applications and desktops alongside your other managed services. For more information, see the topic Providing Applications and Desktops to Customers with Citrix CloudPortal Services Manager.

Working with the App Studio Console

The App Studio console is a Web-based console that enables you to manage your App Studio deployment.

Menu Bar

The menu bar appears at the top of console and enables you to access all console pages. The menu bar is composed of the following sections:

- Home: Displays the console dashboard.
- System: Provides access to the Infrastructure and Workflows pages. On the Infrastructure page, you can view Web Interface servers, manage administrators, and access App Studio global settings. On the Workflows page, you can monitor App Studio processes.
- Provisioning: Provides access to the Workload Catalogs and Farm Catalogs pages where you can create new catalogs and manage member servers.
- Services: Provides access to the Advertisements and Workloads pages. On the Advertisements page, you can make new services available to tenants and subscribe tenants to services. On the Workloads page, you can view the workloads associated with subscriptions and manage workload capacity.
- Tenants: Displays the list of all tenants in the deployment and enables you to add new tenants and create subscriptions.

Dashboard

The dashboard is the home page of the App Studio console and provides an at-a-glance view of your App Studio deployment. The dashboard is composed of the following sections:

- Workflows
- Provisioning (farm catalogs and workload catalogs)
- Tenants
- Services (advertisements and workloads)

These sections provide overviews of the processes, components, services, and tenants in your deployment. Each section displays the following types of notifications:

- Active, in-progress, or failed workflows
- Errors or warnings associated with a tenant, service, workload, or catalog

- Conditions that require your attention such as overallocated workload catalogs, tenants who are not yet subscribed to services, advertisements that do not yet have subscriptions, or empty farm or workload catalogs

- Status of certain workflows such as transitioning to a new version of a workload catalog

The Actions list, on the right side of the dashboard, provides one-click access to common tasks for administering your deployment. Clicking these links takes you to the appropriate console area to perform the selected task and, if required, launches the appropriate wizard. For example, clicking Manage administrators takes you to the Infrastructure page of the console where the Administrators tab displays a list of administrator users. Clicking Advertise new services takes you to the Advertisements console page and launches a wizard so you can select services and make them available to tenants.

Understanding Workflows

A workflow consists of a set of PowerShell scripts that are executed when App Studio detects a specific action, such as creating an advertisement, adjusting the capacity of a workload, or adding users to a subscription. Workflows often consist of multiple steps.

When you complete a task, App Studio logs the workflows that are initiated and displays information on the following console pages:

- On the App Studio Home page, the total number of active workflows are displayed. Clicking this number takes you to the Workflows page.
- On the Workflows page (System > Workflows), App Studio displays a list of active workflows by default.
- On the Workflows tab located on the console page associated with a specific workload or farm catalog, a specific advertisement or workload, or a specific tenant. This tab also appears on the Infrastructure console page. For example, when you subscribe a tenant to an advertised service, the Workflows tab on the advertisement's console page displays the active workflows as they occur.

Workflow States

The following table describes the states that workflows assume as they are completed.

Name	Description
Pending	The workflow is waiting for another workflow to finish before it runs.
Ready	The workflow is ready to execute and will run the next time the agent polling interval happens.
Running	The workflow is currently executing.
Succeeded	The workflow executed successfully. Workflows that finish successfully are displayed on the Workflows console page, in the History view.
Cancelling	The workflow is in the process of being cancelled. If you cancel a workflow that is in Ready or Started states, App Studio waits for the agent to acknowledge that the workflow has been cancelled. In the event a workflow completes cancellation before the agent can acknowledge it, the workflow appears in the History view as Succeeded or Failed, as applicable, rather than Cancelled.

Cancelled	The workflow has completed cancellation. A cancelled workflow can block other workflows from executing until it is retried or superseded. See Resolving Workflow Issues for more information.
Superseded	A configuration change was made after the workflow was scheduled, rendering execution unnecessary. Other workflows waiting for this workflow to execute enter Ready states. Superseded workflows appear in the History view.
Failed	The workflow did not execute successfully. Failed workflows can block other workflows from executing until it is retried or superseded. See Resolving Workflow Issues for more information.

Using the Workflows Console Page

The Workflows console pages displays workflows in the following contexts:

Current view

The Current workflow view displays a list of all the workflows that are active at any given moment. You can sort this list alphabetically and filter according to the workflow's current status (Errors, Warnings, or Active). As the workflow progresses, its status changes. You can view this progress by clicking Refresh. To view the tasks included in the workflow, expand the workflow entry. When the workflow finishes, App Studio records it in the workflow history.

