Citrix Virtual Delivery Agent for macOS

Contents

Citrix Virtual Delivery Agent for macOS

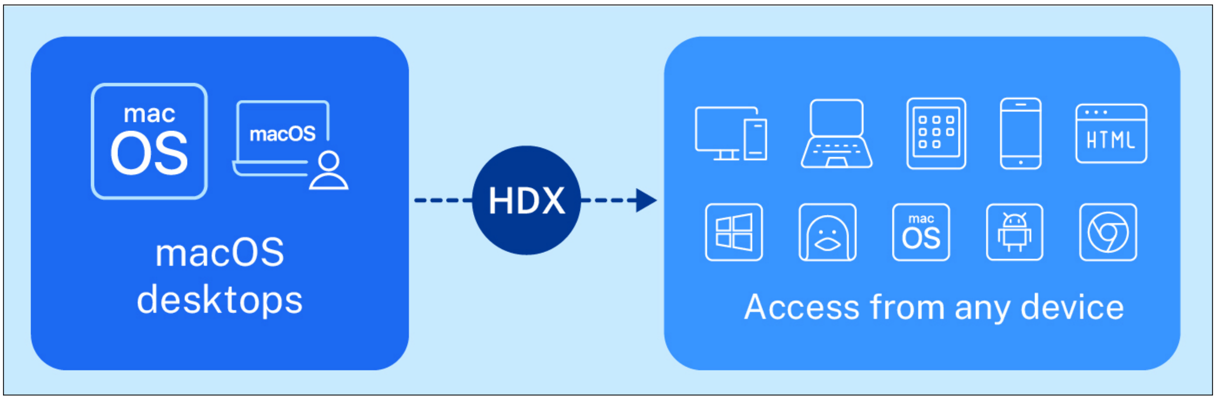
December 22, 2025

At Citrix, we are committed to exploring new technologies and driving innovation to address market needs and solve customer challenges everyday.

This mindset and our dedication has established our leadership position in DaaS and VDI solutions.

First we delivered Windows multi-session apps and desktops building upon Terminal Services and Remote Desktop Services. Then VDI came along with Windows single-session desktops offering end users both non-persistent and persistent varieties for expanded use cases. Later we expanded to offer multi-session and single-session Linux desktops which are popular with engineers, developers, and other power users.

Now, we are thrilled to present to our customers another major stride in the evolution of workload delivery options: Citrix VDA for macOS (macOS VDA) to continue the innovation journey! In this release, we did a very comprehensive integration test with the latest CVAD LTSR 2507 CU1 and CVAD 2511. For customers who prefer to use LTSR, refer to the related information to setup your environment to start the macOS VDA journey; meanwhile, we continue to ship exciting features such as session watermarking, "Shield V2", smart card support etc. to enhance our use cases and contribute to the **Secure AI Developer** ecosystem growth. Refer to What's New and the corresponding feature pages for details.



The new VDA is available in our official download page. Follow this product documentation to start deployment of this new VDA in your organization.

> **Note:**
>
> Our architecture utilizes non-domain-joined websocket technology, though Mac devices can be part of Active Directory (AD) if organizations would like to configure as such. For DaaS users, while Cloud Connectors aren't required (currently macOS VDA supports Connector Appliance), Rendezvous V2 is necessary for session traffic when using Citrix Gateway Service if session is not brokered from Netscaler/StoreFront. Please go through following sections if you need a quick

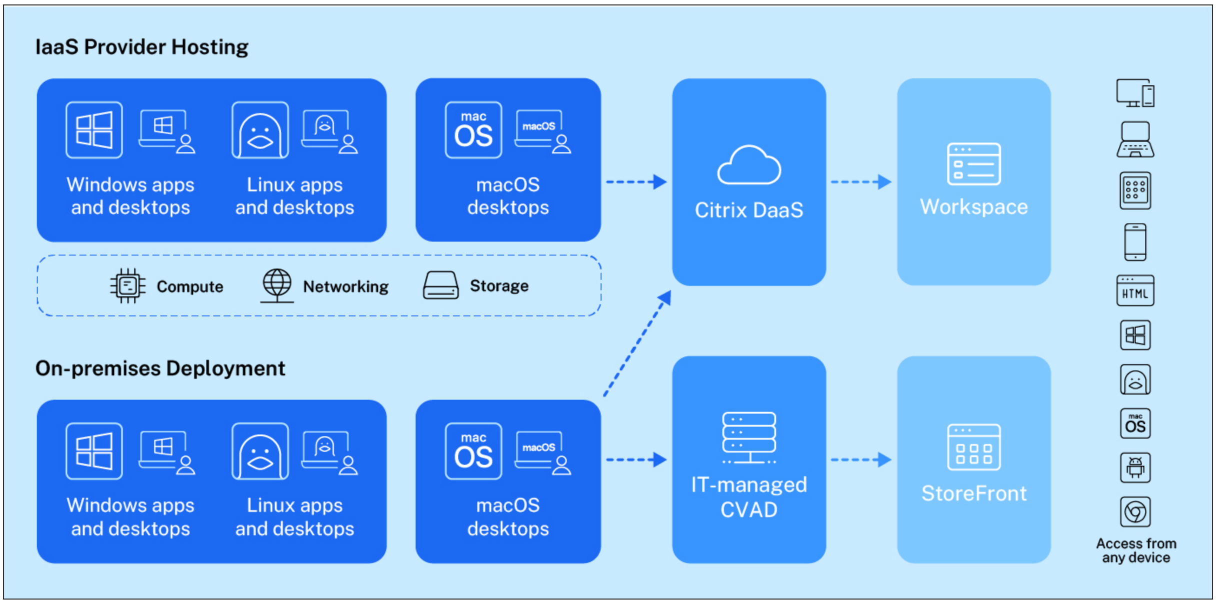
> start:

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

In general, using Citrix VDA for macOS follows similar workflows as Windows and Linux VDAs making it easy for existing Citrix customers:

- Install the VDA on Mac devices that meet the system requirements by using the installer provided or your preferred UEM solution, register it with a Machine Catalog in the management plane, and grant related macOS access rights to the VDA.
- Configure the Delivery Group through Web Studio then apply Citrix Policies and related configurations.
- Use Web Studio to make the macOS desktop available to your end user(s) through Workspace/-StoreFront - then both your end user and IT department are ready to go.

Citrix VDA for macOS can be deployed to wherever physical Mac machines reside - workplaces to serve as "Remote PC", in the on-premises data center or an IaaS provider such as MacStadium or AWS. Please also refer to this deployment guide that provides more detailed guidance.



Third party notices

December 22, 2025

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)

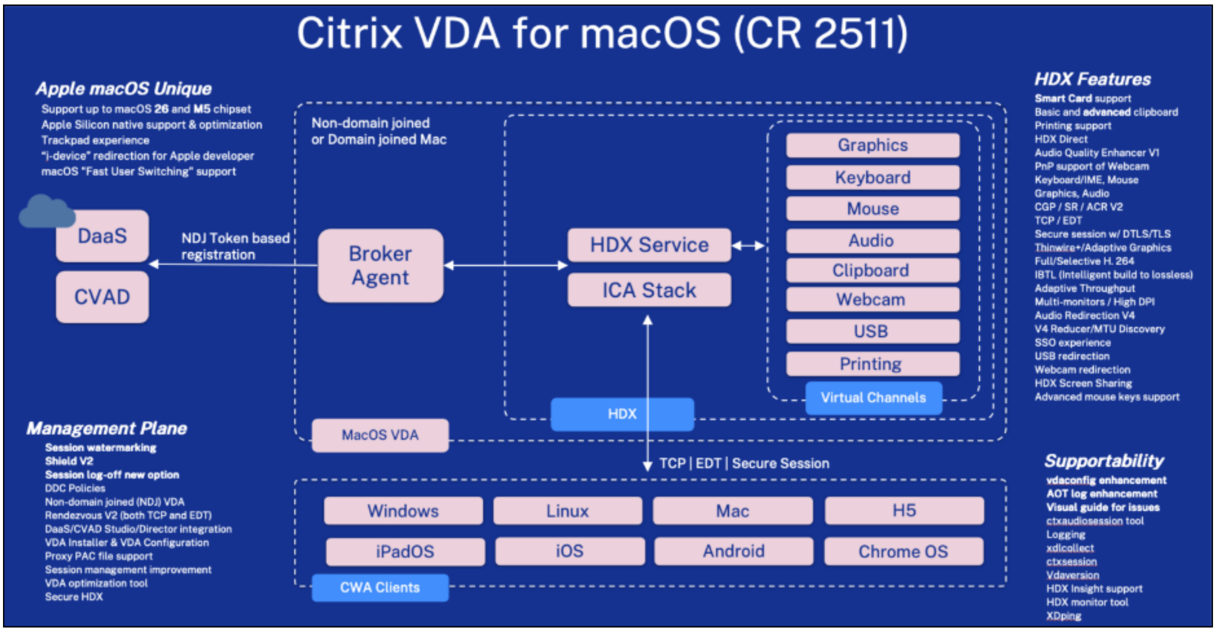
Citrix VDA for macOS - Remoting Mac for Enterprise with HDX™

December 22, 2025

Many enterprises have a long time need for remote access to their Mac devices powered by a secure and comprehensive delivery platform such as Citrix DaaS/CVAD. At the same time, Mac users will not accept any compromise regarding performance and graphics/audio fidelity degrading - this is exactly where Citrix HDX user experience technology comes into play given our over three decades experience in this domain.
We have architected the Citrix VDA for macOS with the following major personas/use cases in mind:

- **Developer**, where all iOS, ipadOS, macOS, watchOS, tvOS, and visionOS development and test work is performed in a macOS environment with XCode and related toolchain.
- **Designer**, in the multimedia and entertainment industry (Film, Audio, Game, 3D Simulation, etc …) where macOS-based applications are heavily used and well-loved by professionals.
- **Remote PC** use case, that organization can provide the latest powerful & economical Mac mini etc. for any knowledge workers in the financial vertical, educational institutions, medical industry where security performance and experience are also key considerations for remote access.

From our initial architecture design of this solution and throughout previous preview programs & GA release, we have planned and implemented major features and capabilities to align with these user personas & constantly evolving our roadmap according to customer needs & ecosystem trend, in this **2511** release, major features and general architecture of the product can be referenced from below diagram:



Citrix VDA for macOS (CR 2511)

Apple macOS Unique

Support up to macOS **26** and **M5** chipset
Apple Silicon native support & optimization
Trackpad experience
"i-device" redirection for Apple developer
macOS "Fast User Switching" support

Management Plane

Session watermarking
Shield V2
Session log-off new option
DDC Policies
Non-domain joined (NDJ) VDA
Rendezvous V2 (both TCP and EDT)
DaaS/CVAD Studio/Director integration
VDA Installer & VDA Configuration
Proxy PAC file support
Session management improvement
VDA optimization tool
Secure HDX

HDX Features

Smart Card support
Basic and **advanced** clipboard
Printing support
HDX Direct
Audio Quality Enhancer V1
PnP support of Webcam
Keyboard/IME, Mouse
Graphics, Audio
CGP / SR / ACR V2
TCP / EDT
Secure session w/ DTLS/TLS
Thinwire+/Adaptive Graphics
Full/Selective H. 264
IBTL (Intelligent build to lossless)
Adaptive Throughput
Multi-monitors / High DPI
Audio Redirection V4
V4 Reducer/MTU Discovery
SSO experience
USB redirection
Webcam redirection
HDX Screen Sharing
Advanced mouse keys support

Supportability

vdaconfig enhancement
AOT log enhancement
Visual guide for issues
ctxaudiosession tool
Logging
xdlcollect
ctxsession
Vdaversion
HDX Insight support
HDX monitor tool
XDping

What's New in 2511

January 27, 2026

Citrix VDA for macOS has been fully GA since 2503 release, for this CR2511, we had done intensive integration test with the latest CVAD LTSR 2507 CU1, to ensure customers who prefer to use LTSR will have a smooth experience deploying macOS VDA during their upgrade to the new LTSR. Alongside, we also added many exciting features in this release:

- **Session watermarking**, this is an important security feature requested by many customers. Now we're fully supporting this capability, include choosing various fields from the session or user information, and also customizable text. For more information about how to enable and configure it, please refer to the feature page.
- **Shield V2 support:** this is another important user experience feature while macOS VDA can continue provide remote macOS desktop during Citrix Cloud disruption caused by network etc. issues; when enabled, end user can continue enjoy seamless remote desktop experience without notice of the control plane turbulence. For more information, please check out the feature page.
- **File copy-paste support:** administrator now can fine tuning Citrix security policy to allow end user to do copy and paste for various file formats; for details what format are supported and how to configure policies, accordingly, please refer to related section for details:
    - Clipboard support

    - Copy-paste file
    - MacOS VDA policy

- **Smartcard support:** macOS VDA now also supports secure authentication using smart card within HDX sessions on macOS, providing security through hardware-based authentication tokens. The implementation supports both traditional smart card authentication and modern FIDO2 password-less authentication. For details, please refer to feature page.
- **Multiple audio feature enhancements** : Starting with the 2507 version, audio quality enhancer is enabled by default for adaptive audio over EDT loss tolerant mode for audio, and in Tech Preview over reliable transport. Further, audio volume synchronization is now available with macOS VDA, and the audio diagnostic tool has undergone significant improvements in this release.

Several important **system level enhancements** for end user and admin experience:

- We did some revamp of VDA Configuration tool by adding power management check option for admin/end-user
- We now provided graphs for end-user self-troubleshooting when they encounter blank screen when launch session
- Administrator now able to configure VDA session to be log-off once end user log-off macOS system (or vice versa) for needed situations
- We also enhanced the performance metric of "ICA RTT"so that it more accurately reflects user-interactive RTT, so administrators can observe these metrics in Director that can further assist troubleshooting
- For also updated OPUS audio codec to latest v1.5 for enhanced audio experience
- Critical bug fixes for various areas that improves the performance and stability of this new release

In summary, CR2511 is an exciting release from Citrix containing both feature and performance enhancement. Meanwhile, we're continuing to evolve our roadmap according to customer requirements and Apple ecosystem trends.

What's New in 2503

August 1, 2025

General Availability for Citrix Virtual Apps and Desktops™

Leveraging the latest Citrix Virtual Apps™ and Desktops(CVAD) 2503 features and incorporating positive customer feedback from the Public Tech Preview program, this release introduces General Availability (GA) support for Citrix Virtual Apps and Desktops VDA.

This release has also conducted a full integration test with the latest CVAD 2503. For more information, see Prepare in On-Premises CVAD.

Plug and Play capability support for WebCam redirection

This release of the Citrix VDA for macOS introduces plug-and-play support for webcam redirection, simplifying the user experience. Webcams are automatically detected and configured for use within virtual sessions, removing the need for manual configuration or session reconnections, meanwhile, multiple resolutions of the peripheral camera are supported to redirect as the resolutions of Citrix HDX™ Webcam.
For more information, see Webcam Redirection.

Printing support

This release introduces printing redirection, enabling users to easily print documents and other files from within their macOS VDA desktops to printers connected to their local machines.
Citrix PDF Universal Printer driver is supported in this release.
For more information, see Printing support and Policy Support List.

HDX Direct support

When accessing macOS VDA, HDX Direct allows internal client devices to establish a secure direct connection with the session host if direct communication is possible. This new feature enhances the end user experience even further.
For more information, see HDX Direct.

AQE (Audio Quality Enhancer)

AQE V1 is introduced for Adaptive Audio from this release, Audio Quality Enhancer prevents audio degradation by restoring lost packets and reconstructing audio in real time. It self-adjusts in response to network conditions to optimize audio quality.

Audio diagnostic tool

Citrix Audio Diagnostic Tool is also added for macOS VDA since this release to troubleshoot and monitor Citrix HDX Audio. For more information, see Audio diagnostic tool

Others

Some minor updates to Limitation and network configuration in System Requirement (Proxy Configuration article also moved to under System Requirement) in this release.

What's new in earlier releases

For new features included in the earlier releases, see What's new history.

What's New in 2411

August 1, 2025

Support for new macOS release and Mac devices running Apple Silicon M4:

- macOS sequoia 15.1
- macOS sequoia 15.2
- Apple Silicon M4 based Mac mini and MacBook Pro

For more information, see System Requirements.

Loss tolerant mode for audio

Audio is now supported over the Enlightened Data Transport (EDT) loss tolerant protocol.

This feature increases the user experience for real-time streaming when users are connecting through networks with high latency and packet loss.

When this feature is enabled, Adaptive Transport in Citrix Virtual Apps and Desktops™ uses the EDT loss tolerant transport protocol for a better audio experience.

This feature is disabled by default. For more information, see Loss tolerant mode for audio section.

Extend more Citrix Policies support for Auto Client Reconnect feature

This release extends two more Citrix Policies for Auto Client Reconnect(ACR):

- Auto client reconnect timeout
- Auto client reconnect authentication

For more information, see Policy Support List and Auto Client Reconnect.

Integration with Citrix Virtual Apps™ and Desktops 2411

This release has conducted full integration test with the latest release Citrix Virtual Apps and Desktops(CVAD) 2411. For more information, see Prepare in On-Premises CVAD.

System Requirements

December 22, 2025

System requirements of Citrix VDA for macOS contain both hardware and software aspects. The delivery model is Remote PC Access based on physical Mac devices and the product has been optimized to run exclusively on Apple Silicon (from M1 to M4). The underlying devices must be within the Apple product families listed below to guarantee support and proper operation.

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

Supported Hardware Platforms

- Mac mini
- MacBook Air
- MacBook Pro
- iMac
- Mac Studio
- Mac Pro

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

Supported macOS Versions

Citrix VDA for macOS supports the recent three releases of macOS.

macOS Name	macOS version	VDA Version
Ventura	13.*	Release 2409 and later
Sonoma	14.*	Release 2409 and later
Sequoia	15.*	Release 2411 and later
Tahoe	26.*	Release 2507 and later

> **Note:**
>
> Citrix might be limited in its ability to test all the sub-versions under one major macOS revision.

Network Requirements

For VDA Enrollment and Registration, it is required to configure the VDA outbound traffic to TCP port 443 of the following addresses.

- **For Citrix DaaS™**:
  - **https://[customer_ID].xendesktop.net**
    - delivery controller™ endpoint for your Citrix DaaS
    - [customer_ID] is your Citrix Cloud customer ID as shown in the Citrix Cloud administrator portal.
  - **https://*.*.nssvc.net**
    - Citrix Gateway Service addresses
    - Customers who can"™t enable all subdomains can use the following addresses instead:
      - https://*.g.nssvc.net
      - https://*.c.nssvc.net
  - **https://*.citrixworkspacesapi.net**
    - Used for Gateway Service connectivity check
- **For Citrix Virtual Apps and Desktops™:**
  - **https://[FQDN of On-Premises Delivery Controllers]**
    - Including FQDN of all your delivery controllers

- **For HDX™ sessions connection:**
  - **VDA Inbound Traffic:**
    - UDP and TCP port 2598 and 1494 on VDA must be open.
  - **VDA Outbound Traffic:**
    - VDA to UDP and TCP port 443 of the Citrix Gateway Service addresses ***.*.nssvc.net** must be allowed.
      - The configuration is used when a HDX session is launched through Citrix Gateway Service over Rendezvous protocol. Go to Rendezvous traffic flow for more information.
      - If Citrix Gateway Service is never used, the outbound traffic configuration can be ignored.

You can also view a visual overview of the network configurations based on different remote access options.

See how to disable websocket connection to Citrix Gateway Service if it is never used to access your VDAs.

Proxy configurations

- Proxy configurations for VDA enrollment/registration and HDX session are supported.
- Go to Proxy Configuration support for more information.

Citrix Management Plane Requirement

- Existing DaaS subscription: Standard or above
- Existing CVAD subscription
- Citrix for Private Cloud (CPC)
- Citrix Universal™ Hybrid Multi-Cloud (U-HMC)
- Citrix Platform License (CPL)

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

- Citrix Workspace app 2408 for ChromeOS
- Citrix Workspace app 2404 for HTML5

Additional runtime library

Microsoft .NET Runtime 8.0 is required to install for VDA enrollment and registration.
Install .NET from the Microsoft package feed, for more information, see https://learn.microsoft.com/en-us/dotnet/core/install/macos

Proxy Configuration Support

December 22, 2025

Proxy using PAC file/URI is commonly used in enterprise IT/security management, we have already supported PAC Proxy as part of Citrix VDA for macOS.

Citrix VDA for macOS supports proxy configuration in the following scopes:

- Control traffic (VDA enrollment, registration):
    - VDA local registry settings regarding proxy.
    - macOS system proxy setting including BYPASS, PAC, HTTP, HTTPS proxies.
- HDX™ session traffic:
    - Citrix DDC policy (Rendezvous proxy configuration policy, applied to Citrix DaaS™ only).
    - VDA local registry settings regarding proxy.
    - macOS system proxy setting including BYPASS, PAC, HTTP, HTTPS, SOCKS proxies.

> **Note:**
>
> Conventionally, network communication between VDA and Citrix Control Plane (DaaS or CVAD) is called **Control Traffic**, and between VDA and Citrix Workspace™ app (CWA) is called **HDX Traffic** or **Session Traffic**. VDA **enrollment, registration, and CGS registration** are in the category of control traffic while **Rendezvous** is in the category of HDX traffic.

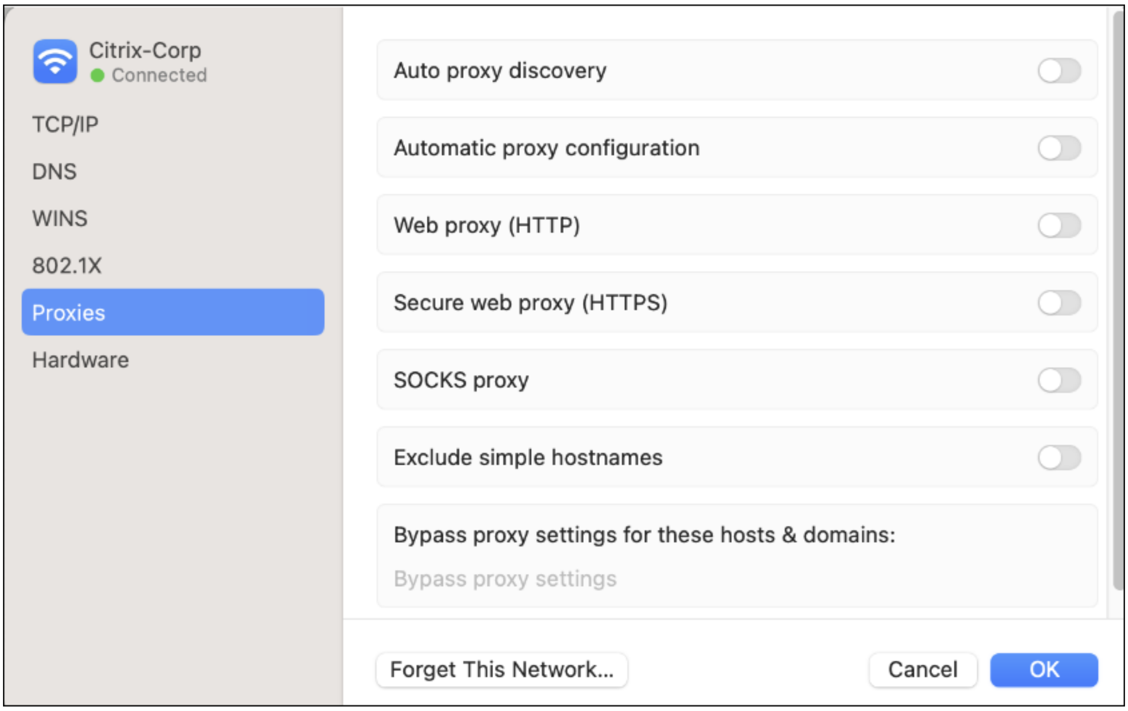
Proxy Configuration

The VDA supports connecting through proxies for both control traffic and HDX traffic. The requirements and considerations are different, please review them accordingly.

Proxy Configuration Methods

- Citrix DDC policy
    - Configure the policy by Admins: Rendezvous proxy configuration
    - Work with the policy Rendezvous Protocol, and applied to Citrix DaaS with Citrix Gateway Service only
- VDA local registry setting:
    - Run the command: `sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\Software\Citrix\VirtualDesktopAgent"-t "REG_SZ"-v "ProxySettings"-d "<Proxy address or PAC file>"--force`
        - Proxy type format: `<http://<URL or IP>:<port> or socks5://<URL or IP>:<port>>`
        - PAC file format: `<http://<URL or IP>/<path>/<filename>.pac>`

        > **Note:**
        >
        > .pac is required as part of PAC file
- macOS system proxy setting:
    - Configure system proxy through System Settings and then Network.
    - We have supported the following system proxy configurations: BYPASS, PAC, HTTP, HTTPS, SOCKS5



Auto proxy discovery ○
Automatic proxy configuration ○
Web proxy (HTTP) ○
Secure web proxy (HTTPS) ○
SOCKS proxy ○
Exclude simple hostnames ○
Bypass proxy settings for these hosts & domains:
Bypass proxy settings

Control traffic proxy considerations

- Only HTTP proxy type is supported through:
    - VDA local registry setting
    - macOS system proxy setting
- Proxy Configuration Priority:
    - If both proxy configurations are set, VDA local registry setting takes precedence over macOS system proxy setting.
- Packet decryption and inspection are not supported. Configure an exception rule in your proxy setting, so the control traffic is not intercepted, decrypted, or inspected. Otherwise, the connection will fail.
- Proxy authentication is not supported.

Refer to network requirements and Proxy Configuration Methods to configure proxy for VDA enrollment and registration.

HDX traffic proxy considerations

> **Note:**
>
> Proxy configuration for HDX traffic is only applied to Citrix DaaS with Citrix Gateway Service.

- It is NOT recommended to configure a proxy for HDX traffic because HDX connection performance may be affected by increased network latency when using a proxy.
- HTTP and SOCKS5 proxy types are supported through:
    - Citrix DDC policy
    - VDA local registry setting
    - macOS system proxy setting
- Proxy Configuration Priority:
    - If Citrix DDC policy is configured, it”™s the highest priority, and then VDA local registry setting takes precedence over macOS system proxy setting.
- HDX Adaptive transport/EDT can only work with SOCKS5 proxies, while TCP will work as the transport protocol for HDX with HTTP and SOCKS5 proxies.
- Packet decryption and inspection are not supported. Configure an exception so the HDX traffic is not intercepted, decrypted, or inspected. Otherwise, the connection fails.
- Proxy authentication is not supported.

Refer to network requirements and Proxy Configuration Methods to configure proxy for HDX session outbound traffic.

Zscaler Private Access

If using Zscaler Private Access (ZPA), it is a transparent proxy for Citrix VDA for macOS, VDA will work without proxy configurations listed above.

But it is strongly recommended that you configure bypass settings for the Gateway Service to avoid increased latency and the associated performance impact for your HDX sessions which are through Citrix Gateway Service.

To do so, you must define ZPA application segments for the Gateway Service addresses which are specified in the network requirements of HDX sessions, and set them to always bypass. For information on configuring application segments to bypass ZPA, see the Zscaler documentation.

Zscaler Client Connector

If using Zscaler Client Connector on the macOS VDA device, it is strongly recommended that you configure bypass settings for NetScaler Gateway to avoid increased latency or network blocking for your HDX sessions which are through on-premises NetScaler Gateway.

To do so, you must configure traffic bypass for VPN Gateway Bypass to add the NetScaler Gateway SNIP, and also configure IPv4/IPv6 Inclusions and Exclusions for IP Bypass for the NetScaler Gateway SNIP.

Installation Overview

December 10, 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 and Workspace ONE as examples. There are other ways to use Jamf PRO etc. software that can achieve similar results as such.

Meanwhile, the general workflow to install, publish and use Citrix VDA for macOS with Cloud-based control plane DaaS or on-prem CVAD (Citrix Virtual App & Desktop) are very similar, in this document, we will highlight areas that are specific to on-prem CVAD using words like "for CVAD customers"or "for CPC (Citrix Private Cloud) customers"as these are content new in this update.

This section guides you through the following procedures:

- Prepare Installation using Non-domain Joined VDA

    - Prepare in On-Premises CVAD
    - Prepare in DaaS
- Use the Installer of Citrix VDA for macOS
- VDA Deployment Recommendation
- Example Using UEM/MDM
- Upgrade Existing VDAs

Prepare Installation Non-Domain joined VDAs

August 1, 2025

This section guides you to prepare the control planes both for CVAD customers and DaaS customers, so you can later install the non-domain joined (NDJ) Citrix VDA for macOS to connect with, then manage the VDAs in the control plane accordingly.

The workflows are quite similar between on-prem CVAD and DaaS, while the most essential step is to generate enrollment tokens from the control plane so the Non-Domain Joined VDA can enroll and register accordingly.

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

> **Important:**
>
> Non-domain-joined VDAs are supported for both Citrix DaaS™ and CVAD.
>
> - 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
> - 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 V2 shall be configured; 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; for more information, please refer to Citrix DaaS install and configure overview.

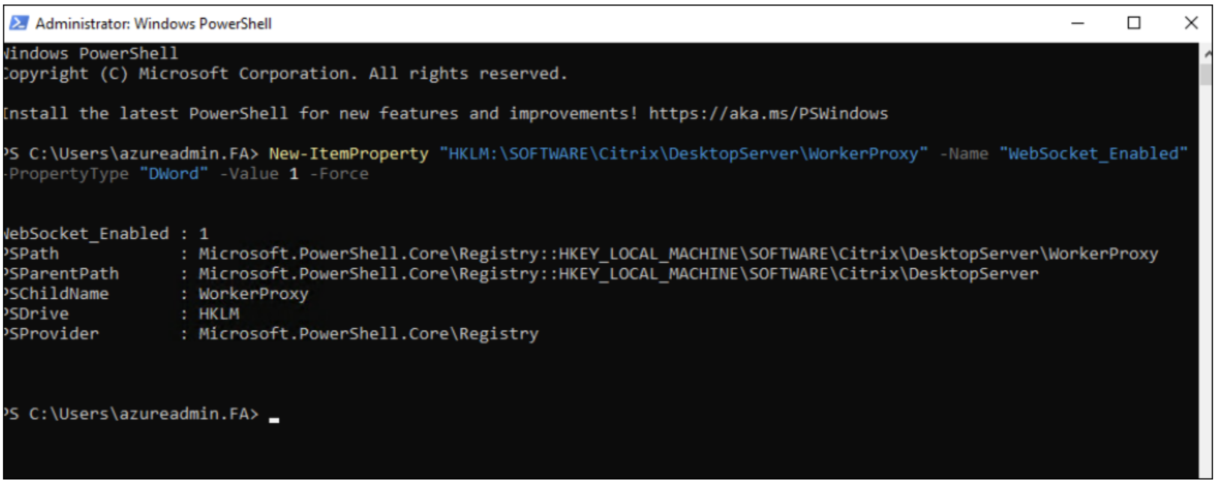
Prepare in On-Premises CVAD

August 1, 2025

Before proceeding, please make sure your CVAD product is revision CR2407 or later, and key components such as Web Studio are all installed correctly.

