Citrix Virtual Desktops Essentials

May 22, 2019

Contributed by: C J

IN THIS ARTICLE

Citrix Virtual Desktops Essentials allows management and delivery of Windows 10 virtual desktops from Microsoft Azure.

Virtual Desktops Essentials is designed specifically for the Azure Marketplace. Citrix and Microsoft partner to deliver an integrated experience for Virtual Desktops Essentials and Azure IaaS. This partnership gives you a single interface to deliver a complete Windows 10 digital workspace from Azure.

Using Virtual Desktops Essentials, you can:

- Deploy and secure Windows 10 virtual desktops on Azure
- Deliver best-in-class user experience by using Citrix HDX capabilities
- Provide secure access on any device by using Citrix Workspace app
- Manage and administer the deployment from Microsoft Azure and Citrix Cloud

Citrix Virtual Desktops Essentials simplifies Windows 10 deployment. You can deploy desktops quickly, manage at scale, and deliver a rich user access experience from a single management plane.

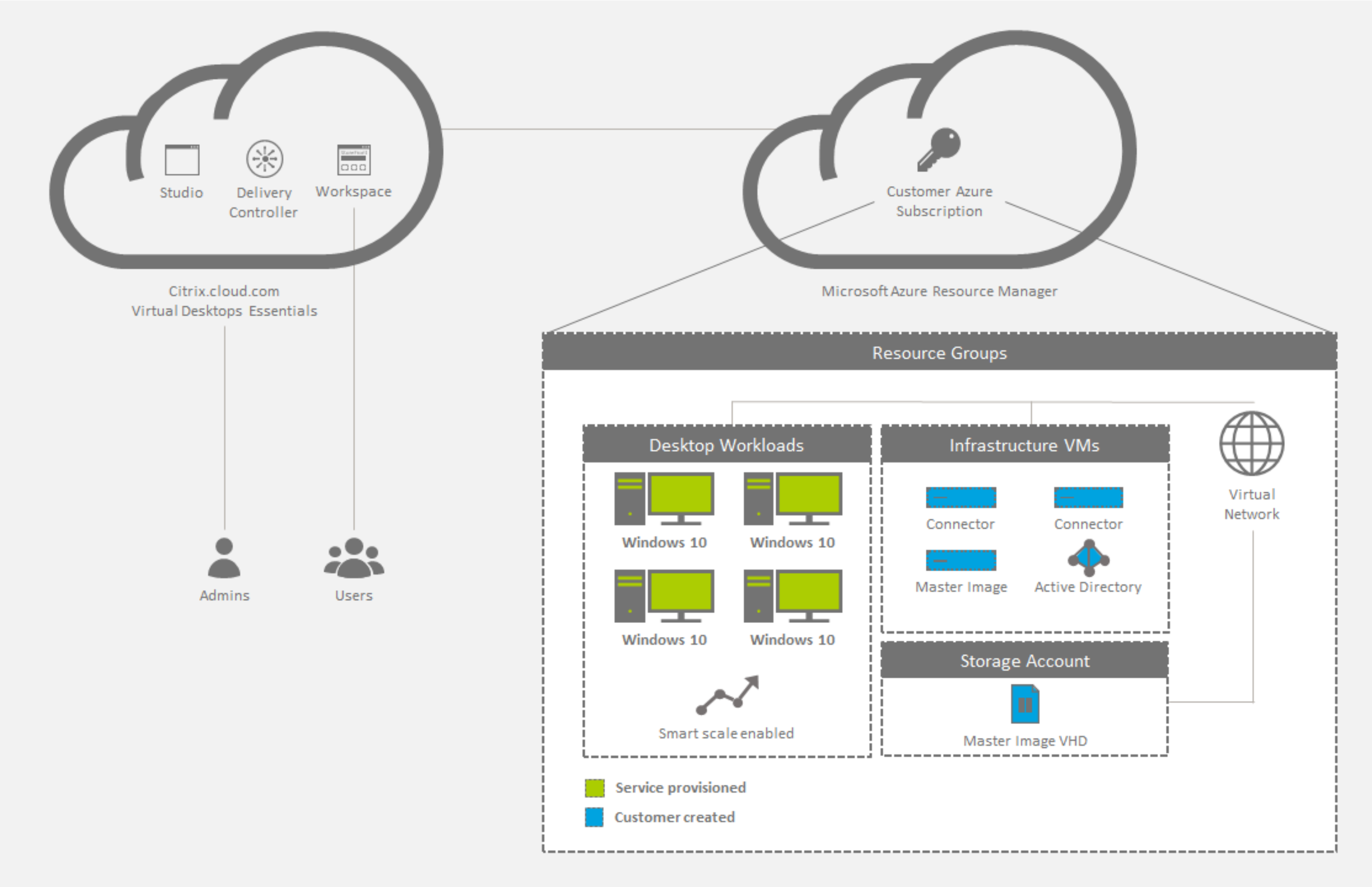
You manage the Windows 10 desktops using Studio and monitor sessions using Director. Users connect to their Windows 10 virtual desktops by logging on with Citrix Workspace app.