History view

App Studio maintains a record of every successful and unsuccessful workflow for the life of the deployment. To view this record, click the History option on the Workflows page. You can sort and filter this record according to the following criteria:

- Sort by age: Newest First or Oldest First
- Filter by workflow result: Succeeded, Failed, Superseded, or Cancelled

For each workflow entry, App Studio displays the state of each task in the workflow and the time and date at which the workflow completed or failed. App Studio also provides information about the actions that occurred in a successful workflow or why a workflow failed. To view this information, expand the workflow entry.

Resolving Workflow Issues

Workflow issues can arise in the following ways:

Workflow failure

When a workflow fails, App Studio records error information on the Workflows page. To view this information, expand the workflow entry.

Workflow delays

Some workflows take a long time to execute, such as when draining session hosts. Other workflows, such as editing a subscription, generally execute quickly but might appear to be delayed for some reason.

When executing a workflow, the agent sends progress updates to App Studio at intervals until the workflow is completed, regardless of how much time is required. As long as the agent sends updates to indicate the workflow is still active, App Studio allows the workflow to continue. However, if the agent does not send updates, App Studio considers the workflow unresponsive and marks its entry on the Workflows console page with a Warning icon. After 60 minutes, App Studio terminates the workflow.

If a workflow takes longer than expected to execute, you can cancel the workflow and retry it later. This allows you to troubleshoot and correct any issues that might be causing the delay. To cancel a workflow, click the Cancel button for the selected workflow entry. When all issues have been addressed, you can restart the workflow by clicking the Retry button.

Note: You can cancel and retry only the workflows that appear in the Current view. You cannot retry failed workflows in the History view.

Unresponsive agents

If the agent responsible for executing the workflow has stopped responding, App Studio marks the workflow entry on the Workflows console page with a Warning icon. App Studio then elects another agent to execute the workflow, typically an agent in the affected XenApp farm. This process can take up to 20 minutes. If this interval passes and the agent is still unresponsive, you can cancel the workflow and retry it later.

If a workflow fails or is cancelled, App Studio might prevent other workflows from running. This occurs because the workflow failure causes the deployment to be incorrectly or incompletely configured. To rectify this, perform the following actions:

- Troubleshoot and correct any issues outside of App Studio. Examples include network outages, offline or overloaded servers, or issues involving Active Directory permissions. Afterward, you can retry the workflows that failed or were cancelled. Workflows are designed to perform only actions that have not yet been performed, so it is safe to retry partially completed workflows or to retry workflows after performing configurations outside of App Studio. After the workflow finishes, any Pending workflows are updated to Ready.

- If the problem cannot be resolved outside of App Studio, determine the configuration within App Studio that triggered the workflow and alter that configuration. Afterward, App Studio marks workflows that are no longer necessary as Superseded, even if those workflows have failed or have been cancelled. For example, if a catalog import OU specifies a location that App Studio does not (and should not) have permission to access, you can correct it by changing the import OU. App Studio supersedes the existing Update-ImportOU workflow and creates a new workflow targeting the corrected OU.

To adjust workload capacity

Workloads are created when you advertise shared services or create subscriptions to advertised services and specify the capacity. When creating a workload, App Studio requires that you specify a capacity of at least one session host. After you create the workload, it is reused for any service that shares the same farm catalog, workload catalog, and tenant.

Capacity refers to the number of session hosts that are allocated to the services and tenants hosted by the workload. You can adjust the capacity as needed to host more or fewer users or services. Workflows are then initiated that perform the following tasks:

- If increasing capacity: Add session hosts to the farm and move them to the appropriate workload OU for the farm.
- If decreasing capacity: Drain session hosts to allow users to complete any open or disconnected sessions, remove the session hosts from the farm, and move the session hosts to the Decommissioned Servers OU.

Important: Before increasing the capacity of a workload, ensure there is a sufficient number of session hosts in the workload catalog for allocation. If you increase the capacity, but there are not enough session hosts in the catalog, App Studio reports that the workload and workload catalog are overallocated. To resolve this, import additional session hosts to the workload catalog OU. After App Studio detects these machines, the workflows for increasing capacity occur.