Step 1: Enable WebSocket Feature in DDC

Open a powershell and run follow command, then reboot the DDC `New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy"-Name "WebSocket_Enabled" -PropertyType "DWord"-Value 1 -Force`.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\azureadmin.FA> New-ItemProperty "HKLM:\SOFTWARE\Citrix\DesktopServer\WorkerProxy" -Name "WebSocket_Enabled"
-PropertyType "DWord" -Value 1 -Force


WebSocket_Enabled : 1
PSPath            : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer\WorkerProxy
PSParentPath      : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
PSChildName       : WorkerProxy
PSDrive           : HKLM
PSProvider        : Microsoft.PowerShell.Core\Registry


PS C:\Users\azureadmin.FA> _
```

Step 2: Create the Machine Catalog and generate enrollment token for VDA

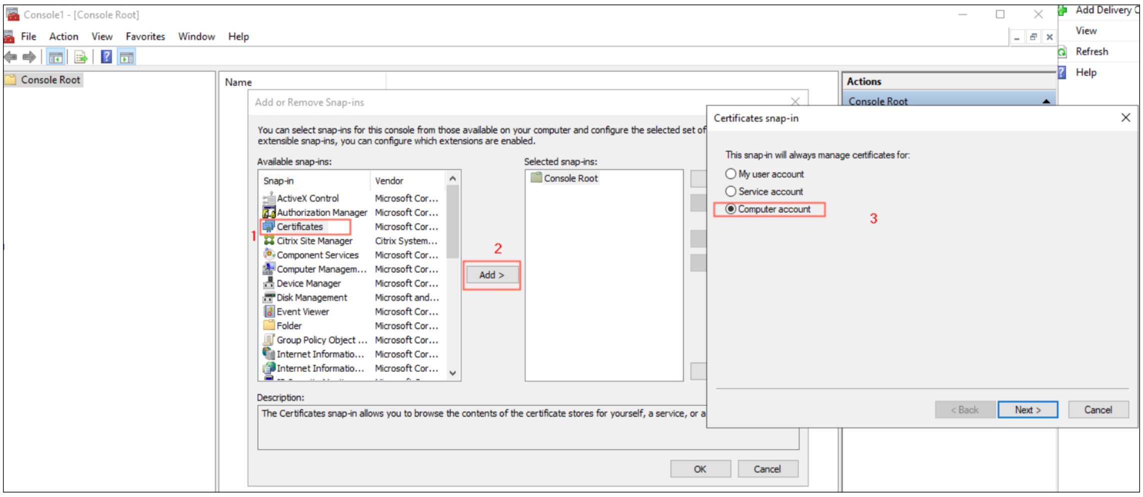
1. Create an empty Single-session OS catalog with no PVS/MCS and no power managed from the web studio. Right click the empty catalog, click Manage Enrollment Tokens.
2. Click Generate and Input the token name, select the Start date and End data. Input the times the token can be used. Click Generate, copy or download the token.

> **Note:**
>
> You can refer to the 1st step of DaaS part for screenshots that are mostly similar.

Step 3: Export self-signed certificate on DDC machines, and then install certs on each VDA machine

The following steps will guide you how to trust DDC self-signed certificates on each VDA machine, but you can also configure VDA with Enterprise/Domain Certificates if you would like.

1. Run MMC to open the console, and then `File`>`Add`/`Remove Snap-in..`>`Certificates`>`Add`>`Computer account`>`Next`>`Finish`>`OK`

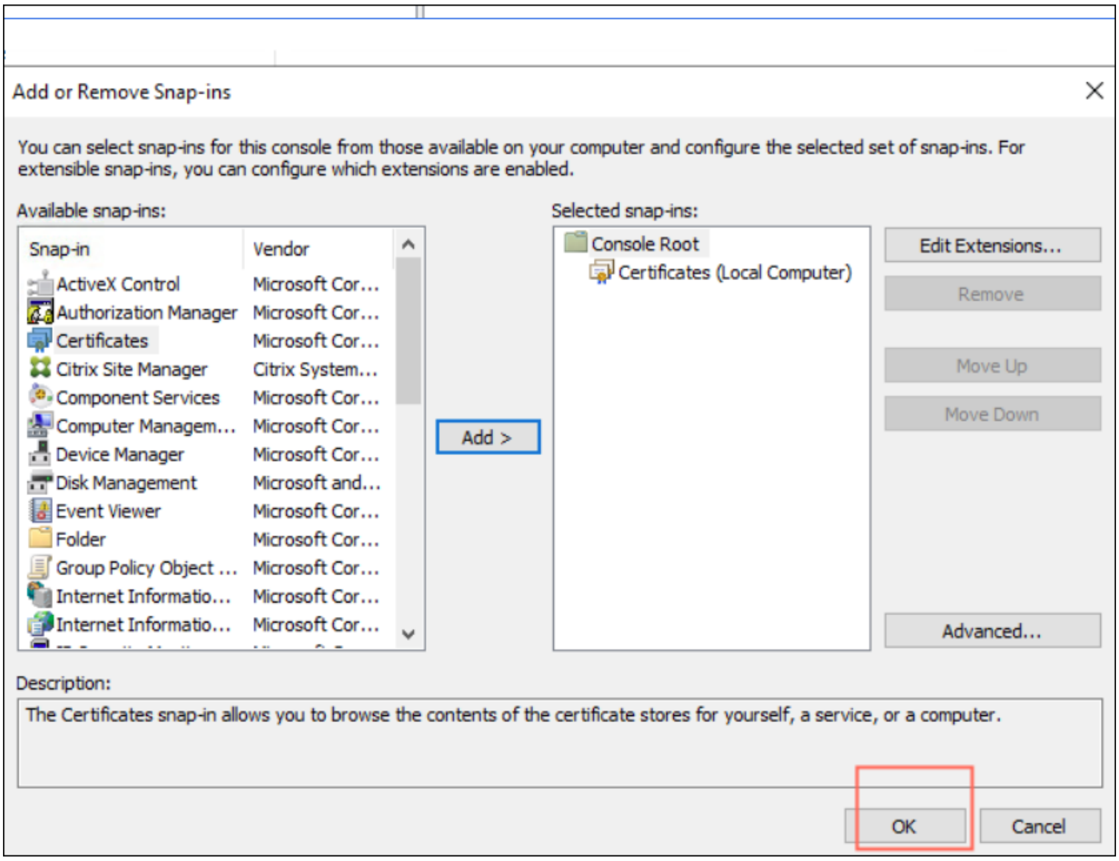


You can select snap-ins for this console from those available on your computer and configure the selected set of extensible snap-ins, you can configure which extensions are enabled.

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a

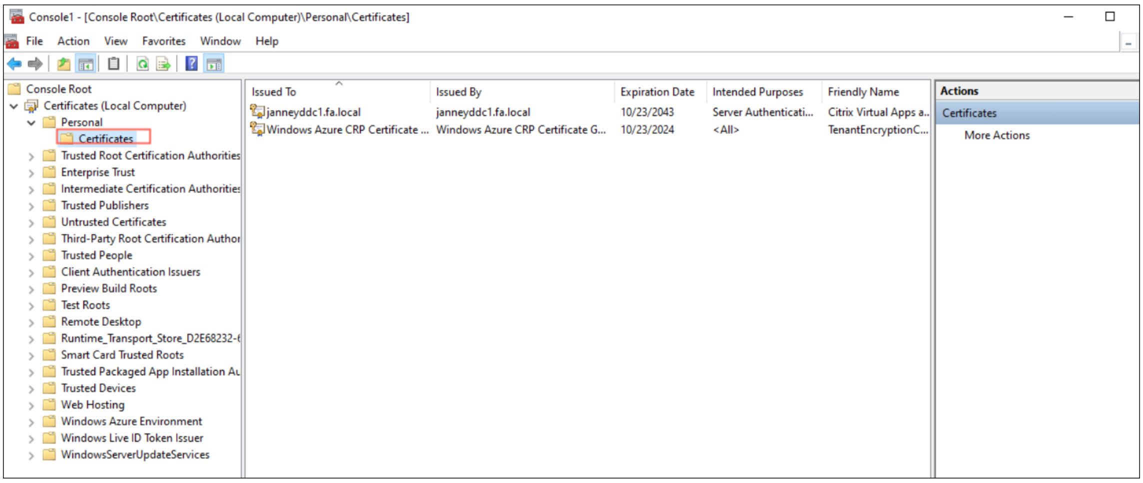


Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

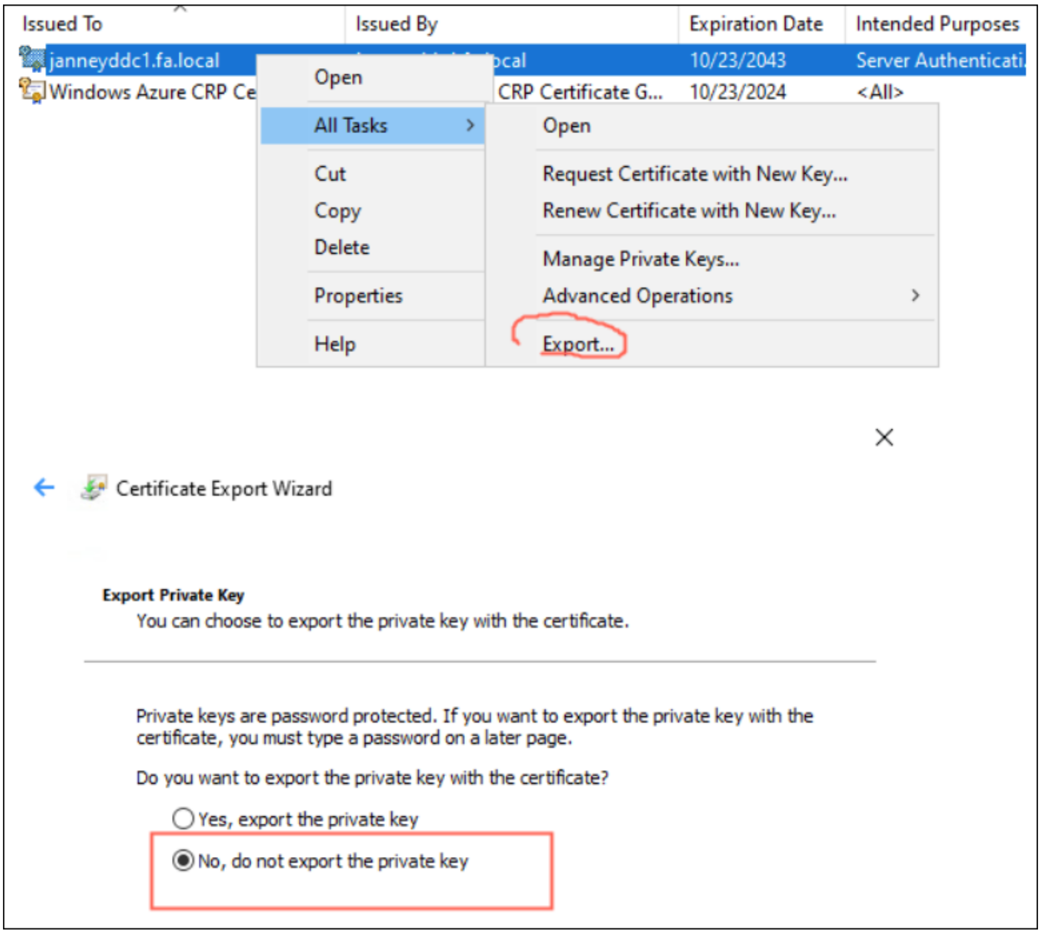
2. Export Certificates with Certificates(Local Computer)>Personal>Certificates.



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Author
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
Remote Desktop
Runtime_Transport_Store_D2E68232-f
Smart Card Trusted Roots
Trusted Packaged App Installation Au
Trusted Devices
Web Hosting
Windows Azure Environment
Windows Live ID Token Issuer
WindowsServerUpdateServices
Actions
Certificates
More Actions

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
janneyddc1.fa.local	janneyddc1.fa.local	10/23/2043	Server Authenticati...	Citrix Virtual Apps a...
Windows Azure CRP Certificate ...	Windows Azure CRP Certificate G...	10/23/2024	<All>	TenantEncryptionC...

3. Select the **certificate > All Tasks > Export**.



Issued To	Issued By	Expiration Date	Intended Purposes
janneyddc1.fa.local	ocal	10/23/2043	Server Authenticati
Windows Azure CRP Ce	CRP Certificate G...	10/23/2024	<All>

Export Private Key

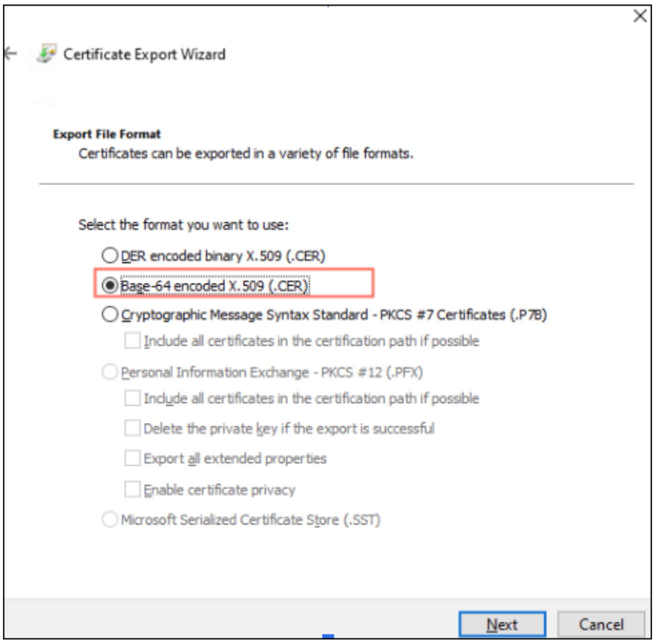
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

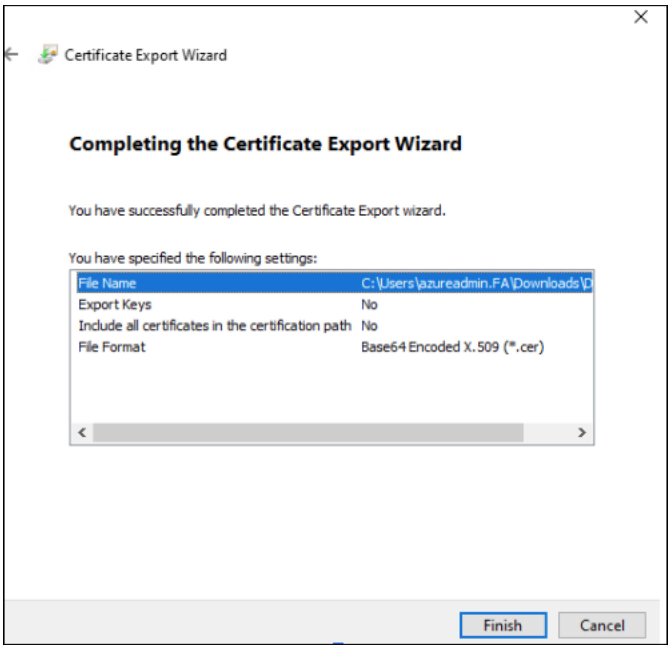
● No, do not export the private key



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  □ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
  □ Include all certificates in the certification path if possible
  □ Delete the private key if the export is successful
  □ Export all extended properties
  □ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

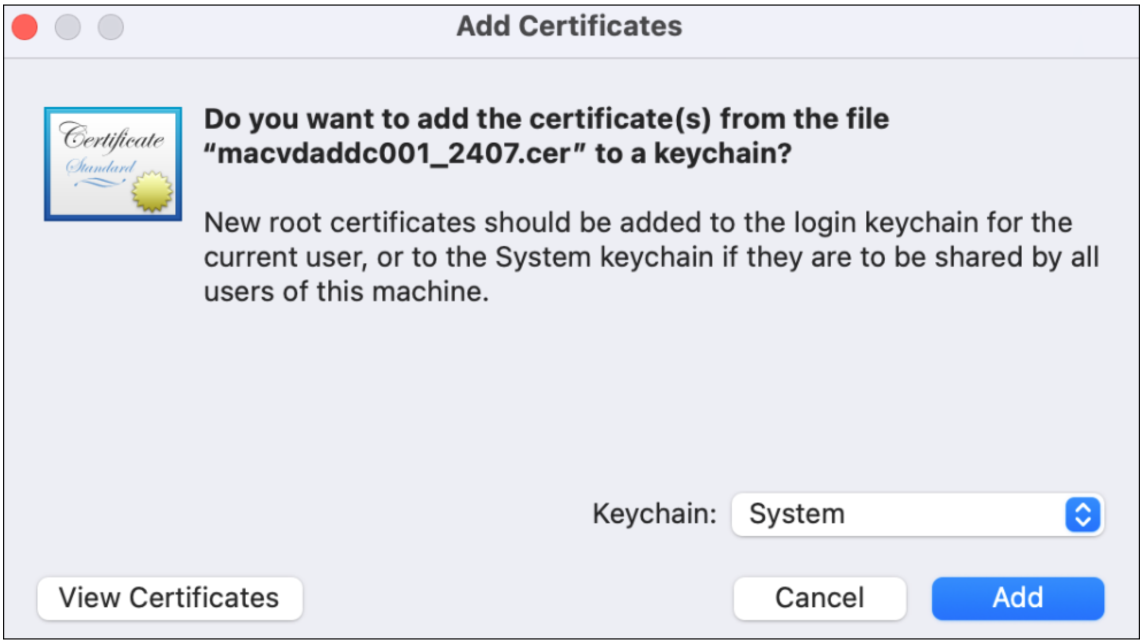
You have specified the following settings:

File Name	C:\Users\azureadmin.FA\Downloads\D
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

Execute steps 2.1-2.3 in other DDCs on the same site.

Step 4: Trust the certificates in Citrix VDA for macOS machine

1. Open the certificates by **Keychain Access** app, and make sure the certificates are added to the **System** keychain.



Add Certificates

Do you want to add the certificate(s) from the file "macvdaddc001_2407.cer" to a keychain?

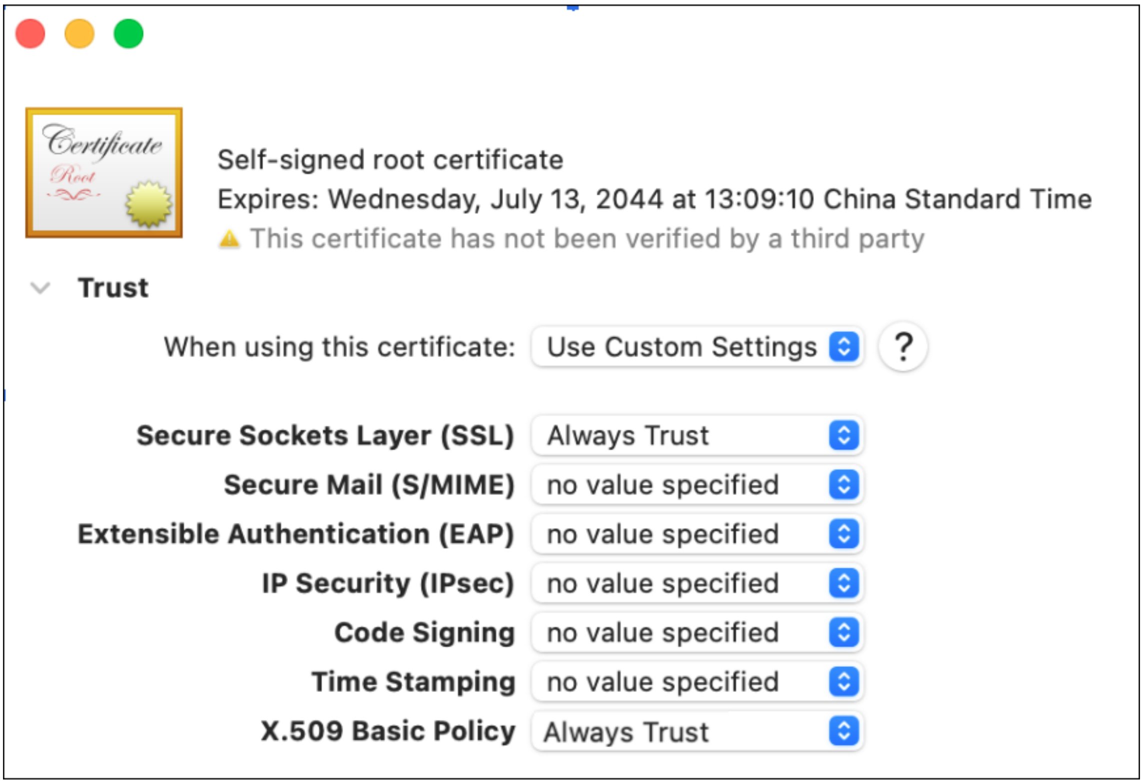
New root certificates should be added to the login keychain for the current user, or to the System keychain if they are to be shared by all users of this machine.