After you configure Citrix Virtual Desktops Essentials, you provide your users with a URL to Citrix Workspace. Users connect to their desktops through the Citrix Workspace app on their devices, with the URL you provide. When users log on to the Citrix Workspace app, the Windows 10 desktop icon appears in the workspace window.

> **IMPORTANT:**
>
> Virtual Desktops Essentials includes a Citrix Workspace URL, usually in the format `https://<yourcompanyname>.cloud.com`. After you set up Virtual Desktops Essentials, test and share the workspace URL link with your subscribers to give them access to their desktops. Virtual Desktops Essentials does not support on-premises StoreFront.

For details about the workspace, see Workspace configuration.

The diagram shows an architectural overview of a Virtual Desktops Essentials deployment.



What's new

December 2018: **Cloud-hosted StoreFront removed**

Cloud-hosted StoreFront is no longer available for use with Virtual Desktops Essentials. Customers who purchased Virtual Desktops Essentials (formerly XenDesktop Essentials) before December 2017 can use Citrix Workspace as described in this article to provide subscriber access to desktops.

August 2018: **New product names**

If you've been a Citrix customer or partner for a while, you'll notice new names in our products and product documentation. If you're new to this Citrix product, you might see different names for a product or component.

The new product and component names stem from the expanding Citrix portfolio and cloud strategy. This article uses the following names.

- **Citrix Virtual Desktops Essentials:** The technology that made XenDesktop the industry leader is now Citrix Virtual Desktops, and it brings VDI into a modern, contextual, secure app that allows the preferred way to securely access all your work applications. XenDesktop Essentials is now Citrix Virtual Desktops Essentials.
- **Citrix Workspace app:** The Citrix Workspace app incorporates existing Citrix Receiver technology as well as the other Citrix Workspace client technologies. It has been enhanced to deliver additional capabilities to provide end users with a unified, contextual experience where they can interact with all the work apps, files, and devices they need to do their best work.
- **Citrix Gateway:** The NetScaler Gateway, which allows secure, contextual access to the apps and data you need to do your best work, is now Citrix Gateway.

In-product content might still contain former names. For example, instances of earlier names in console text, messages, and directory/file names. It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.

Related product documentation and other resources (such as videos and blog posts) that are linked from this product's documentation might still contain former names. Your patience during this transition is appreciated. For more detail about our new names, see https://www.citrix.com/about/citrix-product-guide/.

How to buy Virtual Desktops Essentials

For detailed information about buying or canceling Virtual Desktops Essentials, download How to buy or cancel the Virtual Desktops Essentials Service.

System requirements, prerequisites, and compatibility

Virtual Desktops Essentials requires certain complementary products and components and specific account permissions for installation, configuration, and operation.

Microsoft Azure

Virtual Desktops Essentials is designed to support Microsoft Azure exclusively. Your Azure environment must meet certain minimum requirements to support Virtual Desktops Essentials:

- An Azure subscription with an enterprise agreement, or a Microsoft CSP Azure subscription.
- Windows Server Active Directory or Azure Active Directory Domain Service.
- An Azure Active Directory tenant.

  > **IMPORTANT:**
  >
  > Microsoft requires the Azure Active Directory tenant in the Azure subscription to deploy Windows 10 desktops. You can use the Azure Active Directory tenant or another active directory to identify authorized users.

- An Active Directory domain controller.
- An Azure Resource Manager (ARM) virtual network and subnet in your preferred region. Configure the virtual network with a custom domain name server (DNS) entry pointing to the domain controller. The virtual network must have one subnet that is large enough to hold the desktops.

