Citrix Virtual Delivery Agent for macOS

Contents

Citrix Virtual Delivery Agent for macOS

March 28, 2024

> **Important:**
>
> Public Tech Preview is a process to provide our Customer and Partners with Early Access to new features and capabilities, so Citrix/CSG can collect feedback to shape the final product. It's a collaborative effort that involves multiple functional units between Customer/Partner and Citrix/CSG, and we may not be able to address all the support needs manifested from the evaluation period in a timely manner, meanwhile, the "Public Tech Preview Product"(refer as "Product"in the following context) is not recommended to be used in a full-scale production environment (Refer the Overview and Limitation section for more information), nor be used beyond the Tech Preview trial window, otherwise Citrix/CSG will not bear any obligations for error or data lost if the Product will be used in those conditions.

Citrix Virtual Delivery Agent for macOS (Citrix VDA for macOS) enables HDX access to macOS Remote desktop anywhere from any device where the Citrix Workspace App is installed.

To use Citrix VDA for macOS and deliver the desktops accordingly is a simple process:

- Install the VDA on Mac devices that meet the System Requirements by using either the Installer provided or your favorite MDM interface.
- Configure the delivery group through the DaaS management console, apply DDC Policies and related configurations.
- Then again use the DaaS management console to make the macOS desktop available to your end user through Workspace/StoreFront - then both your end user and IT department are ready to go.

Citrix VDA for macOS is designed and engineered as "yet another VDA"backed by Citrix industry leading HDX technologies within the DaaS/CVAD product family, it adheres to the existing Citrix product architecture and follows all the common roadmap of HDX features and all interfaces defined between key components in DaaS/CVAD - this is to ensure that our customers existing knowledge and experience can be reused fully in this new VDA.

The product had gone through Private Tech Preview in the past months with selective NDA customers and partners in different verticals and received good feedback and suggestions for new features and improvements - with all these inputs together our continued execution on the HDX feature roadmap, these are the capabilities you now see in the Public Tech Preview. Similarly, the primary goal of this preview is to have your feedback so we can continue work on both features and quality to ensure an upcoming successful GA - any suggestions and feature needs are welcome! For this Preview, install and configure the VDA and related components, DDC policies as exactly as possible indicated in the following sections in:

- System Requirements
- Installation
- Limitation
- Known Issues
- Policy Support List

Otherwise we can not guarantee all features work, or may not be able to provide related support.

If you want a quick start, simply check the "System Requirements"and "Installation"parts in this document and you shall be able to use Citrix VDA for macOS right away, but we still recommend you come back later to read other sections in the documentation.

Third party notices

April 18, 2024

This release of Citrix VDA for macOS includes third party software licensed under the terms defined in the document Third Party Notice for Citrix VDA for macOS (PDF Download)

Mac VDA Public Tech Preview EAR EULA

March 19, 2024

This release of Citrix VDA for macOS includes the Early Access Release EULA defined in the document EAR EULA (PDF Download)

Citrix VDA for macOS Overview

April 16, 2024

This Public Tech Preview product supports all major functionalities & key elements in the HDX/ICA stack and integrates seamlessly with the DaaS management plane, extra capabilities has been developed with input from the Private Tech Preview program and the product has been optimized for Apple Silicon chip families. We divided major functionalities into follow categories as a quick introduction, refer to the respective sections in this document for more details.

HDX Features:

- Graphics / Keyboard / Mouse
- Clipboard
- Audio
- CGP / SR / ACR
- TCP / EDT (EDT is enabled by default)
- Secure user sessions using DTLS / TLS through NetScaler Gateway or Citrix Gateway Service (enabled by default)
- Adaptive Graphics / Selective H.264 (enabled by default)
- Adaptive Throughput (enabled by default)
- Multi-monitors
- High DPI
- Multiple client audio redirection support
- V4 Reducer
- MTU Discovery
- Dynamic Keyboard Layout Sync
- Citrix Workspace App ipadOS, iOS and Android Support

Management plane functionalities:

- DDC Policies
- NDJ (Non-domain joined) VDA
- Rendezvous V2 (both TCP and EDT)
- DaaS management console integration
- VDA Installer
- Proxy configuration through PAC support

Mac specific capability support:

- Apple Silicon native support & optimization
- macOS Fast User Switching support
- Trackpad experience

Supportability:

- Logging and Log Enhancement
- xdlcollect
- ctxsession
- vdaversion
- App Center Crash Report
- Log on Performance and ICA RTT Data in DaaS Monitor

What's New

March 28, 2024

This Public Tech Preview is the second release of the Citrix Virtual Delivery Agent for macOS where the first Private Tech Preview that we had conducted with selective NDA customers and partners in the past several months - the feedback, and planned feature roadmap and improvement comprised the additional content compare to Private Tech Preview:

- Support complex network environment and configuration, such as system proxy server configured by PAC; integration and guide for deployment of VDA in scale using UEM/MDM tool; DDC policy parsing optimization and more policy support
- Key features execution in the HDX roadmap: For example selective H.264; advanced keyboard-/IME capabilities; latest audio feature: multiple audio devices redirection.
- Expanded CWA (Citrix Workspace App) integration: connect from iPad, iPhone and Android are fully supported; More capabilities supported in DaaS for better VDA management and monitoring.
- Enhanced supportability: For example, AppCenter crash report support; improved logging; and many improvements for limitations in Private Tech Preview and more.

System Requirements

April 18, 2024

System requirements of Citrix VDA for macOS contain both hardware and software aspects, as the main delivery model is Remote PC Access that is based on physical Mac devices and the product has been optimized specifically for Apple Silicon, hence the underlying devices have to be within the Apple product families listed below.

To ensure access the VDA from different platforms and be managed as other VDA types, both CWA (Citrix Workspace App) and DaaS version requirement have been specified below.

Supported Hardware Platforms

Apple Silicon (M1, M2, and M3 families) based macOS devices:

- Mac mini
- MacBook Air or MacBook Pro
- iMac

- Mac Studio
- Mac Pro

> **Note :**
>
> Intel CPU based Mac devices are not supported.

Supported macOS Versions

This Public Tech Preview product support the two latest versions of macOS.

macOS Name	macOS version
Venture	13.*
Sonoma	14.*

> **Note:**
>
> Citrix might be limited in its ability to test all the sub-versions under one major macOS revision. Contact us if you need to stay in a certain sub-version.

Network Environment Configuration

- Network configuration generally follows the same requirements as in the Citrix Cloud.
- The VDA machine must have the minimal port 443 open for outbound traffic.
- When EDT is enabled (by default), port 2598 and 1494 must be opened when CWA and VDA are within the same network and you must launch from StoreFront or NetScaler.
- Proxy configurations are supported. The priorities are taken as the following orders:
  - Control traffic (VDA enrollment, registration): VDA registry configuration -> system proxy setting (from PAC configuration and so on)
  - HDX session traffic: group policy -> VDA registry configuration -> system proxy setting (from PAC configuration and so on)

> **Note:**
>
> Currently we recommend enabling only one NIC (Network Interface Card) in the VDA machine

Citrix Management Plane Requirement

- Existing DaaS Subscription, Standard or above; CPL (Citrix Platform License) or UL (Universal License)

> **Note:**
>
> CVAD or Citrix Private Cloud is not supported in this Preview - it is expected upon GA fully support these on-prem management plane.

Citrix Workspace App (recommended)

- Citrix Workspace App 2402 for Windows or later
- Citrix Workspace App 2402 for Linux or later
- Citrix Workspace App 2402 for Mac or later
- Citrix Workspace App 2403 for ipadOS/iOS
- Citrix Workspace App 2403 for Android

Additional runtime libraries needed

- Microsoft .NET 6.0 (.NET 8.0 support is planned for GA) macOS ARM64 build - refer Installation part for details

Installation Overview

April 16, 2024

Installation of Citrix VDA for macOS has never been so easy, you can either do it from the all-in-one installer we provided or use UEM/MDM (Unified Endpoint Management/Mobile Device Management) software to do so. This section guides you through both methods, the UEM/MDM part, we're using Jamf PRO as an example. There are other ways to use Jamf PRO or other UEM software that can achieve similar results as such.

This section guides you through the following procedures:

- Prepare Installation using Non-domain Joined VDA
- Use the Installer for VDA Deployment
- VDA Deployment Recommendation
- Example Using UEM/MDM

Prepare Installation Non-Domain joined VDAs

April 16, 2024

This section guides you to prepare for installation in the DaaS management console for creating non-domain joined (NDJ) Citrix VDA for macOS.

Non-Domain Joined (NDJ) Citrix VDAs obliterate the need to join VDAs to Active Directory domains for VDA and user authentication.

When you create a non-domain joined VDA, we use secure public-private key-pairs for registering the VDA to the DaaS control plane.

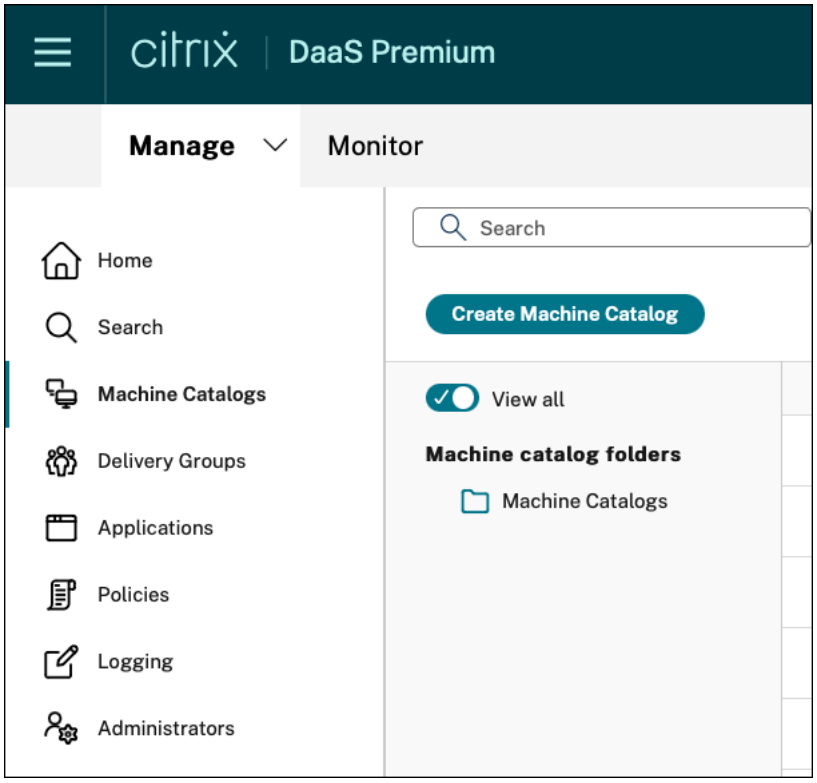
Thus, to join an Active Directory domain is no longer required.

> **Important:**
>
> - Non-domain-joined VDAs are supported for Citrix DaaS.
>   - For this public tech preview, your control plane must be deployed over Citrix DaaS.
>   - You can deploy non-domain joined VDAs in a macOS hosting provider's environment or your on-premises environment such as a data center or your end user's machine for them to perform a remote access from home and so on.
>   - Non-domain-joined VDAs are managed by the control plane in the Citrix DaaS.
>   - The Non-domain-joined VDA is connected to the Citrix DaaS control plane through Rendezvous V2 that do not require any Cloud Connector presence, where the corresponding policy for Rendezvous is configured to Rendezvous V2.
>   - To launch the VDA, besides **Workspace** configured by the DaaS control plane, you can also launch the VDA from **StoreFront** or/and **NetScaler with Cloud Connector point to the Cloud Tenant you register a VDA to**. For more information, see the Citrix DaaS install and configure overview.

Steps to prepare in DaaS management console:

1. Create a **Machine Catalog** for Citrix VDA for macOS which is a common step that you do for both **Windows** and **Linux VDA**.

   > **Note:**
   >
   > Citrix VDA for macOS currently only supports as a single session or a remote PC machine catalog.

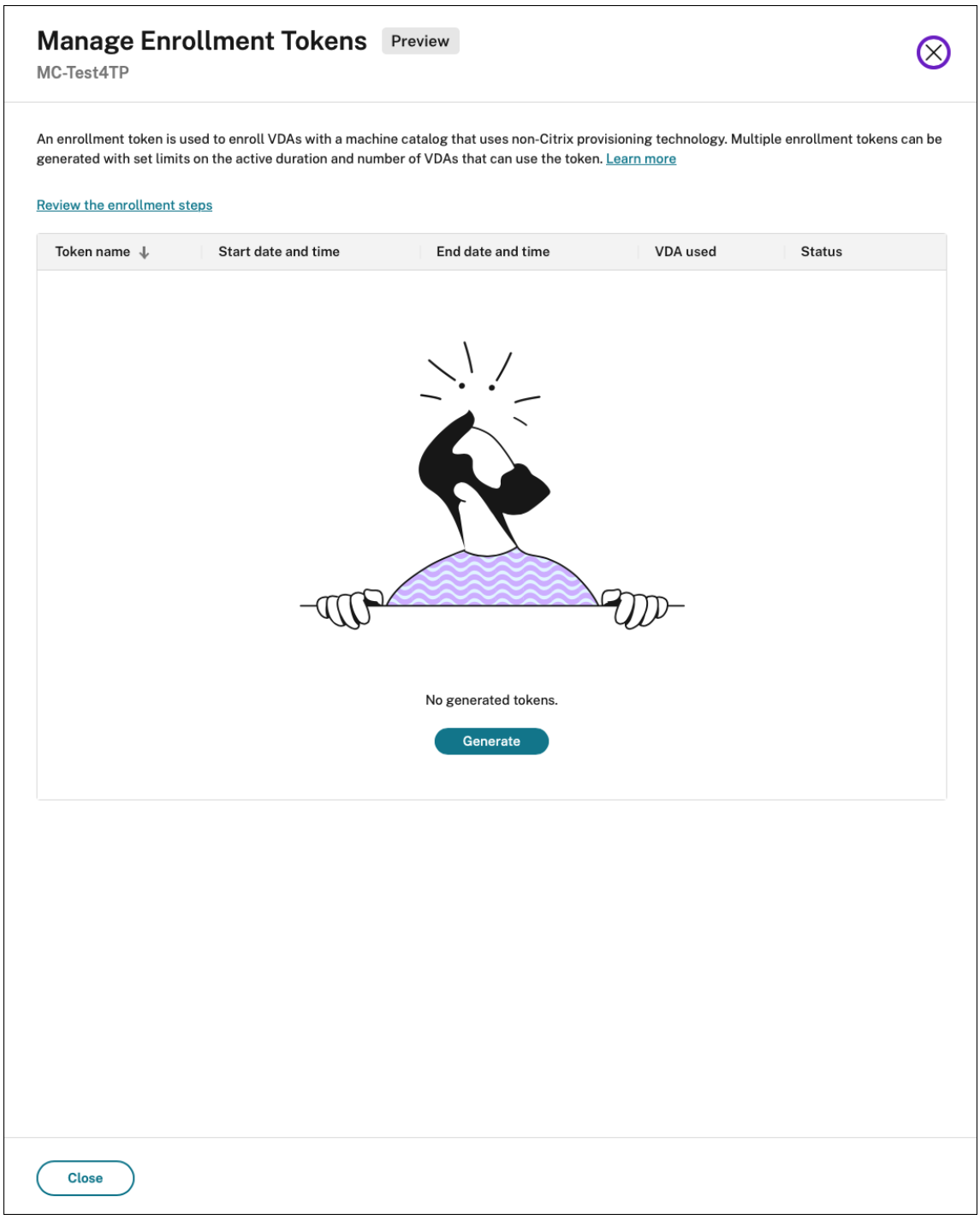


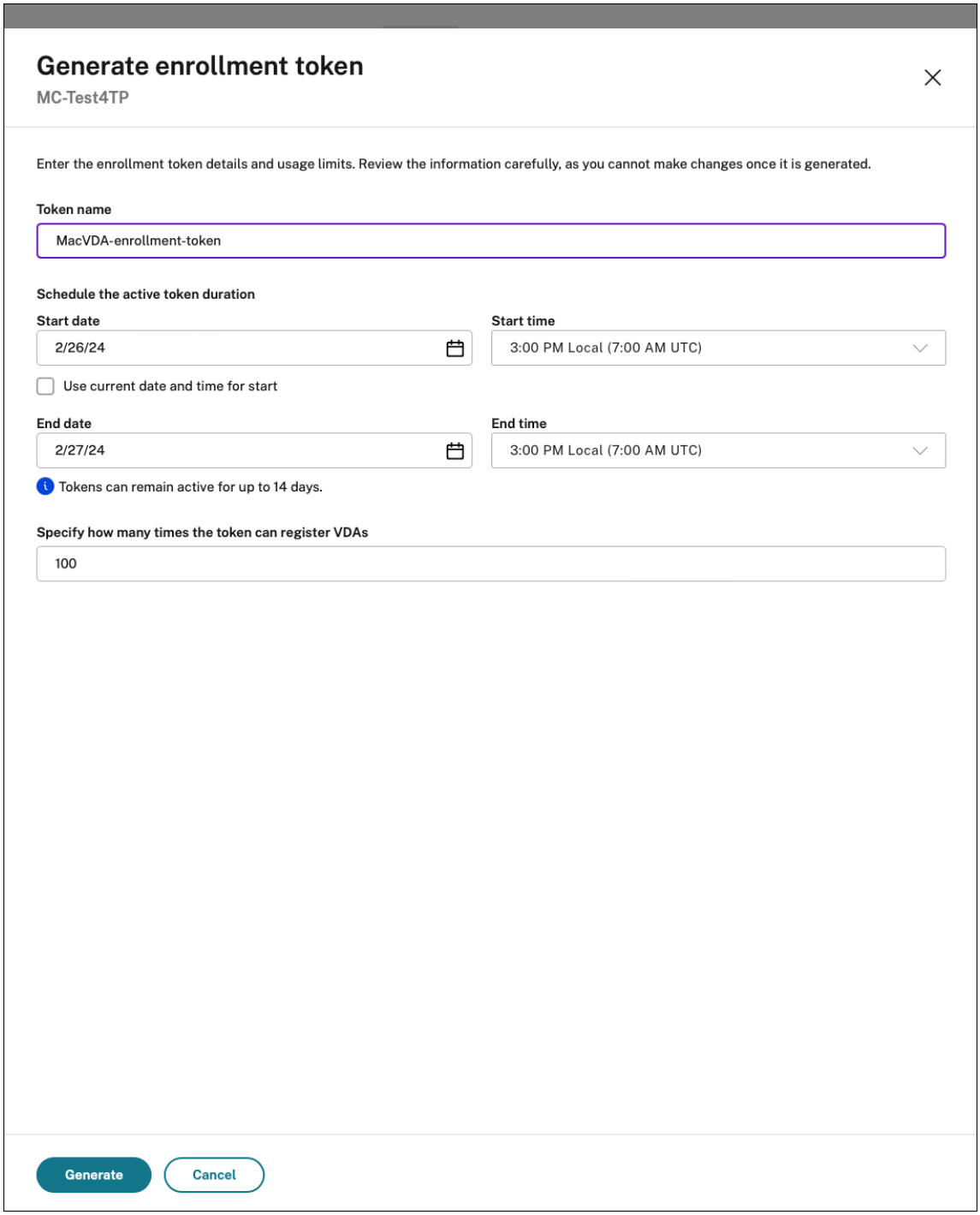
Make sure the configuration is similar to the screenshot provided.