Keychain: System

2. Find the certificates in **System** keychain, and set them to **Always Trust** for at least two categories:

   - Secure socket Layer(SSL)
   - X.509 Basic Policy

   to enable VDA enrollment and registration.



Self-signed root certificate
Expires: Wednesday, July 13, 2044 at 13:09:10 China Standard Time
⚠ This certificate has not been verified by a third party

Trust

When using this certificate: Use Custom Settings

Secure Sockets Layer (SSL)	Always Trust
Secure Mail (S/MIME)	no value specified
Extensible Authentication (EAP)	no value specified
IP Security (IPsec)	no value specified
Code Signing	no value specified
Time Stamping	no value specified
X.509 Basic Policy	Always Trust

Alternatively, you can execute the following commands in Terminal App to trust the certificates:

1. Add one certificate into System keychain and trust it for **Secure socket Layer(SSL)** and **X.509 Basic Policy**.

   ```
   security add-trusted-cert -d -r trustRoot -p basic -p ssl -k /
   Library/Keychains/System.keychain <cert file name>
   ```

2. Verify if the certificate is trusted.

   ```
   security verify-cert -c <cert file name>
   ```

Step 5: Configure Date&Time and DNS on Citrix VDA for macOS machine

1. Set time and date on your Mac to ensure the time synchronization between VDA and DDC has no time offset.
2. Add DNS server to your Mac to resolve DDCs'FQDN, or add new host entries for DDCs into `/etc/hosts`.
3. Verify if the DNS configuration and Certificates are correctly set up

   ```
   curl -w "\nStatus code: %{ http_code } \n"-vI https://<FQDN of On
   -Premises Delivery Controllers>.
   ```

Before proceeding to the next step, ensure that the curl command output ends with the message: **Status code: 200**.

If the status code is not 200, you may need to check the following points:

- Check the certificate, you can also find the certificate information in the curl output under "Server certificate"to verify.
- Verify that the DNS server is configured correctly.
- Ensure that the time synchronization between the VDA and DDC has no time offset.

Once the verification is OK, other steps, such as creating a Machine Catalog and Delivery Group, are the same as when managing Windows and Linux VDAs. Go to Prepare in DaaS Management Console to check the detailed steps.

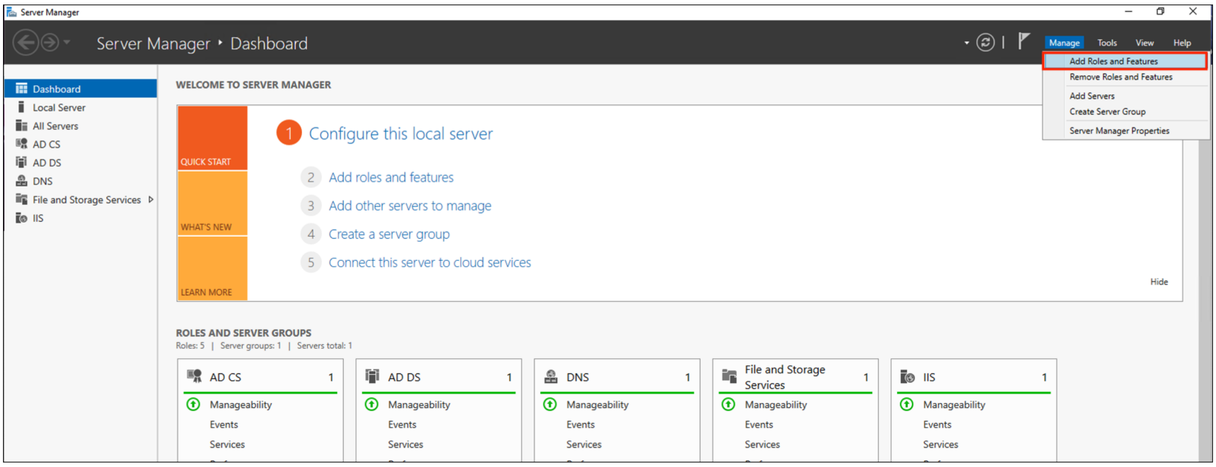
Configure VDA with Enterprise / Domain Certificates

November 12, 2025

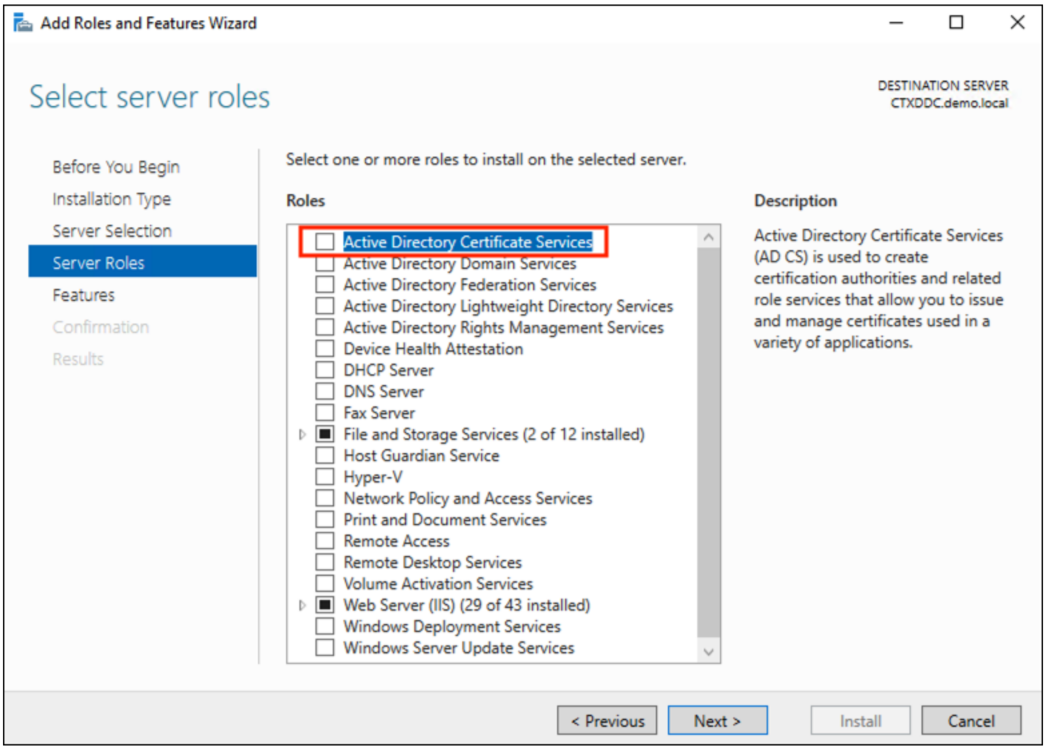
Besides DDC self-signed certificates, there is another option to configure VDA with AD CS issued CA certificates, so that you can configure all Citrix components with one CA certificate. Follow the instructions to Configure VDA with Enterprise/Domain certificates.

Install Active Directory Certificate Services

Log on Active Directory Server, Open Server Manager and click Manage, and then click Add Roles and Features. The Add Roles and Features Wizard opens.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD CS 1
AD DS 1
DNS 1
File and Storage Services 1
IIS 1
Manageability
Events
Services

In Select Server Roles, in Server Roles, select Active Directory Certificate Services.



Select one or more roles to install on the selected server.

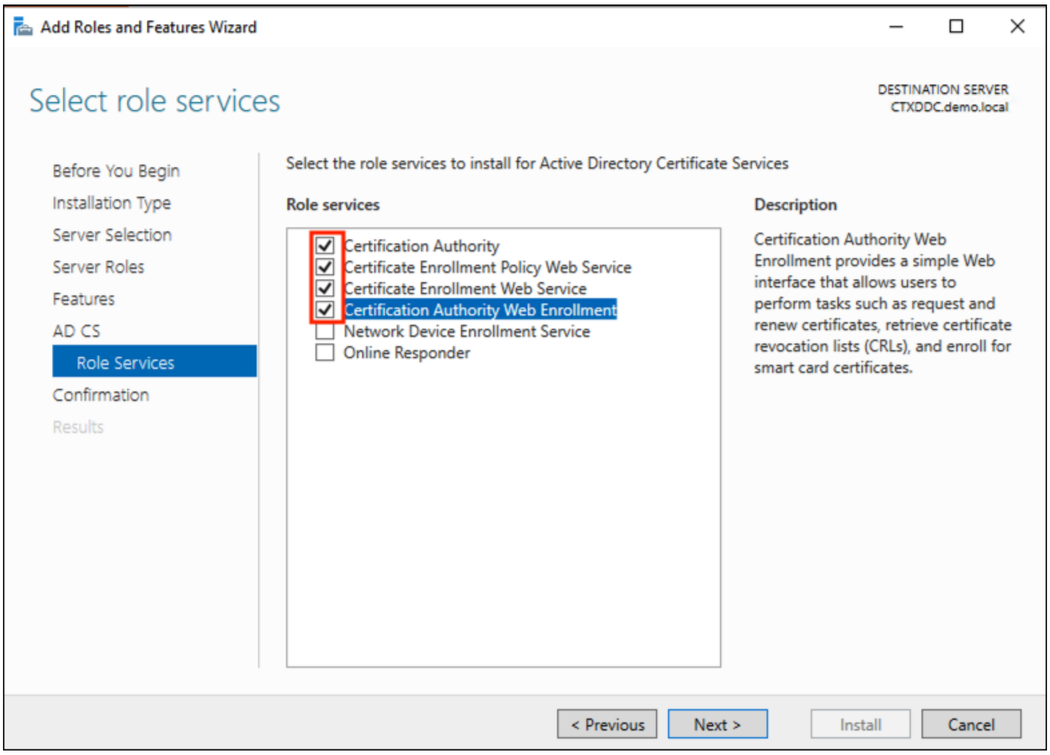
Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (29 of 43 installed)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

In Role Services, Click following items



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
CTXDDC.demo.local

Select the role services to install for Active Directory Certificate Services

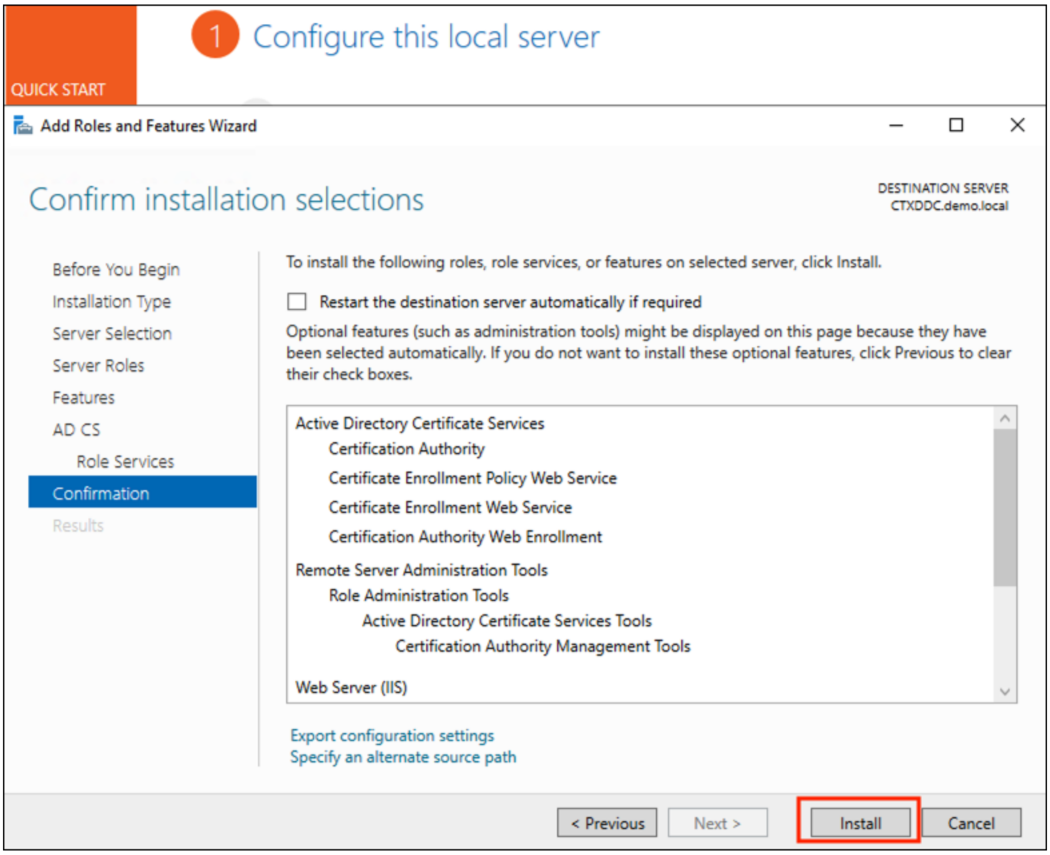
Role services

- ☑ Certification Authority
- ☑ Certificate Enrollment Policy Web Service
- ☑ Certificate Enrollment Web Service
- ☑ Certification Authority Web Enrollment
- □ Network Device Enrollment Service
- □ Online Responder

Description

Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

In Confirmation,, Click Install



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
CTXDDC.demo.local

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

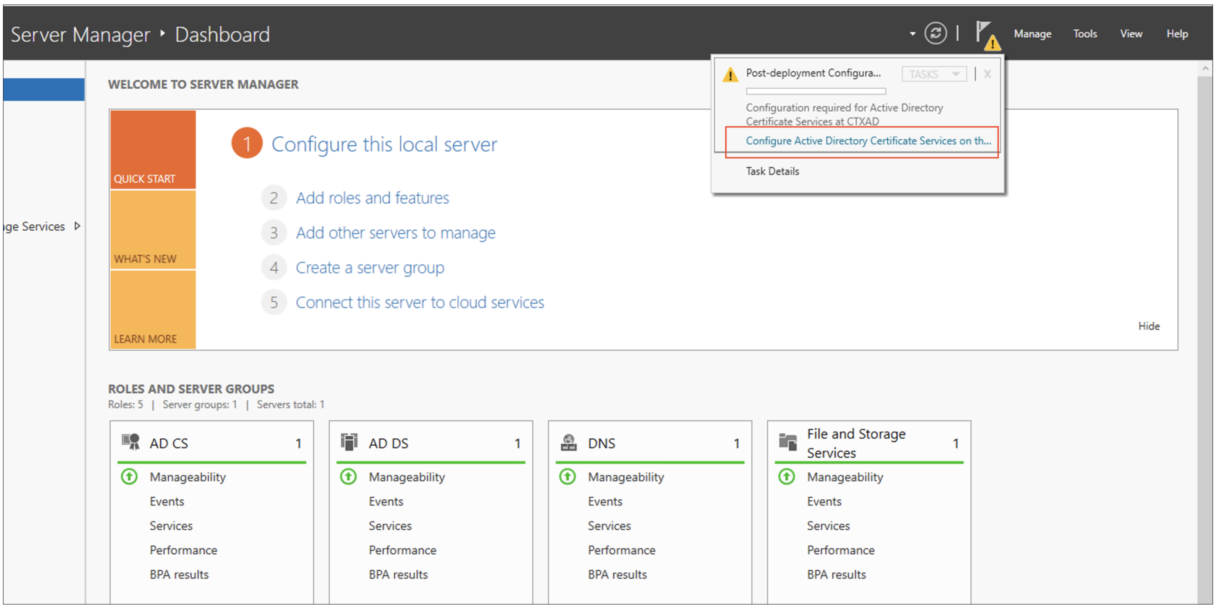
Active Directory Certificate Services
    Certification Authority
    Certificate Enrollment Policy Web Service