  Use the same virtual network for the DNS entry and desktop subnet.

- An Azure Active Directory user with contributor (or greater) permissions within the subscription.
- One virtual machine that has Microsoft Windows 10 installed, including your required customizations and apps.

Citrix Cloud Connector

Citrix Cloud Connector authenticates and encrypts communications between Citrix Cloud and your resource locations. With Virtual Desktops Essentials, your resources are located in Microsoft Azure. Citrix Cloud requires that you install the Citrix Cloud Connector on two Windows server VMs to ensure continuous availability of your resource locations.

For more information about Cloud Connectors, see Citrix Cloud Connector

Citrix Cloud

- A Citrix Cloud account.
- Access to the Citrix Virtual Apps and Desktops service within Citrix Cloud, which is enabled as a part of your Virtual Desktops Essentials purchase.
- (Optional) One Citrix ADC VPX configured in ICA Proxy mode, for access from outside the corporate network.
  - ICA Proxy enables secure access to the applications and desktops offered to your users.
  - For information about setting up the Citrix ADC VPX, see Deploying Citrix NetScaler VPX on Microsoft Azure.

Known issues

- The Citrix Help Desk Administrator custom access role does not work correctly. As a workaround, use the Cloud Administrator role, or enable Full access. [BRK-3589]
- If you use Azure AD Domain Services: Workspace logon UPNs must contain the domain name that was specified when enabling Azure AD Domain Services. Logons cannot use UPNs for a custom domain you create, even if that custom domain is designated as primary.

Step 1: Connect your Azure subscription to Virtual Desktops Essentials

1. Sign in to the Azure portal.
2. In Azure, open a domain-joined Windows Server virtual machine and then open a web browser.
3. In the web browser on the VM, sign in to Citrix Cloud. The Virtual Apps and Desktops service opens.
4. From the upper left menu, select **Resource Locations**.
5. On the **Resource Locations** page, click **Download**. The file `cwcconnector.exe` downloads.
6. Double-click the downloaded program to start the installer.
7. When prompted, enter your Citrix Cloud credentials. Follow the on-screen instructions to install and configure the Citrix Cloud Connector.
8. Repeat steps 4 through 7 on at least one more server VM, to install another Cloud Connector.

During installation, the Cloud Connector accesses Citrix Cloud to authenticate, validate the installer permissions, and then download and configure the services that the Cloud Connector provides. The installation uses the privileges of the user who initiated the installation.

After installation, Citrix Cloud registers your domain in **Identity and Access Management**. For more information, see Identity and Access Management.

Step 2: Create a host connection

Before you start, ensure that you have your Azure Active Directory credentials and your subscription ID available. The Azure AD user who creates the host connection must be a native cloud user in the Azure AD or synchronized for the enterprise domain. The user account cannot be an invited or delegated Microsoft account.

1. Sign in to Citrix Cloud.
2. In the upper left menu, select **My Services > Virtual Apps and Desktops**.
3. Click **Manage**. The Studio management console opens.
4. Select **Configuration > Hosting** in the Studio navigation pane.

5. Click **Add Connection and Resources** in the Actions pane.

6. On the **Add Connection and Resources** page:

   a. In **Connection type**, select **Microsoft Azure**.

   b. In the Azure environment, select **Azure Global** and then click **Next**.

7. In **Connection Details**:

   a. In **Subscription ID**, type the Azure subscription ID.

   b. In **Connection name**, type a name for the connection and then either:

      a. Click **Create new** and then follow the procedure Option 1: To create a connection.”

      b. Click **Use existing** and continue configuring the settings. Follow the procedure Option 2: Use an existing host connection.”

Option 1: Create a connection

1. Sign in to Azure with the subscription contributor (or greater) account.

2. Azure creates the host connection automatically. In Studio, a green check mark with the word **Connected** appears on the **Add Connection and Resources** page.

3. Click **Next**.

4. On the **Region** page, select the region where your virtual network resides, and then click **Next**.

5. On the **Network** page:

   a. Type a name for the resources.

   b. Select the virtual network for the resource group.

   c. Select the subnet that applies to the resource group and then click **Next**.