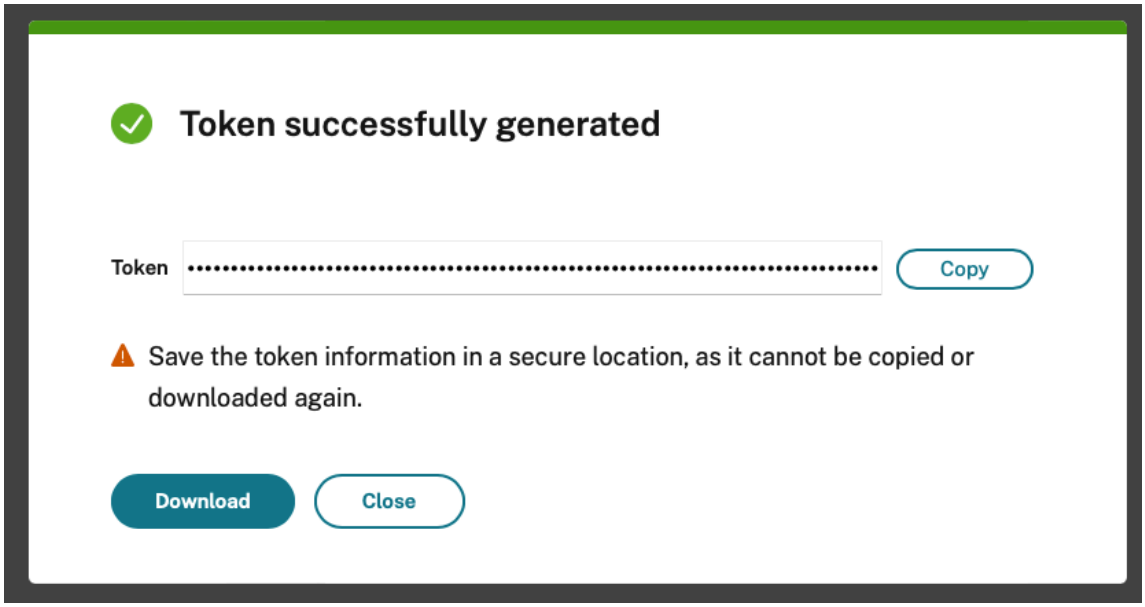
2. Generate an enrollment token for the VDA using **Manage Enrollment Token (preview).**

   In this step, you generate an enrollment token that can be reused by different VDA machines to be enrolled towards the DaaS Cloud tenant that you're performing the operation on.

   For more details of this new feature see Generate and Manage Enrollment Tokens







> **Note:**
>
> Select the **Use current date and time for start** checkbox if you want to use the enrollment token immediately.

3. Use the enrollment token (generated as part of Step 1 and Step 2) to perform VDA installation and enrollment, and come back to the **DaaS management console** to validate if the VDA has changed from **Initialization State** to **Registered**.
4. Create a **Delivery Group** for your end user with machine/desktop assigned according to common steps. For more information, see, Create Delivery Groups.
5. After you install and configure **Citrix DaaS**, you will get a workspace URL link.

   The workspace URL is posted in two places:

   - From the Citrix Cloud console, select **Workspace Configuration** from the menu in the upper left corner. The **Access** tab contains the Workspace URL.
   - From the **Citrix DaaS Welcome** page, the workspace URL appears at the bottom of the page.

   For more information, see Delivering applications and desktops to users
6. **[Optional]** Configure Rendevous V2 under the **policy** section in your DaaS environment.

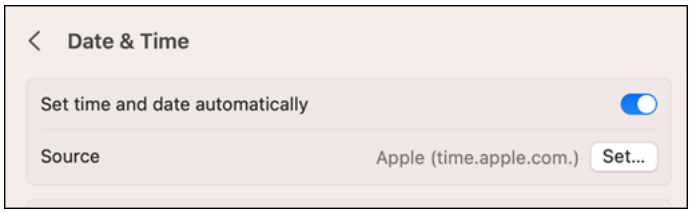
> **Note :**
>
> - Test and then share the workspace URL link with your subscribers (users) to give them access to their apps and desktops.

- Your subscribers can access the workspace URL without any additional configuration.

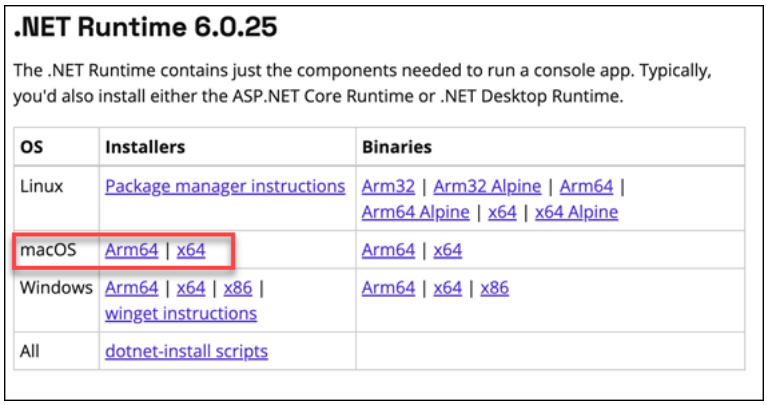
Using Installer of Citrix VDA for macOS

April 16, 2024

1. Before installation, make sure the system time is synced via Apple NTP server.



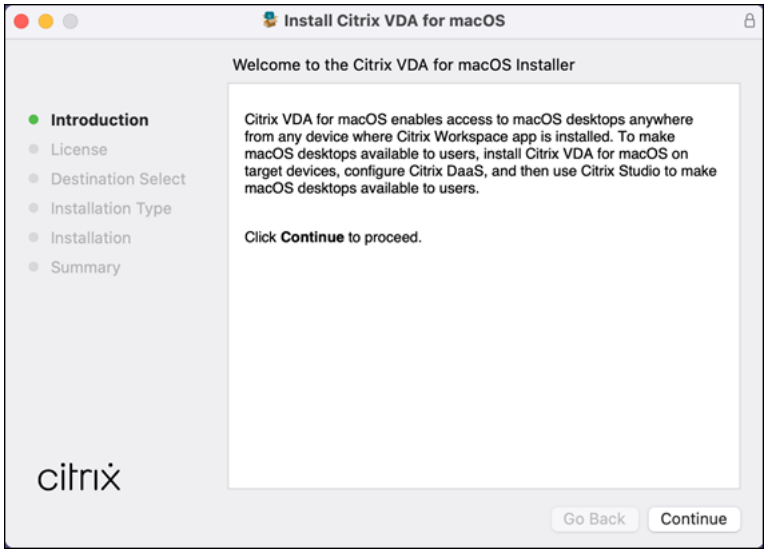
2. Download **.Net 6.0** from https://dotnet.microsoft.com/en-us/download/dotnet/6.0
3. Install the **Arm64 .Net Runtime** package for macOS and check the installation directory path using command `which dotnet`.



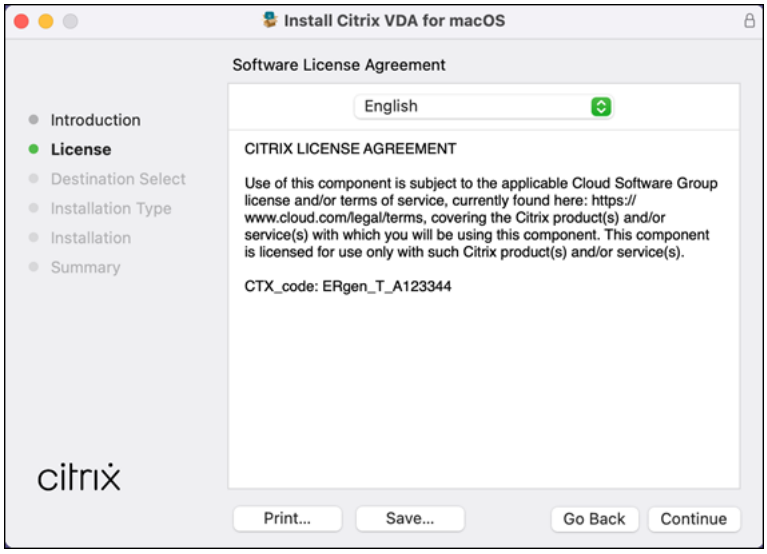
4. Double click the **Citrix VDA for macOS installer** to begin installation.

   During the initial phase of the pkg installation, it will check whether you have already installed .NET, and if your macOS version is compatible.

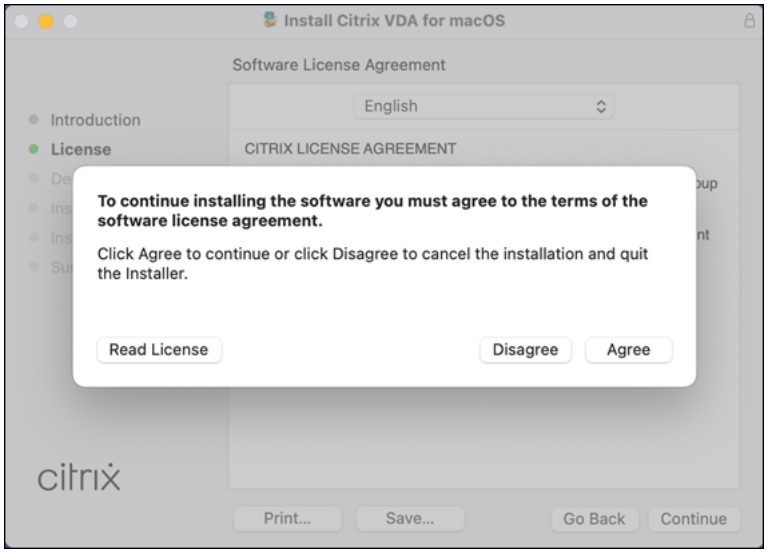
5. Click **Continue** to continue installation.



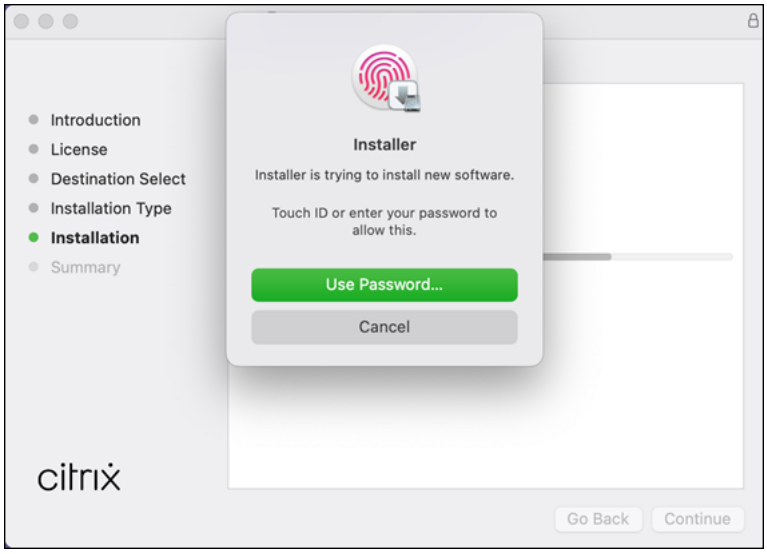
6. Click **Continue** to proceed to the license agreement page..



7. Read and Click **Agree** to continue. If you disagree, the installation process aborts.



8. You must have administrator credentials to enable installation and the related services, by either typing admin password or enable through fingerprint as below shown:

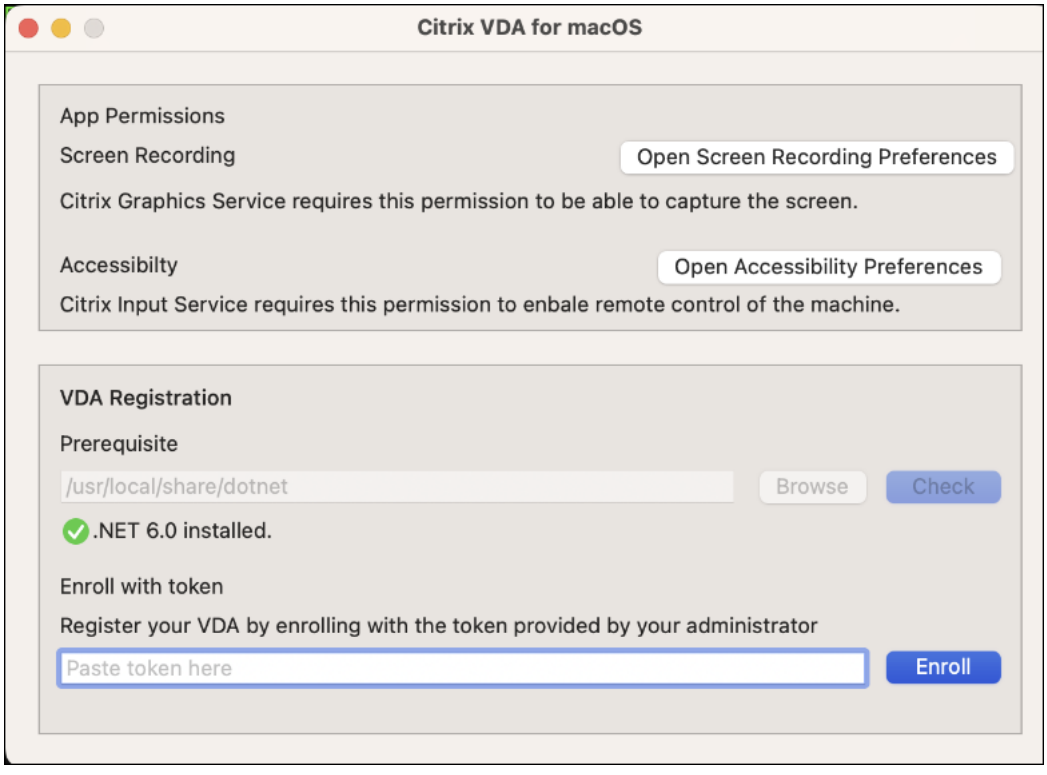


9. Choose the required option on **vdaconfig** UI and perform actions as described below.

   - Click **Open Screen Recording Preference** to enable **Citrix Graphics Service**

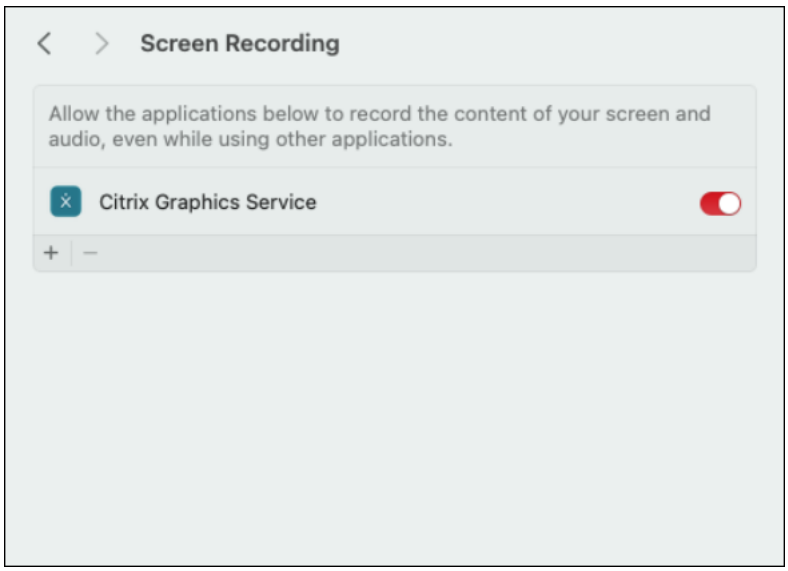
     AND

   - Click **Open Accessibility Preferences** to enable **Citrix Input Service**

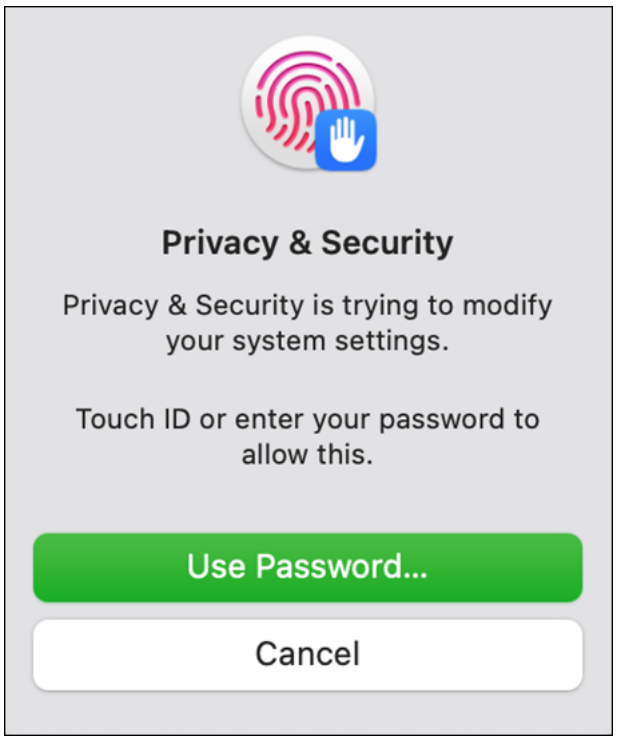


> **Note :**
>
> For first time installation, you can also enable **Citrix Graphics Service** through the system

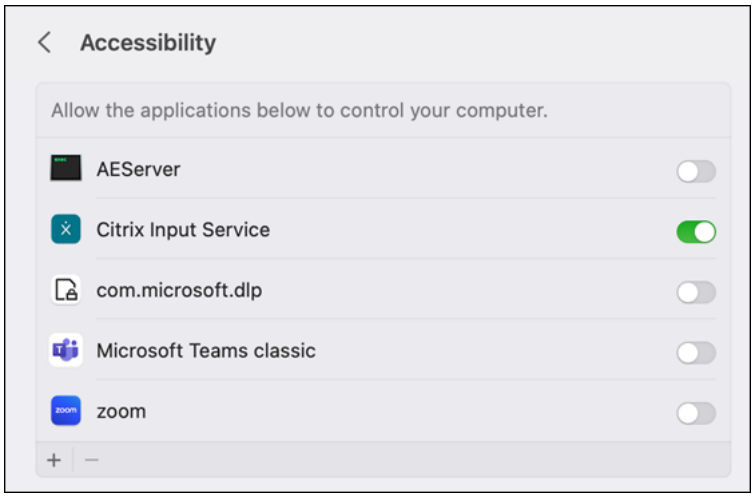
> pop-up message box by clicking “Open System Settings”.