    Certificate Enrollment Web Service
    Certification Authority Web Enrollment
Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools
Web Server (IIS)

Export configuration settings
Specify an alternate source path

For more information, see Install the certification authority.

Configure Active Directory Certificate Services

In Server Manager, click on AD CS on the left pane. If there is a warning mark, then click on the flag on the right corner, then click Configure Active Directory Certificate Services to start the configuration



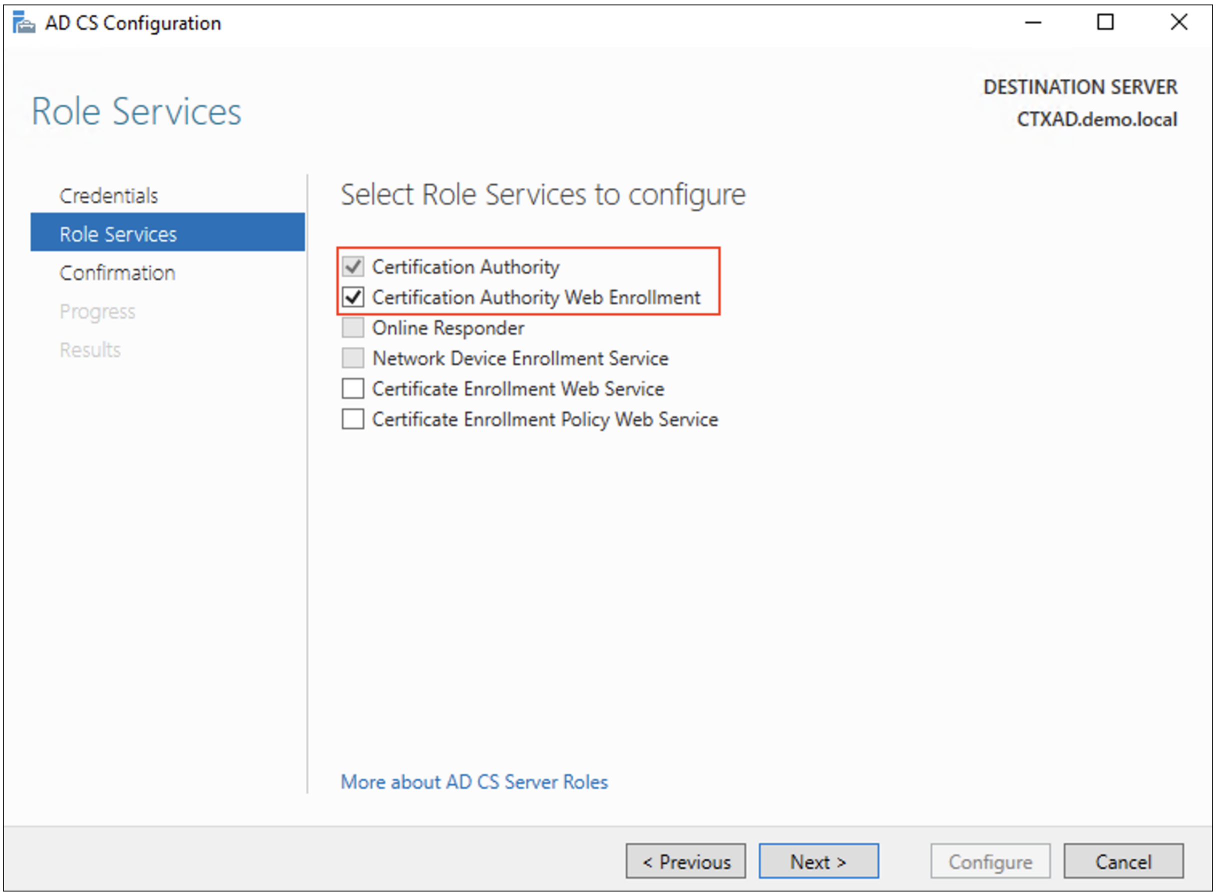
Post-deployment Configura...

Configuration required for Active Directory Certificate Services at CTXAD

Configure Active Directory Certificate Services on th...

Task Details

Server Manager ‣ Dashboard
Manage
Tools
View
Help
TASKS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ge Services
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD CS 1
AD DS 1
DNS 1
File and Storage Services 1
Manageability
Events
Services
Performance
BPA results

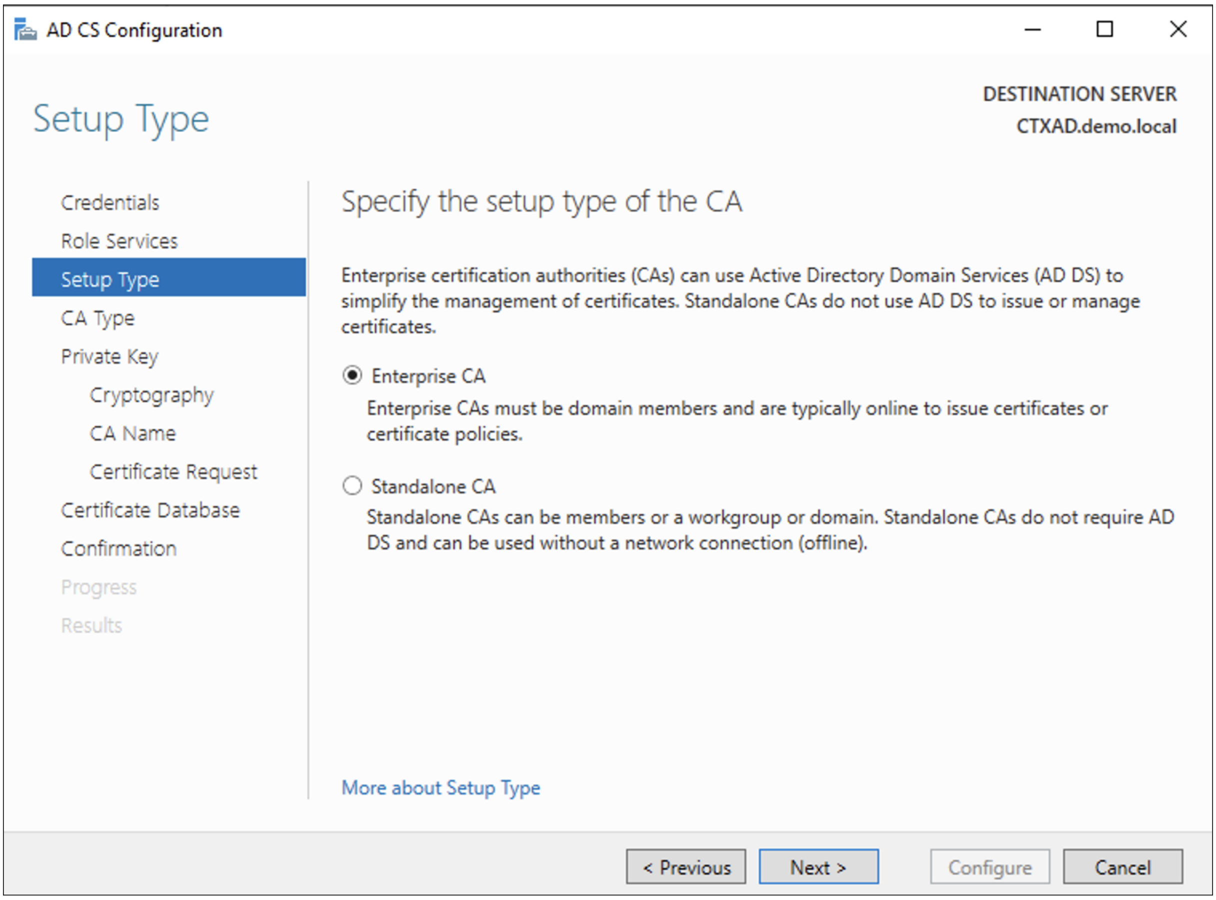


Role Services

DESTINATION SERVER
CTXAD.demo.local

Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service



Specify the setup type of the CA

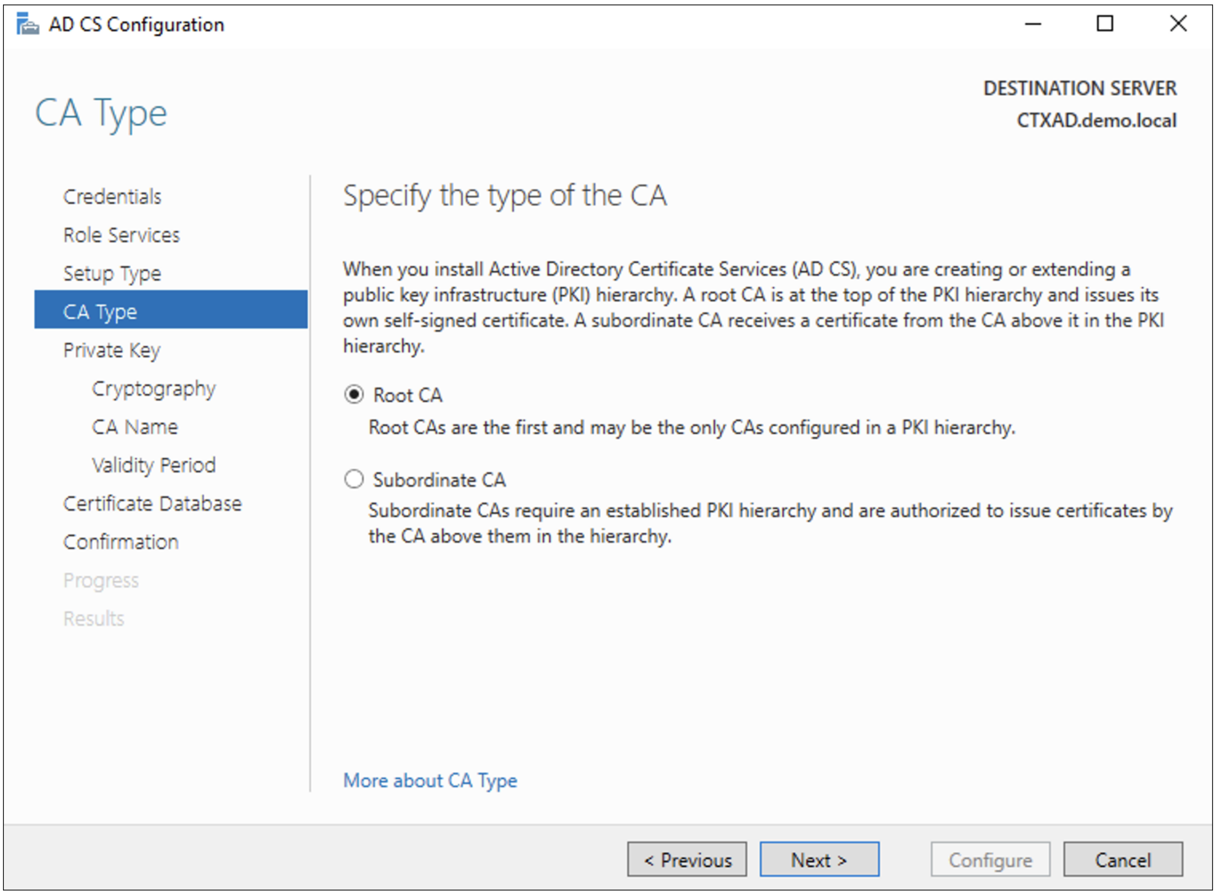
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

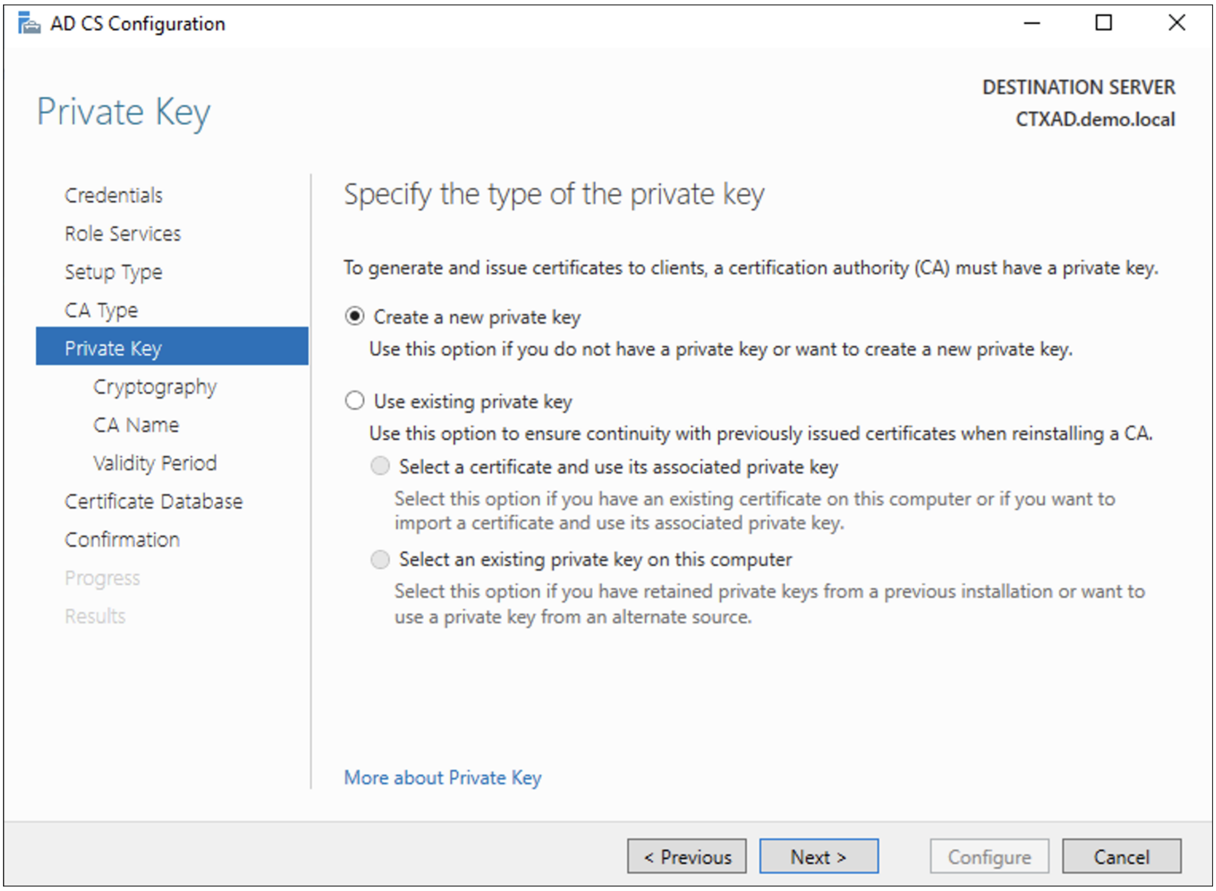


Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.



Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key

Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key

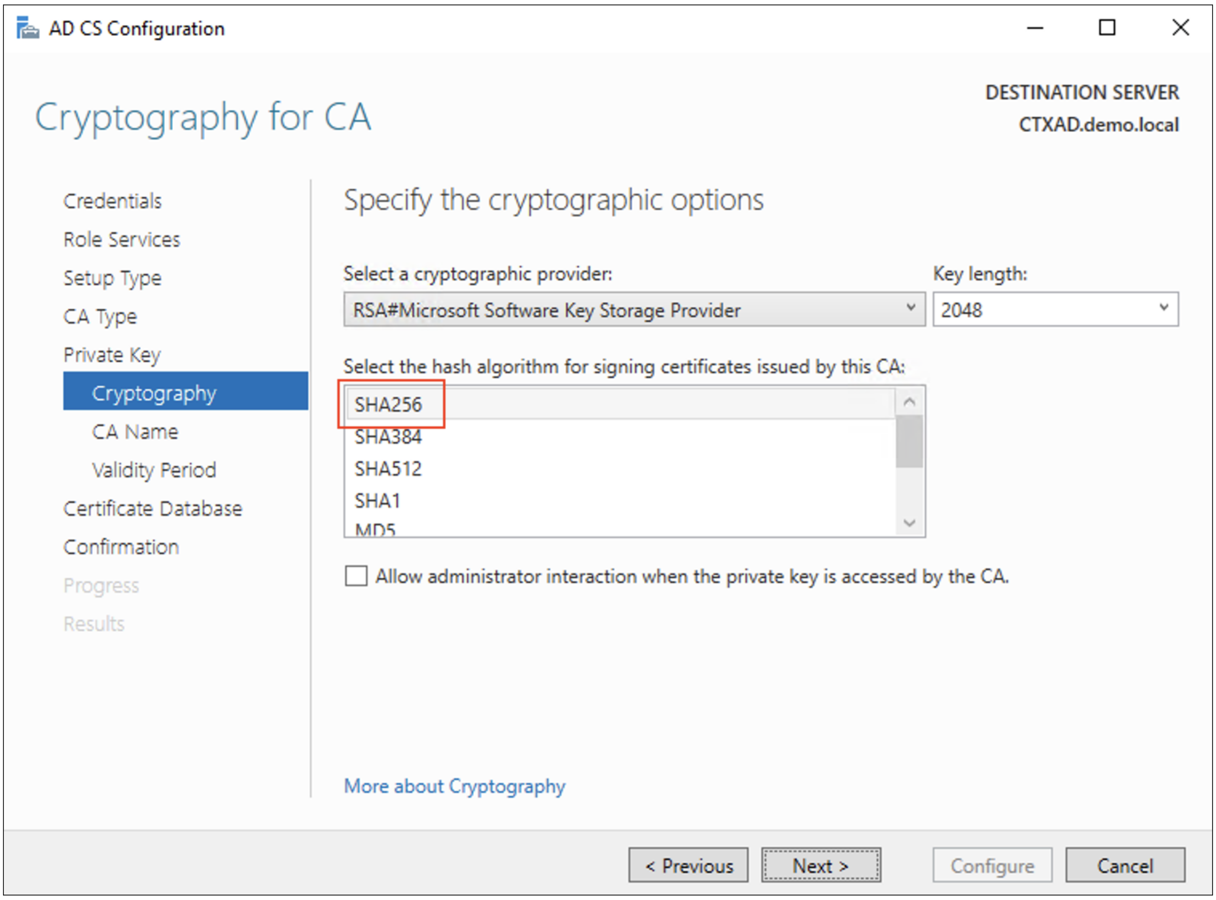
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key

Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.



AD CS Configuration

Cryptography for CA

DESTINATION SERVER
CTXAD.demo.local

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

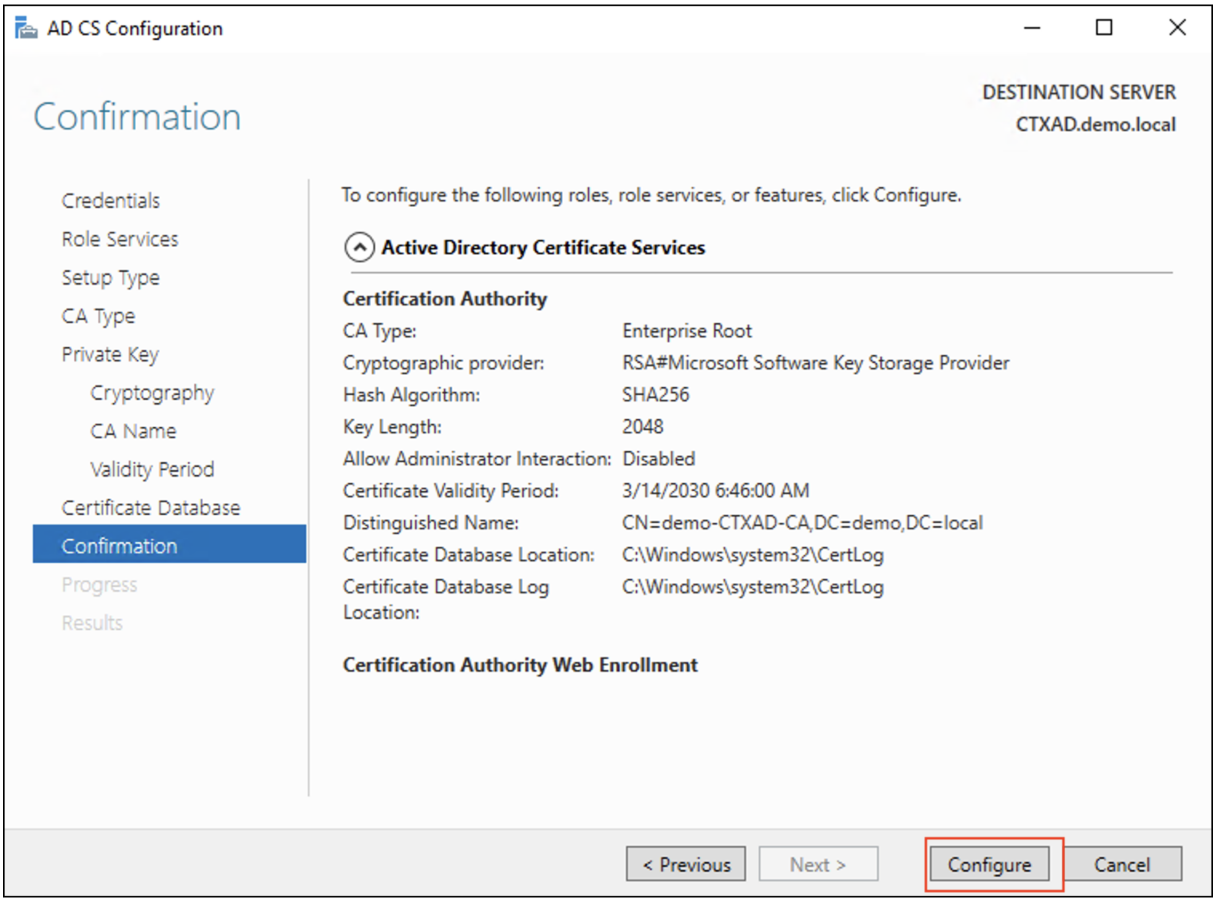
Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

□ Allow administrator interaction when the private key is accessed by the CA.

More about Cryptography



Confirmation

DESTINATION SERVER
CTXAD.demo.local

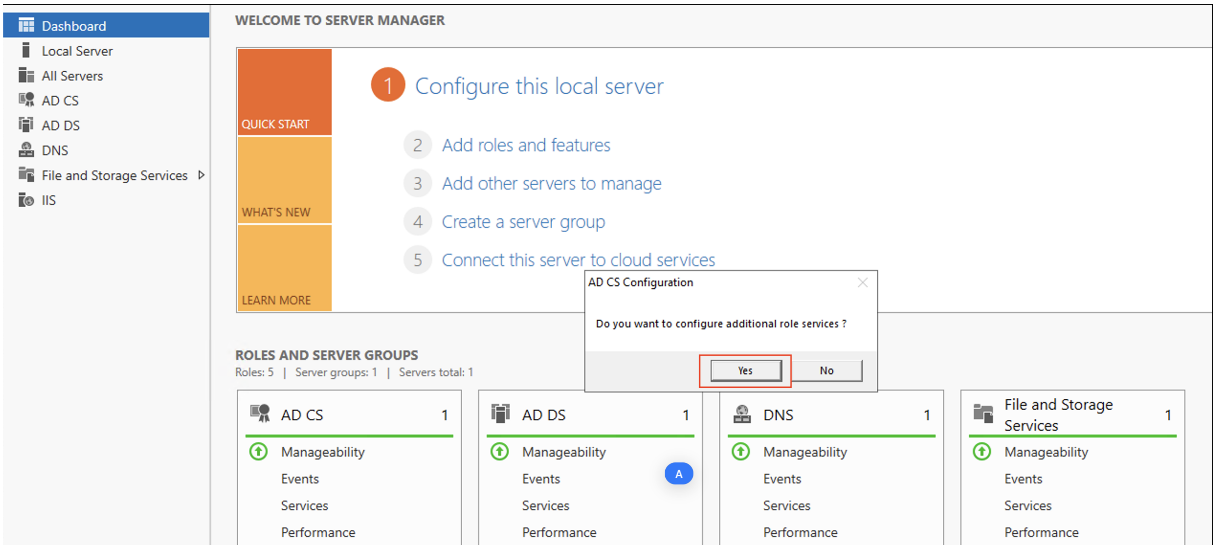
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	3/14/2030 6:46:00 AM
Distinguished Name:	CN=demo-CTXAD-CA,DC=demo,DC=local
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Certification Authority Web Enrollment

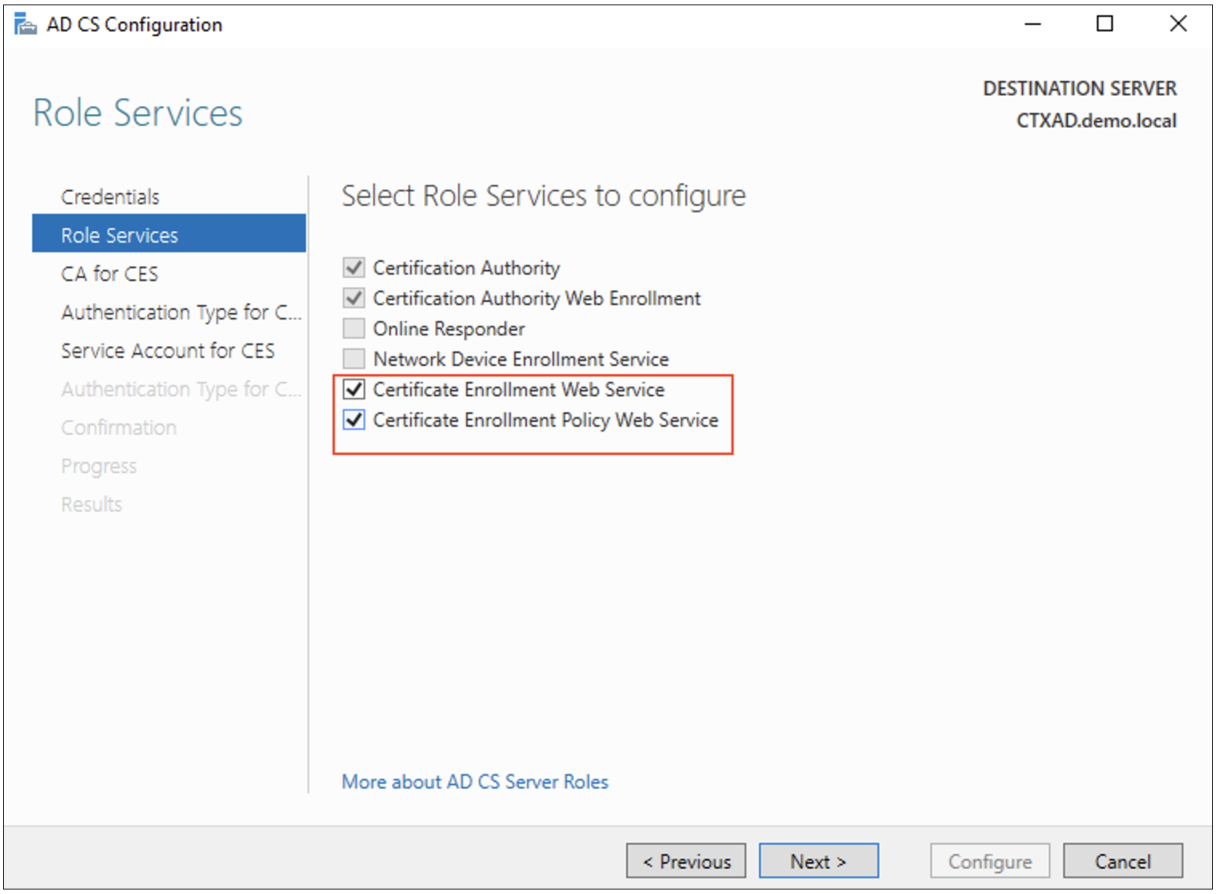


Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD CS 1
AD DS 1
DNS 1
File and Storage Services 1
Manageability
Events
Services
Performance
A

AD CS Configuration

Do you want to configure additional role services ?

Yes No



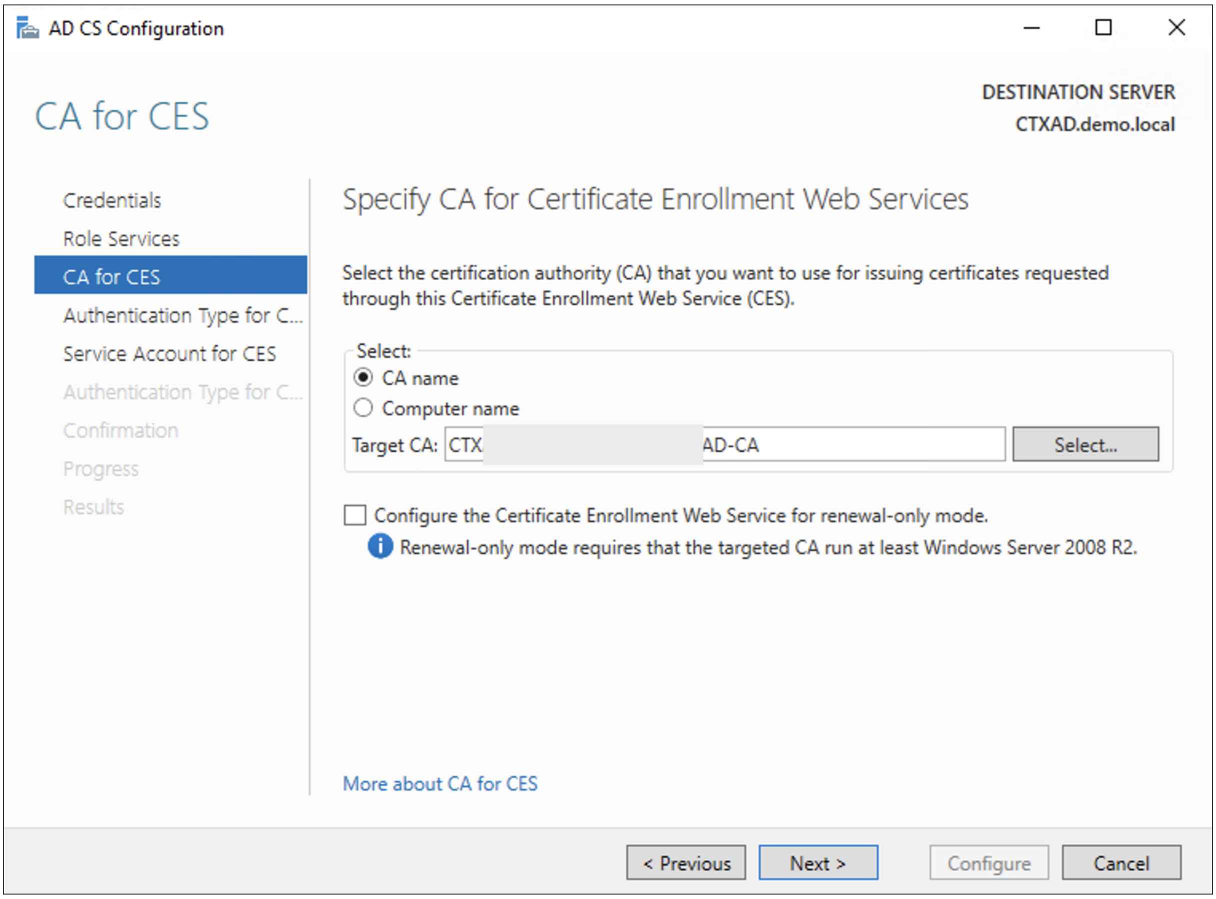
AD CS Configuration

Role Services

DESTINATION SERVER
CTXAD.demo.local

Select Role Services to configure

- ☑ Certification Authority
- ☑ Certification Authority Web Enrollment
- □ Online Responder
- □ Network Device Enrollment Service
- ☑ Certificate Enrollment Web Service
- ☑ Certificate Enrollment Policy Web Service



AD CS Configuration

DESTINATION SERVER
CTXAD.demo.local

CA for CES

Specify CA for Certificate Enrollment Web Services

Select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web Service (CES).

Select:

● CA name

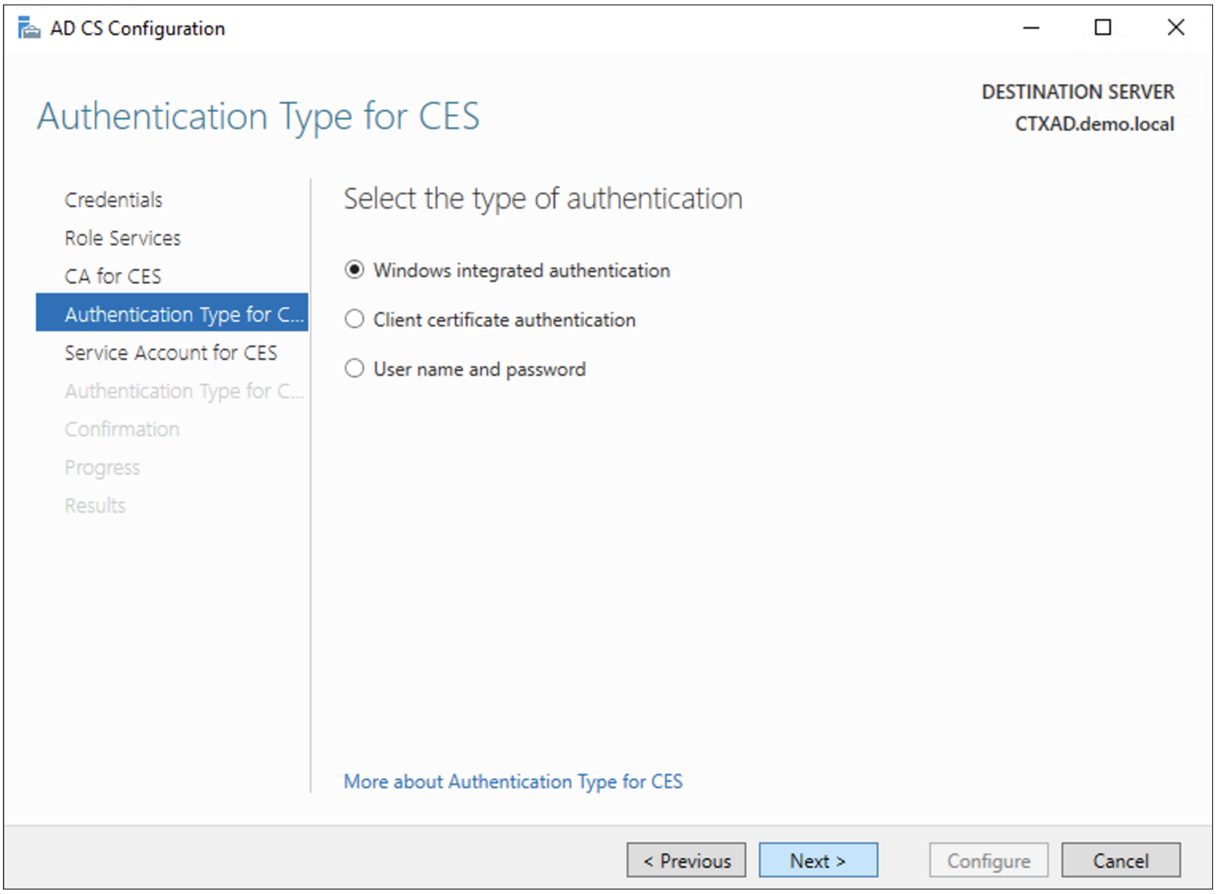
○ Computer name

Target CA: CTX[redacted]AD-CA

□ Configure the Certificate Enrollment Web Service for renewal-only mode.

Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2.

More about CA for CES



AD CS Configuration

Authentication Type for CES

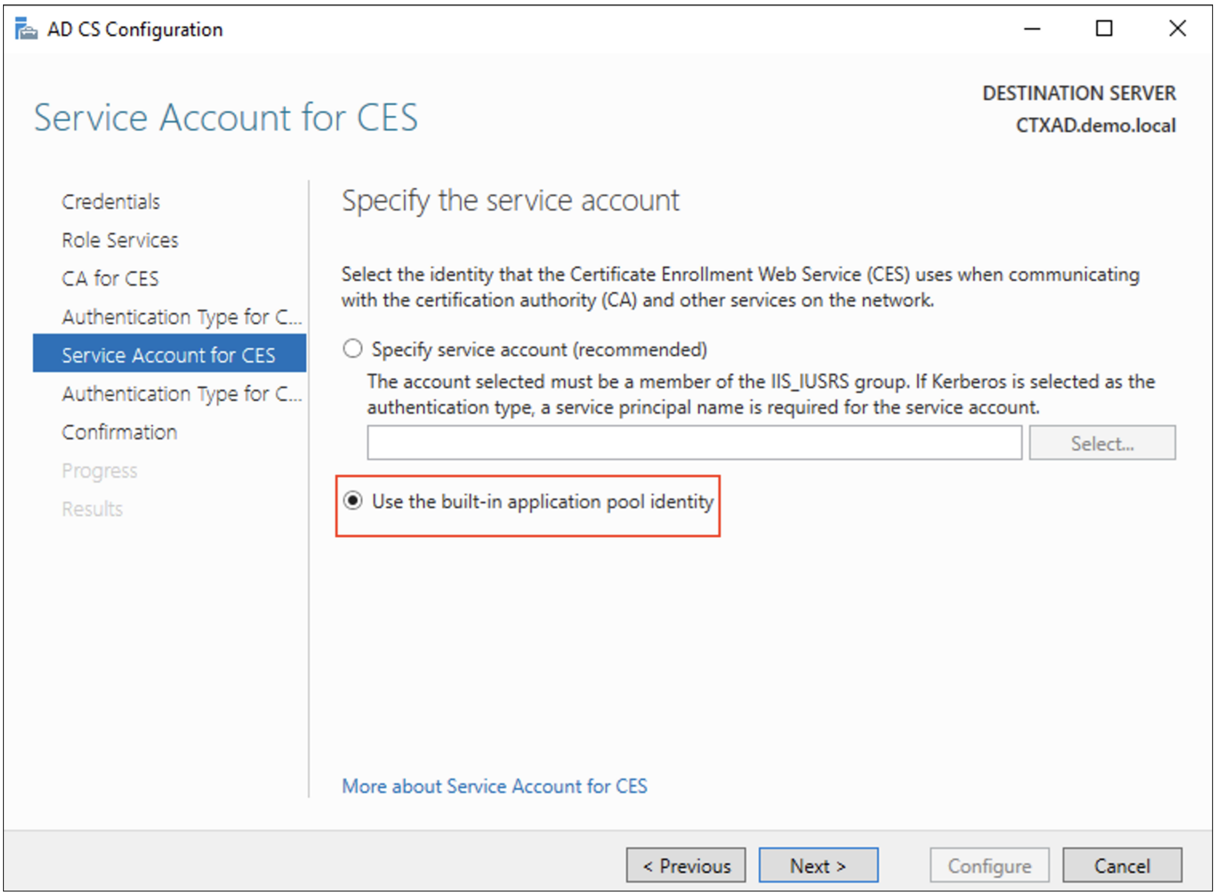
DESTINATION SERVER
CTXAD.demo.local

Select the type of authentication

● Windows integrated authentication

○ Client certificate authentication

○ User name and password



Service Account for CES

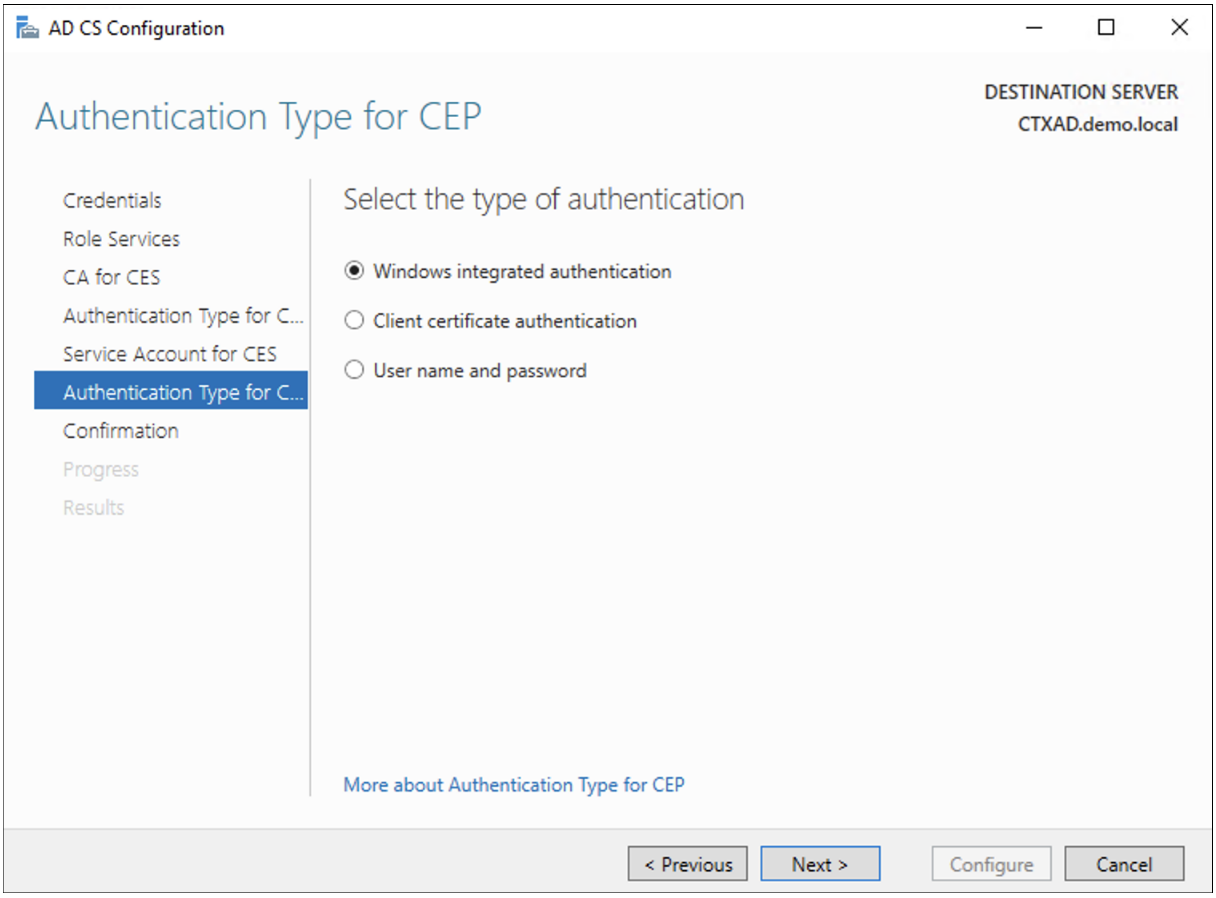
Specify the service account

Select the identity that the Certificate Enrollment Web Service (CES) uses when communicating with the certification authority (CA) and other services on the network.

○ Specify service account (recommended)

The account selected must be a member of the IIS_IUSRS group. If Kerberos is selected as the authentication type, a service principal name is required for the service account.

● Use the built-in application pool identity

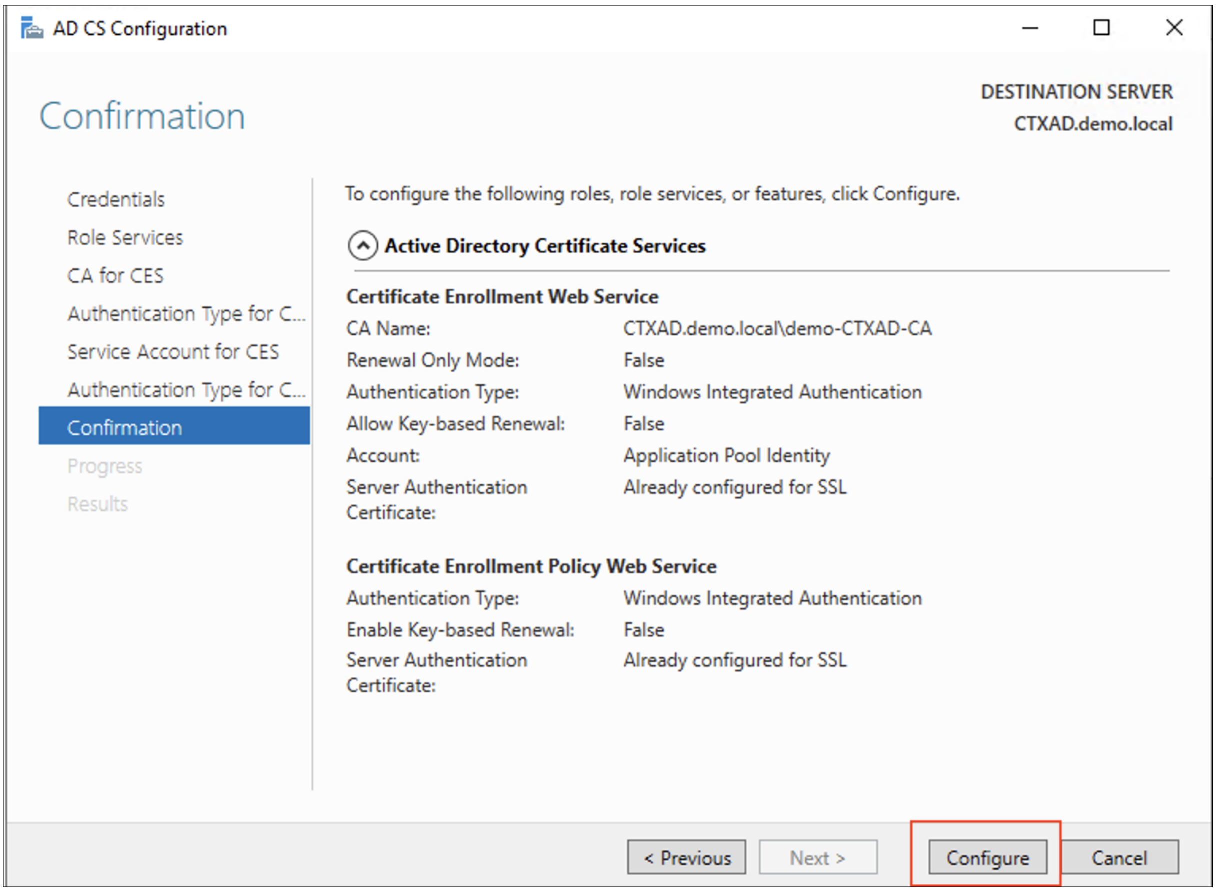