1. From the App Studio Home page, under Actions, click Manage workloads. The Workloads page appears.
2. Click the name of the workload whose capacity you want to adjust. The workload page appears.
3. Click Edit Capacity and then, in Capacity, enter the number of session hosts you want to allocate to the workload.
4. Click Save. The workload page refreshes to display the state of the active session hosts.

To create a new version of a workload catalog

During the life of your deployment, you might want to update the session hosts in a workload catalog. For example, you need to apply a hotfix, add new applications, or upgrade to more efficient hardware. To do this, you perform the following tasks:

1. Prepare new servers with the updates you want to introduce to your App Studio deployment. For example, install new applications, apply patches, etc.

2. Using the App Studio console, create a new version of the workload catalog. App Studio creates a new workload machine import OU where the new session hosts will reside.

3. Import the new servers by running the New-CamSessionHost script. For more information, see To add XenApp session hosts.

The restrictions that App Studio normally enforces when adding new session hosts to a workload catalog are relaxed when you create a new version of a workload catalog. App Studio accepts differences in installed applications, applied hotfixes, and hardware configuration such as memory and CPU because the new session hosts are imported to a different workload machine import OU.

Important: In addition to the updates you install, you must ensure the new session hosts have exactly the same applications installed that are already being advertised in the original workload catalog. The executable path for each installed application must match that of the advertised application. Otherwise, the workload catalog will fail to update and the App Studio console will report that certain applications are missing. For example, if you are advertising Microsoft Word 2010 to users, you can update that advertisement to Microsoft Word 2010 SP1 because the path to WINWORD.EXE is the same in both versions. However, if you are advertising Microsoft Word 2007 to users, you cannot update that advertisement to Microsoft Word 2010 because the executable path is different in each version. Instead, you might include both Word 2007 and 2010, and advertise Word 2010 as a new application.

After you create the new workload catalog version and import new session hosts, App Studio drains the original session hosts, allowing users to complete existing sessions and log off. When users log back on, App Studio directs them to the session hosts in the new catalog version. App Studio directs users to machines in the newest version of a workload catalog, regardless of the number of workload catalog versions you create. For example, if you create a V2 catalog and then, soon afterward, create a V3 catalog, App Studio directs users who log off machines in the V1 and V2 catalogs to machines in the V3 catalog for new sessions.

When the session hosts from the original catalog version are fully drained, they are removed from the App Studio console and moved to the Decommissioned Servers OU.

1. From the menu bar of the App Studio console, click Provisioning > Workload Catalogs. The Workload Catalogs page appears.

2. Click the name of the workload catalog you want to update. The workload catalog page appears.

3. Click Create New Version. The Create New Version screen appears.

4. In Workload Machine Import OU, verify the path to the new OU.

   Note: By default, App Studio creates a new OU based on the workload catalog's original OU, but you can change this to reflect any OU in the shared allocation domain. The new OU must be different from the original OU so that App Studio can recognize the new version of the catalog and assign the appropriate session hosts.

5. Click Create New Version. The App Studio console displays the new workload catalog page.

After the new catalog version is created, you can import the session hosts that will reside in the new version's Workload Machine Import OU. For more information, see To add XenApp session hosts.

Advertising Services to Tenants

You can make the desktops and applications residing on XenApp session hosts available to tenants through advertising. You can then subscribe tenants to these advertised services to provision access to their users.

When you create an advertisement, you choose the farm catalog from which to allocate XenApp controllers, the workload catalog from which to allocate the session hosts hosting the advertised service, and the level of isolation you want to provide to tenants accessing the service. The isolation level refers to whether the farm and session hosts used for the advertisement are shared with other tenants or allocated only to the subscribing tenant. You can choose one of the following levels:

- Isolated farm & isolated workload machine: The advertisement uses farm servers and session hosts that are allocated only to the subscribing tenant. When a tenant subscribes to this advertisement, App Studio creates OUs in Active Directory for these machines within the tenant's OU. App Studio then moves the machines from the selected catalogs to the appropriate OU. Only the tenant's users can use these machines to access the subscribed service.

- Shared farm & isolated workload machine: The advertisement uses farm machines that are shared with other tenants and session hosts that are allocated only to the subscribing tenant. When a tenant subscribes to this advertisement, App Studio creates an OU in Active Directory for the session hosts within the tenant's OU. App Studio then moves the machines from the selected workload catalog to the workload machine OU. When the tenant's users access the service, they use the same farm as other tenants but no other tenants use the subscribing tenant's session hosts.