10. You must have administrator credential to enable services.



11. Click **Open Accessibility Preference** to enable the “Citrix Input Service”.



12. If you’ve installed an incorrect version of .NET, or if there’s an issue with the .NET installation location, you’ll be prompted to enter the correct .NET path during the prerequisite stage.

    a) Click **Browse** to select the .NET installation path, or you can manually input the .NET installation path directly.

    b) Click **Check** to check if the path entered is valid.

    If you encounter any issues, you can try using a command to complete the enrollment process.


```
sudo /opt/Citrix/VDA/bin/ctxreg create -k 'HKLM/\Software/\
Citrix/\VirtualDesktopAgent'-t 'REG_SZ'-v 'DotNetRuntimePath'
-d '<dotnet path>'--force && launchctl kickstart -kp system/
com.citrix.ctxvda
```

This process requires administrator privileges.

13. If your .NET installation is correct, we'll proceed to the enrollment stage.

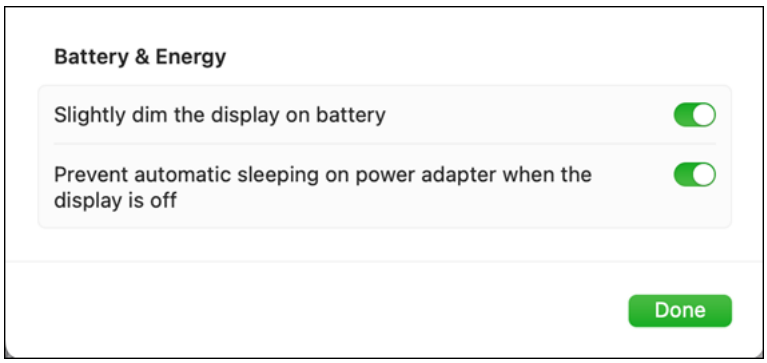
    a) Copy and paste the token provided by the administrator in the Prepare Installation Non-Domain joined VDAs and click **enroll** to enroll and register the VDA to DaaS management plane.

Generally, this process completes within a few seconds if the network conditions are favorable.

If you encounter any issues, you can try using a command to complete the enrollment process.
`sudo /opt/Citrix/VDA/bin/VdaEnrollmentTool -EnrollmentToken:<token> -Restart`

This process requires administrator privileges.

> **Note :**
>
> If your VDA machine is used solely by remote access after installation, it is recommended to turn on **Prevent automatic sleeping on power adapter when display is off** under the **Battery & Energy** section in your macOS settings like below. If your 1st installation failed or you have an older VDA but you like to enroll it towards a new DDC, please invoke "sudo /opt/Citrix/VDA/bin/vdaconfig"to re-open the vdaconfig tool UI to perform corresponding actions.



VDA Deployment Recommendation

April 16, 2024

If you have the requirements of external remote access to **Citrix VDA for macOS**, but haven't installed any **on-premise NetScaler Gateway** before, you can enable **Citrix Gateway service for external remote access**. See, Citrix Gateway service for more information.

When using the **Citrix Gateway Service**, the Rendezvous protocol policy must be enabled through **Citrix Cloud control plane**. The policy is disabled by default. For more information, see, Rendezvous V2.

Example using UEM / MDM

April 16, 2024

In case of deployment for **Citrix VDA for macOS** in scale, you can use a **UEM (Unified Endpoint Management) or MDM (Mobile Device Management)** tool to assist or automate the whole process.

> **Note:**
>
> Microsoft .NET 6.0 is required before processing the following steps. You may also deploy the .NET package to target devices directly from the Jamf Pro.

General Workflow:

Roles	Responsibilities
IT Admin	• Add the VDA package to JamfPro • Add a policy to install the package and run the script on the target devices • Add a script to enroll the VDAs to Citrix DaaS • Add a configuration profile to configure the privacy permissions for VDA
End User	• Enable the screen recording permission for VDA locally or remotely • Create delivery groups and assign the desktops to users from Citrix DaaS • Sign in to the Citrix workspace and launch sessions

In this section, we use **Jamf PRO** as an example to provide a possible workflow and steps that you could reference.

Key steps include

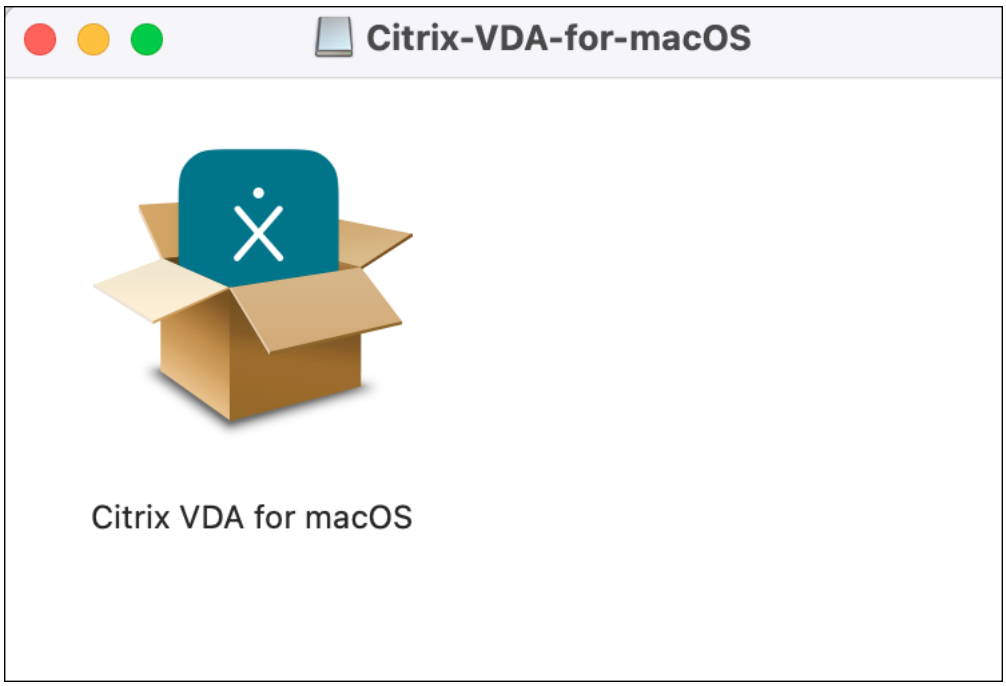
Section 1 - Deploy the virtual delivery agent for macOS package

This section describes the steps to install the virtual delivery agent for macOS on Mac devices and enroll the devices to the Citrix DaaS.

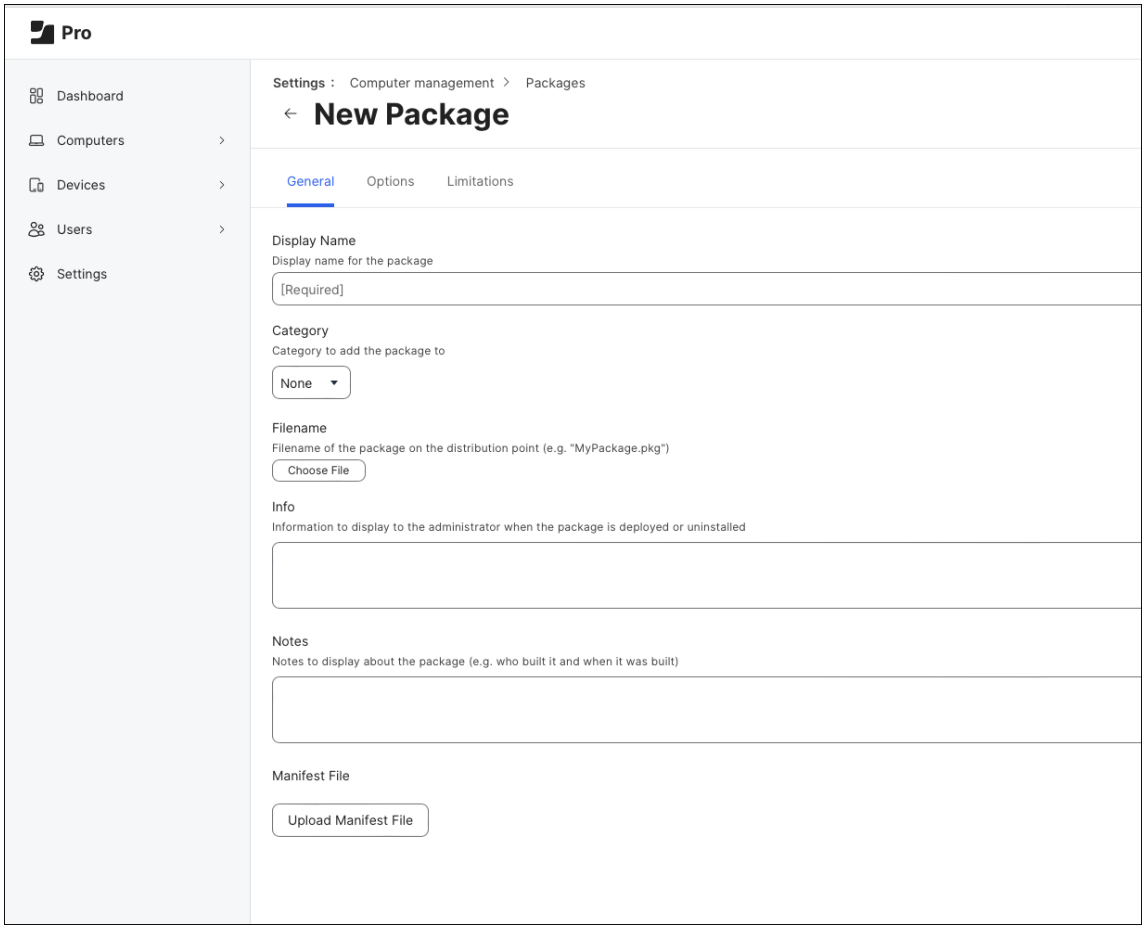
Add the package for virtual delivery agent for macOS:

1. Double click the **Apple Disk Image** (.dmg) file provided by **Citrix**.
2. Copy the package file **Citrix VDA for macOS.pkg** in it to another location.

> **Note:**
>
> We will upload this file to the Jamf Pro console later.



3. Login to the **Jamf Pro** console, and navigate to **Settings** -> **Computer management** -> **Packages**.
4. Click **New** to add a new package.
5. Enter a display name for the package and upload the package file copied in step 1.



6. **Save** the package.

Add a script to enroll the Mac devices to Citrix DaaS:

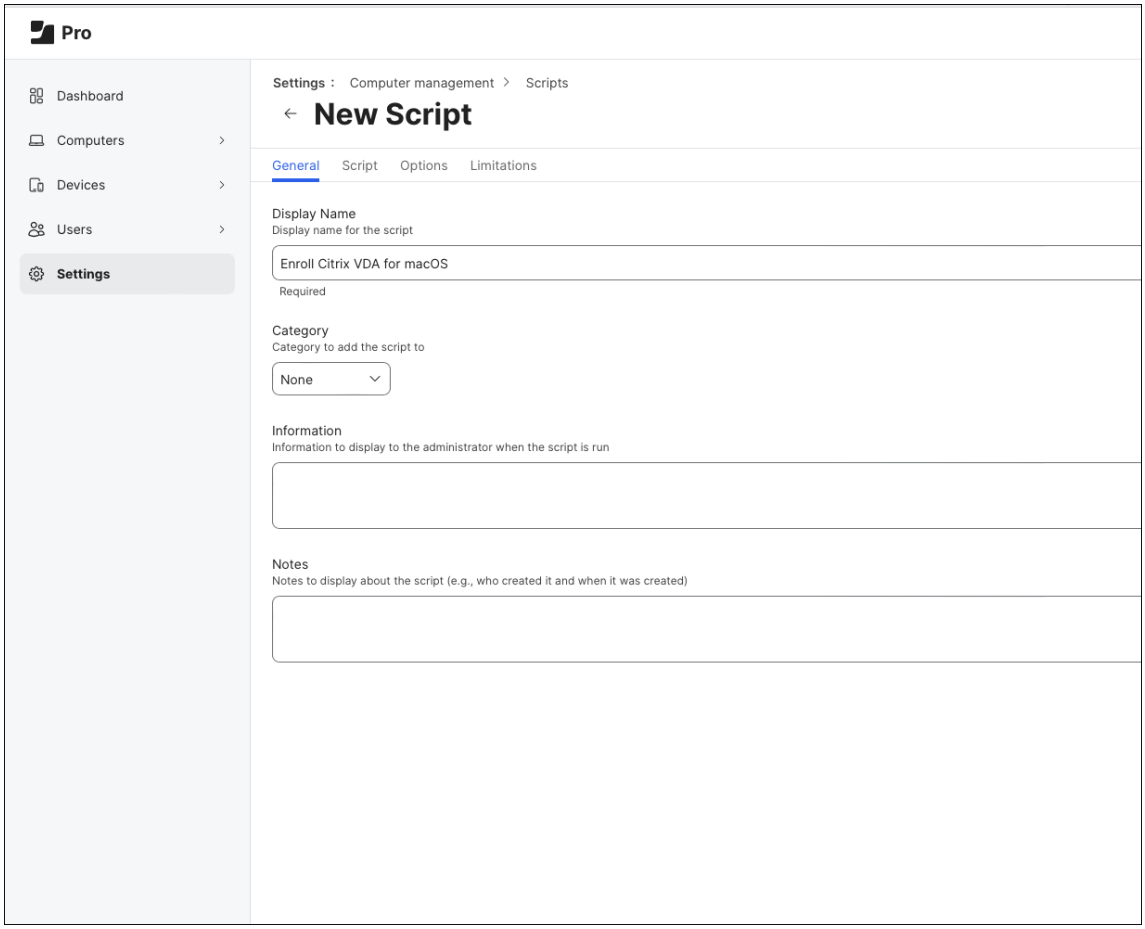
1. Login to the **Jamf Pro** console, and navigate to **Settings** -> **Computer management** -> **Scripts**.
2. Click **New** to add a new script.
3. Enter the following fields for the script.

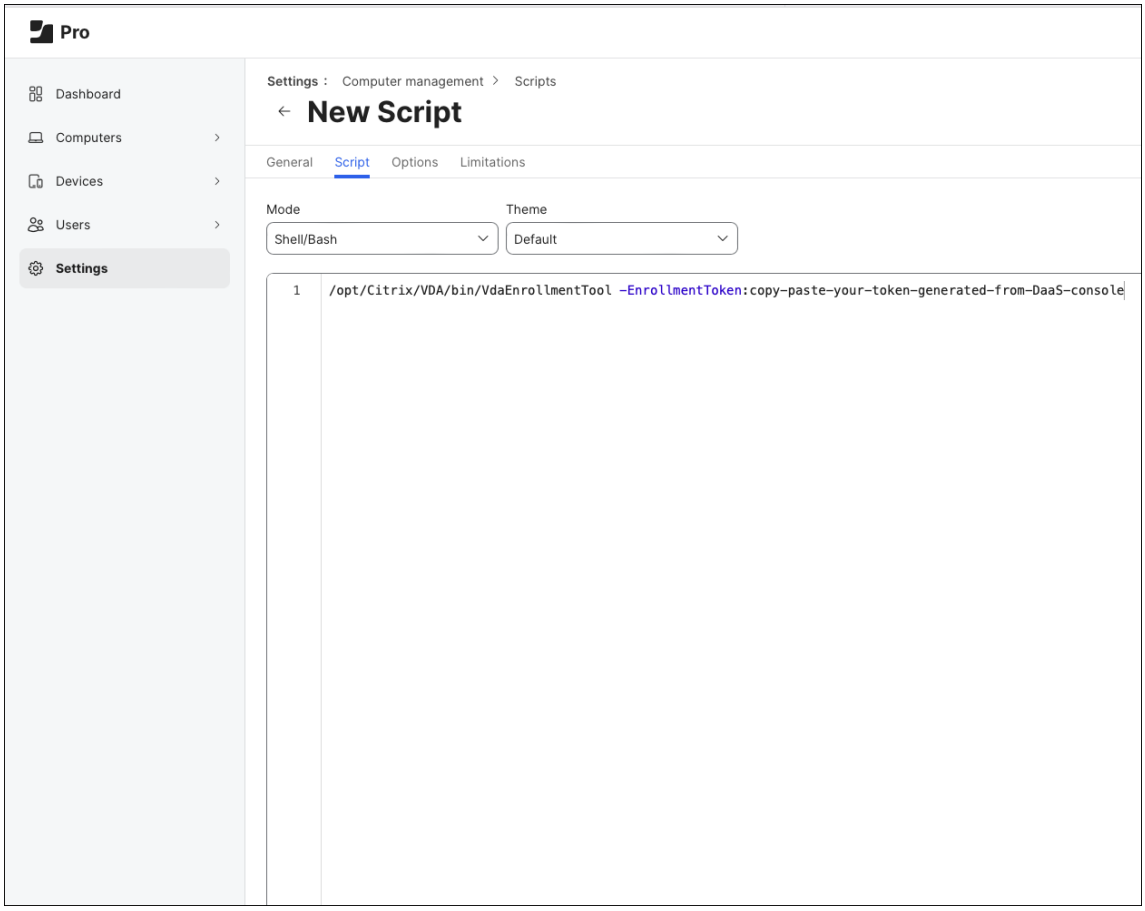
   Leave the other fields with default values or enter values based on your environment.