Select the type of authentication

● Windows integrated authentication

○ Client certificate authentication

○ User name and password



To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certificate Enrollment Web Service

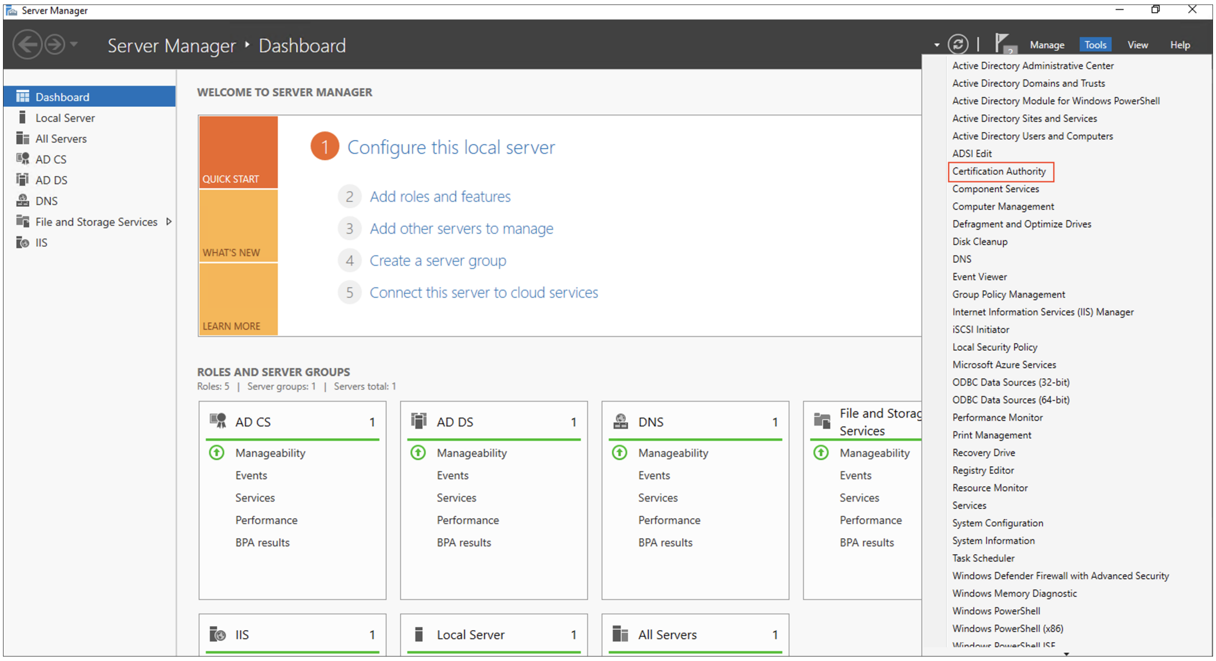
CA Name:	CTXAD.demo.local\demo-CTXAD-CA
Renewal Only Mode:	False
Authentication Type:	Windows Integrated Authentication
Allow Key-based Renewal:	False
Account:	Application Pool Identity
Server Authentication Certificate:	Already configured for SSL

Certificate Enrollment Policy Web Service

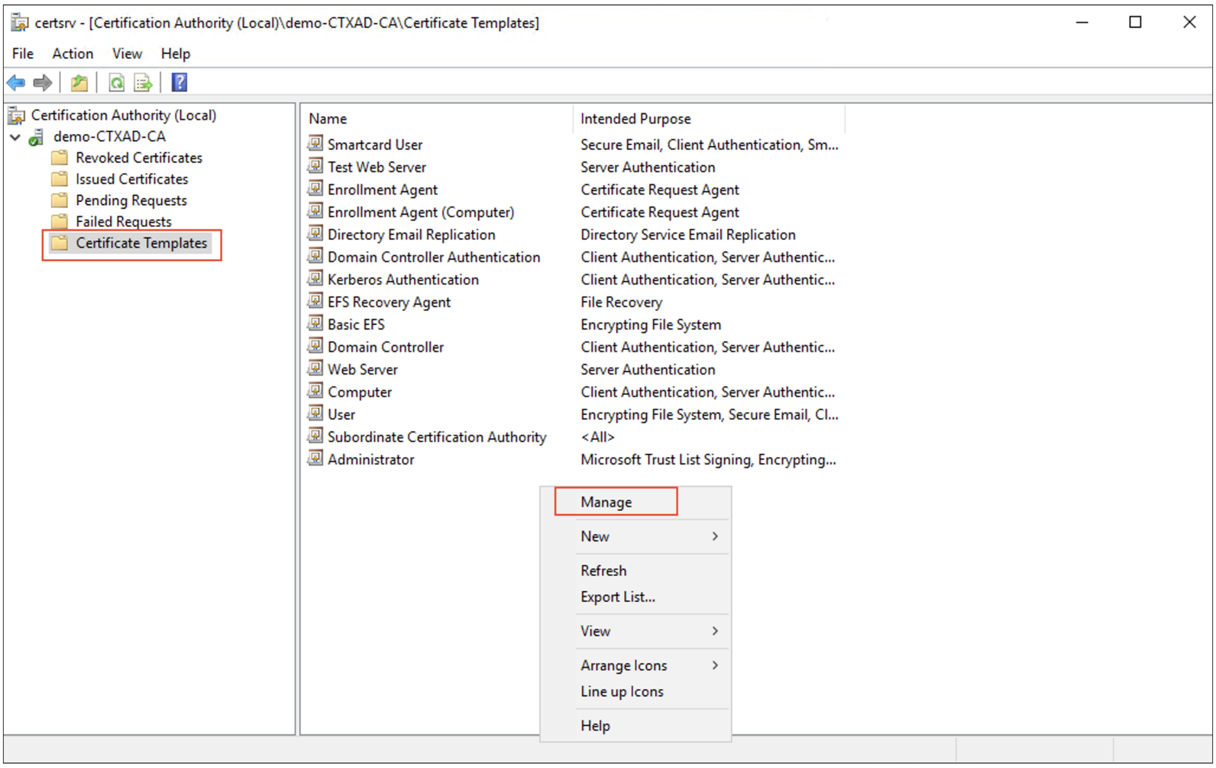
Authentication Type:	Windows Integrated Authentication
Enable Key-based Renewal:	False
Server Authentication Certificate:	Already configured for SSL

Create Customized Web Server Certificate Template

On Active Directory Server, Open Certification Authority

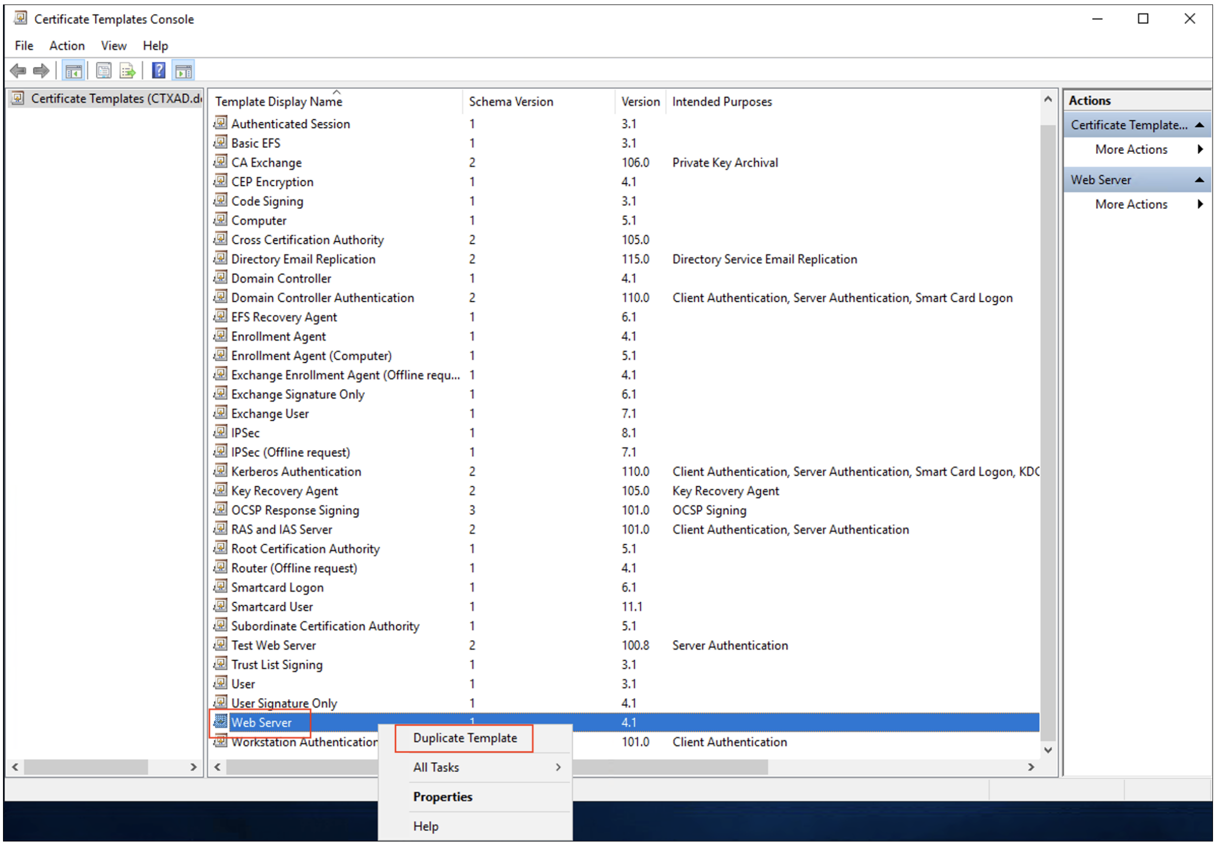


Create customized certification template



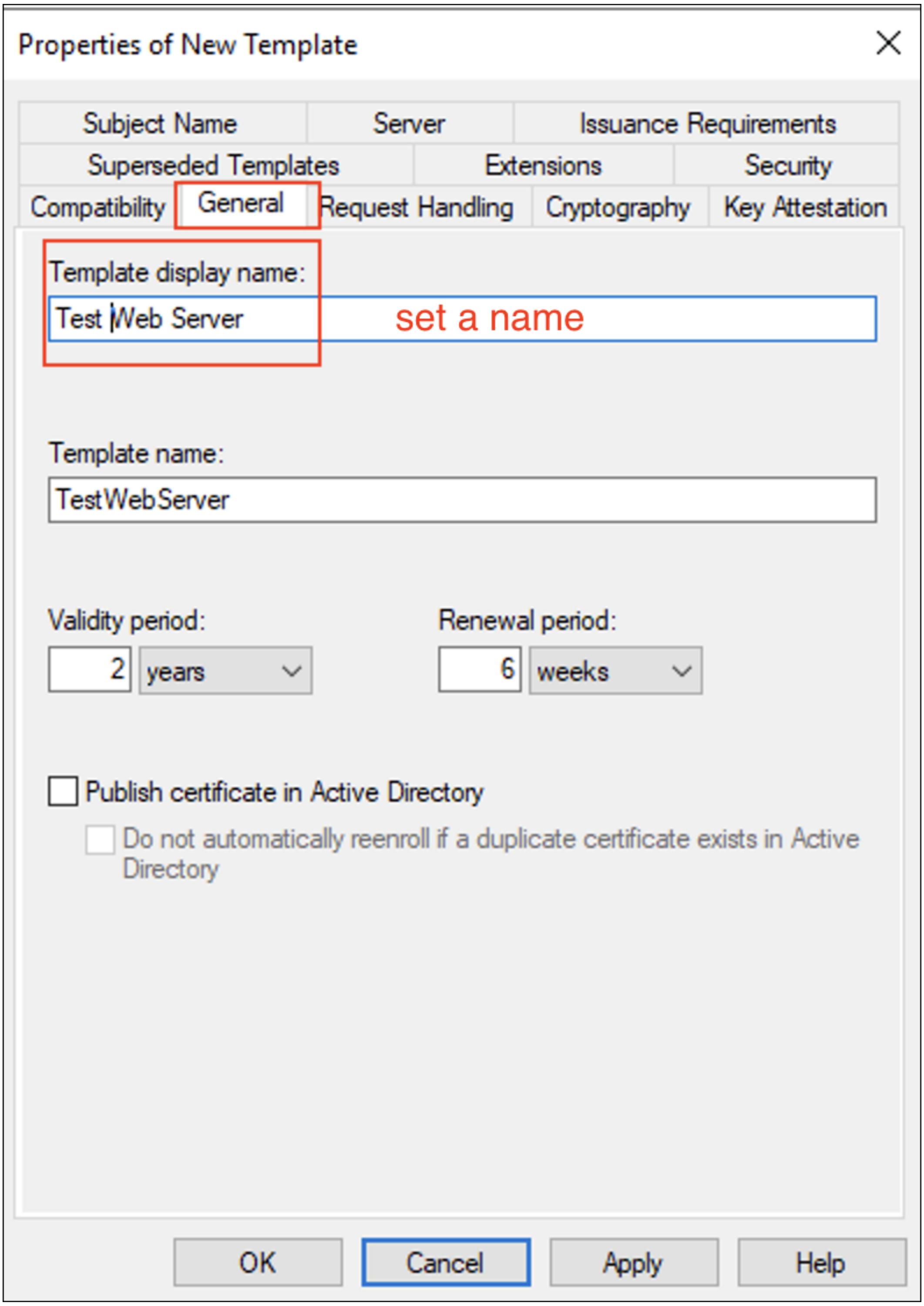
Name	Intended Purpose
Smartcard User	Secure Email, Client Authentication, Sm...
Test Web Server	Server Authentication
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

Web Server â†'Duplicate Template



Template Display Name	Schema Version	Version	Intended Purposes
Authenticated Session	1	3.1	
Basic EFS	1	3.1	
CA Exchange	2	106.0	Private Key Archival
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Directory Service Email Replication
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon, KDC
Key Recovery Agent	2	105.0	Key Recovery Agent
OCSP Response Signing	3	101.0	OCSP Signing
RAS and IAS Server	2	101.0	Client Authentication, Server Authentication
Root Certification Authority	1	5.1	
Router (Offline request)	1	4.1	
Smartcard Logon	1	6.1	
Smartcard User	1	11.1	
Subordinate Certification Authority	1	5.1	
Test Web Server	2	100.8	Server Authentication
Trust List Signing	1	3.1	
User	1	3.1	
User Signature Only	1	4.1	
Web Server	1	4.1	
Workstation Authentication		101.0	Client Authentication

Configure the Properties of New Template



Properties of New Template

Template display name:

Test Web Server

set a name

Template name:

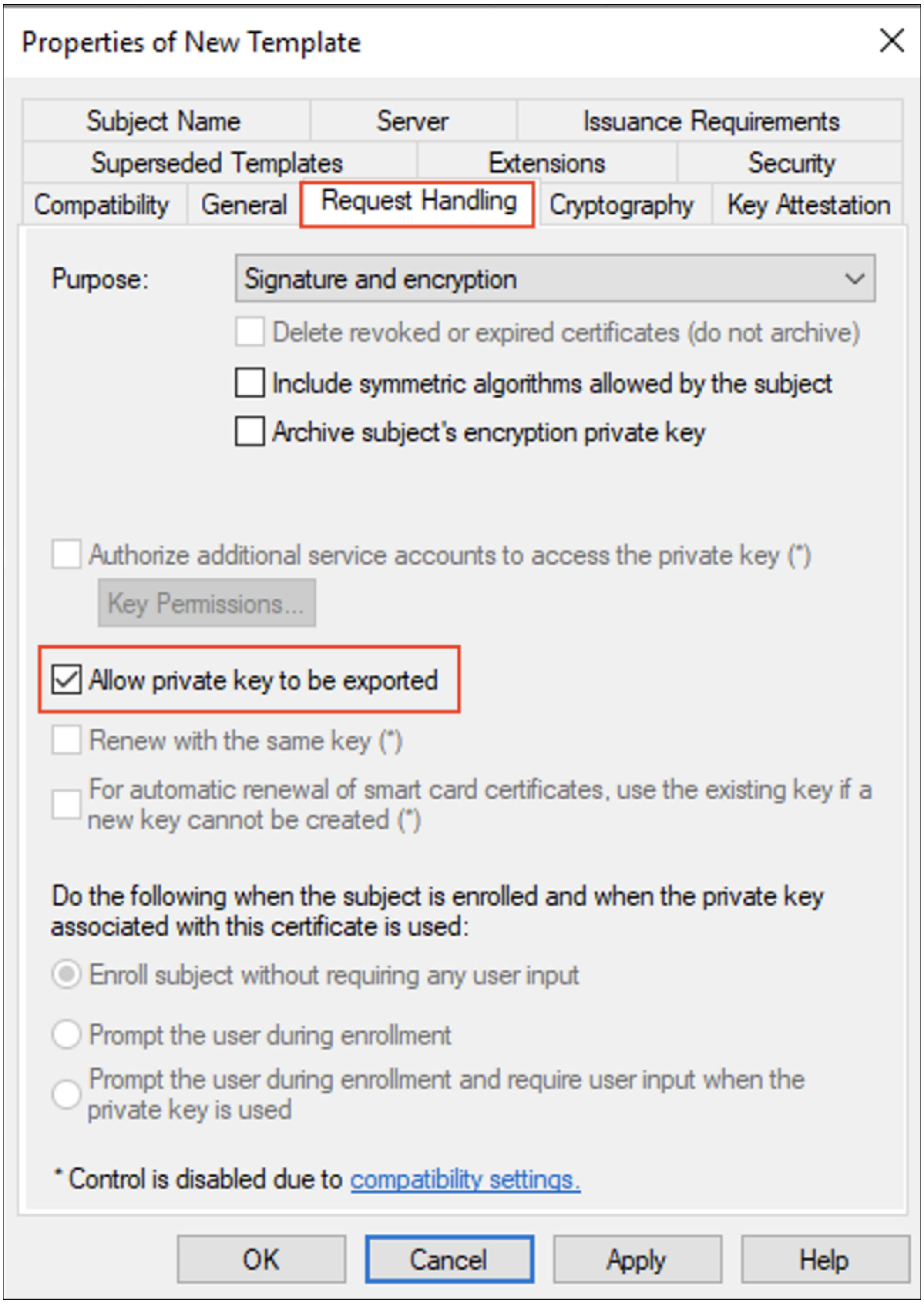
TestWebServer

Validity period: 2 years

Renewal period: 6 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory



Properties of New Template

Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Authorize additional service accounts to access the private key (*)

☑ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

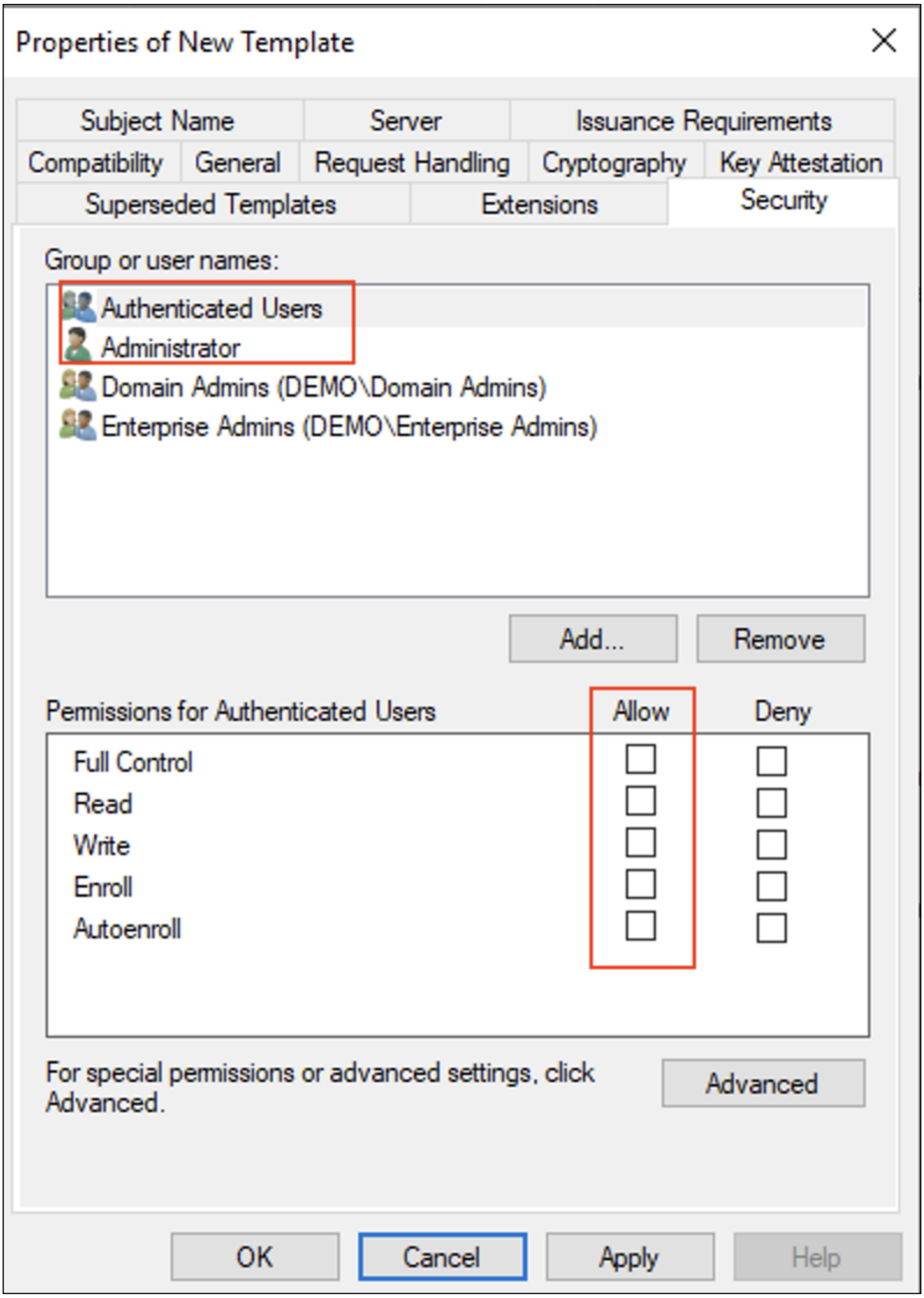
Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.



Group or user names:

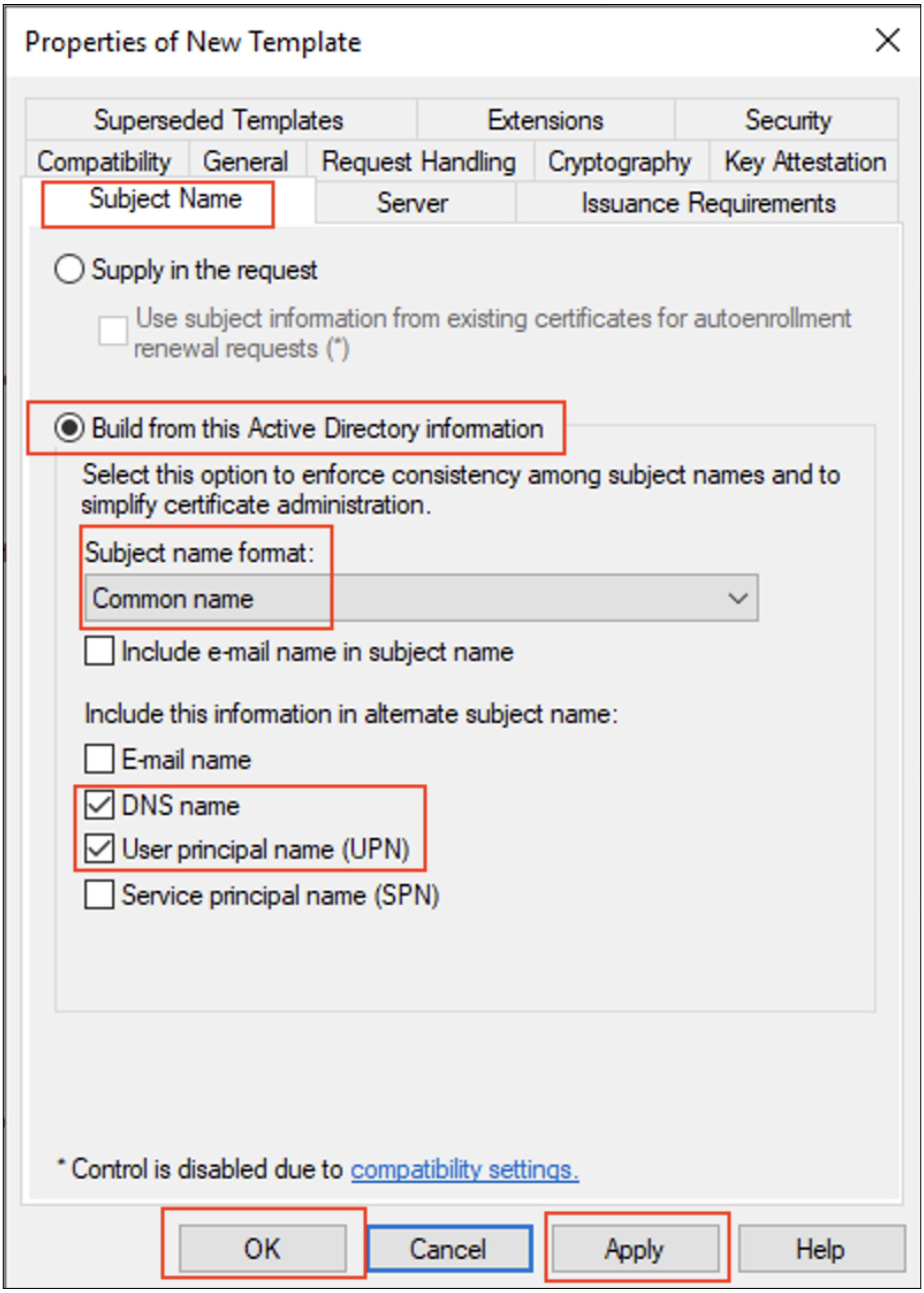
- Authenticated Users
- Administrator
- Domain Admins (DEMO\Domain Admins)
- Enterprise Admins (DEMO\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	□	□
Write	□	□
Enroll	□	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

Note:

Administrator to evaluate and grant Permissions for Authenticated Users based on security considerations.



○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Common name

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

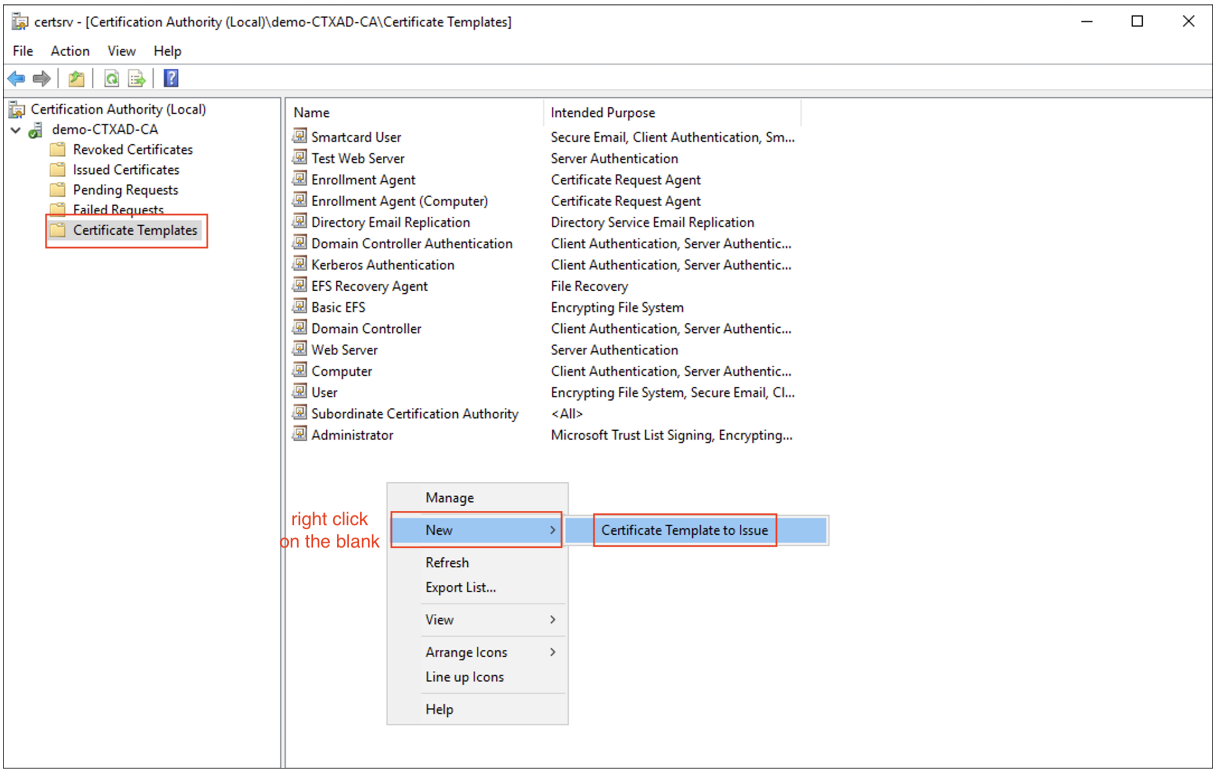
☑ DNS name

☑ User principal name (UPN)

□ Service principal name (SPN)

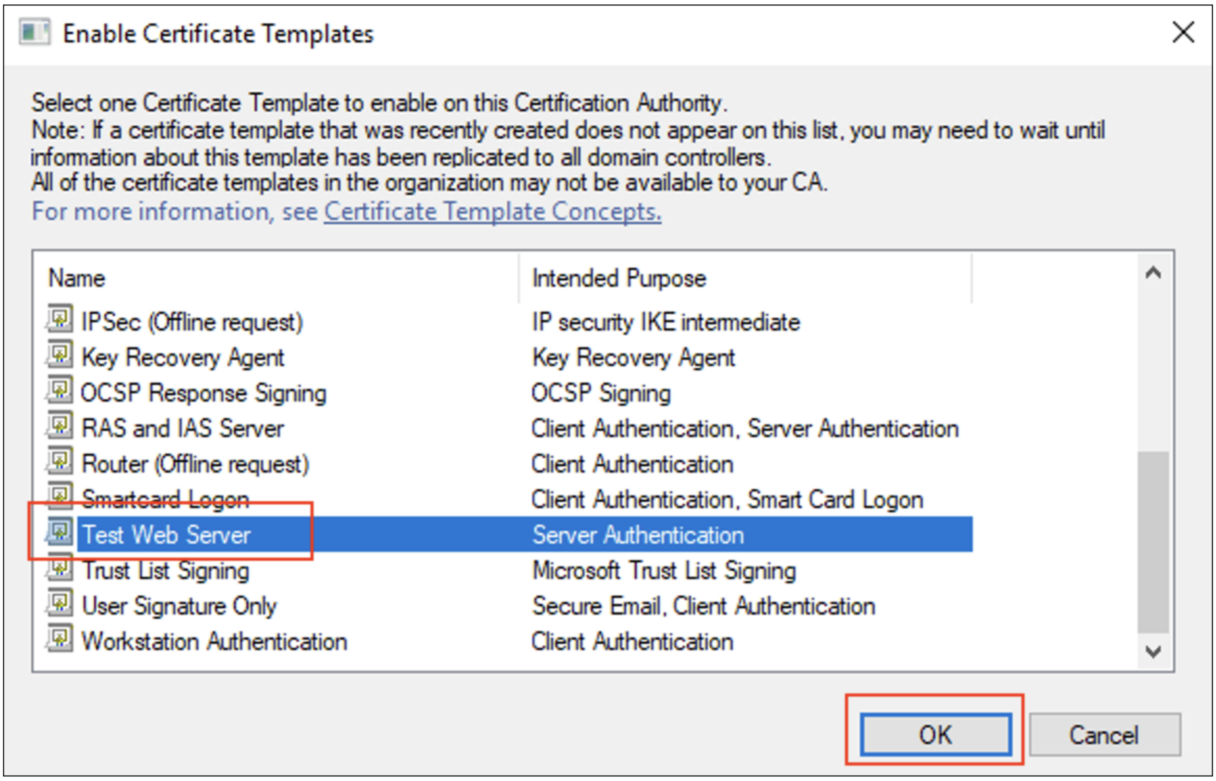
* Control is disabled due to compatibility settings.

Back to Certification Authority to issue the Certificate Template



Name	Intended Purpose
Smartcard User	Secure Email, Client Authentication, Sm...
Test Web Server	Server Authentication
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

right click on the blank

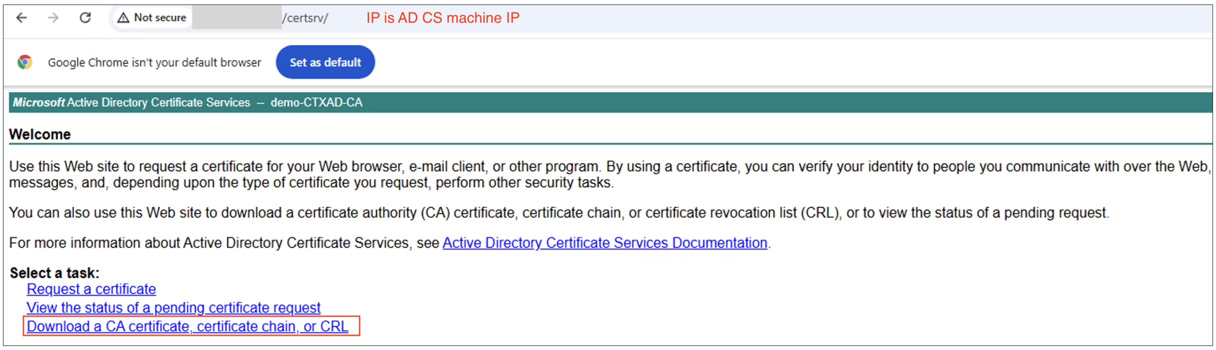


Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
IPSec (Offline request)	IP security IKE intermediate
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Test Web Server	Server Authentication
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication
Workstation Authentication	Client Authentication

Install Certificate on DDC

First on DDC machine, open (http://<AD CS machine IP>/certsrv) via the browser to download and install the certificate



Not secure [redacted] /certsrv/ IP is AD CS machine IP

Google Chrome isn't your default browser **Set as default**

Microsoft Active Directory Certificate Services – demo-CTXAD-CA