- Shared farm & shared workload machine: The advertisement uses farm servers and session hosts that are allocated as shared among other tenants. For advertisements with this isolation level, you must ensure the advertisement has sufficient capacity to provide access to all subscribers. When you add capacity to the advertisement, App Studio moves the allocated session host to the appropriate shared OU. Tenants can access the service in the same farm and on the same session hosts as all other tenants subscribed to the advertisement.

After creating the advertisement, you can configure the following settings:

Property Group	Setting Name	Description

Basic Properties	Display name	Change the advertisement name displayed to tenants. By default, tenants see the display name that appears in the Start menu of the session hosts in the workload catalog.
	Description	Change the tooltip text for the application shortcut displayed to users.
	Enabled	Control user access to the subscribed application on Web Interface sites. Select Yes to allow users to see the application on their Web Interface site and launch a session. Select No, but still visible to allow users to see the application but prevent them from launching a session. Select No, and not visible to prevent users from seeing or launching the application.
	Security	Require user devices to employ a secure ICA connection when accessing the application. When this option is selected, user devices must connect with a minimum encryption level of 128-bit RC-5 encryption.

Session properties	Color depth	Control the color depth displayed in the session.
	Window size	Control the default size of the session window. Select Full Screen to allow the session window to encompass the entire screen. Select Exact pixel size to specify a preferred screen resolution for the session. Select Percent to specify a percentage of the user's screen.
	Legacy audio	Control whether or not audio is enabled for the session. Select Required to launch the application only if the user device supports audio. Select Enabled to allow audio on all user devices. Select Disabled to prevent audio on all user devices.

Advanced properties	Program executable	The executable path of the application on the XenApp server. This setting is read-only.
	Command-line arguments	Pass client-supplied command-line parameters to the application. Enter the percent and asterisk symbols enclosed in double quotation marks ("%*") to act as a placeholder. When a user launches a session through Citrix Receiver, the XenApp server replaces the placeholder with the application parameters Receiver provides.
	Working directory	Specify the directory on the user device in which the application runs. By default, applications start in the user's home directory on the XenApp session host.
	Client folder	Specify the folder on the user device in which to place a shortcut.
	Start menu	Control whether or not add a shortcut to the user's Start menu and specify the folder in which the shortcut appears.
	Client folder	Control whether or not to add a shortcut to the user's Desktop.
	CPU priority level	Control the resource allotment for the session. By default, Normal is selected. Select a higher priority to increase the resource allotment and devote more CPU cycles to the session.
	Startup	Require the application to delay startup until printers are created for the session.

For more information about application properties, refer to the following topics in Citrix eDocs:

- To configure locations of published applications
- To pass parameters to published applications

- To configure shortcuts for user devices

To advertise services to tenants

1. From the App Studio Home page, perform one of the following actions:
   - If you are advertising services for a new deployment, click Make desktops and apps available.
   - If you are advertising additional services for an existing deployment, click Create new advertisements.

   The Select Services screen appears, listing all the applications available for advertisement.
2. In Workload catalog, select the workload catalog you want to use.
3. Select the applications you want to make available to tenants and then click Next.
4. On the Select Farm Catalog screen, select the farm catalog you want to use and the isolation mode.
5. If you are advertising a service using the Shared farm & shared workload machine isolation mode, add capacity to the advertisement, if applicable:
   a. Under Shared workload, expand the farm catalog and click Add.
   b. In Capacity to add, type the number of servers hosting the selected applications that will be allocated.
6. On the Advertisement Names screen, enter the service name for each application and then click Next. These names are visible in the App Studio console and, if applicable, in the Citrix CloudPortal Services Manager control panel.
7. Click Finish to save your selections.

After you finish advertising services, you can add tenants and subscribe them to the advertised services. For more information about adding tenants, see To import tenants. For more information about creating subscriptions, see Subscribing Tenant Users to Services.

To modify advertisements

1. From the menu bar of the App Studio console, click Services > Advertisements.
2. Click the name of the advertised application you want to modify. The application's advertisement page appears.
3. Click Edit. The Edit Advertisement screen appears.
4. Modify the desired information on the following screens:
   - Click Basic properties to change the advertisement's display name and description, change the subscription availability, and require client encryption.
   - Click Session properties to change the color depth and window size of accessed applications, and to enable or disable session audio.
   - Click Advanced properties to change where application shortcuts appear on the user's device, CPU priority, and to enable or disable printer creation on session startup.
5. Click Save Advertisement to save your selections.