6. On the **Summary** page, click **Finish**. The host connection to the Microsoft Azure Resource Manager is complete.

Option 2: Use an existing host connection

After you click **Use existing**, the **Existing Service Principal Details** page appears:

1. In **Subscription ID**, type the Microsoft Azure subscription ID.

2. In **Subscription name**, type the name of the Azure subscription.

3. Click **OK**.

4. On the **Connection** page:

   a. Click **Create a new Connection**, type your Microsoft Azure subscription ID and a connection name (optional), and then click **Create new**. The Microsoft authentication dialog box appears.

      If you want to use a connection that you created at another time, choose **Use an existing connection**. Then, select the connection.

   b. Type the user name and password for the Microsoft Azure Active Directory user. Citrix Cloud creates a service principal with the rights to create and manage machines for this subscription.

5. On the **Region** page, select the Azure region where your Microsoft Azure resource group is located.

6. On the **Network** page:

a. Type a name for the resources. If you typed a connection name, use it as the name for the Resources name.

b. Choose the virtual network for your Microsoft Azure resource group.

c. Select the subnets to use for this connection. If only one subnet exists, it is selected by default.

Step 3: Create a pool of Windows 10 desktops

In preparation for hosting the desktops, install the Citrix Virtual Delivery Agent (VDA) software on the Windows 10 virtual machine. The VDA:

- Enables the machine to register with Virtual Desktops Essentials.
- Establishes and manages the connection between the machine and the user device.
- Verifies that a Citrix license is available for the user or session.
- Applies any configured policies for the session.
- Communicates session information to Virtual Desktops Essentials.

To install the VDA on the base image

1. Start the Windows 10 image.
2. Go to https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html and download a VDA for Desktop OS.
3. Start the VDA installation.
4. On the **Environment** page, click **Create a master image using MCS**.
5. On the **Additional Components** page, select all of the components except **Enable Citrix App-V**.
6. On the **Delivery Controller** page, enter the locations of your Cloud Connector virtual machines. Click **Next** and confirm any warning messages.
7. On the **Features** page, keep the default settings and click **Next**.
8. Click **Next** to accept the default settings on the remaining pages.
9. On the **Summary** page, click **Install**.
10. Restart the virtual machine and sign back in.
11. Confirm that the settings have taken effect.
12. Shut down the virtual machine. Shutting down the virtual machine is required for VDA registration.

Create a Storage Account

In Microsoft Azure, you need a storage account to host the base image virtual hard disk. You can host the drive in an existing storage account or create a storage account.

> IMPORTANT:
>
> Upload the Windows 10 master image to the destination storage account in Azure before you create the machine catalog.

To create a storage account for images

1. In the Microsoft Azure navigation pane, click **Storage accounts**.
2. On the **Storage accounts** page, click **Add**.
3. In **Name**, provide a name.
4. In **Deployment model**, select **Resource manager**.
5. In **Performance**, select **Standard**.
6. For **Replication**, **Storage service encryption**, and **Subscription**, leave the default settings.
7. In **Resource group**, click one of the following:
   a. Click **Create new** to create a resource group. Type the name of the group.
   b. Click **Use existing** to use an existing resource group. Select a group.
8. To have the storage account appear on the dashboard, click **Pin to dashboard**.
9. Click **Create**.

After you create a storage account, create a blob container and then name it to reflect the virtual hard disk, such as "VHDs."

To create a blob container for image VHDs

1. In the Microsoft Azure navigation pane, click **Storage accounts** and navigate to the storage account that you created previously.
2. In the center navigation pane, under **BLOB SERVICE**, click **Containers**.
3. In the details pane, click **Container**.
4. In the **New container** pane, give the container a name.
5. In **Access type**, select **Blob** and then click **Create**. The new blob container appears in the pane.
6. Copy the blob URL and save it in a text file. The URL is used later to upload the converted VHD.

Create a machine catalog for Citrix Virtual Desktops Essentials

Machine catalogs are collections of virtual desktops that you manage as a single entity. These virtual desktops are the resources you provide to your users. All the machines in a catalog have the same operating system and the same VDA installed.

Typically, you create a master image and use it to create identical virtual machines in the catalog.