Welcome

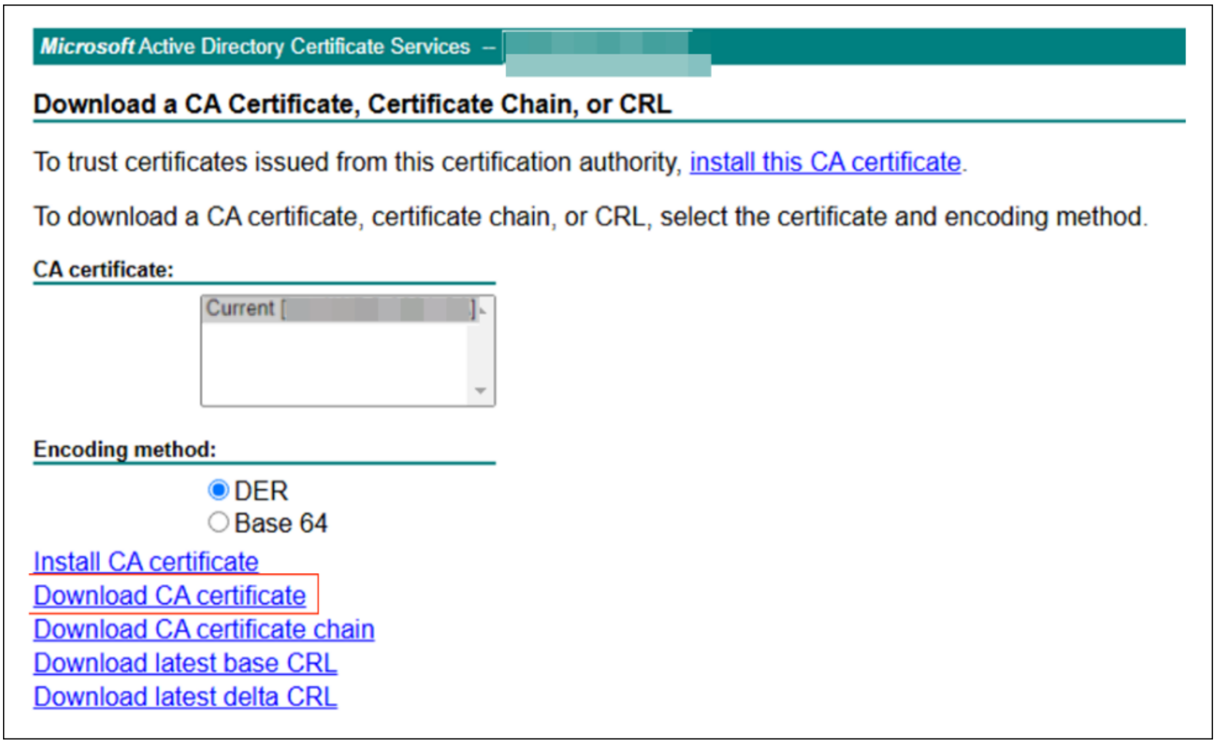
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL



Microsoft Active Directory Certificate Services – [redacted]

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

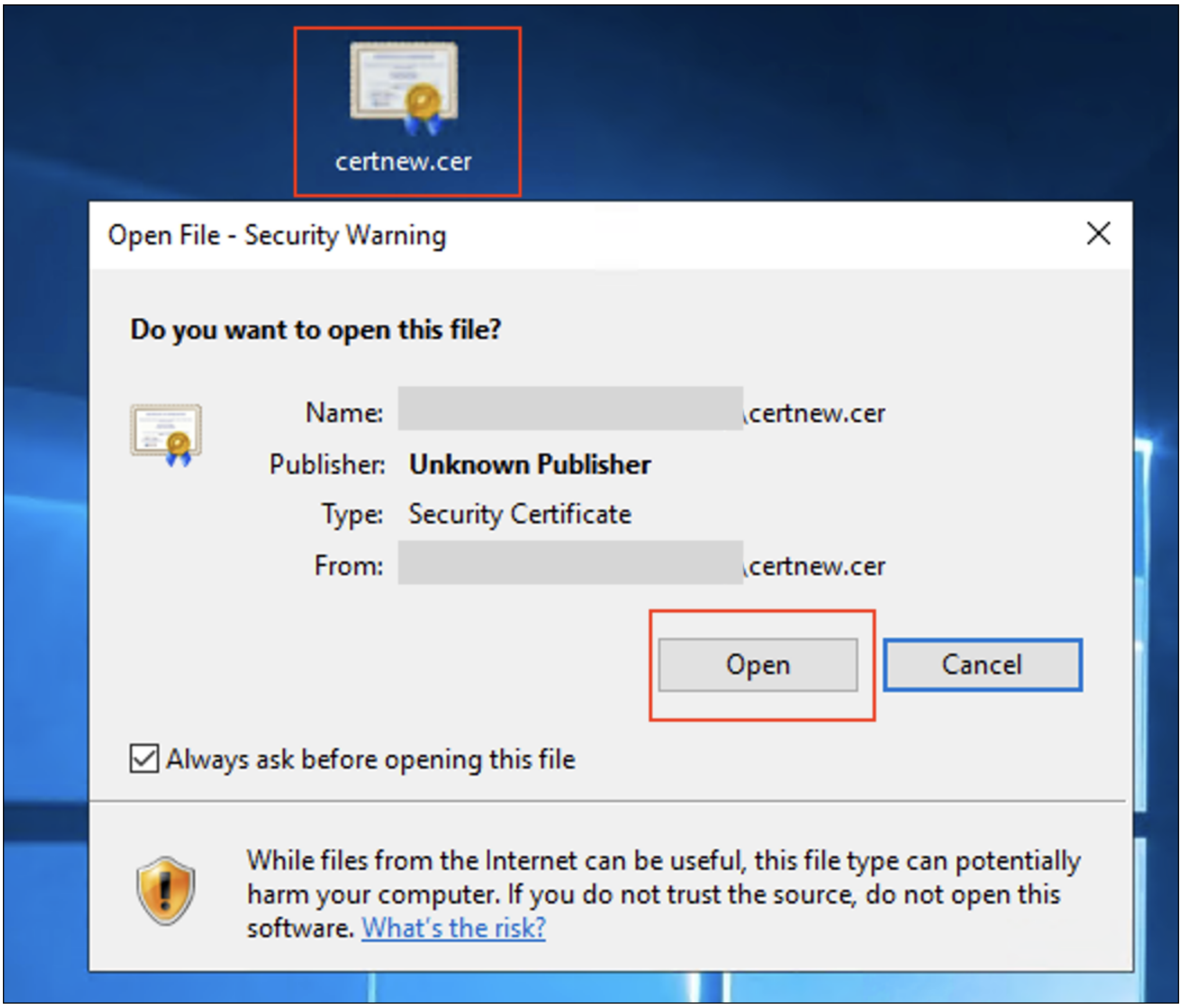
Current [[redacted]]

Encoding method:

● DER
○ Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Double click on the downloaded certificate file to install



Open File - Security Warning

Do you want to open this file?

Name: \certnew.cer

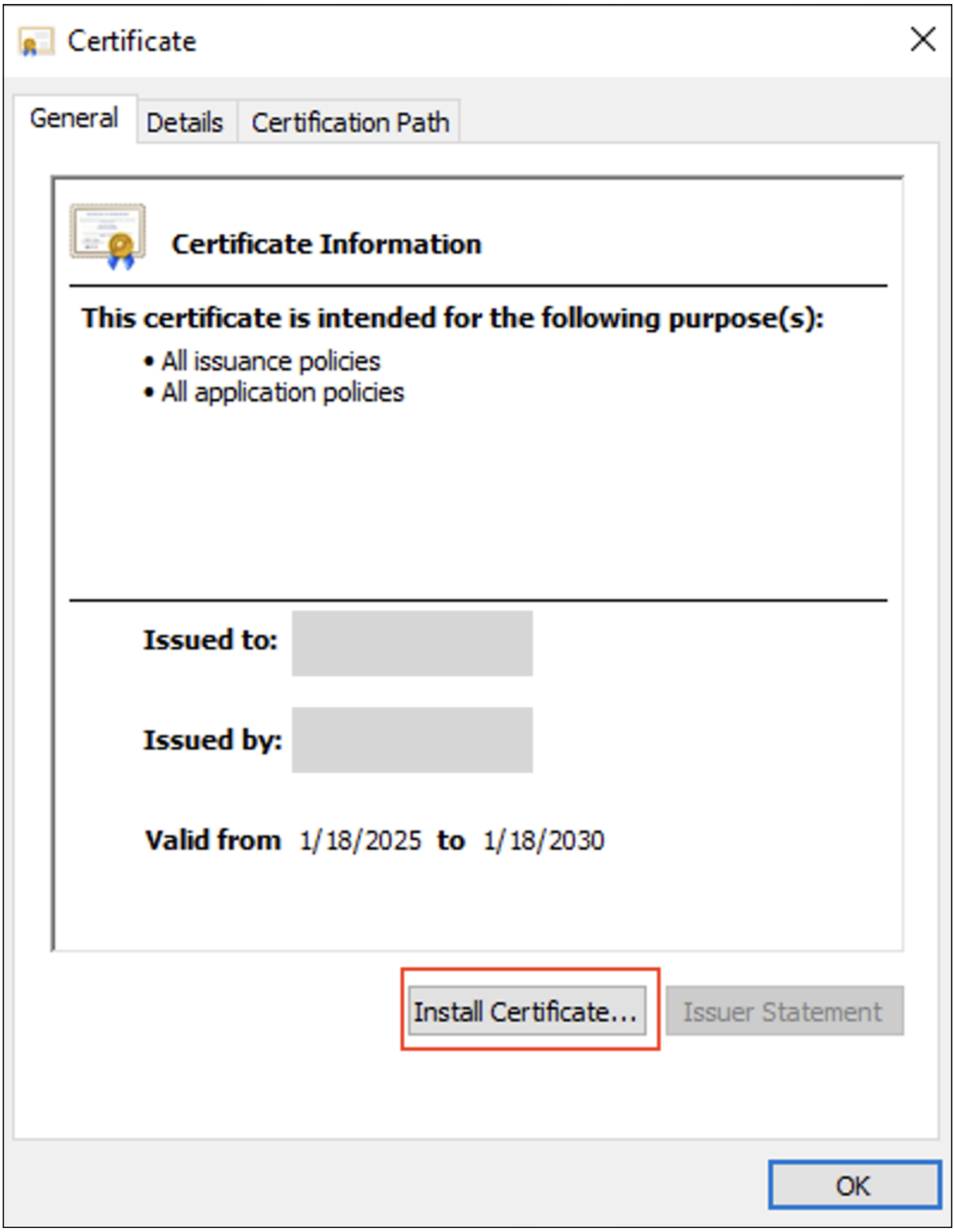
Publisher: **Unknown Publisher**

Type: Security Certificate

From: \certnew.cer

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?



Certificate Information

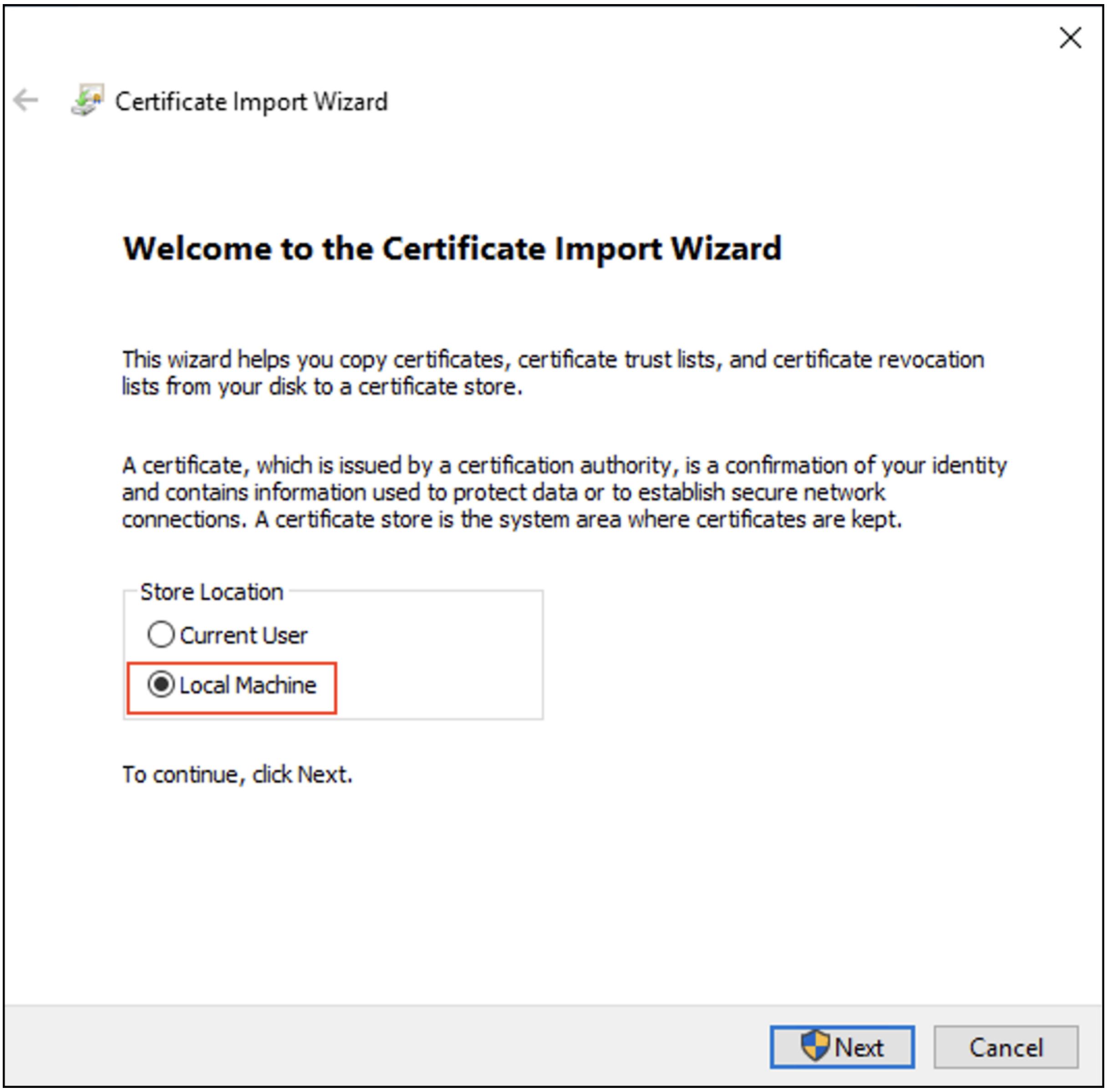
This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: [redacted]

Issued by: [redacted]

Valid from 1/18/2025 to 1/18/2030



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

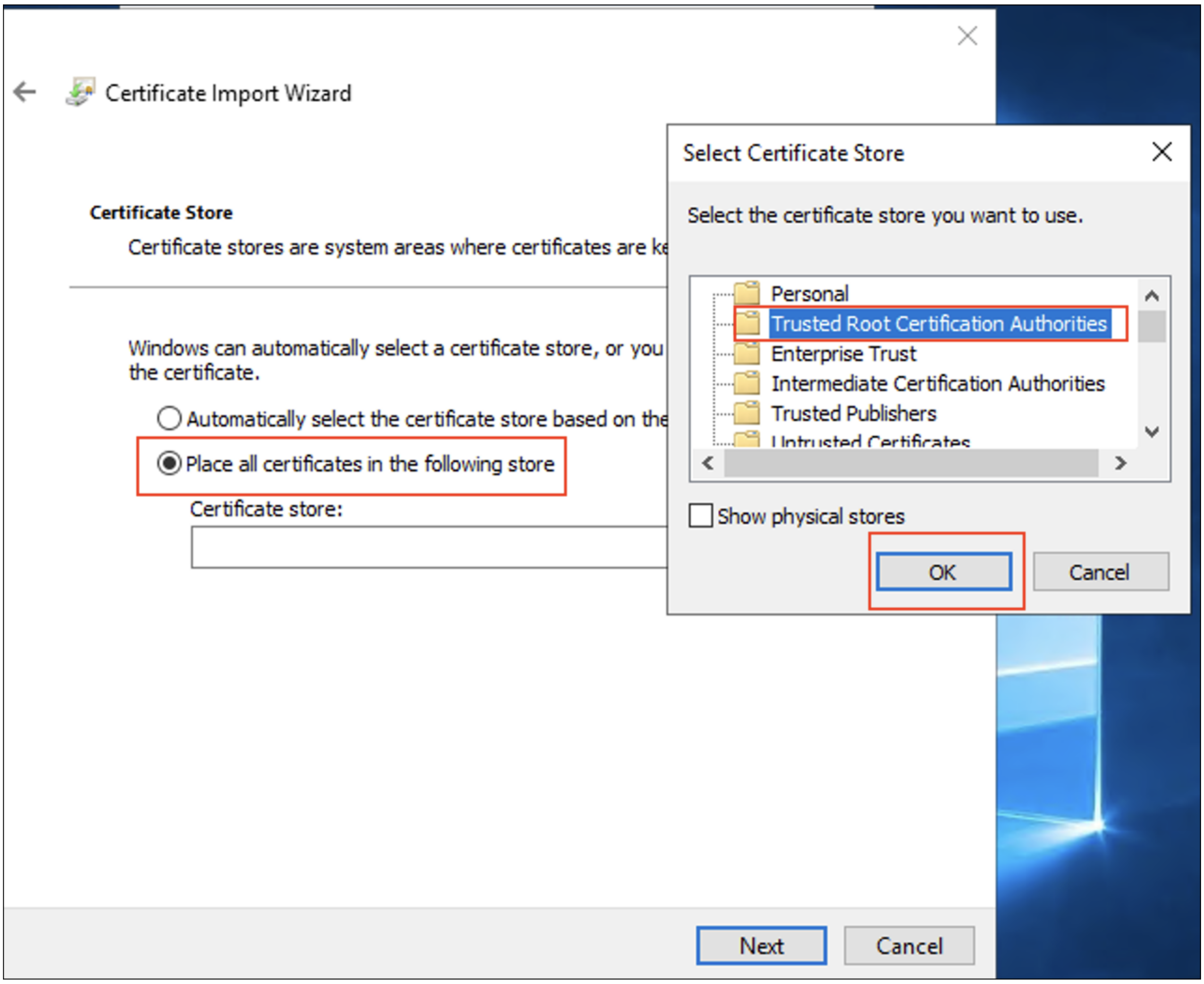
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

○ Current User

● Local Machine

To continue, click Next.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are ke

Windows can automatically select a certificate store, or you the certificate.

○ Automatically select the certificate store based on the

● Place all certificates in the following store

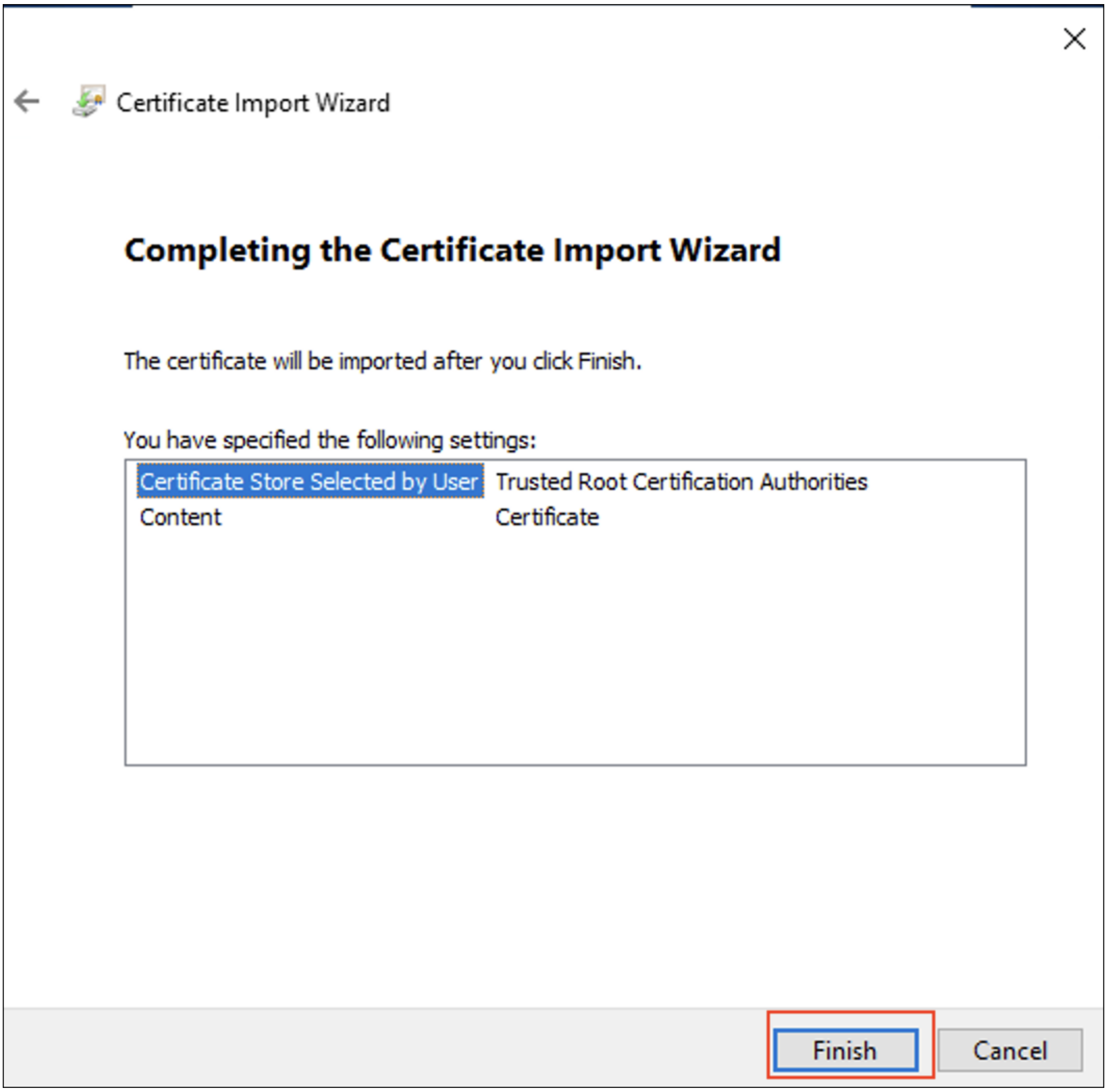
Certificate store:

Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores



Certificate Import Wizard

Completing the Certificate Import Wizard

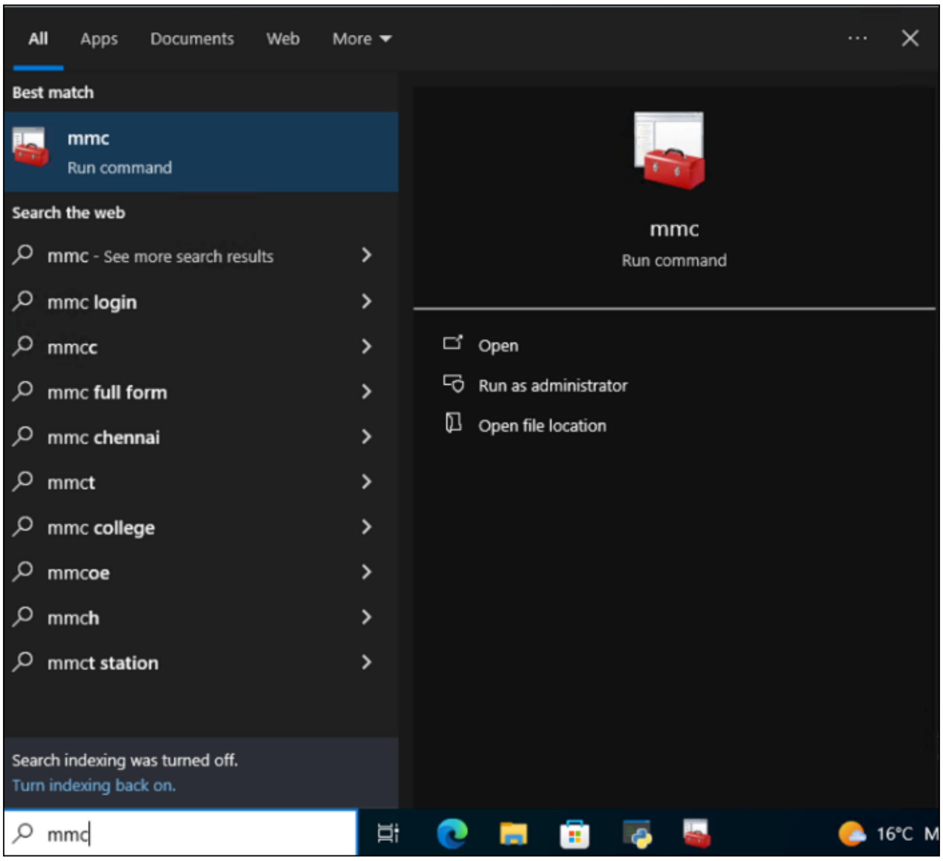
The certificate will be imported after you click Finish.

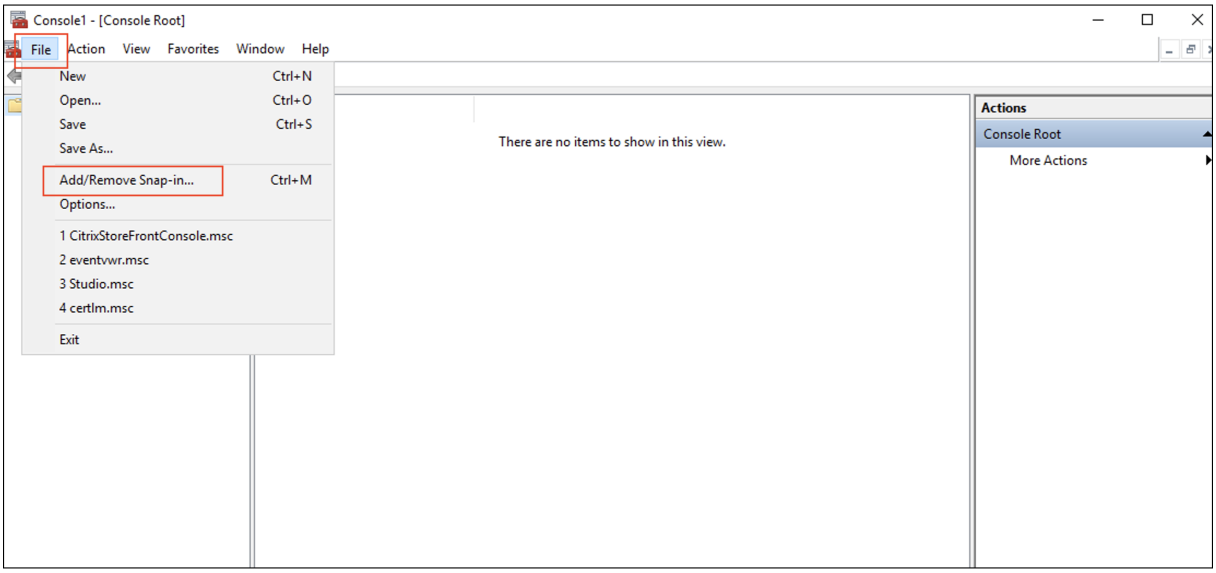
You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

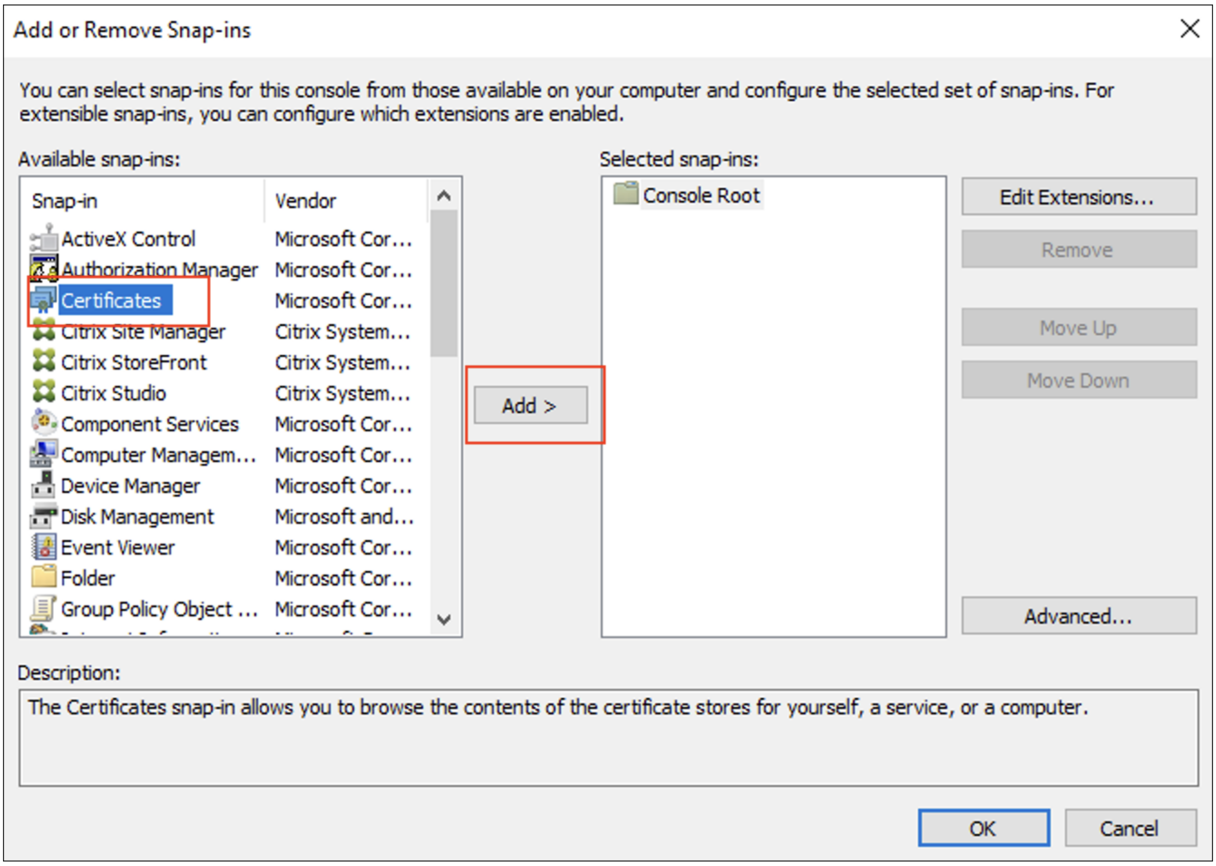
Request New Certificate on DDC

On DDC machine, open MMC and Request New Certificate as following





There are no items to show in this view.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

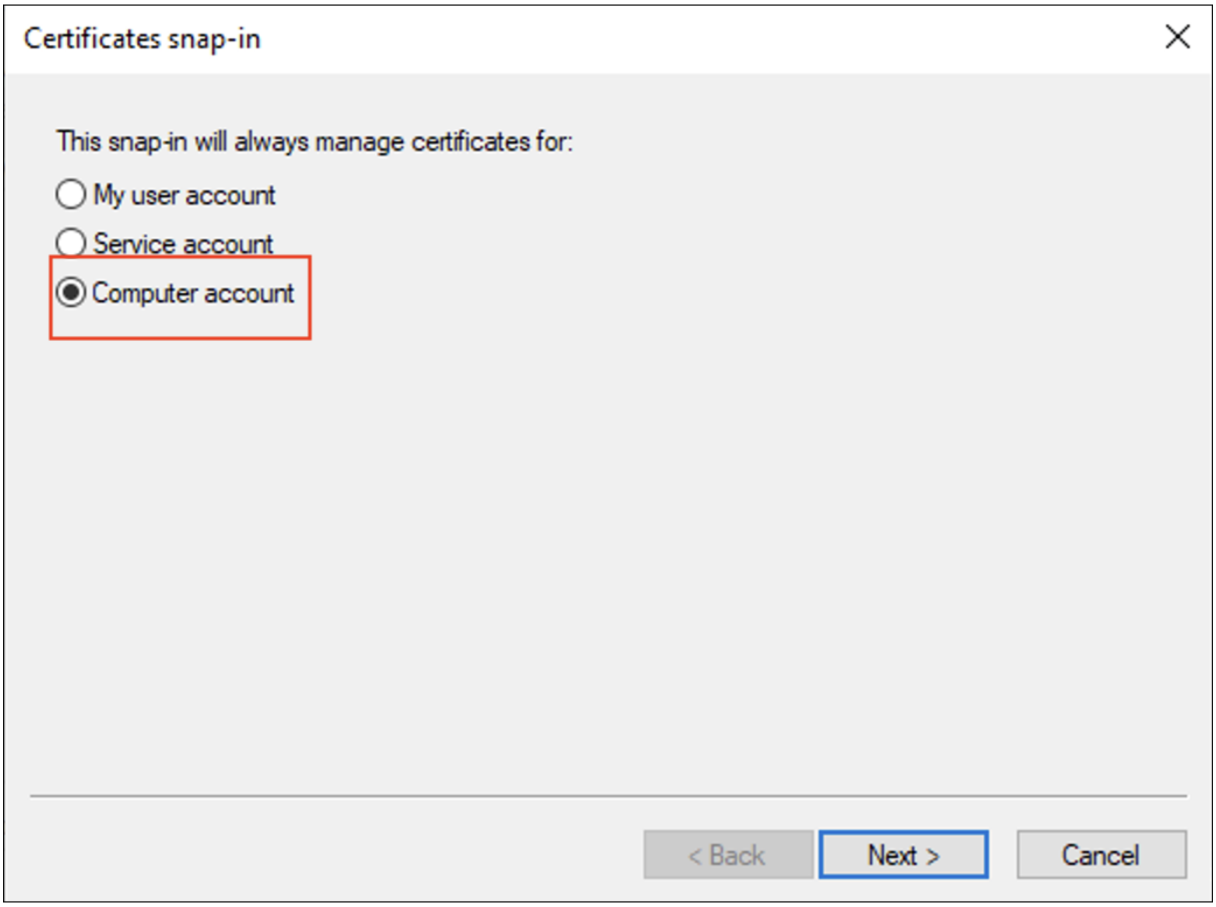
Snap-in	Vendor
ActiveX Control	Microsoft Cor…
Authorization Manager	Microsoft Cor…
Certificates	Microsoft Cor…
Citrix Site Manager	Citrix System…
Citrix StoreFront	Citrix System…
Citrix Studio	Citrix System…
Component Services	Microsoft Cor…
Computer Managem…	Microsoft Cor…
Device Manager	Microsoft Cor…
Disk Management	Microsoft and…
Event Viewer	Microsoft Cor…
Folder	Microsoft Cor…
Group Policy Object …	Microsoft Cor…

Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.



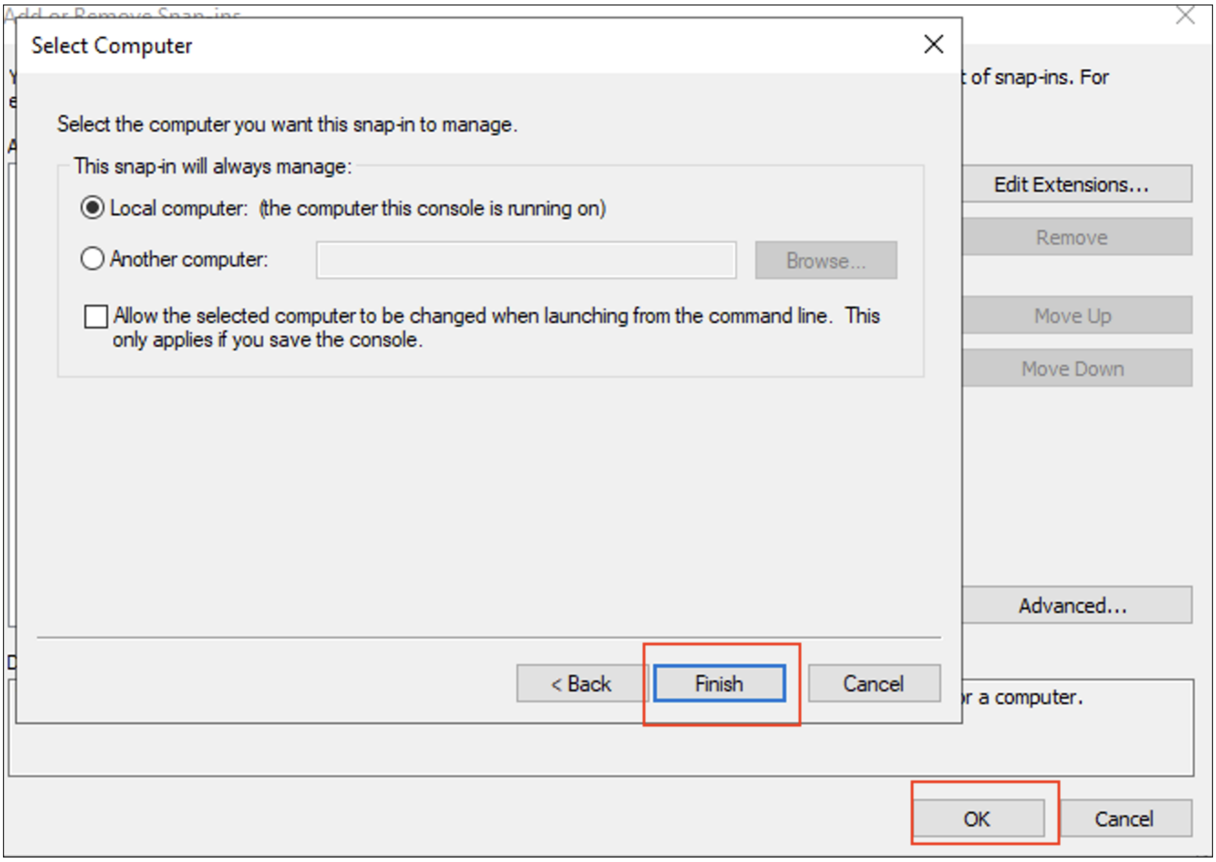
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account



Select Computer

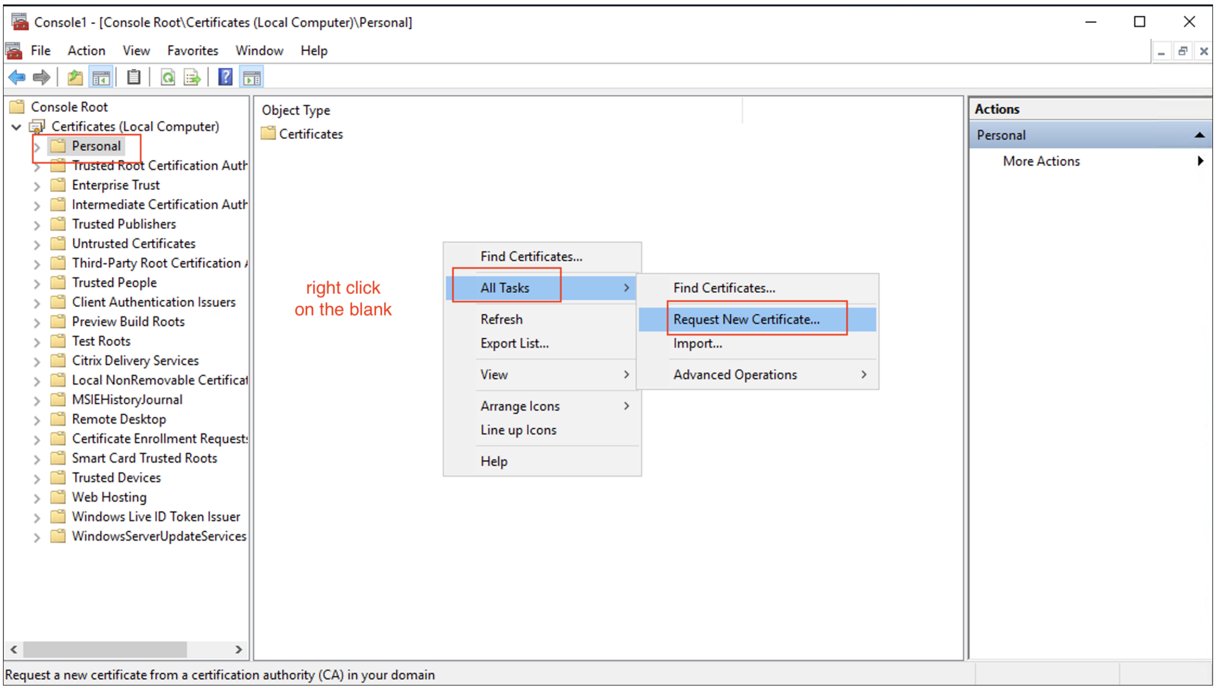
Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

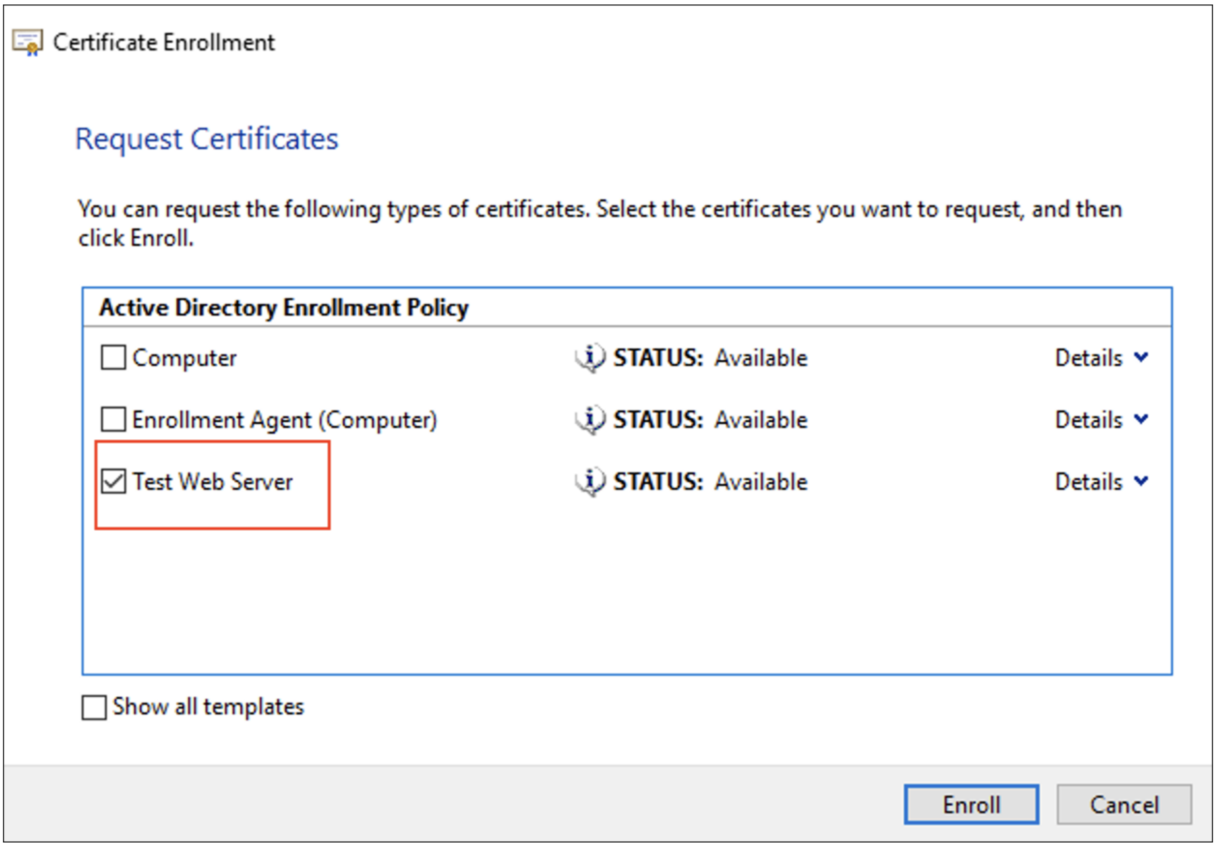
○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.



Console1 - [Console Root\Certificates (Local Computer)\Personal]

Request a new certificate from a certification authority (CA) in your domain



Certificate Enrollment

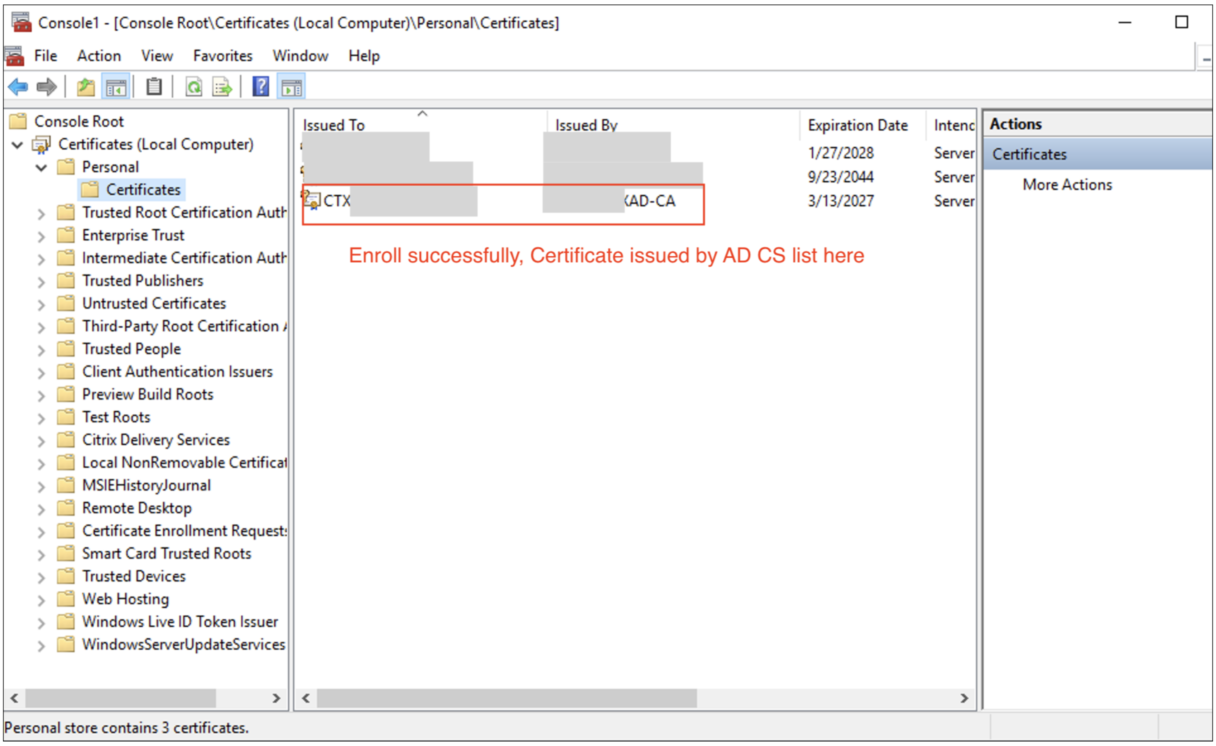
Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

□ Computer	STATUS: Available	Details
□ Enrollment Agent (Computer)	STATUS: Available	Details
☑ Test Web Server	STATUS: Available	Details

□ Show all templates



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Auth
    - Enterprise Trust
    - Intermediate Certification Auth
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification
    - Trusted People
    - Client Authentication Issuers
    - Preview Build Roots
    - Test Roots
    - Citrix Delivery Services
    - Local NonRemovable Certificat
    - MSIEHistoryJournal
    - Remote Desktop
    - Certificate Enrollment Request
    - Smart Card Trusted Roots
    - Trusted Devices
    - Web Hosting
    - Windows Live ID Token Issuer
    - WindowsServerUpdateServices

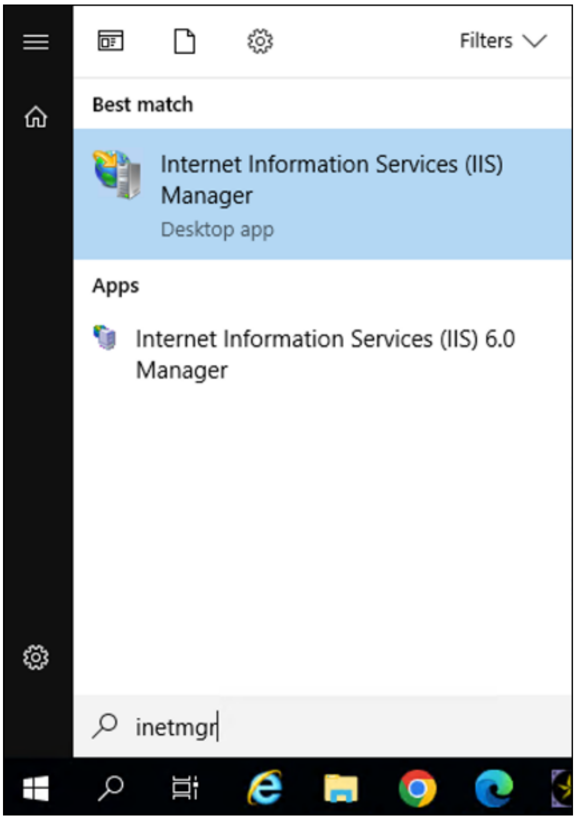
Issued To	Issued By	Expiration Date	Intenc
[redacted]	[redacted]	1/27/2028	Server
[redacted]	[redacted]	9/23/2044	Server
CTX[redacted]	[redacted]AD-CA	3/13/2027	Server

Enroll successfully, Certificate issued by AD CS list here

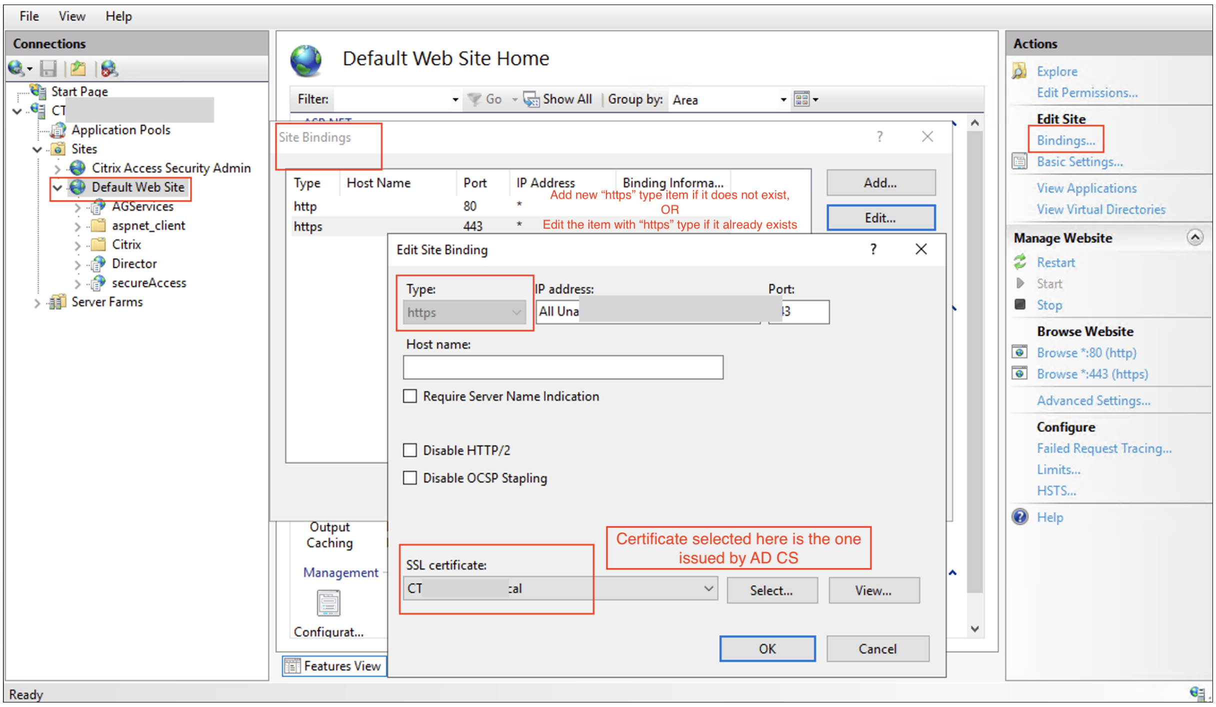
Personal store contains 3 certificates.

Binding Certificate on DDC IIS

On DDC machine, open IIS and Edit Site Binding.


Filters
Best match