To remove advertisements

You can remove advertisements in the following ways:

- Delete: App Studio executes workflows to remove the selected advertisement and any associated subscriptions from the deployment. The Advertisements console page continues to display the advertisement, indicating it is being deleted. When the workflows are completed, the Advertisements page displays only the remaining advertisements.
- Force Delete: If deletion is unsuccessful, you can forcibly delete the advertisement. App Studio removes the advertisement and associated subscriptions from the App Studio database without attempting any further cleanup activities.

1. From the menu bar of the App Studio console, click Services > Advertisements.
2. Click the name of the advertised application you want to delete. The application's advertisement page appears.
3. To delete the advertisement, perform the following actions:
   a. Click Delete. A message appears, confirming you want to delete the selected advertisement.
   b. Click Delete Advertisement. App Studio removes the advertisement from the database and the Advertisements page displays only the remaining advertisements.
4. If deleting the advertisement is unsuccessful, perform the following actions:
   a. Click the Workflows tab and cancel any workflows for the advertisement that are in Pending or Ready states.

b. Click Force Delete. A message appears, confirming you want to forcibly delete the advertisement.

c. Click Forcibly Delete Advertisement. App Studio removes the advertisement and associated subscriptions from the database and the Advertisements page displays only the remaining advertisements.

Managing Tenants

After installing and configuring your deployment, you *import* tenants for whom you create subscriptions to advertised services. When you import a tenant, you specify the tenant's OU where the tenant's users and any private farms and servers reside. By default, App Studio expects the tenant's OU to reside within the Tenants root OU. However, you can specify any OU within the shared allocation domain as the tenant's OU.

Isolation Levels

When you import a tenant, you can choose the isolation level of the tenant's Web Interface site. These isolation levels are:

- Shared site: To access subscribed applications, the tenant's users log on to a shared Web Interface site on a shared Web Interface server. Other tenants use the same site URL on this server to access their own subscriptions.

- Private site: To access subscribed applications, the tenant's users log on to a private Web Interface site on a shared Web Interface server. Other tenants use this server to access their subscriptions, but no other tenants have access to the subscribing tenant's site. This option is useful for providing tenants a custom-branded Web Interface site without dedicating additional server resources.

- Private server: To access subscribed applications, the tenant's users log on to a private Web Interface site on a dedicated Web Interface server. When you import the tenant, you specify the path to the tenant's Web Interface server import OU. App Studio then creates an Infrastructure OU for the tenant which you specify when you add Web Interface servers using the New-CamWIServer script. Because the Web Interface server is allocated only to the subscribing tenant, the server does not host the sites of other tenants and no other tenant's users can access the subscribing tenant's Web Interface site.

After you import the tenant, App Studio creates the XenApp Web and XenApp Services (PNA) sites according to the isolation level you specified and displays the URLs on the tenant's console page. The tenant uses these URLs to access subscribed applications using a Web browser or Citrix Receiver, respectively. By default, the tenant's XenApp Web site URL is shown. To view the tenant's XenApp Services site URL instead, click Show PNA sites. To view the XenApp Web site URL, click Show Web Interface sites.

Accessing Hosted Desktops

When tenants access hosted desktops, the Desktop Viewer displays the desktop and enables tenants to access any installed or hosted applications. However, the Desktop Viewer is not enabled by default when Web Interface servers are added to the deployment or when App Studio creates a tenant's Web Interface site. If you intend to offer hosted desktops to tenants, ensure the Desktop Viewer is enabled on each Web Interface server in your deployment. For instructions, see To enable the Desktop Viewer.

Importing and Modifying Tenants

App Studio manages associations between tenants' users and hosted applications and desktops. However, it does not manage tenant creation or onboarding. These functions are typically handled by other customer portal or control panel products such as Citrix CloudPortal Services Manager, or by CSP-specific onboarding scripts.

Before adding a tenant, perform the following actions:

- Create the tenant's root OU within the shared allocation domain and ensure the tenant's users reside within this OU. During tenant import, App Studio verifies the presence of this OU and returns an error if it cannot be found. Additionally, App Studio places any privately allocated XenApp controllers, session hosts, or Web Interface servers within this OU.