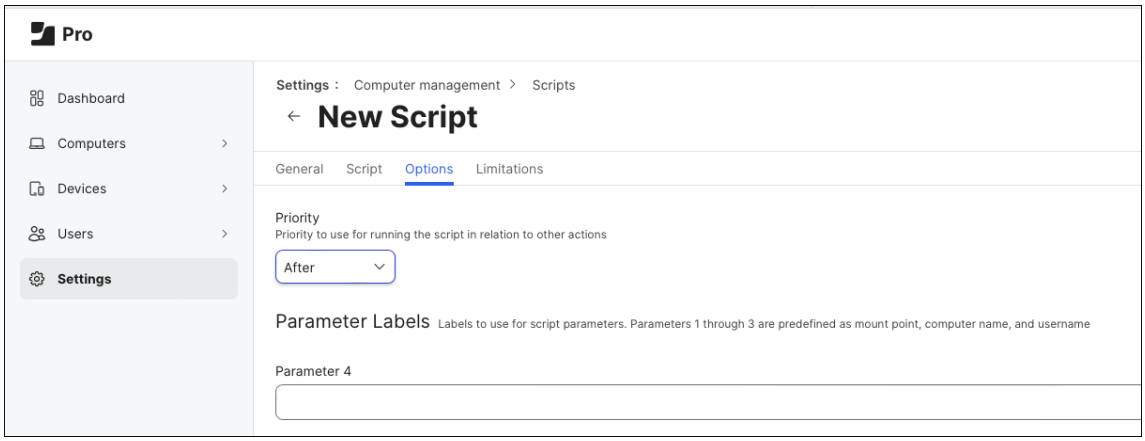
   - **Display Name:** Enroll Mac Devices to Citrix DaaS (you can change this name on your own)
   - **Script:** Select **Shell/Bash** for the mode and enter the following as the content. Replace the enrollment token with your own token in the script that was described in Steps to prepare in DaaS management console

     ```
     /opt/Citrix/VDA/bin/VdaEnrollmentTool -EnrollmentToken:eyJhbGciOiJSUzI
     (use-your-own-enrollment-token-here)-Restart
     ```

   Priority: After





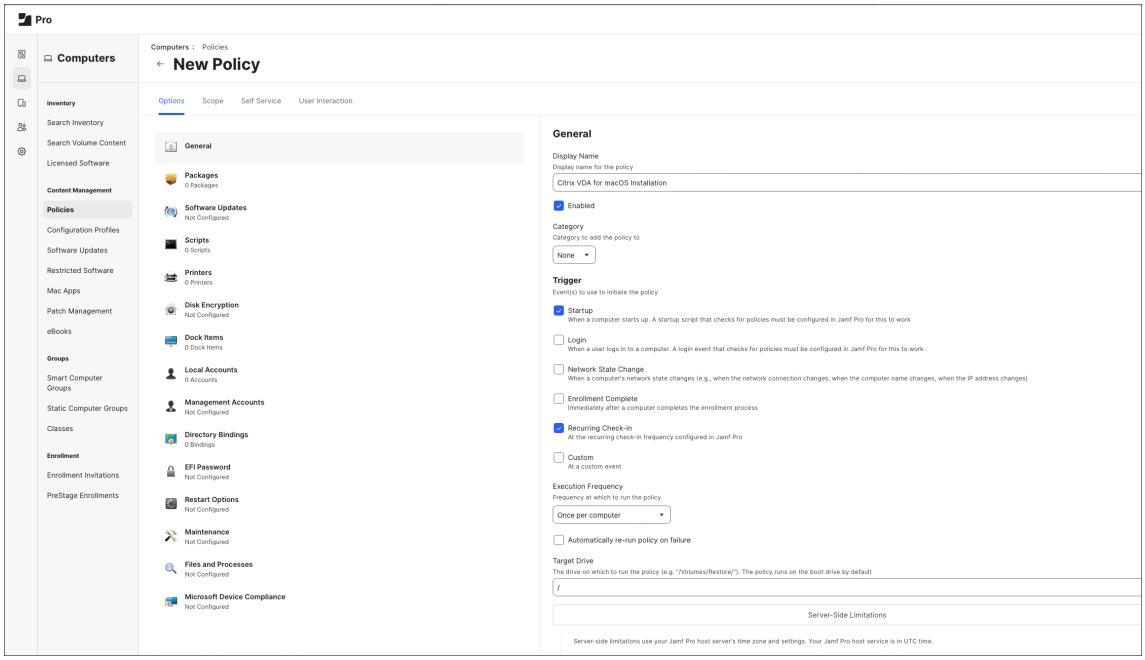


4. **Save** the script.

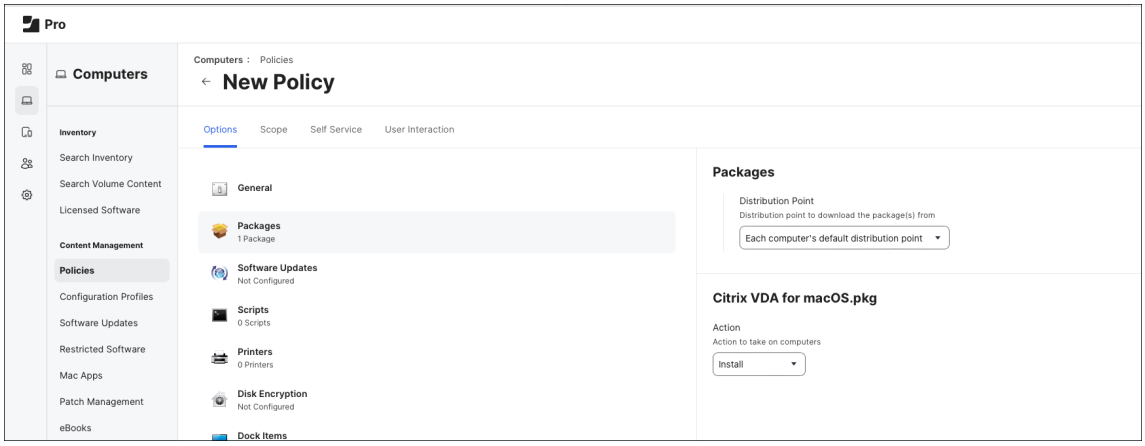
Add a policy to install the package and execute the script:

1. Login to the **Jamf Pro** console, and navigate to **Computers** -> **Policies**.
2. Click **New** to add a new policy.
3. Enter the following fields for the General part.
    - **Display Name:** Install VDA for macOS (you can change this name on your own)

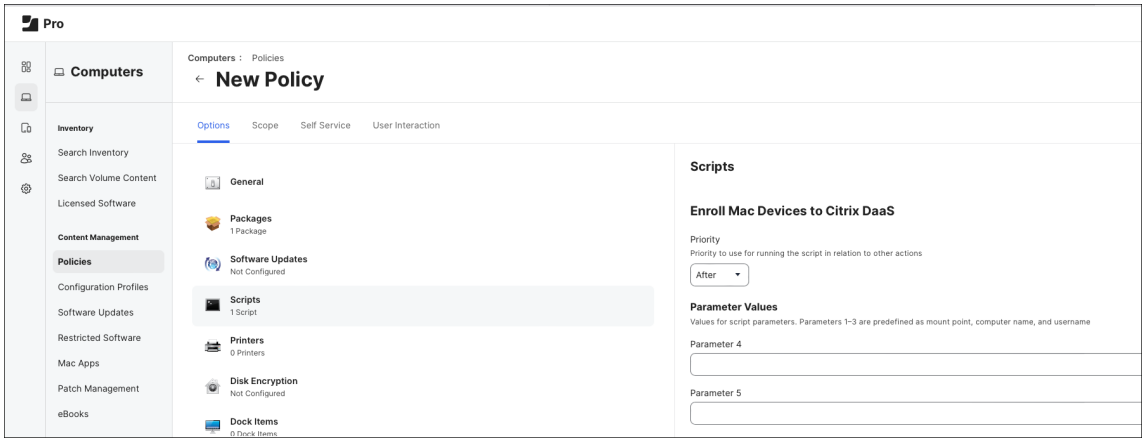
- **Trigger:** Enter required details. This guide uses **Recurring Check-in** as the trigger events. Enter values based on your environment.
- **Execution frequency:** Once per computer.



4. Click **Packages**, and add the package we created in the previous steps.
5. Select **Install** for the action to take on computers.



6. Click **Scripts** and add the script we created in the previous steps.
7. Select **After** for the priority.



8. Click the **Scope** tab, and specify the scope for this policy.
9. Click **Save** to save the policy.

   When the policy is pushed to the managed devices, the virtual delivery agent for macOS is installed according to the trigger events you specify for the policy. You can then go to the Citrix DaaS console to view or assign the devices.

Section 2 - Create a Privacy Preferences Policy Control profile

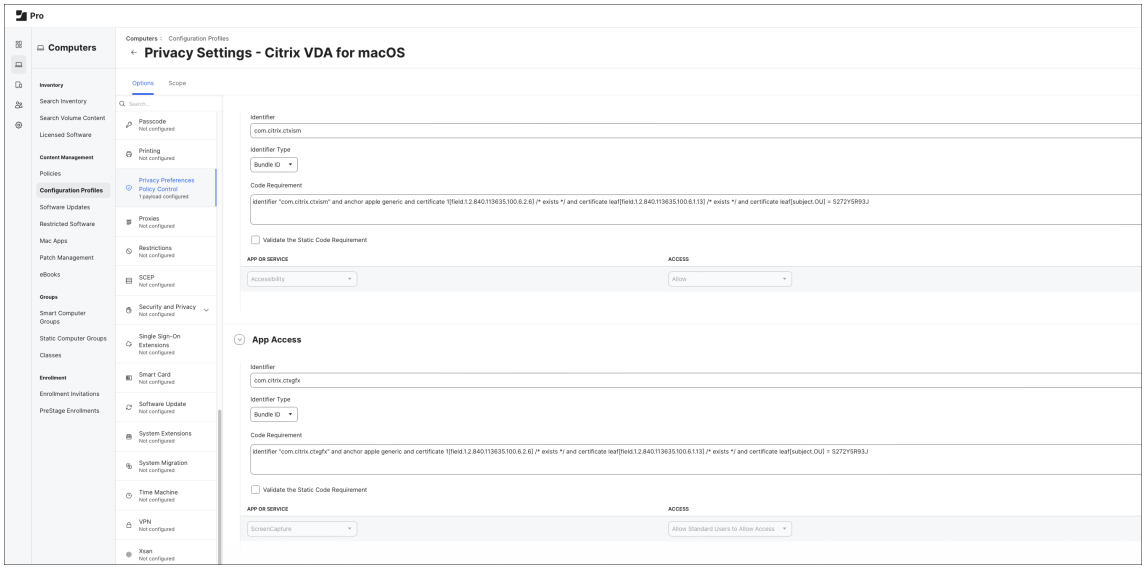
In this section, we will create a PPPC profile for the virtual delivery agent for macOS.

This allows the virtual delivery agent to access Accessibility, and also allows a standard user to allow the virtual delivery agent to access Screen Recordings.

1. Login to the **Jamf Pro** console, and navigate to **Computers** -> **Configuration Profiles**.
2. Click **New** to add a new configuration profile.
3. Enter a display name for the new profile, e.g. **Privacy Settings - Citrix VDA for macOS**.
4. Select **Privacy Preferences Policy Control**.
5. Click **Configure**.
6. Add the following **App Access** configuration:

   - **Identifier:** com.citrix.ctxism
   - **Identifier Type:** Bundle ID
   - **Code Requirement:** identifier "com.citrix.ctxism"and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /*exists*/ and certificate leaf[field.1.2.840.113635.100.6.1.13] /*exists*/ and certificate leaf[subject.OU] = S272Y5R93J
   - **APP or SERVICE:** add a new item and select Accessibility and Allow.

7. Add the following **App Access** configuration.
    - **Identifier:** com.citrix.ctxgfx
    - **Identifier Type:** Bundle ID
    - **Code Requirement:** identifier "com.citrix.ctxism"and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /*exists*/ and certificate leaf[field.1.2.840.113635.100.6.1.13] /*exists*/ and certificate leaf[subject.OU] = S272Y5R93J
    - **APP or SERVICE:** Add a new item and select **ScreenCapture** and A**llow Standard Users to Allow Access**.
8. Specify the scope for the configuration profile on your own needs.
9. **Save** the configuration profile.



After the configuration profile is pushed and installed to the managed devices, the **Accessibility** privacy permission is automatically allowed for the Citrix VDA but for the **Screen Recording** permission, it will still need a standard user to approve before the Citrix VDA can access it.

Section 3 - Allow Screen Recording for Citrix VDA on managed devices

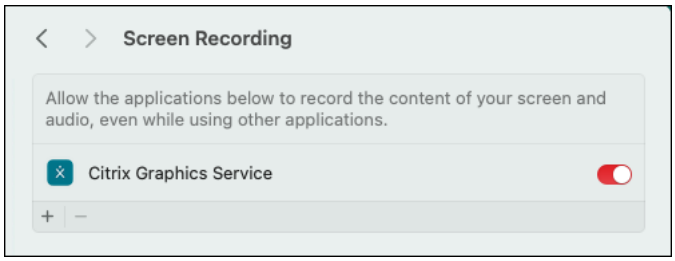
This section describes the steps to allow screen recording for Citrix VDA on the managed devices.

When the configuration profile created in the previous step is installed on the managed devices, the screen recording permission still needs to be allowed manually to make Citrix VDA work.

1. Logon to the target Mac devices using any standard or admin user.

> **Note:**
>
> You may consider enabling remote desktop for the target devices to allow remote access if the target devices cannot be accessed locally.
>
> Check the **Remote Commands** for Computers for more information from the Jamf Pro docs. After this command is performed on a target device, users can then remotely access this device using any VNC clients.

2. Open the **System Settings** app, and navigate to **Privacy & Security**.
3. Click **Screen & System Audio Recording**.
4. Find **Citrix Graphics Service** in the list and **click the toggle** to enable it.



After the permission is properly configured, this target device will be ready for session launches from Citrix Workspace App.

Configuration

November 17, 2023

This section details the features of the VDA for macOS, including feature description, configuration, and troubleshooting.

Administration

April 16, 2024

In this section, we provide details on some common tools that can assist an IT administrator to supervise and diagnose the VDA machine.

We also provide some guideline regarding HDX session management and its relationship with local user account.

Log Collection

April 15, 2024

Overview

By deafult, the log collection is enabled after you install Citrix VDA for macOS.

Configuration

The configuration package includes the `ctxlogd` daemon and the `setlog` utility.

By default, the `ctxlogd` daemon starts after you install and configure the VDA.

The ctxlogd daemon

All the other services that are traced depend on the `ctxlogd` daemon.

> **Note:** You can stop the `ctxlogd` daemon if you do not want to trace the VDA for macOS.

The setlog utility

Log collection is configured using the `setlog` utility, which is under the `/opt/Citrix/VDA/bin/` path and only the root user has the privilege to run it.

You can use the GUI (by simply running a command `/opt/Citrix/VDA/bin/setlog`, the GUI is available for usage) or run commands to view and change the configurations.

Run the following command for help with the setlog‘ utility:

```
`setlog help`
<!--NeedCopy-->
```

Values By default,

- **Log Output Path** is set to `/var/log/xdl/hdx.log`
- **Max Log Size** is set to **200 MB**

and you can save up to two old log files under **Log Output Path**.

View the current `setlog` values:


```
setlog values

log_path (Log Output Path) = /var/log/xdl/hdx.log

log_size (Max Log Size (MiB)) = 200

log_count (Max Old Log Files) = 2
<!--NeedCopy-->
```

View or set a single `setlog` value:

```
setlog value <name> [<value>]
<!--NeedCopy-->
```

For example:

```
setlog value log_size 100
<!--NeedCopy-->
```

Levels By default, log levels are set to **warning** (case-insensitive).

- To view log levels set for different components, run the following command:

  ```
  setlog levels
  <!--NeedCopy-->
  ```

- To set log levels (including Disabled, Inherited, Verbose, Information, Warnings, Errors, and Fatal Errors), run the following command:

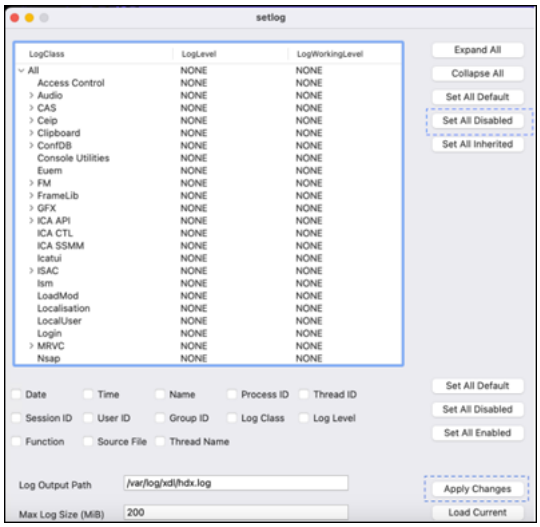
  ```
  setlog level <class> [<level>]
  <!--NeedCopy-->
  ```

Log Level	Command Parameter (Case-Insensitive)
Disabled	none
Inherited	inherit
Verbose	verbose
Information	info
Warnings	warning
Errors	error
Fatal Errors	fatal
Trace	trace

You can also use the GUI applet to change logging levels.

For example, follow the steps to disable all logs.

1. Click **Set All Disabled** on the top right.
2. Click **Apply Changes** to make the change.



The **<class>** variable specifies one component within the VDA. To cover all components, set it to all. For example:

```
setlog level all error
<!--NeedCopy-->
```

Flags By default, the flags are set as follows:

```
setlog flags

DATE = true

TIME = true

NAME = true

PID = true

TID = true

SID = true

UID = false

GID = false

CLASS = true
```



```
20
21 LEVEL = true
22
23 FUNC = false
24
25 FILE = false
26
27 TNAME = false
28 <!--NeedCopy-->
```

- View the current flags:

```
1 setlog flags
2 <!--NeedCopy-->
```

- View or set a single log flag:

```
1 setlog flag <flag> [<state>]
2 <!--NeedCopy-->
```

Restore Defaults Revert all levels, flags, and values to the default settings:

```
1 setlog default
2 <!--NeedCopy-->
```

> **Important:**
>
> The `ctxlogd` service is configured using the **/var/xdl/.ctxlog** file, which only the root users can create.
>
> **Recommended:**
>
> Do not give write permission to other users.

Failure to comply, can cause the arbitrary or malicious configuration to `ctxlogd`, which affects the server performance and the user experience.

Tools and Utilities

April 16, 2024

The `xdlcollect` shell script

The `xdlcollect` shell script integrated into the VDA software installation process collects logs and is located under `/opt/Citrix/VDA/bin`.

Once you install the VDA, run the `/opt/Citrix/VDA/bin/xdlcollect.sh` script to collect logs.

When you run the `xdlcollect.sh`, the following information and logs are collected and packaged:

System Information:

- macOS Release Version
- Memory and CPU usage
- General Disk Information
- Loaded Kernel Extensions
- List of PCI and USB devices
- Running Processes
- Services
- System Messages (dmesg)
- System Logs
- Package Installation Logs
- Network Information:
- Host Name
- DNS Servers

Network interfaces:

- Routes
- Firewall Configuration

Additional Information:

- VDA Logs and related configuration
- Crash Dump

Some basic tests are performed to check connectivity to:

- DNS Severs
- Citrix DaaS control plane

After log collection, a compressed log file is generated in the same folder as the script.

The vdaversion script

The **vdaversion** script is integrated into the VDA software installation process and located under `/opt/Citrix/VDA/bin`.

After you install the VDA, run the `./vdaversion` under the folder mentioned to check your **VDA revision number** to validate if you installed the latest or chosen version of **VDA**.

The ctxsession tool

The `ctxsession` tool is integrated into the VDA software installation process and located under `/opt/Citrix/VDA/bin`.

The `ctxsession` is a diagnostic tool that assists you to check your **VDA** and **CWA** session information.

> **Note:**
>
> You can run it either without any parameters or in a verbose mode.

For example `./ctxsession -v`

The Citrix support team uses the information to assist in troubleshooting.

Session and Account

April 16, 2024

This section describes some general guidelines regarding HDX session management and its relationship with macOS user account setup.

Citrix VDA for macOS does not change or manage user accounts in macOS.