Internet Information Services (IIS) Manager
Desktop app
Apps
Internet Information Services (IIS) 6.0 Manager

inetmgr



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Add new "https" type item if it does not exist,
OR
Edit the item with "https" type if it already exists

Edit Site Binding

Type: https

IP address: All Una[redacted]

Port: [redacted]3

Host name:

□ Require Server Name Indication

□ Disable HTTP/2

□ Disable OCSP Stapling

SSL certificate: CT[redacted]:al

Select... View...

OK Cancel

Certificate selected here is the one issued by AD CS

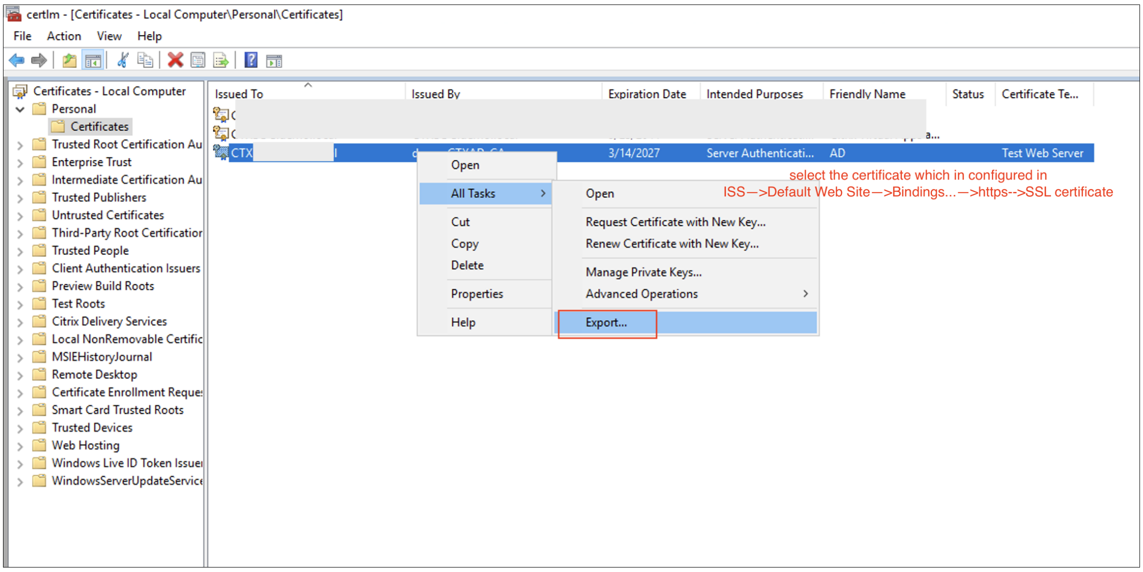
> **Note:**
>
> 1. There is no need to reboot IIS or server after changing SSL certificate for DDC site.
> 2. WebStudio is a prerequisite for websocket VDA since token generation is only available in WebStudio.
> 3. If there are multiple DDC machines, the step to bind the certificate shall be done for all DDC machines, and ensure they are all binding the same certificate.

Install the Certificate on Mac

There are two ways to install the AD CS issued certificate on the Mac machine
Method1:

1. On DDC machine, open the **Manage computer certificates** by `certlm.msc` command.

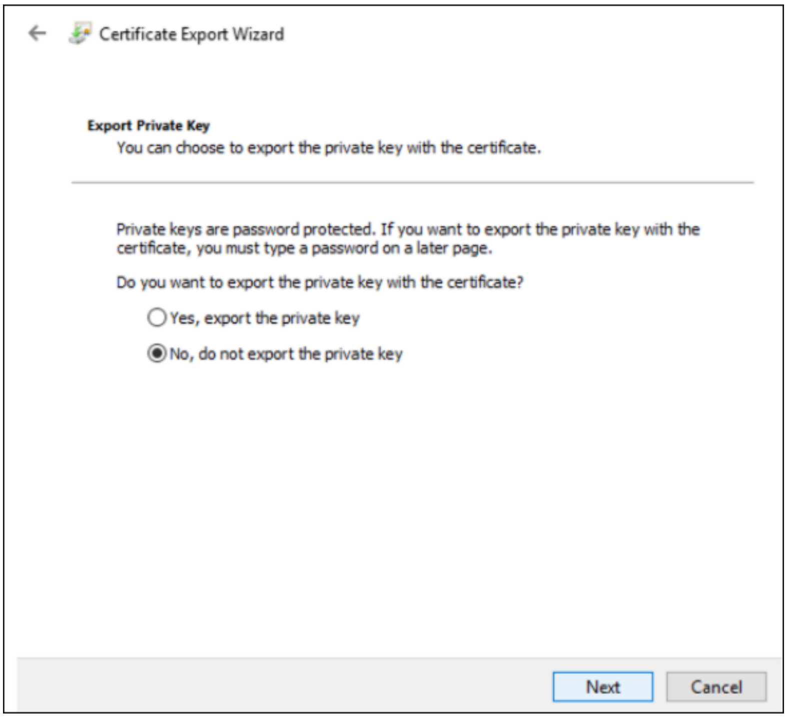
   Make sure to select the certificate which is selected in Step Binding Certificate on DDC IIS and Export the certificate.



certlm - [Certificates - Local Computer\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
CTX[redacted]	[redacted]	3/14/2027	Server Authenticati...	AD		Test Web Server

select the certificate which in configured in
ISS—>Default Web Site—>Bindings...—>https-->SSL certificate



Certificate Export Wizard

Export Private Key

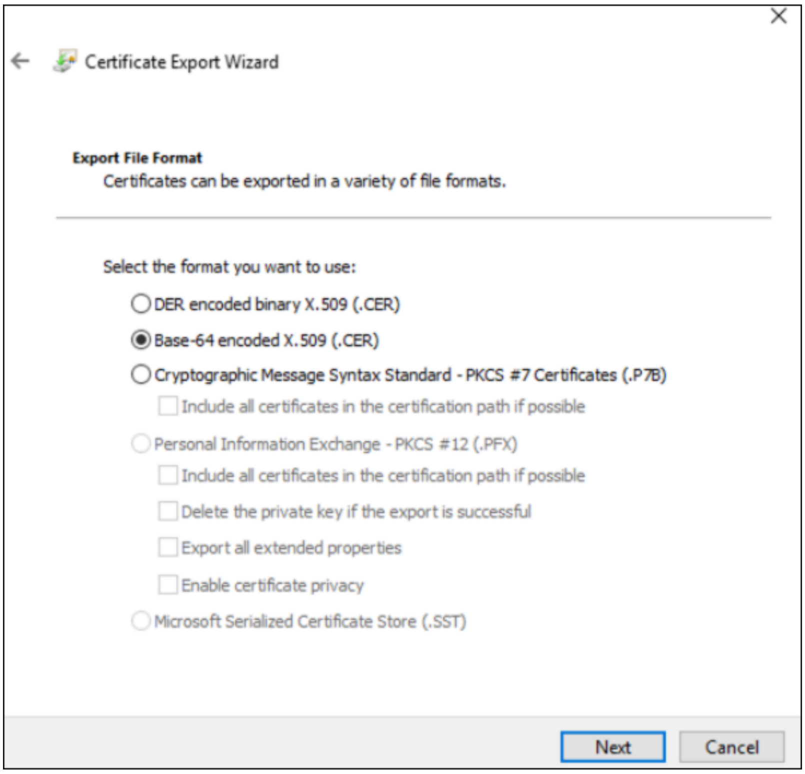
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

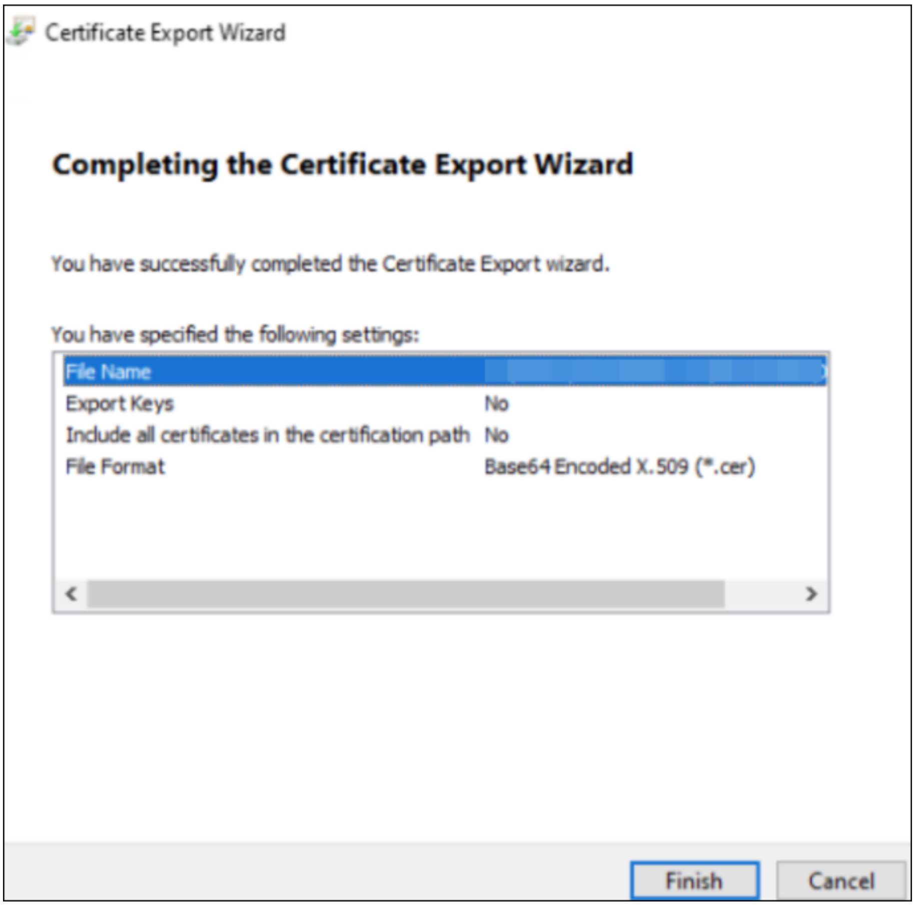
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)



Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

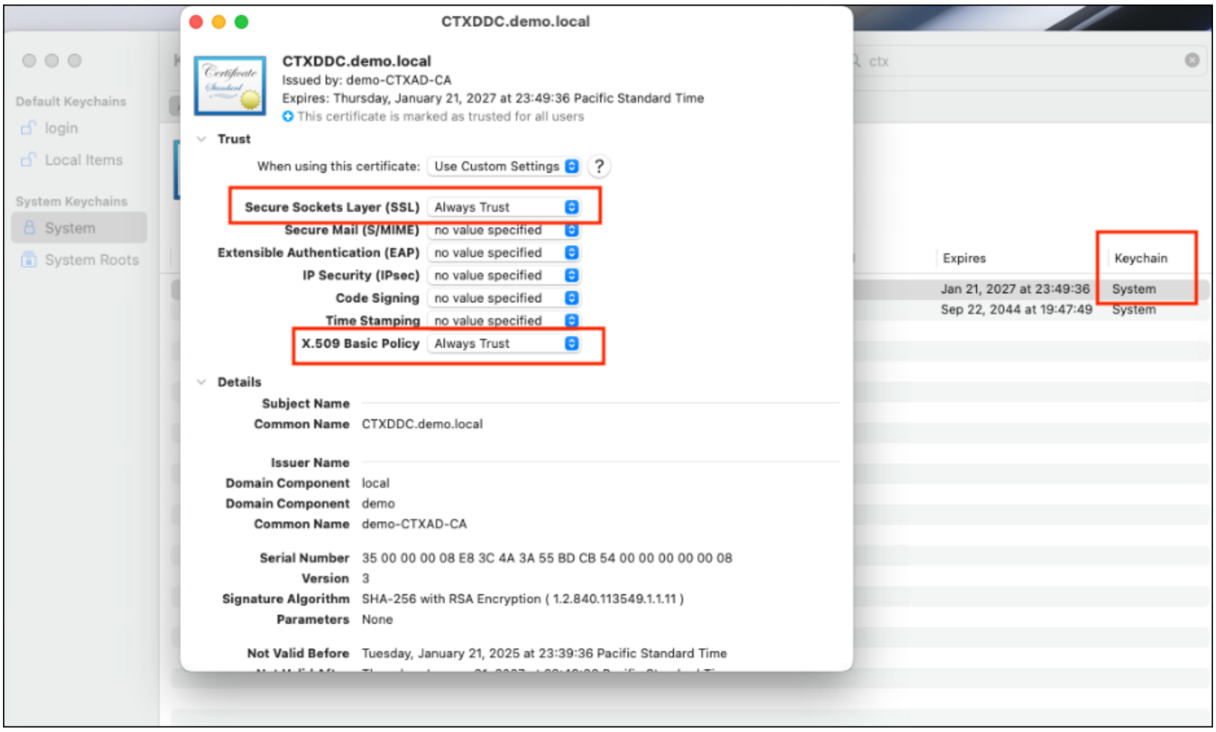
You have specified the following settings:

File Name	
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

2. Transfer the exported certificate in above step to Mac machine,execute the following commands in Terminal App to trust the certificate:

   ```
   sudo security add-trusted-cert -d -r trustAsRoot -p basic -p ssl
   -k /Library/Keychains/System.keychain <path/to/cert file name>
   ```

3. Open Keychain Access app, double confirm the certificate is added to System keychain and trust it for Secure socket Layer(SSL) and X.509 Basic Policy.



CTXDDC.demo.local

CTXDDC.demo.local
Issued by: demo-CTXAD-CA
Expires: Thursday, January 21, 2027 at 23:49:36 Pacific Standard Time
This certificate is marked as trusted for all users

Trust

When using this certificate: Use Custom Settings

Secure Sockets Layer (SSL): Always Trust
Secure Mail (S/MIME): no value specified
Extensible Authentication (EAP): no value specified
IP Security (IPsec): no value specified
Code Signing: no value specified
Time Stamping: no value specified
X.509 Basic Policy: Always Trust

Details

Subject Name
Common Name: CTXDDC.demo.local

Issuer Name
Domain Component: local
Domain Component: demo
Common Name: demo-CTXAD-CA

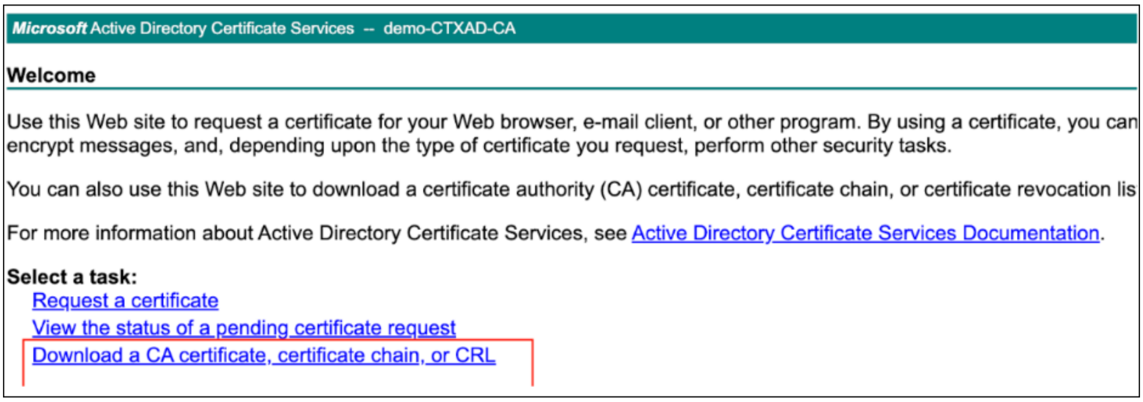
Serial Number: 35 00 00 00 08 E8 3C 4A 3A 55 BD CB 54 00 00 00 00 00 08
Version: 3
Signature Algorithm: SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters: None

Not Valid Before: Tuesday, January 21, 2025 at 23:39:36 Pacific Standard Time

Expires	Keychain
Jan 21, 2027 at 23:49:36	System
Sep 22, 2044 at 19:47:49	System

Method2:

1. On Mac machine, open the Browser and input http://<AD CS IP>/certsrv



Microsoft Active Directory Certificate Services -- demo-CTXAD-CA

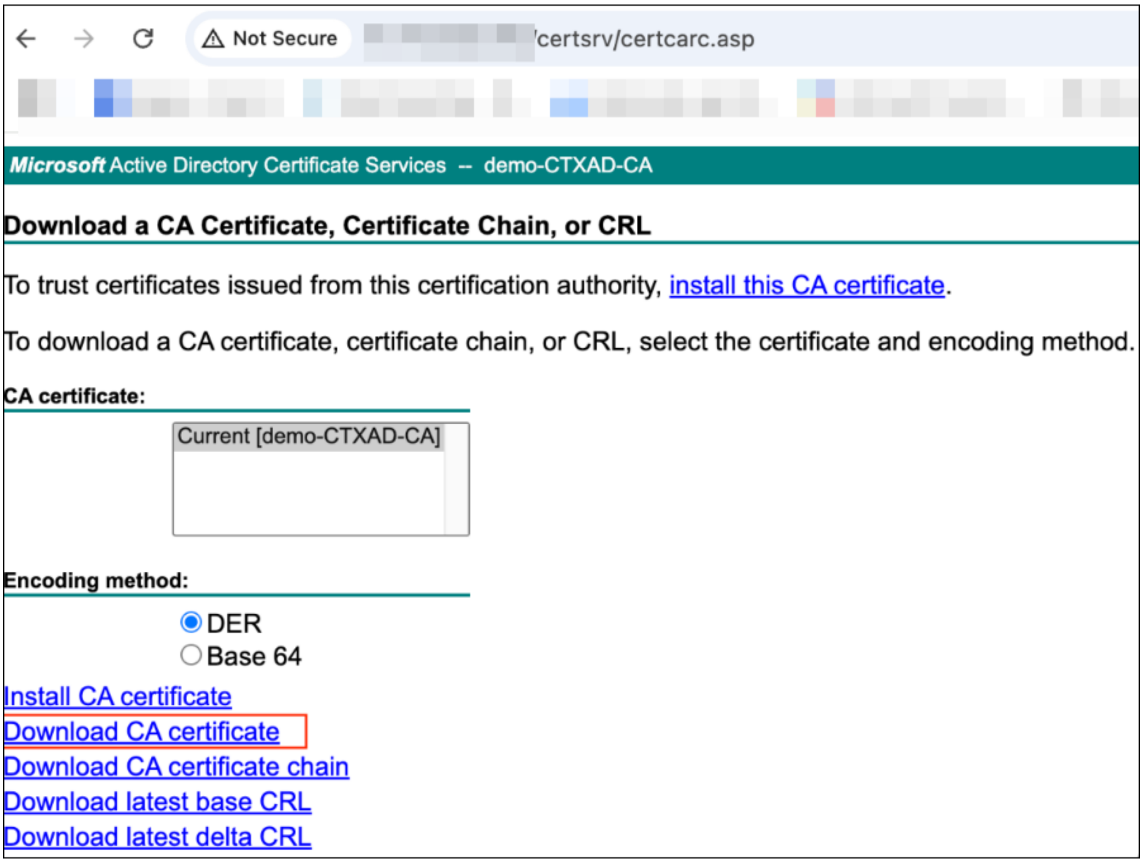
Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation lis

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL



Not Secure [redacted]/certsrv/certcarc.asp

[redacted]

Microsoft Active Directory Certificate Services -- demo-CTXAD-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [demo-CTXAD-CA]

Encoding method:

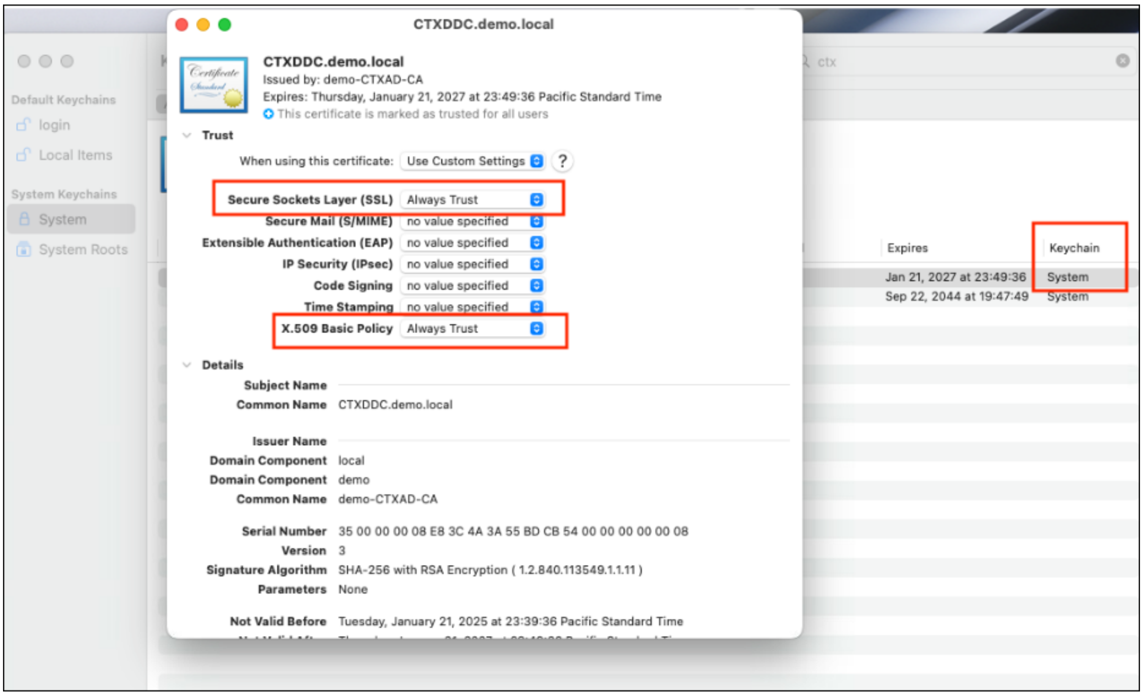
● DER
○ Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

2. Execute the following commands in Terminal App to trust the downloaded certificate in above step