- If your deployment is not integrated with Citrix CloudPortal Services Manager, ensure the Tenants root OU is sufficiently isolated. This ensures that only the App Studio configuration servers and XenApp controllers have Read access to the Tenants OU to add tenants and create subscriptions. The *Tenants root OU* refers to the root OU where individual tenant OUs reside. When you add tenants, App Studio suggests "Tenants" as the root OU by default; but you can modify this to reflect any OU in the shared allocation domain. For example, mydomain.com/CloudAppManagement/Tenants/ or mydomain.com/CSP_Tenants/.

To isolate the Tenants root organizational unit

1. From the Active Directory Users and Computers console, click View > Advanced Features.

2. Remove the Authenticated Users group from the Tenants root OU.

    a. Right-click the Tenants root OU and then click Properties.

    b. Click the Security tab and then select the Authenticated Users group.

    c. Click Remove and then click Apply.
3. Create a new security group in the shared allocation domain and add the computer accounts of the App Studio configuration servers and the XenApp controllers in your deployment.

    a. In the tree pane, right-click the domain and select New > Group.

    b. In Group name, enter a name for the group. In Group Type, ensure Security is selected. Click OK.

    c. Right-click the new group and select Properties.

    d. Click the Members tab and then click Add.

    e. Click Object Types and select Computers. Enter the computer names of the App Studio configuration servers and XenApp controllers in your deployment. Click OK.
4. Assign the new security group Read permissions to the Tenants root OU.

    a. Right-click the Tenants root OU and click Properties.

    b. Click the Security tab and then click Add. Enter the name of the new security group and then click OK.

    c. In Permissions for, in the Allow column, select Read.

    d. Click OK.
5. Reboot the App Studio configuration servers and XenApp controllers to enable the security settings to take effect.

To import tenants

1. From the App Studio Home page, perform one of the following actions:
   - If you are adding tenants to a new deployment, click Add tenants to the system.
   - If you are adding more tenants to an existing deployment, under Actions, click Import a tenant.
2. On the Tenant Information screen, enter the following information and then click Next:
   - In Name, enter a name for the new tenant.
   - In Tags, type labels, separated by commas, that identify the tenant. For example, you might enter tags that represent the tenant's billing group, license type, or service level.
   - In Tenant root OU, enter the path to the Active Directory OU where the tenant's users and any privately allocated farms and session hosts will reside.

     Note: When you enter the tenant's name, the Tenant root OU field is populated automatically. However, you can modify this entry to reflect any OU in the shared allocation domain.
3. On the Choose Web Interface Site Isolation screen, choose one of the following options:
   - Shared site: Choose this option to specify a shared Web Interface site for the tenant.
   - Private site: Choose this option to allocate a private Web Interface site for the tenant.
   - Private server: Choose this option to allocate a private server to host a private Web Interface site for the tenant. In Web Interface server import OU, specify the OU where you place the tenant's private Web Interface server.
4. Click Finish to create the tenant.

After adding a tenant to a new deployment, the Home page refreshes, indicating all initial App Studio configuration tasks are completed. Click Setup Complete! Go to the Dashboard to view the App Studio dashboard. From the dashboard, you can advertise services and create tenant subscriptions. For more information, see Advertising Services to Tenants and Subscribing Tenant Users to Services.

To modify tenant information

1. From the menu bar of the App Studio console, click Tenants. The Tenants page appears, listing all the imported tenants.
2. Click the name of the tenant you want to modify. The tenant's page appears.
3. Click Edit. The Edit Tenant screen appears.
4. Perform the following actions and modify the information in each field as desired:
    a. Click General to modify the tenant's basic information.
    b. Click Isolation to modify the tenant's Web Interface information.
5. Click Save Tenant to save your changes.

To remove a tenant

You can remove tenants in the following ways:

- Delete: App Studio executes workflows to delete the tenant and any associated subscriptions from the deployment. Additionally, if any farm controllers, session hosts, or Web Interface servers are privately allocated to the tenant, App Studio moves these servers to the Decommissioned Servers OU. The Tenants console page continues to display the tenant, indicating that the tenant is being deleted.
- Force Delete: If the deletion workflows do not complete successfully, you can forcibly delete the tenant. App Studio removes the tenant and any associated subscriptions from the App Studio database without attempting any further cleanup activities.