1. Sign in to Citrix Cloud. In the upper left menu, select **My Services > Virtual Apps and Desktops**.
2. Select the **Manage** tab.
3. Click **Machine Catalogs** in the Studio navigation pane.
4. Click **Create Machine catalog** in the Actions pane.
5. On the **Operating System** page, Desktop OS is the only option available. Select it and then click **Next**.
6. On the **Desktop Experience** page:
   a. Select **I want users to connect to the same (static) desktop each time they log on**.
   b. Select **Yes, create a dedicated virtual machine and save changes on the local disk**.
7. On the **Master Image** page:

   a. Navigate to and select the VHD in the blob storage you created previously. The structure of the navigation tree aligns with the Azure hierarchy:

      - Resource group
      - Storage accounts
      - Containers
      - Virtual hard disks (VHDs)
      - Image names

   b. Keep the default selection in **Select the minimum functional level for this catalog**.

8. On the **Storage and License Types** page, select the destination storage type and your license preference.
9. On the **Virtual Machines** page, select the number of virtual machines and the Azure virtual machine size.
10. On the **Network Interface Cards** page, select a network adapter to associate with the Azure subnet name for your Citrix machines. You can also click **Add Card** to add another network adapter.
11. On the **Computer Accounts** page:

    a. Click **Create new Active Directory accounts**.

    b. Choose the domain for the computer accounts.

    c. Navigate to the organizational unit (OU) for the new machines.

    d. Type an account naming scheme for the new machines. Include two number signs (##) to increment numbers automatically. Select number or letters. The pound signs translate to the naming scheme. For example, mymachcatalog## becomes mymachcatalog01 or mymachcatalogAB.

12. On the **Domain Credentials** page, click **Enter Credentials** and then in the **Windows Security** dialog box, type your user name and password. This account is used to create the computer accounts.
13. On the **Summary** page, type a name for the catalog and a description for administrators.
14. Click **Finish**.

The virtual machines are created and a new storage account appears in the Microsoft Azure dashboard. While Machine Catalog Services deploys the virtual machines, a preparation virtual machine with a VHD is created temporarily in Azure.

To identify the image name in Microsoft Azure

1. Sign in to the Azure portal.
2. In the Dashboard navigation pane, click **All resources**. A list of subscriptions appears.
3. Choose the subscription.
4. Click **All settings**.
5. Click **Resource groups**.
6. Select the resource group.
7. Select the Windows 10 virtual machine that contains the Citrix VDA.
8. Click **All settings**.
9. Click **Disks**.

10. Select the OS disk. The first text box in the OS disk window contains the URL for the image, which is structured as shown in the following example. You can obtain the storage account name and image name from the URL. For example: `https://<storage account name>.blob.core.window.net/vhds/<image name>`.

11. On the **Machines** page, the templates listed are retrieved directly from your Azure subscription.

Step 4: Assign Windows 10 desktops to your users

A Delivery Group is a collection of machines selected from one or more machine catalogs. The Delivery Group specifies which users can use those machines.

1. Select **Delivery Groups** in the Studio navigation pane and then select **Create Delivery Group** in the Actions pane.

2. Specify how many machines that you want to make available to the Delivery Group. The number you specify cannot exceed the number of available machines in your machine catalog.

3. On the **Delivery Type** page, choose **Desktops**.

4. On the **Users** page, choose the option to leave user management to Citrix Cloud. Selecting this option allows you to use Citrix Cloud to manage who can access machines in the Delivery Group. (You can also add users through Studio.)

5. On the **Summary** page, provide a name and (optionally) a description for the Delivery Group.

After completing these steps, edit the delivery group to configure access for users. You can add or remove users and change user settings.

Add or remove users in a Delivery Group through Studio

1. Select **Delivery Groups** in the Studio navigation pane.

2. Select a group and then click **Edit Delivery Group** in the Actions pane.

3. On the **Users** page, to add users, click **Add**, and then specify the users you want to add. To remove users, select one or more users and then click **Remove**. You can also select or clear the check box that enables or disables access by unauthenticated users.

4. Click **OK**.

Change user settings in a Delivery Group through Studio

The name of this page can appear as either **User Settings** or **Basic Settings**.

1. Select **Delivery Groups** in the Studio navigation pane.

2. Select a group and then click **Edit Delivery Group** in the Actions pane.

3. On the **User Settings** (or **Basic Settings**) page:

   a. In **Description**, type the text that the workspace displays to users.

   b. Set the time zone to match the Azure time zone.

   c. Select **Enable Delivery Group**.

   d. Set the maximum number of desktops per user.