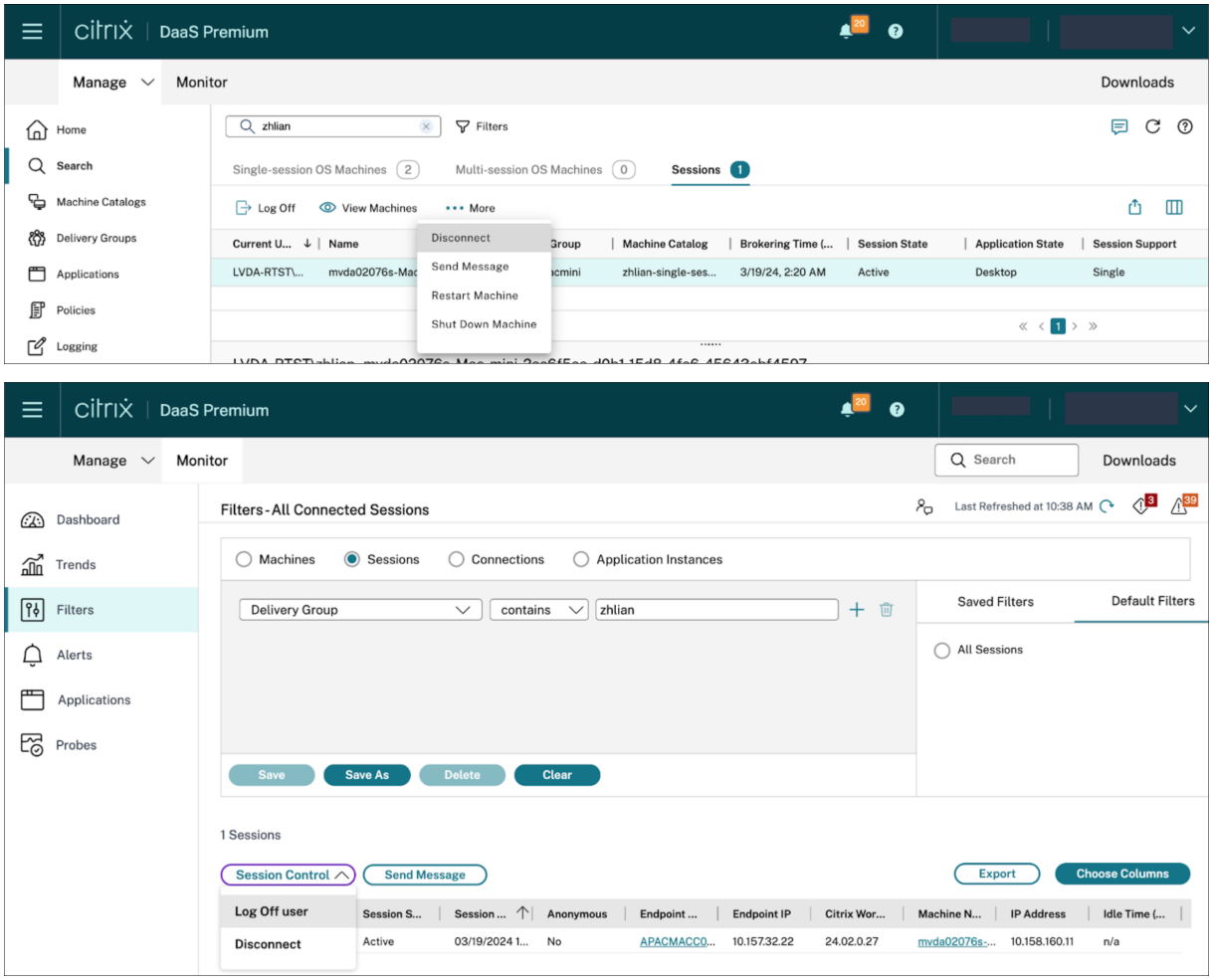
End users can log out or switch user accounts inside an active HDX session, which follows default macOS behaviors.

For HDX session, two different operations can be performed:

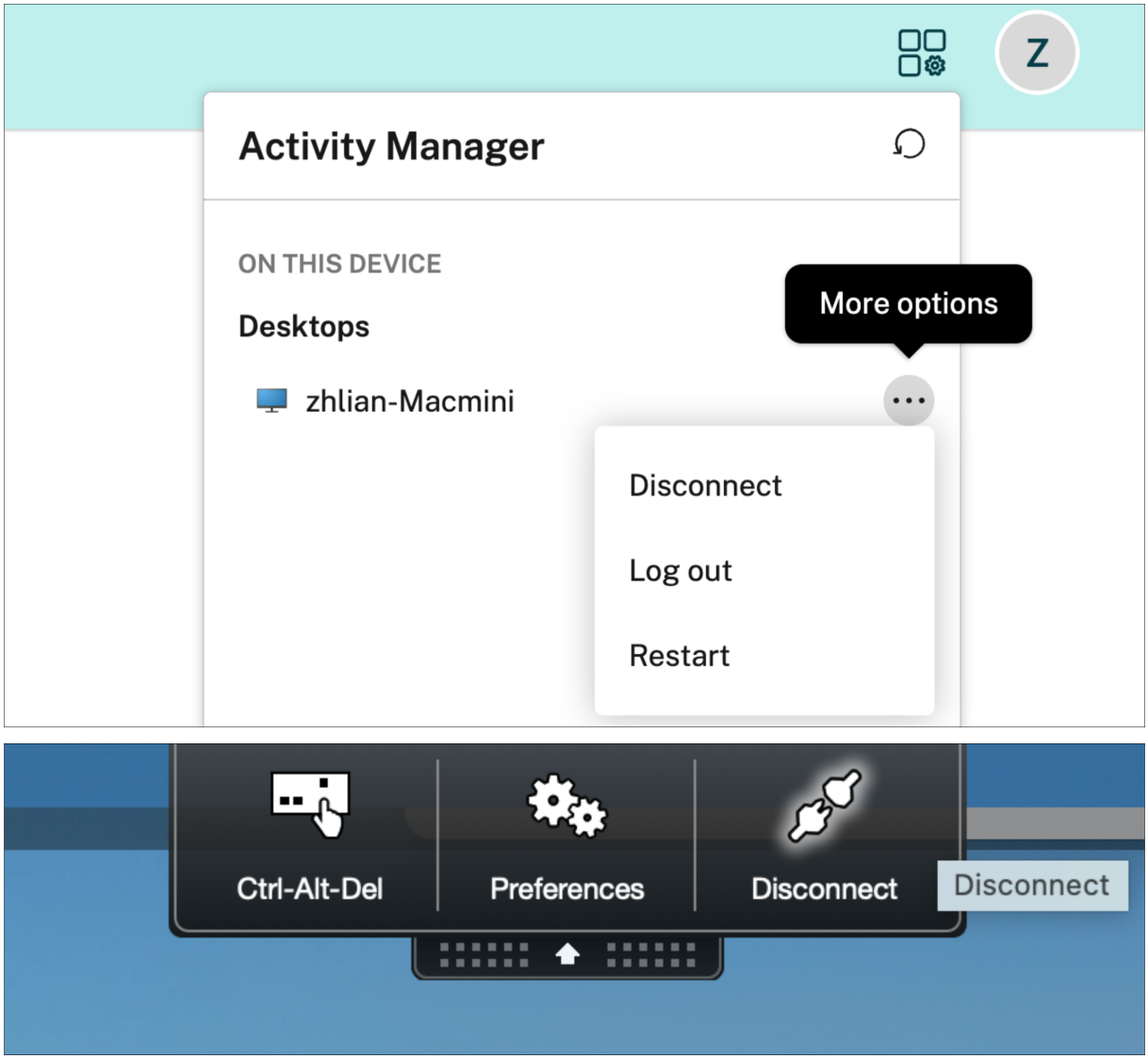
- **Disconnect**: ends the current active connection towards VDA. However, the HDX session for Citrix VDA for macOS is still alive and hence, the session is blocked and can be reused only by the last user connected.
- **Logoff**: terminates the current HDX session and the VDA is able to establish new session upon new broking requests from DDC.

Administrators and end users can disconnect or logoff HDX session through different approaches respectively.

For administrators, session can be disconnected or logged off through the **WebStudio** and **Monitor Service Panel** as shown in the following screenshots.



For end users, session can be disconnected or logged off through **Activity Manager** at the top right of workspace page as shown in the following screenshots.



Alternatively, an administrator or an end user can run the command `sudo /opt/Citrix/VDA/bin/ctxlogoff` to logoff a session directly from the VDA machine.

Administrators should guide their end users to logoff the session each time after usage who want to maximize the usage of certain underlying devices with multiple user accounts configured.

Meanwhile, configure **Machine Catalog - Desktop Experience** as **Random** and related **Delivery Group settings** to allow unbinding between HDX session and the user.

> **Note:**
>
> Sending a message from DaaS management console to VDA session is not supported at the moment.

Authentication

April 16, 2024

To use Citrix VDA for macOS, the administrator needs to configure both **Authentication for Workspace subscribers according to Identity Access Management** and also **macOS local user account** separately.

Non-SSO Authentication

April 16, 2024

This section describes the authentication steps before you can use the VDA session.

Overview

To use **Citrix VDA for macOS**:

1. Sign in to the **Workspace** or **StoreFront**.
2. Sign in to the machine.

The organization's administrator configures both the sign-in credentials (using DaaS console and MDM software).

> **Note:**
>
> SSO authentication isn't supported at the moment.

General Content Redirection

April 16, 2024

Citrix VDA for macOS general content redirection capabilities follows HDX roadmap, in this Public Tech Preview, we support

- Clipboard Redirection
- Audio Redirection
- Multiple Audio Devices Redirection

> **Note:**
>
> USB and other types of redirection are not support in this Public Tech Preview product.

Clipboard Redirection

April 16, 2024

Clipboard redirection allows you to copy and paste data between your device and the applications running in the VDA session.

Citrix policies for clipboard redirection

Citrix policies that allow you to achieve clipboard redirection.

Client Clipboard Redirection

The clipboard redirection setting either allows or prevents the clipboard on your device to map on to the VDA clipboard.

By default, clipboard redirection is set to **Allowed**.

To prevent copy-and-paste data transfer between a session and the local clipboard, select **Prohibited**.

You can still copy and paste data between applications running in sessions.

Audio Redirection

March 28, 2024

Audio redirection is enabled by default. It supports the following Citrix Workspace App clients (recommended):

- Citrix Workspace App 2309.1 for Windows or later
- Citrix Workspace App 2309 for Linux or later
- Citrix Workspace App 2309 for Mac or later
- Citrix Workspace App 2403 for ipadOS/iOS
- Citrix Workspace App 2403 for Android

Multiple Audio Devices Redirection

April 16, 2024

Overview

Citrix VDA for macOS has integrated and supported a new capability in HDX.

Multiple audio devices redirection

The feature allows multiple audio devices on the client machine where the Citrix Workspace App is installed to be redirected to the remote Mac VDA session.

With the feature enabled:

- All local audio devices on the client machine are displayed in a session.
  - Instead of Citrix Audio Device, the audio devices appear with their respective device names.
  - You can select an audio device in an app in a session or use the default audio device during a session which is also the default audio device of the client machine.
  - If necessary, you can change the default audio device from the system settings of the client machine.
  - After the default audio device of the client machine is updated, the new device appears as the default audio device in the session.
- Audio devices update dynamically within sessions when you plug in or remove one.

Configuration

By default, the audio redirection feature that allows multiple audio device support is enabled. To disable it, run the following command on the Mac VDA:

```
/opt/Citrix/VDA/bin/ctxreg create -k "HKLM\\System\\CurrentControlSet
\\Control\\Citrix\\VirtualChannels\\Audio"-v "fEnableAudioRedirectionV4
"-t BIN -d "0"
```

To enable or re-disable the feature, run the following commands, respectively:


```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\\System\\CurrentControlSet
\\Control\\Citrix\\VirtualChannels\\Audio"-v "fEnableAudioRedirectionV4
"-d "1"
```

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\\System\\CurrentControlSet
\\Control\\Citrix\\VirtualChannels\\Audio"-v "fEnableAudioRedirectionV4
"-d "0"
```

Client Requirements and Settings

The feature is supported only for the following clients:

- Citrix Workspace App for Windows
- Citrix Workspace App for Linux version 2212 and higher
- Citrix Workspace App for HTML5 version 2306 and higher
- Citrix Workspace App for Chrome version 2306 and higher
- Citrix Workspace App for Mac version 2311 and higher

Proper settings are required on **Citrix Workspace App** for the feature to function as expected. For more information, see the Citrix Workspace App documentation.

Graphics

April 16, 2024

In this section, we provide details on the common HDX Graphics capabilities that can enhance your end user experience.

Automatic DPI Scaling

April 16, 2024

The macOS VDA supports automatic DPI scaling. When you open a virtual desktop or application session, the **DPI value** in the session automatically changes to match the **DPI setting** on the client side.

The following are some considerations related to this feature:

- The feature requires that you enable **DPI matching for Citrix Workspace**.

  - Select **No, use the native resolution** option for **Citrix Workspace App for Windows**. For more information about configuring **DPI scaling** for Citrix Workspace App for Windows, see DPI scaling.

- For the feature to work in multi-monitor scenarios, each monitor must be configured with the same DPI setting.

  > **Note :**
  >
  > Automatic DPI scaling does not support multi-monitors with different DPI settings.

- The DPI value in the virtual session automatically changes according to the DPI setting on the client side.

Currently, the feature supports only scale factors of 1 and 2. For Example: 100% and 200%.

Graphics Configuration and Fine-Tuning

April 16, 2024

This section describes the macOS VDA graphics configuration and fine-tuning.

For more information, see System Requirements and the Installation Overview section.

Configuration

Video codec for compression

Thinwire is the **display-remoting technology** used in the macOS VDA.

The technology allows graphics generated on one machine to be transmitted, typically across a network, to another machine for display.

The **Use video codec for compression** graphics policy sets the default graphics mode and provides the following options for different use cases:

- **Use when preferred**

  By default, this setting is selected.

  Thinwire is selected for all Citrix connections and is optimized for scalability, bandwidth, and superior image quality for typical desktop workloads.

  No additional configuration is required.

- **For the entire screen**

  Delivers Thinwire with full-screen H.264 to optimize for improved user experience and bandwidth, especially in cases with heavy use of 3D graphics.

- **For actively changing regions**

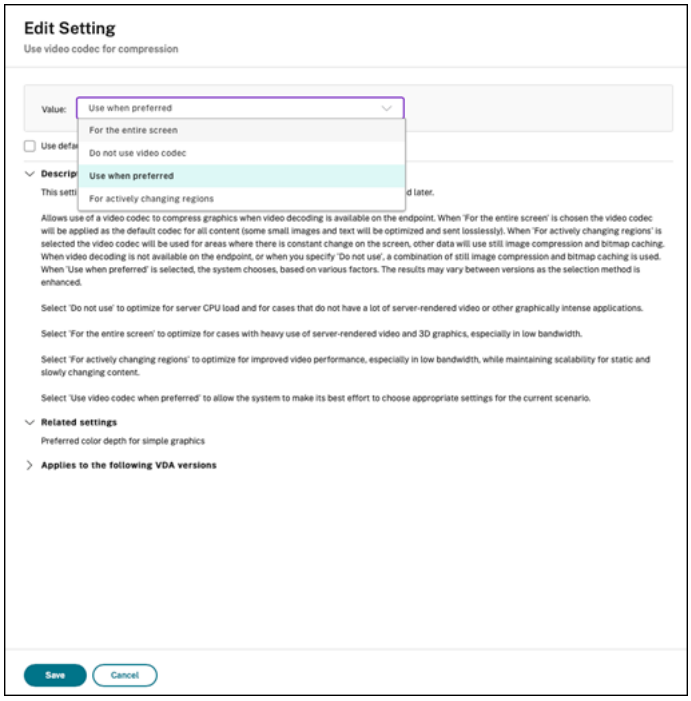
  The adaptive display technology in Thinwire identifies moving images (video, 3D in motion).

  It uses H.264 only in the part of the screen where the image is moving.

  The selective use of the H.264 video codec enables HDX Thinwire to detect and encode parts of the screen that are frequently updated using the H.264 video codec.

  Still image compression (JPEG, RLE) and bitmap caching continue to be used for the rest of the screen, including text and photographic imagery.

  You get the benefit of lower bandwidth consumption and better quality for video content combined with lossless text or high-quality imagery elsewhere.



Other policy settings, including the following visual display policy settings can be used to fine-tune the performance of remote display:

- **Target frame rate**
- **H.264 hardware encoding** - Citrix virtual delivery agent for macOS always uses GPU hardware acceleration to compress screen elements with the video codec. GPU hardware acceleration optimizes hardware resource utilization and highly improves the performance of frames per second (FPS).

Troubleshooting

Check which graphics mode is in use

Run the following command to check which graphics mode is in use (**0** means TW+. **1** means full-screen video codec):

```
sudo /opt/Citrix/VDA/bin/ctxreg dump | grep GraphicsMode
```

The result resembles:

```
create -k "HKLM\Software\Citrix\Ica\Session\4\Graphics"-t "REG_DWORD"
-v "GraphicsMode"-d "0x00000000"--force
```

Multi-Monitor Support

April 16, 2024

Overview

The macOS VDA provides an out-of-the-box multi-monitor support for up to nine monitors.

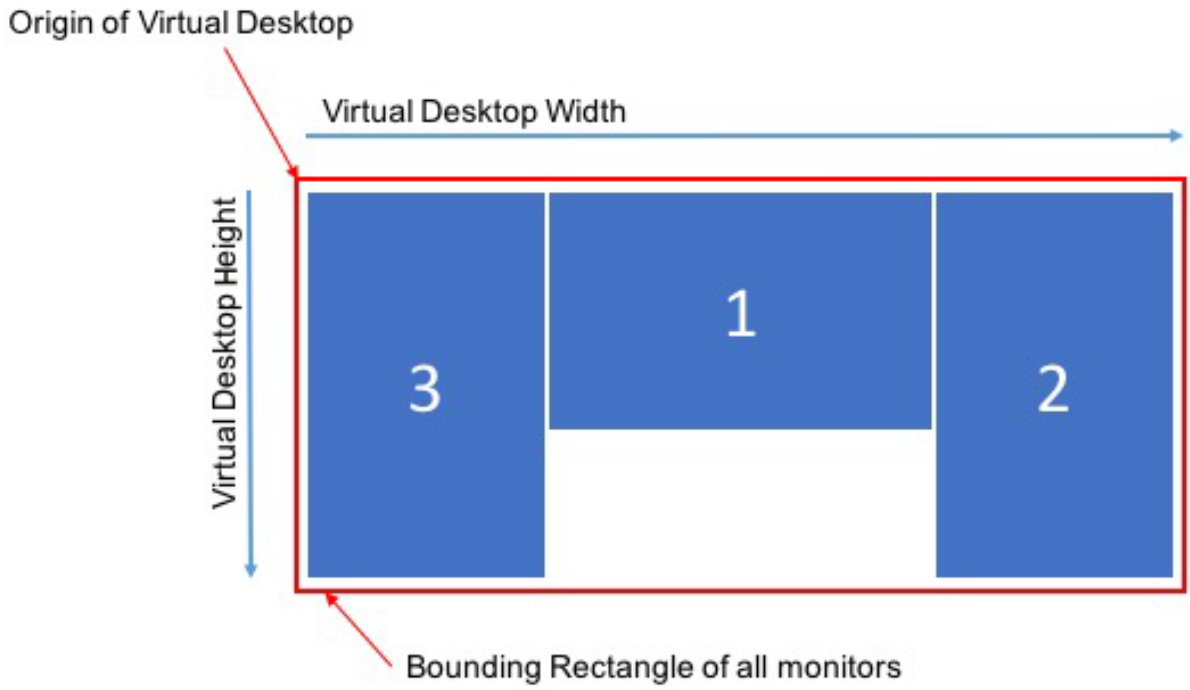
This section tells you how to configure a macOS VDA for different monitor resolutions and layouts.

Virtual session desktop

macOS VDA also has the concept of a multi-monitor virtual desktop like the windows VDA.

A multi-monitor virtual desktop is based on the bounding rectangle of all monitors and not the actual layout of the monitors.

So, theoretically, the area of the virtual desktop can be larger than the area covered by the monitors of the client.



Virtual session desktop size

The origin of a virtual session desktop is calculated from the top-left corner of the bounding rectangle of all monitors.

That point locates at X = 0, Y = 0, where X and Y are the horizontal and vertical axes, respectively.

The width of the virtual session desktop is the horizontal distance, in pixels, from the origin to the top-right corner of the bounding rectangle of all monitors.

Similarly, the height of the virtual session desktop is the vertical distance, in pixels, from the origin to the bottom-left corner of the bounding rectangle of all monitors.

This calculation is important for the following reasons:

- Allowing for different client monitor layouts
- Understanding memory usage on the macOS VDA

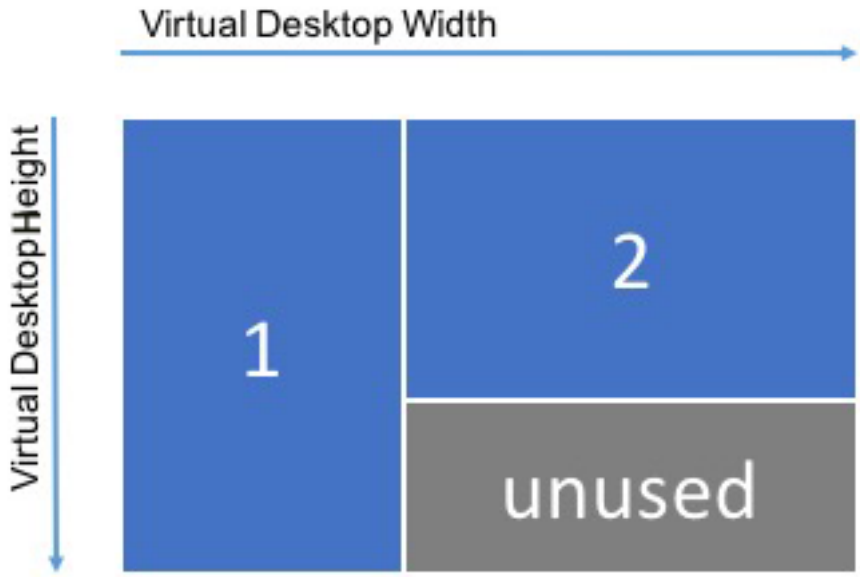
Allowing for different client monitor configurations

Knowing the maximum size of the virtual desktop for your client monitor configurations allow you to configure the macOS VDA to be flexible in terms of client monitor configurations.

Consider the following client monitor configuration:

The diagram shows an out-of-the-box multi-monitor configuration with two monitors, each with a resolution of 2560×1600.

Now, consider connecting to the same macOS VDA with the following client monitor configuration:



If each monitor in the above diagram has a resolution of 2560×1600, the out-of-the-box multi-monitor configuration parameters are insufficient. The maximum height is too small to accommodate the virtual session desktop for this monitor layout. To accommodate the client monitor configuration in this example, you must set the macOS VDA virtual desktop to a size of 4160×2560.

For the greatest flexibility in a multi-monitor configuration, find the smallest bounding rectangle of all monitor layouts you want to support. For configurations with two 2560×1600 monitors, the possible layouts include:

- **Monitor1** 2560×1600 and **Monitor2** 2560×1600

- **Monitor1** 1600×2560 and **Monitor2** 2560×1600
- **Monitor1** 2560×1600 and **Monitor2** 1600×2560
- **Monitor1** 1600×2560 and **Monitor2** 1600×2560

To accommodate all the layouts above, you need a virtual session desktop of 5120×2560. It is the smallest bounding rectangle that can contain all the desired layouts.

If all your users have only one monitor in the typical landscape layout, set the maximum virtual desktop size to the highest resolution of the monitor. The default configuration is 8000×8000 and two monitors.

> **Note:**
>
> If a desktop displays at an improper resolution in a multi-monitor setup, adjust Dots Per Inch (DPI) settings on the Citrix Workspace App. For more information, see Knowledge Center article CTX230017.

Understanding memory usage on the macOS VDA

Knowing the virtual desktop size allows you to calculate the amount of memory used by each HDX session. This memory is the memory allocated to each session for its graphics data when the session begins. It does not change for the life of the session. While this memory is not the total amount of memory used for the session, it is the easiest way of calculating per-session memory usage.

To calculate how much memory is allocated to each HDX session, use the following formula:

M = X × Y × Z,

Where:

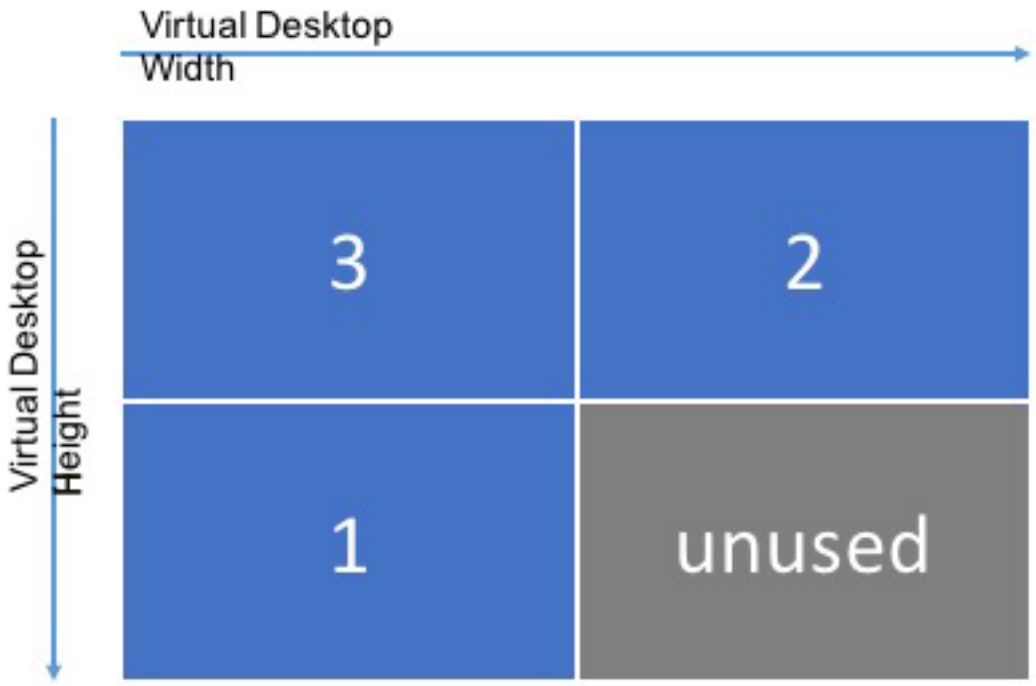
- **M** is the amount of memory used for session graphics.
- **X** is the width of the virtual session desktop.

- **Y** is the height of the virtual session desktop.
- **Z** is the color depth of the HDX session window. The value is in bytes, not bits, so use 4 for 32-bit color.

> **NOTE:**
>
> The color depth of the X server starts and cannot change with the life of the session (**from login through disconnects/reconnects until logoff**). Hence, the macOS VDA always allocates the virtual session desktop as 32-bit and down samples to the color depth requested for the session.
>
> For example, for a 1024×768 session, the memory used is:
>
> 1024 × 768 × 4 / 2^20 MB = 3 MB

It is important to understand the memory usage to understand the increasing session density of VDAs.

Consider the following client monitor configuration:



A virtual session desktop size needs to be 5120×3200 to accommodate the client monitor configuration if each monitor has a resolution of 2560×1600

> **Note:**
>
> The gray area is unused and equates to 16,384,000 (that is, 2560 x 1600 x 4) bytes of wasted memory.

Citrix multi-monitor configuration parameters

You can control the multi-monitor functionality of the macOS VDA by using the following configuration parameters:

- **`MaxScreenNum`**

  Parameter: HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/Citrix/Thinwire/MaxScreenNum

  Description: Number of monitors to support

  Type: DWORD

  Default: 2

  Maximum: 9 for standard VDA

- **`MaxFbWidth`**

  Parameter: HKEY_LOCAL_MACHINE /System/CurrentControlSet/Control/Citrix/Thinwire/-MaxFbWidth

  Description: Maximum width of a virtual session desktop

  Type: DWORD

  Default: 5,120

  Maximum: 16,384 (8,192 x 2)

- **`MaxFbHeight`**

  Parameter: HKEY_LOCAL_MACHINE /System/CurrentControlSet/Control/Citrix/Thinwire/-MaxFbHeight

  Description: Maximum height of a virtual session desktop

  Type: DWORD

  Default: 1,600

  Maximum: 16,384 (8,192 x 2)

Changing the macOS VDA multi-monitor configuration

The following section outlines how to enable, configure, and disable the multi-monitor functionality on the macOS VDA.

Set the maximum number of monitors by using:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE \System\CurrentControlSet\
    Control\Citrix\Thinwire" -t "REG_DWORD" -v "MaxScreenNum" -d "
    NumMons" --force
```



```
<!--NeedCopy-->
```

Where **NumMons** is a value between 1 and 9 for standard VDA or 1 and 4 for HDX 3D Pro VDA.

Set the maximum width of a virtual desktop session by using:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE \System\CurrentControlSet\
   Control\Citrix\Thinwire" -t "REG_DWORD" -v "MaxFbWidth" -d "
   MaxWidth" --force
<!--NeedCopy-->
```

Where **MaxWidth** is a value between **1,024** and **16,384**.

Set the maximum height of a virtual session desktop by using:

```
sudo ctxreg create -k " HKEY_LOCAL_MACHINE \System\CurrentControlSet\
   Control\Citrix\Thinwire" -t "REG_DWORD" -v "MaxFbHeight" -d "
   MaxHeight" --force
<!--NeedCopy-->
```

Where **MaxHeight** is a value between **1,024** and **16,384**.

Thinwire Progressive Display

April 16, 2024

Session interactivity can degrade on low-bandwidth or high-latency connections. For example, scrolling on a webpage can become slow, unresponsive, or choppy. Keyboard and mouse operations can lag behind graphics updates.

You were able to use policy settings to reduce bandwidth consumption by configuring the session to **Low** visual quality.

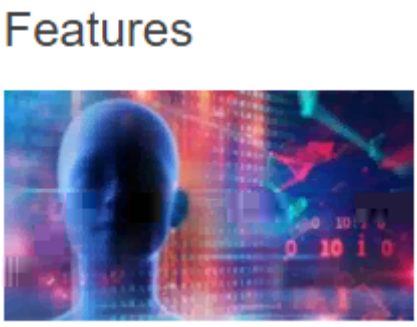
HDX Thinwire switches to a progressive update mode by default in either of the following cases:

- Available bandwidth falls below 2 Mbps.
- Network latency exceeds 200 ms.

In this mode:

For example, in the following graphic where progressive update mode is active, the letters **F** and **e** have blue artifacts, and the image is heavily compressed. This approach significantly reduces bandwidth consumption, which allows images and text to be received more quickly, and session interactivity improves.

When you stop interacting with the session, the degraded images and text are progressively sharpened to lossless. For example, in the following graphic, the letters no longer contain blue artifacts, and the image appears at source quality.



For images, sharpening uses a random block-like method. For text, individual letters or parts of words are sharpened. The sharpening process occurs over several frames. This approach avoids introducing a delay with a single large sharpening frame.

Transient imagery (video) is still managed with adaptive display or Selective H.264.

How progressive mode is used

By default, progressive mode is on standby for the **Visual quality** policy settings: **High**, **Medium** (default), and **Low**.

Progressive mode is forced off (not used) when:

- **Use video codec for compression** = **For the entire screen** (when full-screen H.264 is desired)

> **Note :**
>
> The default graphics mode is thinwire plus, you can try to change it to full screen hardware H.264 by either configuring the policy in the Daas Management Console or you can run the command `sudo defaults write ctxhdx EnableH264 -bool YES` on the VDA machine, and reconnect to the session.

When progressive mode is on standby, by default it is enabled when either of the following conditions occurs:

- Available bandwidth drops below 2 Mbps
- Network latency increases above 200 ms

After a mode switch occurs, a minimum of 10 s is spent in that mode, even if the adverse network conditions are momentary.

Change progressive mode behavior

You can change the progressive mode behavior by running the following command:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKEY_LOCAL_MACHINE\SOFTWARE\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplay" -d "<value>" --force
<!--NeedCopy-->
```

Where <value>:

0 = Always off (do not use under any circumstances)

1 = Automatic (toggle based on network conditions, default value)

2 = Always on

When in automatic mode (1), you can run either of the following commands to change the thresholds at which progressive mode is toggled:

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SYSTEM\
    CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplayBandwidthThreshold" -d "<value>" --force
<!--NeedCopy-->
```

Where <value> is <threshold in Kbps> (default = 2,048)

Example: 4096 = toggle progressive mode on if bandwidth falls below 4 Mbps

```
sudo /opt/Citrix/VDA/bin/ctxreg  create -k "HKEY_LOCAL_MACHINE\SOFTWARE
    \CurrentControlSet\Control\Citrix\Thinwire" -t "REG_DWORD" -v "
    ProgressiveDisplayLatencyThreshold" -d "<value>" --force
<!--NeedCopy-->
```

Where <value> is <threshold in ms> (default = 200)

Example: 100 = toggle progressive mode on if network latency drops below 100 ms.

Keyboard

April 16, 2024

In this section, we give you details on

- Dynamic Keyboard Layout Synchronization
- Keyboard Layout Synchronization
- Keyboard Input Mode

Dynamic Keyboard Layout Synchronization

March 19, 2024

Previously, the keyboard layouts on the Mac VDA and on the client device had to be the same. Key mapping issues might occur, for example, when the keyboard layout changes from English to French on the client device but not on the VDA.

Citrix addresses the issue by synchronizing the keyboard layout of the VDA with the keyboard layout of the client device automatically. Anytime the keyboard layout on the client device changes, the layout on the VDA follows suit.

Configuration

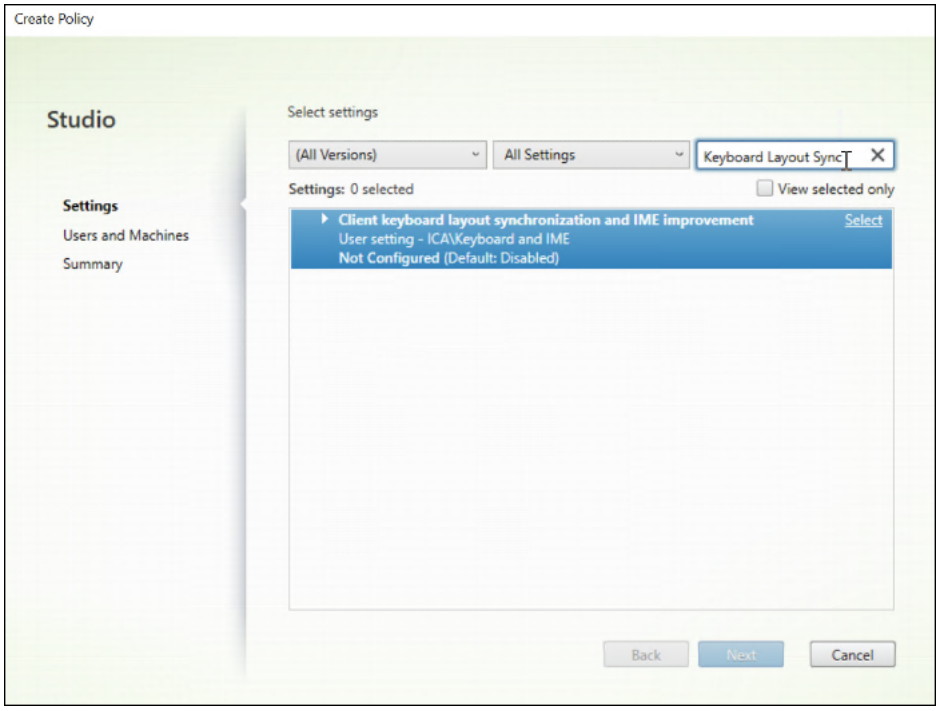
Group Policy

The dynamic keyboard layout synchronization feature is disabled by default. To enable or disable the feature, set the **Client Keyboard Layout Sync** and **IME Improvement policy** or edit the registry.

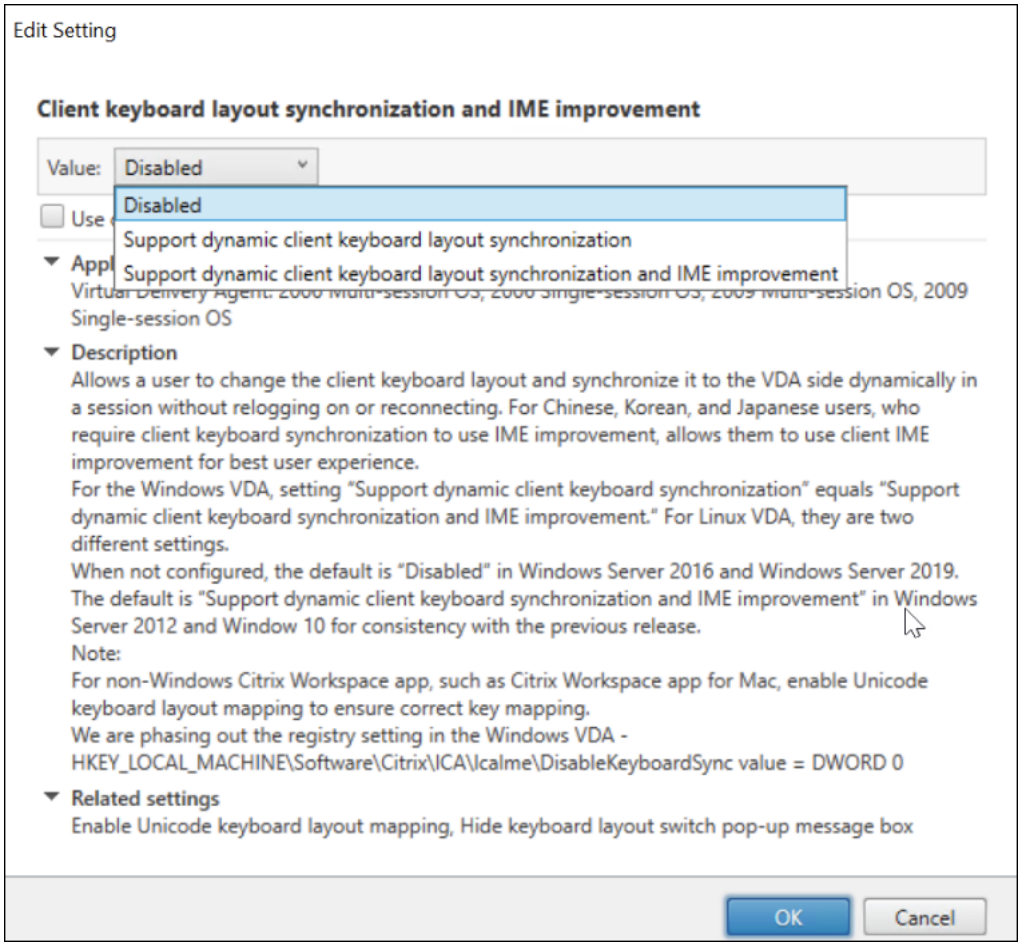
The **Client Keyboard Layout Sync** and **IME Improvement policy** takes priority over registry settings and can be applied to user and machine objects you specify or all objects in your site. Registry settings on a given Mac VDA apply to all sessions on that VDA.

Set the **Client Keyboard Layout Sync** and **IME Improvement policy** to enable or disable the dynamic keyboard layout synchronization feature:

1. In **Studio**, right-click **Policies** and select **Create Policy**.
2. Search for the **Client Keyboard Layout Sync** and **IME Improvement policy**.



3. Click **Select** next to the policy name.
4. Set the **policy**.



There are three options available:

- **Disabled**: disables dynamic keyboard layout synchronization and client IME user interface. There is an exception that when group policy is disabled, end users can still use registry settings to enable the feature manually.
- **Support dynamic client keyboard layout synchronization**: enables dynamic keyboard layout synchronization regardless of the DWORD value of the KeyboardSyncMode registry key at HKLM\Software\Citrix\VirtualDesktopAgent\mac\kbime.
- **Support dynamic client keyboard layout synchronization and IME improvement**: enables both dynamic keyboard layout synchronization and client IME user interface synchronization regardless of the DWORD value of the KeyboardSyncMode registry key at HKLM\Software\Citrix\VirtualDesktopAgent\mac\kbime.

> **Note:**
>
> IME improvement isn't yet supported in Mac VDA.

Registry Setting

To enable dynamic keyboard layout Sync, set **KeyboardSyncMode** to **2** under the key of `HKLM\Software\Citrix\VirtualDesktopAgent\mac\kbime` in ctxreg configure DB

Here is the command example:

```
sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
VirtualDesktopAgent\mac\kbime"-t "REG_DWORD"-v "KeyboardSyncMode"-
d "2"--force
```

If you change to any other value the keyboard dynamic Sync is disabled:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKLM\Software\Citrix\VirtualDesktopAgent
\mac\kbime"-t "REG_DWORD"-v "KeyboardSyncMode"-d "1"
```

Keyboard Layout Synchronization

March 27, 2024

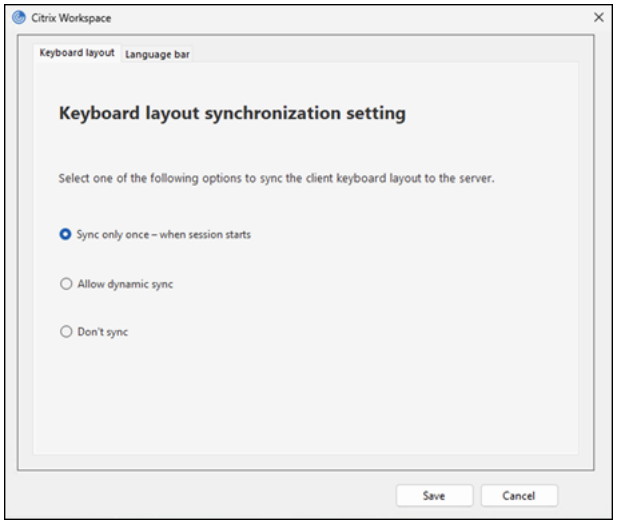
Keyboard layout synchronization enables users to have the same keyboard layout on the macOS VDA and the client device, to guarantee the input experience.

As of the macOS VDA Version, Citrix has added support for synchronizing client-side keyboard layout to macOS VDA when session launches. It requires respective input sources being added ahead in the keyboard settings of the user's desktop.

Configuration from Citrix Workspace App

Citrix Workspace App for Windows

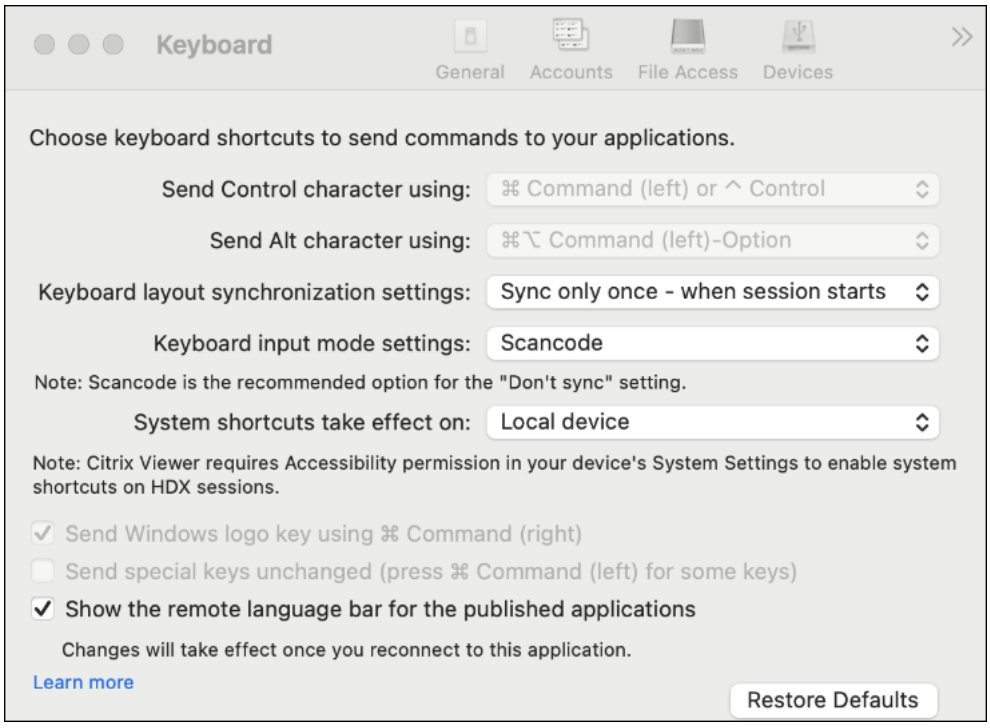
1. Open **Advanced Preferences**.
2. Select the **Keyboard and Language** bar.



3. Select **Allow dynamic sync** in the **keyboard layout** tab.

Citrix Workspace App for macOS

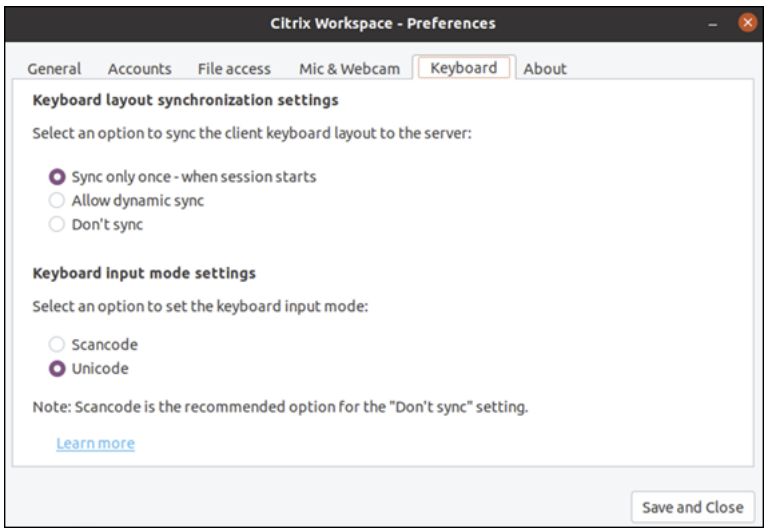
1. Open **Citrix Workspace App Preferences**.
2. Select **Keyboard**.



3. Select **Allow dynamic sync** in the **keyboard layout syncronization** setting dialog box.

Citrix Workspace App for Linux

1. From the **Citrix Workspace App** icon in the notification area.
2. Select **Preferences** and then select **Keyboard**.



3. Select **Allow dynamic sync** in the **keyboard layout syncronization** setting dialog box.

Keyboard Input Mode

April 16, 2024

Citrix Virtual Apps and Desktops support both client keyboard layout and remote keyboard layout through input mode:

1. **Scancode Mode:** Remote keyboard layout is applied no matter which layout the client has. The client sends the scan code to a remote session and the remote keyboard layout interprets it to characters.
2. **Unicode Mode:** Client keyboard layout is applied no matter which layout the remote keyboard has. The client keyboard layout interprets the raw key event (scan code or keycode) to Unicode characters before it's sent to the VDA side.

Citrix has added support for both Scancode and Unicode in macOS VDA.

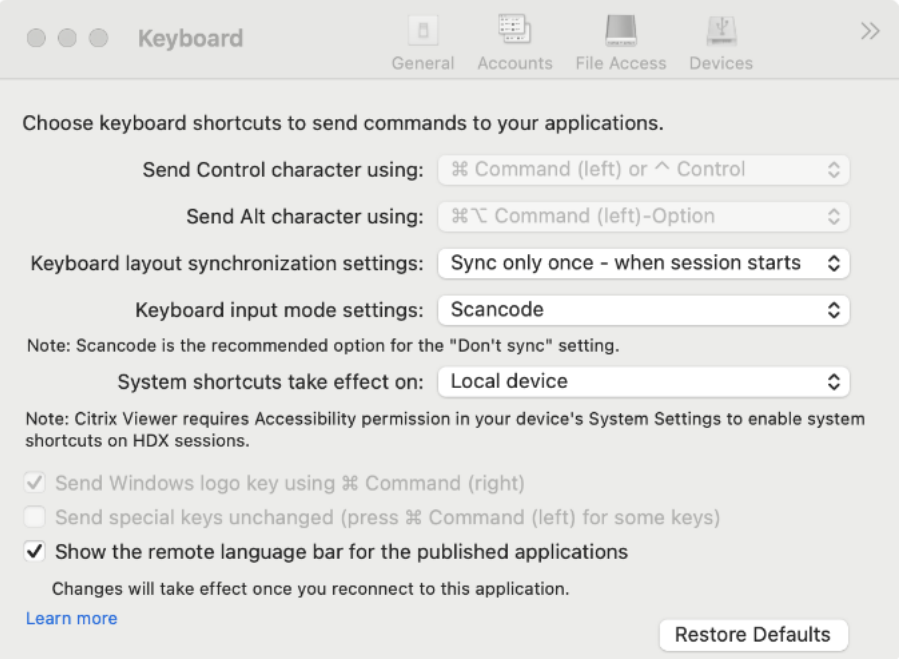
Configuration from Citrix Workspace App

Citrix Workspace App for Windows

CWA for Windows uses Scancode mode by default.

Citrix Workspace App for macOS

1. Open **Citrix Workspace App preferences**
2. Select **Keyboard**.



3. Select **Scancode** or **Unicode** in the keyboard input mode settings dialog box.

> **Note :**
>
> Citrix recommends using the **Scancode** mode to configure the keyboard input mode for VDA

4. Select **Local Device** if you want to use the macOS system shortcuts in the session.

Citrix Workspace App for Linux

1. Select **Preferences** from the Citrix Workspace App icon in the notification area.
2. Select **Keyboard**.
3. Select **Scancode** or **Unicode** in the keyboard input mode settings dialog box.

By using Citrix Workspace App for Mac 2402 and newer versions, the system keyboard shortcuts such as Option-Command-ESC, Command-Space bar, Command-Tab, Control-Command-Q, Shift-Command-Q, Control Up/Down/Left/Right can be used in your Mac VDA sessions. See Workspace App for Mac

Session

April 16, 2024

In this section, we give you details on

- Proxy PAC File Support
- Session Reliability
- Rendezvous V2
- Supportability Service

Proxy Pac File Support

March 19, 2024

PAC files are commonly used to manage employee proxies in many large corporate groups.

Our product also supports reading PAC files to retrieve proxy settings.

Our PAC proxy is primarily applied in the following four business areas:

- Enrollment
- VDA Registration
- NGS Registration
- Rendezvous

Conventionally, traffic between VDA and Citrix Cloud control plane is called **control traffic**, and traffic between VDA and CWA is called **HDX traffic**.

The **Enrollment**, **VDA Registration**, and **NGS Registration** are in the category of control traffic while **Rendezvous** is in the category of HDX traffic.

Proxy Configuration

The VDA supports connecting through proxies for both control traffic and HDX traffic when using Rendezvous.

The requirements and considerations for both types of traffic are different, so review them carefully.

Control traffic proxy considerations

- Only HTTP proxies are supported.
- Packet decryption and inspection are not supported. Configure an exception so the control traffic between the VDA and the Citrix Cloud control plane is not intercepted, decrypted, or inspected. Otherwise, the connection fails.
- Proxy authentication is not supported.
- To configure a proxy for control traffic, edit the registry as follows:

  ```
  /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\
  VirtualDesktopAgent"-t "REG_SZ"-v "ProxySettings"-d "<Proxy
  address or PAC file>"--force
  ```

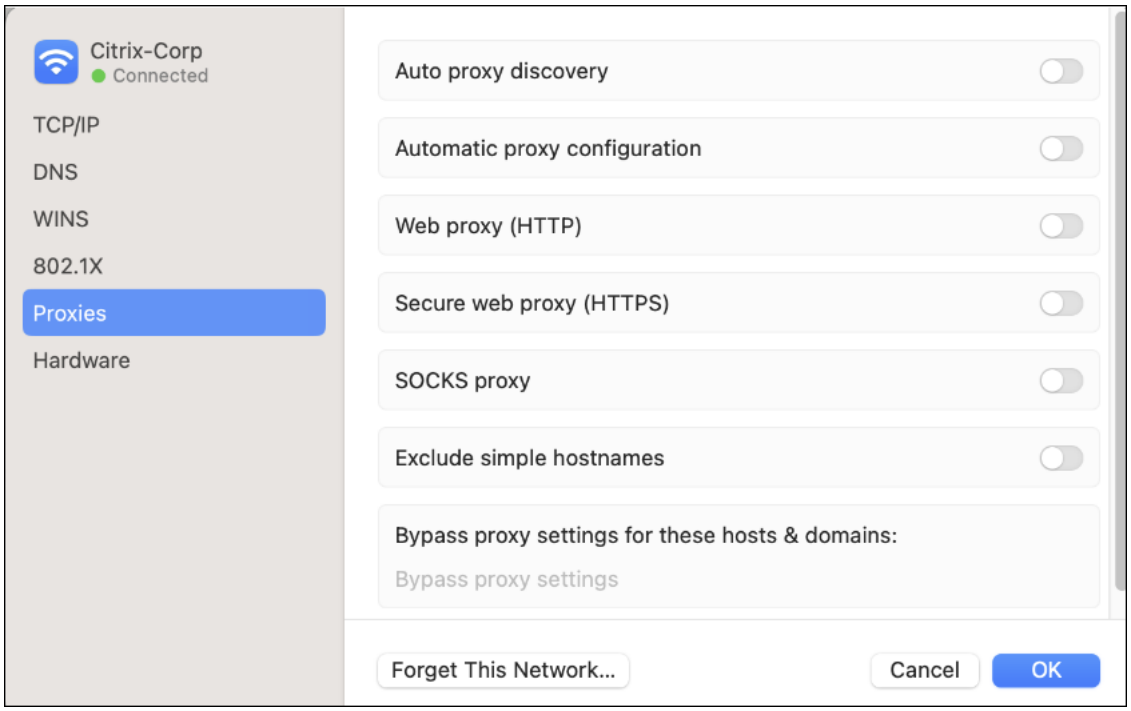
- Proxy address: `http://<URL or IP>:<port>`
- PAC file: `http://<URL or IP>/<path/<filename>.pac`

HDX traffic proxy considerations

- HTTP and SOCKS5 proxies are supported.
- EDT can only be used with SOCKS5 proxies.
- To configure a proxy for HDX traffic, use the Rendezvous proxy configuration policy setting.
- Packet decryption and inspection are not supported. Configure an exception so the HDX traffic between the VDA and CWA is not intercepted, decrypted, or inspected. Otherwise, the connection fails.
- Authentication with a SOCKS5 proxy is not currently supported. If using a SOCKS5 proxy, you must configure an exception so that traffic destined to Gateway Service addresses (specified in the requirements) can bypass authentication.
- Only SOCKS5 proxies support data transport through EDT. For an HTTP proxy, use TCP as the transport protocol for ICA.

Without any proxy being configured through GroupPolicy or a utility **ctxreg**, we also support reading proxy configurations from the macOS system where VDA is located and parsing PAC files to obtain the final proxy configuration.

Traffic interaction is conducted based on the proxy configuration. However, we only support HTTP/HTTPS proxies for the first three business scenarios, while SOCKS proxies will be supported later. Rendezvous supports both HTTP/HTTPS proxies and unauthenticated SOCKS proxies.



With the proxy Pac File Support, our VDA can access https://*.nssvc.net, enabling VDA enrollment and registration to DDC and Gateway. Rendezvous is used during session initiation to allow CWA and VDA to communicate using the Rendezvous protocol.

Rendezvous V2

April 16, 2024

When using the Citrix Gateway service, the Rendezvous protocol allows traffic to bypass the Citrix Cloud Connectors and connect directly and securely with the Citrix Cloud control plane.

There are two types of traffic to consider:

- Control traffic for VDA registration and session brokering.
- HDX session traffic.

Rendezvous V1 allows for HDX session traffic to bypass Cloud Connectors, but it still requires Cloud Connectors to proxy all control traffic for VDA registration and session brokering.

Standard AD domain joined machines and non-domain joined machines are supported for using Rendezvous V2 with single-session and multi-session macOS VDAs.

With non-domain joined machines, Rendezvous V2 allows both HDX traffic and control traffic to bypass the Cloud Connectors.

Requirements

The requirements for using Rendezvous V2 are:

- Access to the environment using Citrix Workspace and Citrix Gateway service.
- Control Plane: Citrix DaaS (formerly Citrix Virtual Apps and Desktops service).
- Enable the Rendezvous protocol in the Citrix policy. For more information, see Rendezvous protocol policy setting.
- The VDAs must have access to `https://*.nssvc.net`, including all subdomains. If you cannot allow list all the subdomains in that manner, use `https://*.c.nssvc.net` and `https://*.g.nssvc.net` instead. For more information, see the Internet Connectivity Requirements section of the Citrix Cloud documentation (under Virtual Apps and Desktop service) and the Knowledge Center article CTX270584.
- The VDAs must be able to connect to the addresses mentioned previously:
  - On TCP 443, for TCP Rendezvous.
  - On UDP 443, for EDT Rendezvous.