1. From the menu bar of the App Studio console, click Tenants. The Tenants page appears, listing all the imported tenants.
2. Click the name of the tenant you want to delete. A message appears, confirming you want to delete the tenant.
3. To remove the tenant, perform the following actions: click Delete Tenant.
    a. Click Delete. A message appears, confirming you want to delete the tenant.
    b. Click Delete Tenant. App Studio deletes the tenant from the database and removes the tenant's root OU from Active Directory. The Tenants page refreshes and displays only the remaining tenants.
4. If deletion is unsuccessful, perform the following actions:
    a. Click the Workflows tab and cancel any deletion workflows for the tenant that are in Pending or Ready states.
    b. Click Force Delete. A message appears, confirming you want to forcibly delete the tenant.
    c. Click Forcibly Delete Tenant. App Studio removes the tenant and associated subscriptions from the App Studio database. As well, the Tenants console page

refreshes and displays only the remaining tenants.

Subscribing Tenant Users to Services

Subscriptions enable tenants' users to access advertised resources through the Web Interface. Depending on the Web Interface isolation level you selected when you imported the tenant, users can log on to a shared or private site URL to access their subscriptions.

When you create a subscription for a tenant, a workload is created to host the subscription if one does not already exist. Whether creating a workload, or using an existing one, App Studio provides an opportunity to add capacity to the workload. Adding capacity causes App Studio to allocate additional session hosts to deliver the subscribed service to the tenant's users. The workload is associated with the workload catalog, farm catalog, and tenant for whom the subscription is created. This workload is reused if another subscription is created for the same tenant using the same workload and farm catalogs.

To create subscriptions

1. From the App Studio Home page, under Actions, click Subscribe users to services.
2. On the Select Tenant screen, select the tenant for whom you want to add subscriptions and click Next.
3. On the Select Advertisements screen, select the services you want to add to the tenant's subscription and then click Next.
4. On the Add Users screen, enter the tenant's users who will use the selected services in "Domain\Username" format. You can enter individual users or Active Directory groups.
5. Click Validate Users and then click Next.
6. On the Select Capacity page, if additional capacity is required, expand the farm catalog you want to use and then click Add. Enter the number of servers that are available to serve resources to the tenant's users.
7. Click Finish to create the subscription.

To add or remove users from subscriptions

1. From the menu bar of the App Studio console, click Tenants.
2. From the Tenants page, click the name of the tenant whose subscriptions you want to modify. The tenant's page appears.
3. On the Subscriptions tab, click the name of the subscription you want to modify. The subscription page appears.
4. To add more users, perform the following actions:
    a. Click Add Users.
    b. Enter the tenant's users who will use the selected services in "Domain\Username" format. You can enter individual users or Active Directory groups.
    c. Click Validate Users and then click Next. The Select Capacity screen appears.
    d. If you are adding several users to the subscription, increase capacity, if necessary. Expand the workload, click Add and enter the number of session hosts to add to the workload. Click Next.
    e. Click Finish.
5. To remove users, perform the following actions:
    a. On the Users tab, for the user or group you want to remove, click Remove. A message appears, confirming you want to remove the user.
    b. Click Remove User. App Studio removes the selected user from the subscription.

To remove subscriptions

You can remove subscriptions in the following ways:

- Delete: App Studio executes workflows to remove the selected subscription from the App Studio deployment. App Studio continues to display the subscription, indicating that it is being deleted. After the workflows are complete, App Studio displays only the remaining subscriptions.
- Force Delete: If deletion is unsuccessful, you can forcibly delete the subscription. App Studio removes the subscription from the App Studio database without attempting any further cleanup activities.

1. From the menu bar of the App Studio console, perform one of the following actions: .
    - Click Tenants, click the name of the tenant whose subscriptions you want to delete.
    - Click Advertisements and then click the name of the advertisement whose subscription you want to delete.
2. On the Subscriptions tab, click the name of the subscription you want to delete.

3. On the subscription console page, click Delete Subscription. A message appears, confirming you want to delete the subscription.

4. Click Delete Subscription. App Studio notes the subscription is being deleted. After the deletion is complete, App Studio displays only the remaining subscriptions.

5. If the deletion is unsuccessful, perform the following actions:

    a. Click the Workflows tab and cancel any workflows for the subscription that are in Pending or Ready states.

    b. Click Force Delete. A message appears, confirming you want to forcibly delete the subscription.

    c. Click Forcibly Delete Subscription. App Studio removes the subscription from the database and displays only the remaining subscriptions.