4. Click **OK** to save settings.

Add user access through the Citrix Cloud

1. Sign in to Citrix Cloud and then click **View Library**.

2. On the desktops tile, click ellipsis (...) in the right corner.

3. Search for the users groups that are allowed access to the Delivery Group and add them to the list.

4. When finished, click the **X** to close the window.

Your Windows 10 virtual desktops are assigned to the groups added to the subscribers list.

Step 5: Configure Citrix ADC VPX in Azure (optional)

The Citrix ADC VPX virtual appliance is available as an image in the Microsoft Azure Marketplace. When you deploy Citrix ADC VPX on Microsoft Azure Resource Manager, you can use the Azure cloud computing capabilities. You can use Citrix Gateway load balancing and traffic management features for your business needs.

You can deploy Citrix ADC VPX instances on Azure Resource Manager in one of two ways:

- A standalone instance.
- A high availability pair in active-active or active-standby modes.

If you have users who connect from a remote location, configure Citrix ADC VPX in Azure to create secure connections between Citrix Workspace app and Windows 10 desktops.

When the deployment is complete, use the Remote Desktop Protocol (RDP) to connect to one of the Cloud Connector machines. When you connect, you continue to the Citrix ADC VPX configuration from the Citrix Gateway administration console.

For complete configuration information, see Deploying Citrix ADC VPX instance on Microsoft Azure.

After you configure Citrix ADC VPX in Azure, enable Citrix Gateway in Citrix Cloud.

To configure the Citrix Gateway settings for secure access

1. Log on to the management console using the Citrix Gateway administrator credentials. You do not need to configure more IP addresses. Click **Skip**.

2. In **Host Name**, **DNS IP Address**, and **Time Zone**, use the IP address and the DNS settings of the virtual network. The settings are on your Active Directory domain controller.

3. Click **Done**. You do not have to restart Citrix ADC VPX now.

4. On the Configuration tab, click **Licenses** and upload the necessary licenses to configure Citrix Gateway.

5. After the licenses upload, restart the appliance.

6. When the virtual machine restarts, log on again by using Citrix Gateway credentials.

Configure Citrix Virtual Desktops Essentials settings in Citrix Gateway

After you configure the previous settings, run the Quick Configuration Wizard in Citrix Gateway. For more information, see Configuring Settings with the Quick Configuration Wizard.

Configure Citrix Gateway for high availability and load balancing

In a Microsoft Azure deployment, a high availability configuration of two Citrix Gateway virtual machines is achieved by using the Azure load balancer. The load balancer distributes client traffic across the virtual servers configured on both the Citrix Gateway instances.

If the client traffic originates from the internet, deploy an external load balancer between the internet and the Citrix Gateway instances to distribute client traffic. For more information about this configuration, see Configure a high-availability setup with a single IP address and a single NIC.

You can also add inbound port 80 to the Citrix Gateway network security group to configure Citrix Gateway by using its public IP address. After the configuration is complete, you can delete the inbound port 80 rule to secure access to the management console.

Step 6: Connect users

Citrix Workspace delivers the service to user devices. In the Citrix Cloud console, select **Workspace Configuration** from the upper left menu.

After you create the first catalog, Virtual Desktops Essentials configures the workspace URL automatically. This URL appears under the catalog details. You can customize the workspace URL and the appearance of workspaces. You can also enable the preview version of federated authentication using Azure Active Directory. For details, see Workspace configuration.

1. In the Citrix Cloud console, select **Workspace Configuration** in the upper left menu. Select the **Service Integrations** tab. The service is listed.

2. Test your connection by logging on to the workspace URL with your domain credentials and starting a desktop.

3. Provide the URL to your users, which they can copy. Users can type or paste that URL in the address bar of their browser or Citrix Workspace app to access desktops.

Remote access using Citrix ADC VPX

1. In the Citrix Cloud console, click **Manage** and then click **Service Delivery**.

2. Enable **Citrix Gateway**.

3. Select **Use your own Citrix Gateway** in the resource location.

4. Type the Citrix Gateway address in the text field. Do not include a protocol. You can include a port number.

5. Enable session reliability, if you want that feature.

6. Save.

7. Test your connection by logging on to the workspace URL with your domain credentials and starting a desktop.

8. Provide the URL to your users, which they can copy. Users can type or paste the URL in the address bar of their browser or Citrix Workspace app to access desktops.

Partner resources

This service is also available through the Microsoft Cloud Solution Provider channel. For details, see Microsoft CSP enablement for Citrix Essentials.