How to configure Rendezvous V2

Following are the steps for configuring Rendezvous in your environment:

1. Make sure that all requirements are met.
2. Create a **Citrix policy**, or edit an existing one:
   - Set the **Rendezvous Protocol** setting to **Allowed**.
   - Set the **Citrix policy** filters properly. The policy applies to the machines that need Rendezvous to be enabled.
   - Set the **Citrix policy** to have the correct priority so that it does not overwrite another one.
3. Restart the VDA machine. The policy may take a few minutes to take effect.

> **Note:**
>
> To disable Rendevous V2, run the following command in the VDA machine:
>
> - `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent"-t "REG_DWORD"-v "GctRegistration"-d "0x00000000"--force`
> - `sudo launchctl kickstart -kp system/com.citrix.ctxvda`

Rendezvous validation

To check whether a session is using the Rendezvous protocol, run the `/opt/Citrix/VDA/bin/ctxsession -v` command in the terminal.

The transport protocols displayed indicate the type of connection:

- TCP Rendezvous: TCP - TLS - CGP - ICA
- EDT Rendezvous: UDP - DTLS - CGP - ICA

If Rendezvous V2 is in use, the protocol version shows 2.0.

> **Tip:**
>
> If the VDA can't reach the Citrix Gateway service directly with Rendezvous enabled, the VDA falls back to proxy the HDX session through the Cloud Connector.

Session Reliability

April 16, 2024

Citrix introduces the session reliability feature to all supported macOS platforms. Session reliability is enabled by default.

Session reliability reconnects ICA sessions seamlessly across network interruptions. For more information about session reliability, see Auto client reconnect and session reliability.

Configuration

Policy settings in the DaaS Management Console

You can set the following policies for session reliability in the DaaS management console:

- Session reliability connections

For more information, see Session reliability policy settings.

> **Note**:
>
> After setting the **Session reliability connections**, restart the VDA service and the HDX service, in this order, for your settings to take effect.

Troubleshooting

Unable to launch sessions after enabling session reliability through the policy setting.

To work around this issue, do the following:

1. Ensure that the VDA service and HDX service are restarted, in this order, after you enable session reliability through the policy setting.
2. On the VDA, run the following command to verify that the session reliability listener is running (using port 2598 as an example).

   ```
   netstat -an | grep 2598
   <!--NeedCopy-->
   ```

   If there is no TCP listener on the session reliability port, enable the listener by running the following command.

   ```
   /opt/Citrix/VDA/bin/ctxreg update -k  "HKEY_LOCAL_MACHINE\SYSTEM\
      CurrentControlSet\Control\Citrix\WinStations\cgp"   -v  "
      fEnableWinStation" -d "0x00000001"
   <!--NeedCopy-->
   ```

Supportability Service

April 17, 2024

Citrix supportability service is launched as a daemon service in VDA.

With this service, anonymous feature usage and diagnostic information is collected and available to assist further troubleshooting and other activities.

Data Point	Key Name	Description
Machine GUID	machine_guid	Used as an identifier the data comes from the same machine
OS name and version	os_name_version	A string denoting the macOS name and version on this machine
Kernel version	kernel_version	A string denoting this machine's kernel version
GPU type	gpu_type	The GPU type on this machine
CPU type	cpu_type	The CPU type on this machine
CPU cores	cpu_cores	Integer denoting the number of CPU cores on this machine
CPU frequency	cpu_frequency	Float denoting the CPU frequency in MHZ
Physical memory size	memory_size	Integer denoting the physical memory size in KB
VDA version	vda_version	A string denoting the installed version of Mac VDA
VDA update or fresh install	update_or_fresh_install	A string denoting the current VDA package is being fresh installed or updated. Enum values • install • update
VDA update or fresh install	update_or_fresh_install	A string denoting the current VDA package is being fresh installed or updated. Enum values • install • update
AD solution	ad_solution	A string denoting this machine's domain join method • NonDomainJoinedMode • DomainJoinedMode
System locale	system_locale	A string denoting the locale of this machine

Data Point	Key Name	Description
VDA virtualization type	vda_virtualization	A string denoting the hypervisor where VDA is created • Physical machine • Virtual machine
Farm Id	farm_id	String denoting the farm id
Session key	session_key	Used to identify the data comes from the same session
Resource type	resource_type	A text string denoting the resource type of the launched session: desktop
Receiver client type	receiver_type	An integer value to represent the receiver type that is used to launch this session, valid values: {“1”, “82”, “257”, “81”, “257”, “84”, “83”}. The meaning 1 Windows 82 Mac 257 Chrome 81 Linux 257 HTML5 84 Android 83 iOS
Receiver client version	receiver_version	A string value to represent the receiver’s version that is used to launch this session
User selected Language	ctxism_select	The string value is a composed long string, which includes all the languages the user selected
Video codec type	grahpic_video_codec_type	The video codec type being used for Thinwire. Valid values: {“H264”, “H265”, “None”}

Data Point	Key Name	Description
Logon credential type	credentials_type	An integer value to represent LVDA logon credential type. Valid values: { "PASSWORD"}
MTU	mtu	A string denoting whether MTU is used in this session, valid values: { “Enabled”, “Disabled” }
MTU MSS	mtu_mss	An integer value donating the MSS size
Keyboard layout Sync mode	VDAKeyboardSync	The keyboard layout synchronization mode: { “Disabled”, “ClientKeyboard-LayoutSyncOnce”, “ClientKeyboardLayoutSync”}
Active keyboard layout	VDAKeyboardLayout	The input source name that getting active in a session, including the ones that dynamically Synced in

Policy Support List

April 16, 2024

Policy support list in Public TP

Work is ongoing to support majority policies that was supported in the Windows and Linux VDA.

For this Public TP, Refer to the table for policy support list:

Policy Name	Key in **Citrix Registry**	Type-Policy Scope	Module - VDA Module	Default Value	When takes Effect	Windows Behavior	VDA Support or Not
ICA keep alives	SendICAKeepAlives	computer	ICA \ Keep Alive	Do not send ICA keep alive messages (0)	reboot		Y
ICA keep alivetime-out	ICAKeepAliveTimeout	computer	ICA \ Keep Alive	60 seconds	reboot		Y
ICA listener port number	IcaListenerPortNumber	computer	ICA	1494	reboot		Y
HDX Adaptive Transport	HDXoverUDP	computer	ICA	Preferred(2)	reboot		Y
Rendezvous protocol	RendezvousProtocol	computer	ICA	Prohibited	reboot		Y
Session reliability connec-tions	AcceptSessionReliabilityConn	computer	ICA \ Session Reliability	Allowed(1)	reboot		Y
Session reliability port number	SessionReliabilityPort	computer	ICA \ Session Reliability	2598	reboot		Y
Session reliability timeout	SessionReliabilityTimeout	computer	ICA \ Session Reliability	180s	reboot		Y
Auto Client Re-connect	AllowAutoClientReconnect	computer	ICA \ Auto Client Re-connect	Allowed (1)	reboot		Y
Reconnection UI trans-parency level	ReconnectionUITransparencyLevel	computer	ICA \ Auto Client Re-connect	80%	reboot		Y

Policy Name	Key in **Citrix Registry**	Type-Policy Scope	Module - VDA Module	Default Value	When takes Effect	Windows Behavior	VDA Support or Not
Client audio redirection	AllowAudioRedir	user	Audio	Allowed (1)	disconn -> reconn	disconn -> reconn	Y
Client microphone redirection	AllowMicrophoneRedir	user	Audio	Allowed (1)	disconn -> reconn	disconn -> reconn	Y
Client clipboard redirection	AllowClipboardRedir	user	Clipboard	Allowed (1)	disconn -> reconn	disconn -> reconn	Y
Target minimum frame rate	TargetedMinimumFramesPerSecond	user	ThinWire	10 fps	sw enc: disconn -> reconn; hw enc: N/A		Y
Target frame rate	FramesPerSecond	user	ThinWire	30 fps	sw enc: disconn -> reconn; hw enc: logoff->login		Y
Visual quality	VisualQuality	user	ThinWire	Medium (3)	sw enc: disconn -> reconn; hw enc: N/A		Y
Use video codec for compression	VideoCodec	user	ThinWire	Use when preferred (3)	sw enc: disconn -> reconn; hw enc: N/A		Y

Policy Name	Key in **Citrix Registry**	Type-Policy Scope	Module - VDA Module	Default Value	When takes Effect	Windows Behavior	VDA Support or Not
Allow visually lossless compression	AllowVisuallyLosslessCompression	User	ThinWire	Disabled (0)	disconn → reconn	disconn → reconn	Y
Preferred color depth for simple graphics	PreferredColorDepth	user	ThinWire	24 bits per pixel(1)	sw enc: disconn -> reconn; hw enc: N/A		Y
ICA round trip calculation	IcaRoundTripCheckEnabled	user	ICA\End User Monitoring	Enabled (1)	reboot	disconn -> reconn;logoff -> logon	Y
ICA round trip calculation internal	IcaRoundTripCheckPeriod	user	ICA\End User Monitoring	15	disconn -> reconn;logoff -> logon	disconn -> reconn;logoff -> logon	Y
ICA round trip calculations for idle connections	IcaRoundTripCheckWhenIdle	user	ICA\End User Monitoring	Disabled (0)	disconn -> reconn;logoff -> logon	disconn -> reconn;logoff -> logon	Y
Session idle timer	EnableSessionIdleTimer	user	Session Timers	Enabled(1)	disconn -> reconn; logoff -> logon	disconn -> reconn; logoff -> logon	Y
Session idle timer interval	SessionIdleTimerInterval	user	Session Timers	1440 minutes	disconn -> reconn; logoff -> logon	disconn -> reconn; logoff -> logon	Y
Disconnected session timer	EnableSessionDisconnectTimer	user	Session Timers	Disabled(0)	active -> disconn	active -> disconn	Y

Policy Name	Key in **Citrix Registry**	Type-Policy Scope	Module - VDA Module	Default Value	When takes Effect	Windows Behavior	VDA Support or Not
Disconnected session timer interval	SessionDisconnectTimer	User	Session Timers	1440 minutes	active -> disconn	active -> disconn	Y
Client keyboard synchro-nization land IME improve-ment	ClientKeyboardLayoutSync	User	Keyboard & IME	Disabled(0)	disconn -> reconn	disconn -> reconn	Y

Known Issues

April 16, 2024

In this section, we provide details on

- Limitations
- Troubleshooting Guide

Limitations

April 16, 2024

Audio Redirection Opus codec is supported with the following limitations or known issues.

- Fast user switch in the session may cause audio to stop working. This issue only happens with Windows CWA.
  - This is a known issue with a solution ongoing to fix.
  - **Workaround** is to do a full logout of the current user before switching.

Keyboard & Mouse:

- Long-pressing vowel keys (a,e,i,o,u) to type accented characters with **Scancode** mode is not supported.
- When you connect from CWA Windows, resizing the session window from window mode to full-screen sometimes results in an inaccurate mouse focus in rare cases.
  - The workaround is to resize the CWA window again.
- When you connect from CWA Windows with Surface Pro, the soft keyboard cannot popup automatically.
  - The workaround is to manually open it from the toolbar.
- Changing the **Natural scrolling** setting in macOS VDA will not take effect, because what you configure is for a physical connected mouse.
  - Workaround is to change the client CWA setting accordingly.
- Insert key in the Windows full-size keyboard is designed to work as a **Fn** key in macOS VDA.
  - It does not support combinations with up / down / left / right keys.

> **Note :**
>
> When you connect from CWA macOS, Citrix recommends you to use **scancode** for keyboard input mode.

Trackpad, currently in this Public Tech Preview, we support:

- Tap to click
- Right-click
- Scroll gestures

Work is in progress to support more functionalities listed in this page: https://support.apple.com/en-us/102482

High DPI, your end-point's monitor must have a resolution greater than 2K to use this feature. If you're connecting to the VDA using CWA Windows, you can:

- Change Windows native scaling to 200%

  OR

- Change the Windows CWA setting in the **monitor layout** - DPI scaling to 200%

Graphics, currently in this Public Tech Preview,

We do not support Spin Cursor and sleep function for the monitor.

Monitor blanking might not work with some special monitors, the monitors which can't be blanked out will not display any application window.

Network, Citrix recommends you to use only one NIC if your VDA machine has multiple NICs.

- The behavior using multiple NICs is not guaranteed.

Clipboard support the following format copy-in/out when policy is configured from the DaaS management console:

- CF_TEXT
- CF_BITMAP

When you use CWA Linux to connect the VDA, copy-in and out for an image file is not supported - this is a known issue from CWA Linux.

DaaS management Console capabilities are under development and are not available at the moment:

- Policies outside the **policy support list** are not supported for the Public Tech Preview.
- In session control, **Shadow User**, **Machine Operations** and **Send Message** are not supported.
- Under **Monitor/Resource Utilization**, **IOPS & Disk Latency** are not fully supported.
- **List and Manage Application** and **Process Information** under **Monitor/Activity Manager** are not supported.
  - Restart/Reset Profile/Reset Personal vDisk is also not supported.

macOS Specific:

- Citrix recommends not to use the macOS VDA session to upgrade the macOS (For example, 13->14).

Tips and Troubleshooting Guide

March 27, 2024

Tips

- If your first installation failed or you have an older VDA but you like to enroll it towards a new DDC, invoke "sudo /opt/Citrix/VDA/bin/vdaconfig"to re-open the vdaconfig tool UI to perform corresponding actions.

- Regarding the performance testing under a high-latency network Env, we can do the following to get a better result.

    1. Change the FPS target from the default value of 30 to 15.
    2. Change to Full-screen H264 and give a test. (The fonts on the desktop may look slightly blurry, but the performance will be improved. It is a handoff between quality and performance).
    3. Change the rate limit from the default of 30 to 20 (it only works to FullScreen H264 and Selective H264)

Troubleshooting Guide

While you deploy and use Citrix VDA for macOS, you may face some problems. Here are some common issues that you may encounter.

The CWA (Citrix Workspace App) cannot launch the session to my remote macOS device

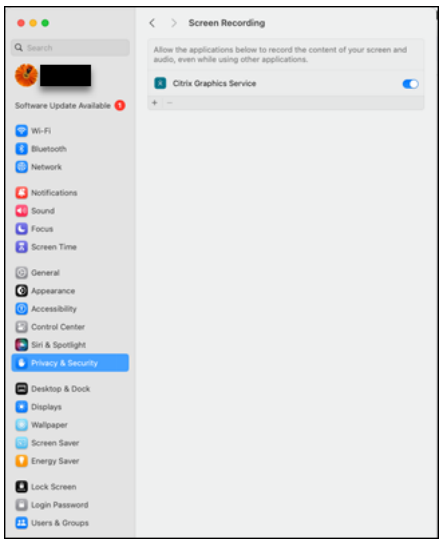
To launch a session successfully, your Citrix VDA must be enrolled and correctly configured in the Citrix DaaS console. Log in to the Citrix DaaS console and check the following items.

1. Make sure that the machine is shown as **Registered**.

2. Assign the user with a machine in the delivery group settings.

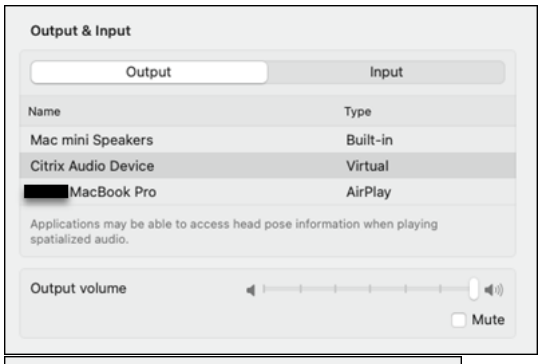
I can connect but the CWA is showing a gray screen

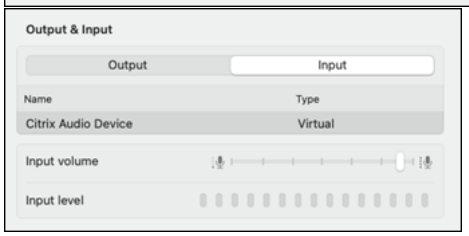
Check whether the **Screen Recording** privacy setting is enabled for **Citrix Graphics Service**.



I cannot hear or record any voice from my CWA side

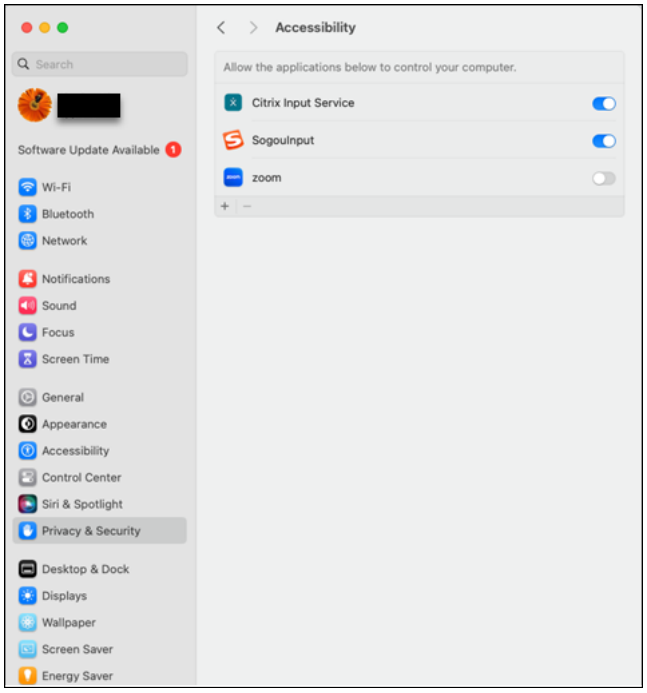
Make sure that your audio input and output is using **Citrix Audio Device**.





I cannot enter the text

Make sure the **Accessibility** permission is assigned to the Citrix Input Service.



For easy troubleshooting on how to enable remote desktop and remote login to VDA machine, Refer

- Remote desktop https://support.apple.com/en-sg/guide/mac-help/mh11851/mac
- Remote login https://support.apple.com/en-sg/guide/mac-help/mchlp1066/mac

What information should I collect if the problem persists?

M: mandatory field O: optional field

[M] Issue Description

[M] Blocking issue (Yes) or (No)

[M] VDA macOS version, apple silicon M1 or M2

[M] VDA version: You can get the version by the following command:

```
$ /opt/Citrix/VDA/bin/vdaversion
```

[M] CWA type and version

[O] Issue reproducible (Yes) or (No)

[O] Screenshots or screen captures (if any)

[M] VDA side system information and logs:
Please run the following command to collect system information and VDA configurations/logs. The

information is packaged as a single file. Please attach this file when you report any issues.

```
$ sudo /opt/Citrix/VDA/bin/xdlcollect.sh
```

In addition, also include the output of the following command. This information includes the session information such as the protocols, connection details

```
$ /opt/Citrix/VDA/bin/ctxsession -v
```