Managing Administrators

In App Studio, you can create the following types of administrator users:

- App Studio administrator: This user has access to all App Studio console functions, including changing the global domain administrator for the deployment.
- Helpdesk administrator: This user can view information for assigned tenants through the Desktop Director console. Assigning the helpdesk administrator role grants privileges only within Desktop Director when used in conjunction with App Studio. This role does not grant privileges to App Studio itself or to the XenApp farms that App Studio manages. For more information about Desktop Director, refer to the Desktop Director topics in Citrix eDocs.

When creating administrator users in App Studio, you can specify individual users or Active Directory groups.

To create a new App Studio administrator

1. From the App Studio Home page, under Actions, click Manage administrators.
2. On the Infrastructure page, click Add Administrators.
3. On the Add Administrators screen, enter the users to whom you want to grant administrative permissions in "Domain\Username" format.
4. Click Validate Users. App Studio validates the entries and notes they will be added as Administrators.
5. Click Add Administrators. The Infrastructure page refreshes and displays the users you added on the Administrators tab.

To create a helpdesk administrator

1. From the menu bar of the App Studio console, click Tenants.
2. Click the name of the tenant and then click Add Helpdesk Administrators.
3. On the Add Helpdesk Administrators screen, enter the users or Active Directory group to whom you want to grant administrative permissions in "Domain\Username" format.
4. Click Validate Users. App Studio validates the users you entered.
5. Click Add Helpdesk Administrators. App Studio adds the users to the Helpdesk Administrators tab on the tenant's console page.

To remove an administrator

1. To remove a global administrator, perform the following actions:

    a. From the App Studio Home page, under Actions, click Manage administrators.

    b. On the Infrastructure page, on the Administrators tab, click Delete for the administrator you want to remove.

    c. Click Delete Administrator. App Studio removes the selected user from the database. Also, the Infrastructure page refreshes, displaying only the remaining administrators.
2. To remove a helpdesk administrator, perform the following actions:

    a. From the menu bar of the App Studio console, click Tenants and then click the name of the tenant whose helpdesk administrators you want to manage.

    b. Click the Helpdesk Administrators tab on the tenant's console page and then click Remove for the helpdesk administrator you want to remove.

    d. Click Remove Helpdesk Administrator. The App Studio console refreshes and the Helpdesk Administrators tab displays only the remaining helpdesk administrators.

Providing Applications and Desktops to Customers with Citrix CloudPortal Services Manager

The CloudPortal Services Manager is data-center installed software that enables you to host, sell, and resell hosted applications and related infrastructure. Managed through a Web browser, the control panel is a scalable environment for service providers and resellers who provision and manage customer solutions.

You can add App Studio as a service, called Hosted Apps and Desktops, to an existing Services Manager deployment. This enables you to use the Services Manager control panel to advertise XenApp and XenDesktop services and subscribe customers, including resellers, to them.

Before you configure the Hosted Apps and Desktops service in Services Manager, ensure you have created in App Studio the advertisements you need for provisioning customers. When you configure the Hosted Apps and Desktops service, you add these advertisements to user plans. The user plans define the App Studio services that are available for selection when you provision Services Manager customers.

When you provision a customer with the Hosted Apps and Desktops service, you are performing the following operations:

- Set the isolation level of the Web Interface site
- Subscribe the customer to advertised services

The isolation levels of Web Interface sites (Shared, Private site, or Private server) available in App Studio are displayed in Services Manager as customer plans that you assign during provisioning. To set the isolation level for the customer's Web Interface site, you select the appropriate customer plan in the Service Plan Configuration. To subscribe a customer to advertisements, you select the user plans to which the customer has access. In Services Manager, subscriptions enable the customer to further provision App Studio services to users.

When you provision a Services Manager customer with the Hosted Apps and Desktops service, the customer is also created as a tenant in App Studio. As well, App Studio creates a Web Interface site for the tenant at the isolation level you selected (through the customer plan) and creates subscriptions for the tenant based on the user plans you selected. After the customer is provisioned with the service, the customer logs in to the Services Manager control panel and selects the user plans with which to provision individual users.

At each step in the provisioning process, App Studio executes workflows that create the tenant, subscribe to advertisements, and create the Web Interface site. You can monitor these workflows in the App Studio console by clicking System > Workflows. After these workflows finish, you can view the customer's tenant information and subscriptions in the App Studio console.

For more information about installing and configuring the Hosted Apps and Desktops service in a Services Manager deployment and provisioning the service to customers and users, refer to the CloudPortal Services Manager product documentation located in Citrix eDocs.