```
sudo security add-trusted-cert -d -r trustRoot -p basic -p ssl -k
 /Library/Keychains/System.keychain <path/to/cert file name>
```

3. Open Keychain Access app, double confirm the certificate is added to System keychain and trust it for Secure socket Layer(SSL) and X.509 Basic Policy



CTXDDC.demo.local

CTXDDC.demo.local
Issued by: demo-CTXAD-CA
Expires: Thursday, January 21, 2027 at 23:49:36 Pacific Standard Time
This certificate is marked as trusted for all users

Trust

When using this certificate: Use Custom Settings

Secure Sockets Layer (SSL)	Always Trust
Secure Mail (S/MIME)	no value specified
Extensible Authentication (EAP)	no value specified
IP Security (IPsec)	no value specified
Code Signing	no value specified
Time Stamping	no value specified
X.509 Basic Policy	Always Trust

Details

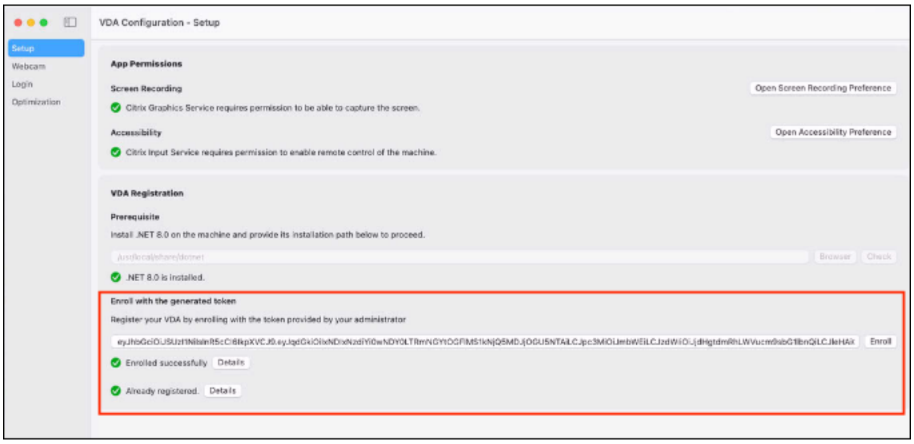
Subject Name	
Common Name	CTXDDC.demo.local
Issuer Name	
Domain Component	local
Domain Component	demo
Common Name	demo-CTXAD-CA
Serial Number	35 00 00 00 08 E8 3C 4A 3A 55 BD CB 54 00 00 00 00 00 08
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Tuesday, January 21, 2025 at 23:39:36 Pacific Standard Time

Expires	Keychain
Jan 21, 2027 at 23:49:36	System
Sep 22, 2044 at 19:47:49	System

Install Citrix VDA for macOS

To install Citrix VDA for macOS, see install VDA.

After installation, open the VDA Configuration app to finish the Enrollment and Registration.



VDA Configuration - Setup

App Permissions

Screen Recording

Citrix Graphics Service requires permission to be able to capture the screen.

Accessibility

Citrix Input Service requires permission to enable remote control of the machine.

VDA Registration

Prerequisite

Install .NET 8.0 on the machine and provide its installation path below to proceed.

/usr/local/share/dotnet

.NET 8.0 is installed.

Enroll with the generated token

Register your VDA by enrolling with the token provided by your administrator

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJqdGkiOiIxNDIxNzdiYi0wNDY0LTRmNGYtOGFlMS1kNjQ5MDJjOGU5NTAiLCJpc3MiOiJmbWEiLCJzdWIiOiJjdHgtdmRhLWVucm9sbG1lbnQiLCJleHAi

Enrolled successfully

Already registered.

Setup
Webcam
Login
Optimization
Open Screen Recording Preference
Open Accessibility Preference
Browser
Check
Enroll
Details
Details

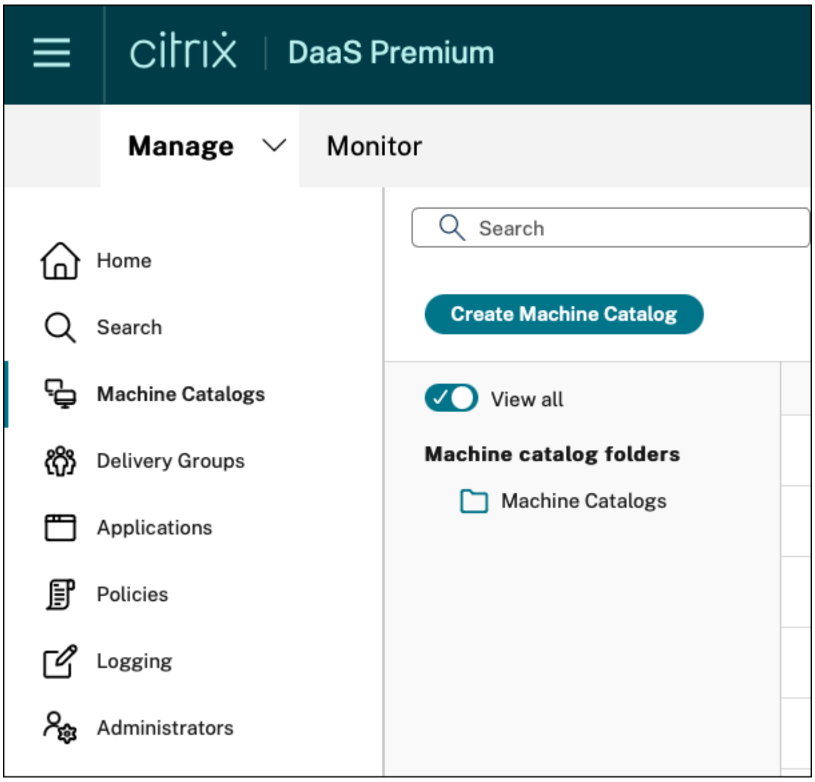
Prepare in DaaS Management Console

August 1, 2025

Steps to prepare in DaaS management console:

1. Create a Machine Catalog for Citrix VDA for macOS.

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

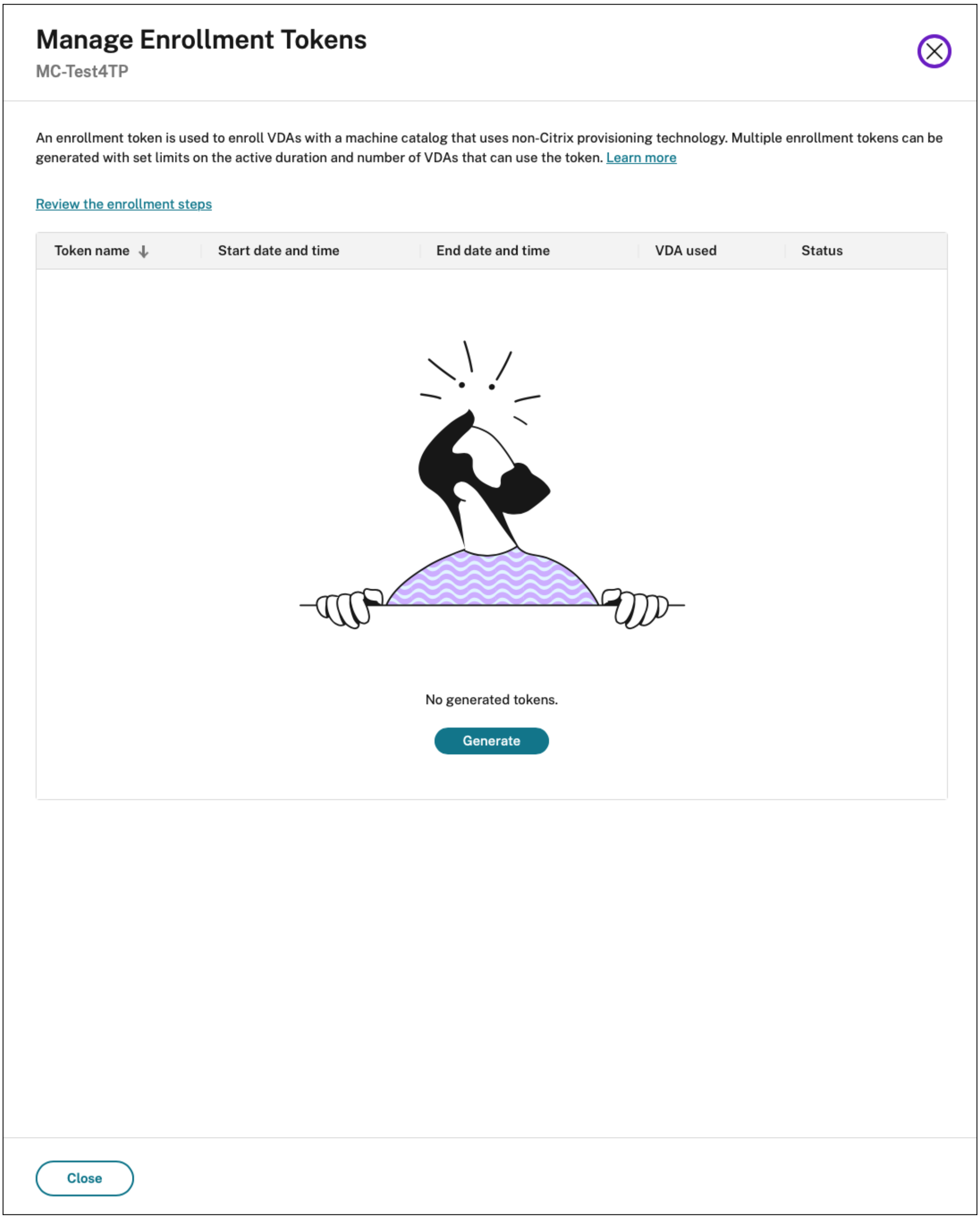
   

   Make sure the configuration is similar to the screenshot provided.

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

   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



Manage Enrollment Tokens

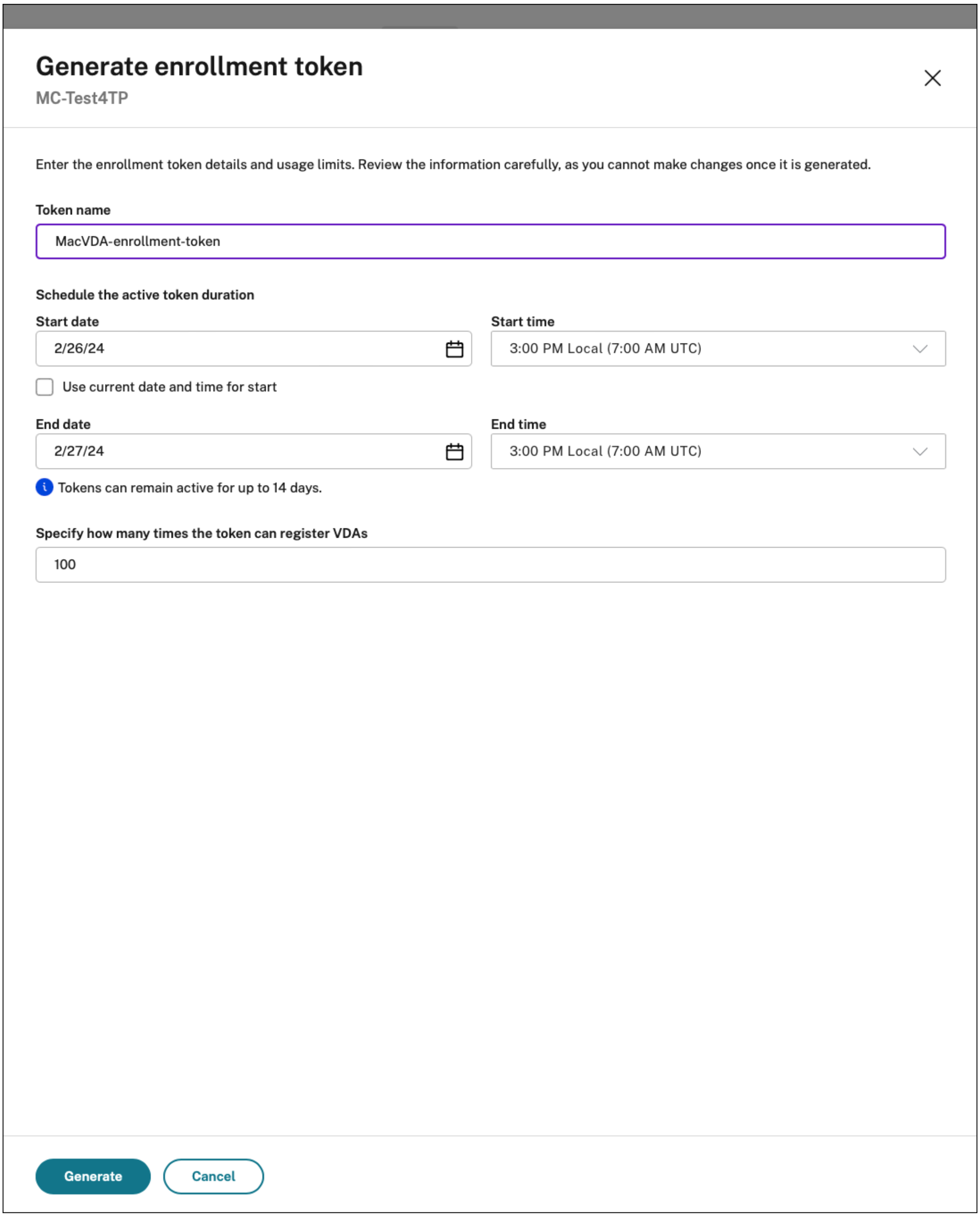
MC-Test4TP

An enrollment token is used to enroll VDAs with a machine catalog that uses non-Citrix provisioning technology. Multiple enrollment tokens can be generated with set limits on the active duration and number of VDAs that can use the token. Learn more

Review the enrollment steps

Token name ↓	Start date and time	End date and time	VDA used	Status

No generated tokens.



Generate enrollment token

MC-Test4TP

Enter the enrollment token details and usage limits. Review the information carefully, as you cannot make changes once it is generated.

Token name: MacVDA-enrollment-token

Schedule the active token duration

Start date: 2/26/24

Start time: 3:00 PM Local (7:00 AM UTC)

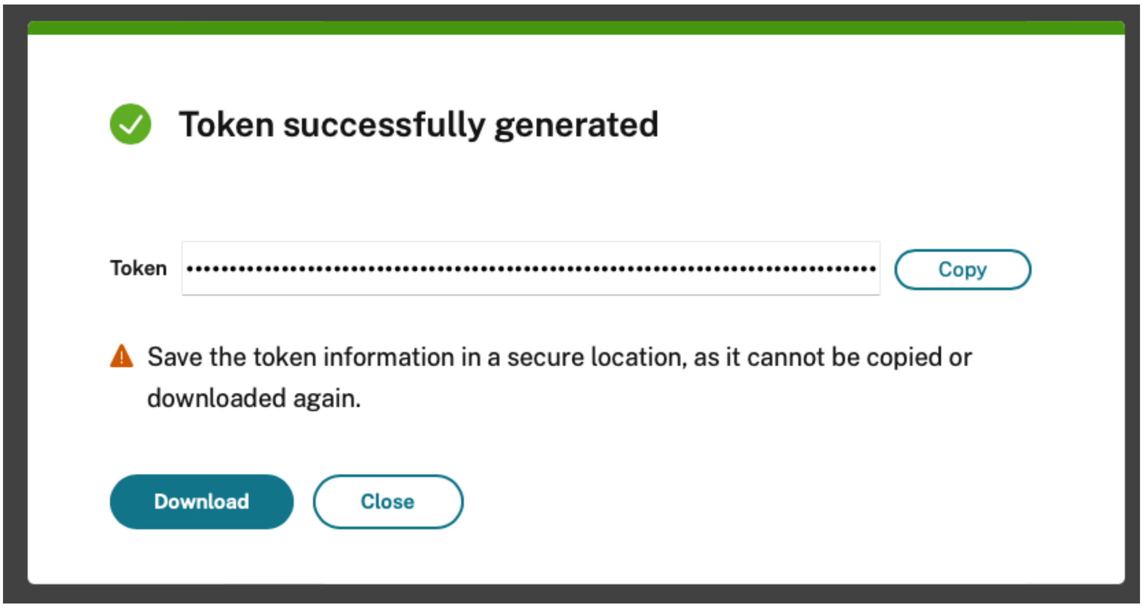
□ Use current date and time for start

End date: 2/27/24

End time: 3:00 PM Local (7:00 AM UTC)

Tokens can remain active for up to 14 days.

Specify how many times the token can register VDAs: 100



Token successfully generated

Token ••

Save the token information in a secure location, as it cannot be copied or downloaded again.

> **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.

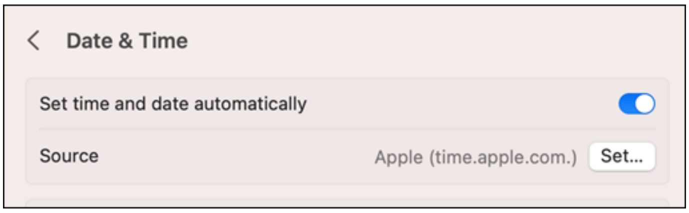
> **Note :**
>
> - Test and then share the workspace URL link with your subscribers (users) to give them access to their apps and desktops.

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

Use the Installer of Citrix VDA for macOS

January 19, 2026

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

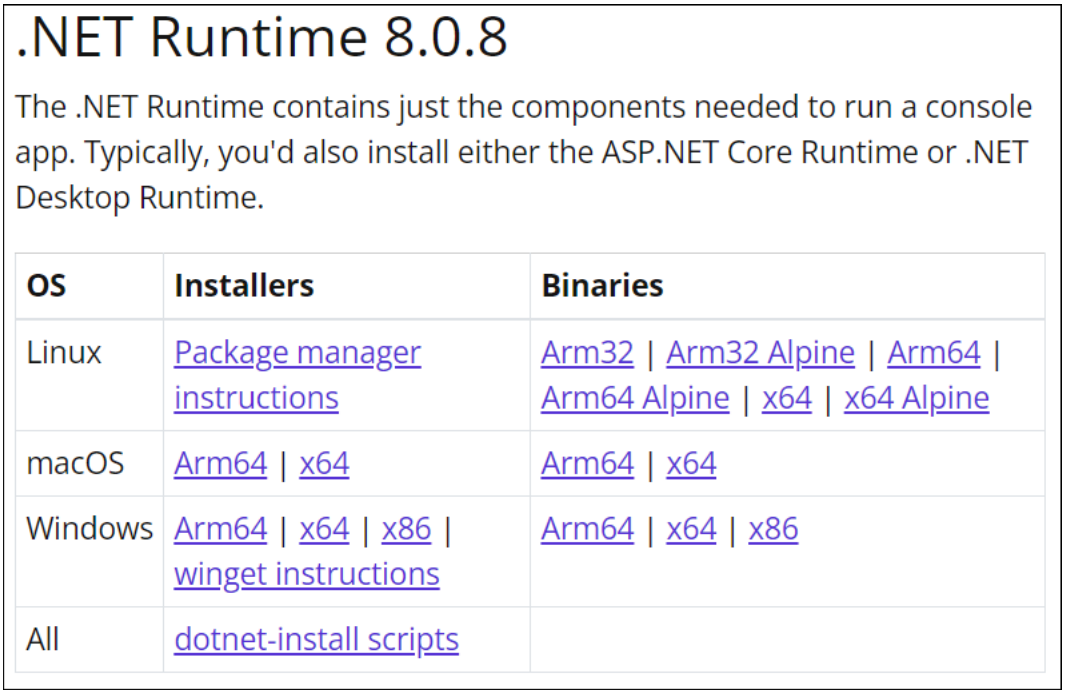
   Date & Time

   Set time and date automatically

   Source Apple (time.apple.com.) Set...

2. Download **.Net 8.0** from https://dotnet.microsoft.com/en-us/download/dotnet/8.0

3. Install the **Arm64 .Net Runtime** package from download table similar as below.

   # .NET Runtime 8.0.8

   The .NET Runtime contains just the components needed to run a console app. Typically, you'd also install either the ASP.NET Core Runtime or .NET Desktop Runtime.

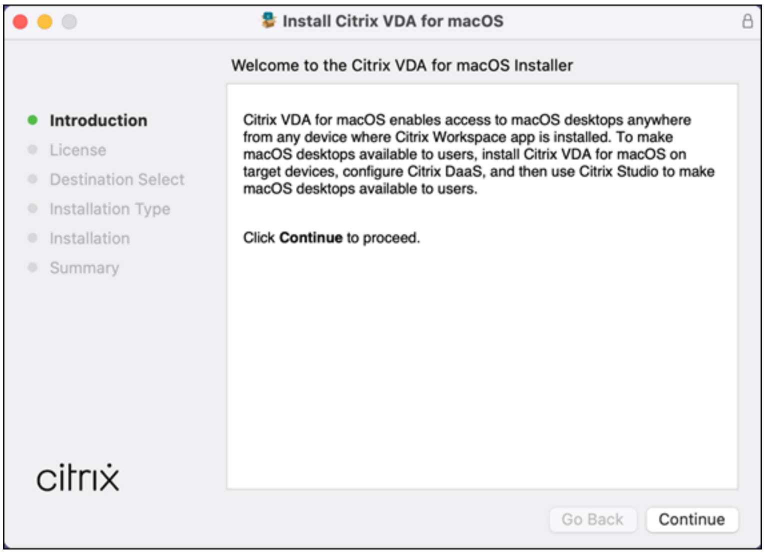
OS	Installers	Binaries
Linux	Package manager instructions	Arm32 | Arm32 Alpine | Arm64 | Arm64 Alpine | x64 | x64 Alpine
macOS	Arm64 | x64	Arm64 | x64
Windows	Arm64 | x64 | x86 | winget instructions	Arm64 | x64 | x86
All	dotnet-install scripts	

   You can later check the installation directory path using command from terminal: `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.

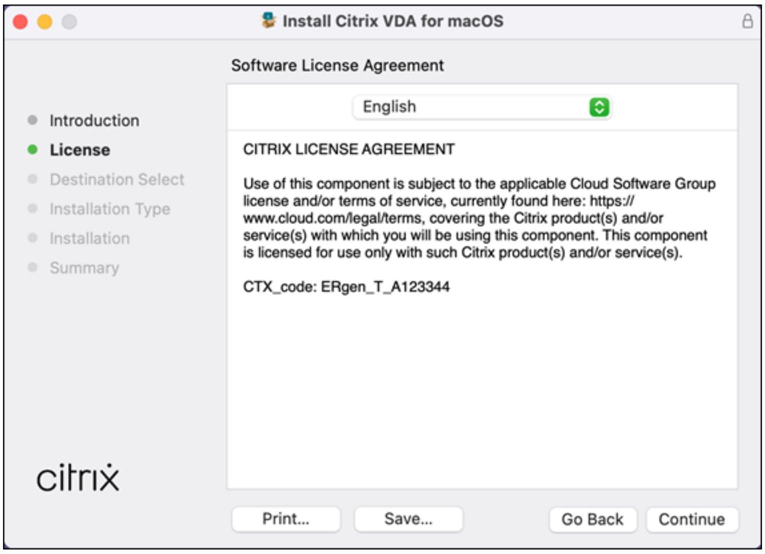


Welcome to the Citrix VDA for macOS Installer

Citrix VDA for macOS enables access to macOS desktops anywhere from any device where Citrix Workspace app is installed. To make macOS desktops available to users, install Citrix VDA for macOS on target devices, configure Citrix DaaS, and then use Citrix Studio to make macOS desktops available to users.

Click **Continue** to proceed.

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

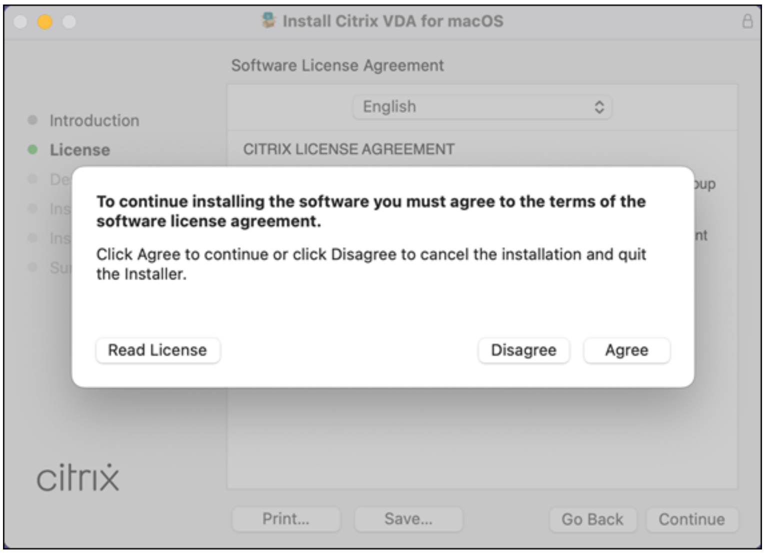


CITRIX LICENSE AGREEMENT

Use of this component is subject to the applicable Cloud Software Group license and/or terms of service, currently found here: https://www.cloud.com/legal/terms, covering the Citrix product(s) and/or service(s) with which you will be using this component. This component is licensed for use only with such Citrix product(s) and/or service(s).

CTX_code: ERgen_T_A123344

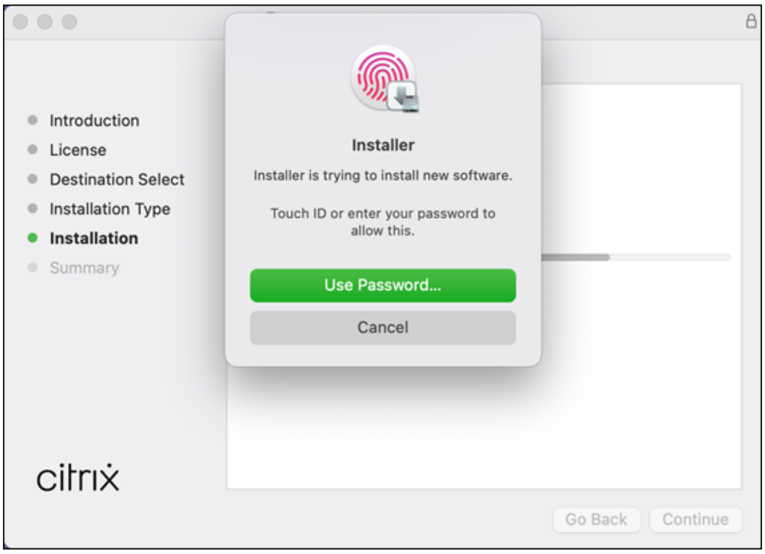
7. Read and Click **Agree** to continue. If you disagree, the installation process aborts.



To continue installing the software you must agree to the terms of the software license agreement.

Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

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



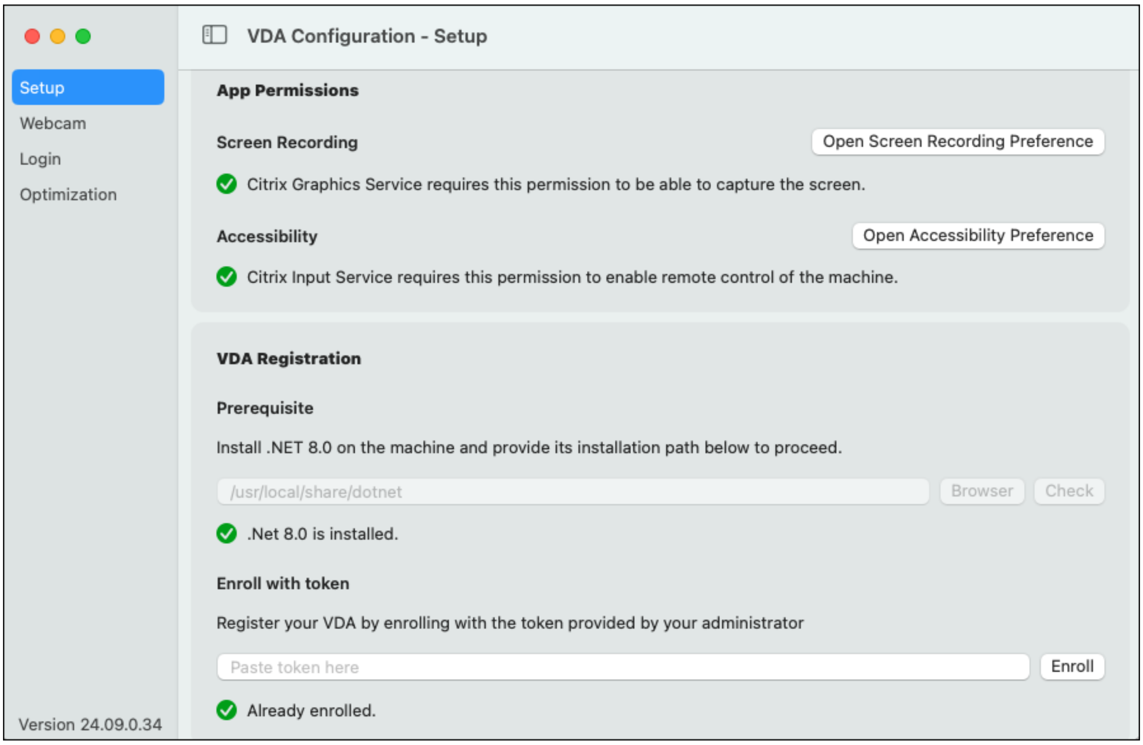
Installer

Installer is trying to install new software.

Touch ID or enter your password to allow this.

9. The VDA Configuration tool provides a one-stop-shop experience for change related settings that enables basic HDX™ services and new features such as SSO, Webcam redirection and optimization etc.

   Enable Screen Recording (Citrix Graphics Service) and Accessibility (Citrix Input Service) in the Setup tab by clicking Open Screen Recording Preference to enable Citrix Graphics Service AND Click Open Accessibility Preferences to enable Citrix Input Service, these two are required services so your end user can launch and use the HDX session. For other configuration such as SSO (Single Sign-On), Webcam and VDA optimization, you can always come back to VDA Configuration later to change them, for details please refer to Configuration -> Administration -> Tools & Utilities -> VDA Configuration in this document.


VDA Configuration - Setup
Setup
Webcam
Login
Optimization
Open Screen Recording Preference
Open Accessibility Preference
Browser
Check
Enroll
Version 24.09.0.34

App Permissions

Screen Recording

✓ Citrix Graphics Service requires this permission to be able to capture the screen.

Accessibility

✓ Citrix Input Service requires this permission to enable remote control of the machine.

VDA Registration

Prerequisite

Install .NET 8.0 on the machine and provide its installation path below to proceed.

/usr/local/share/dotnet

✓ .Net 8.0 is installed.

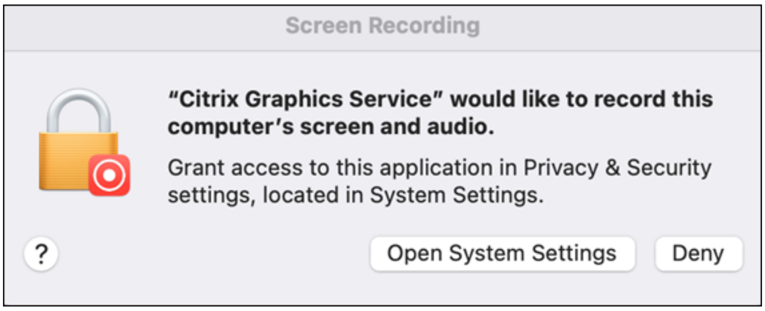
Enroll with token

Register your VDA by enrolling with the token provided by your administrator

Paste token here

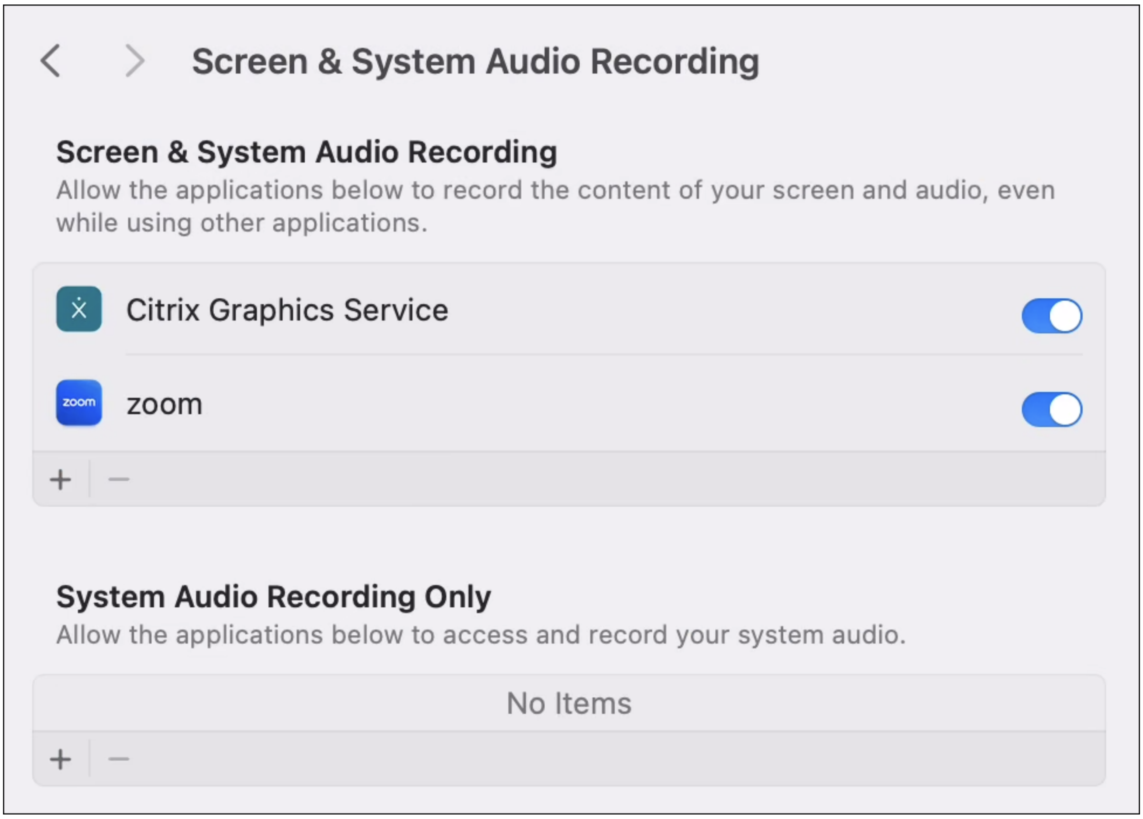
✓ Already enrolled.

> **Note :**
>
> For first time installation, you can also enable **Citrix Graphics Service** through the system pop-up message box by clicking **Open System Settings**.



"Citrix Graphics Service" would like to record this computer's screen and audio.

Grant access to this application in Privacy & Security settings, located in System Settings.



Screen & System Audio Recording

Screen & System Audio Recording

Allow the applications below to record the content of your screen and audio, even while using other applications.

Citrix Graphics Service ●

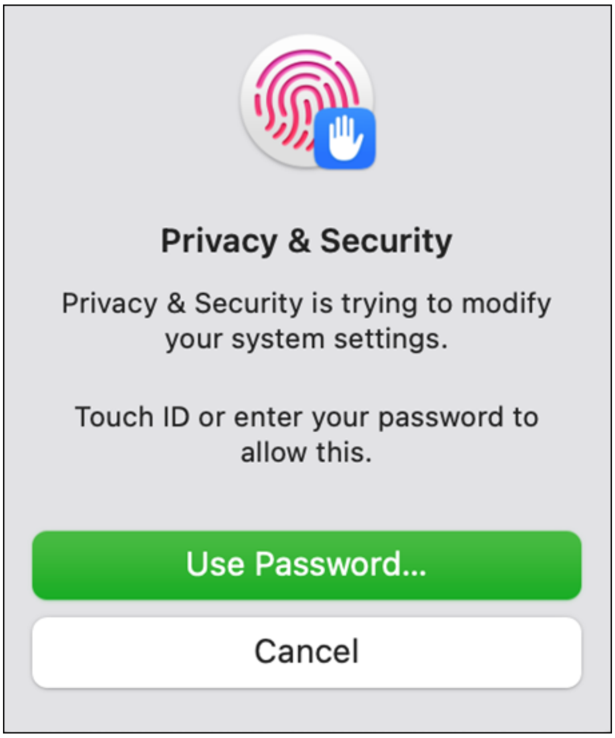
zoom ●

System Audio Recording Only

Allow the applications below to access and record your system audio.

No Items

10. You must have administrator credential to enable services.

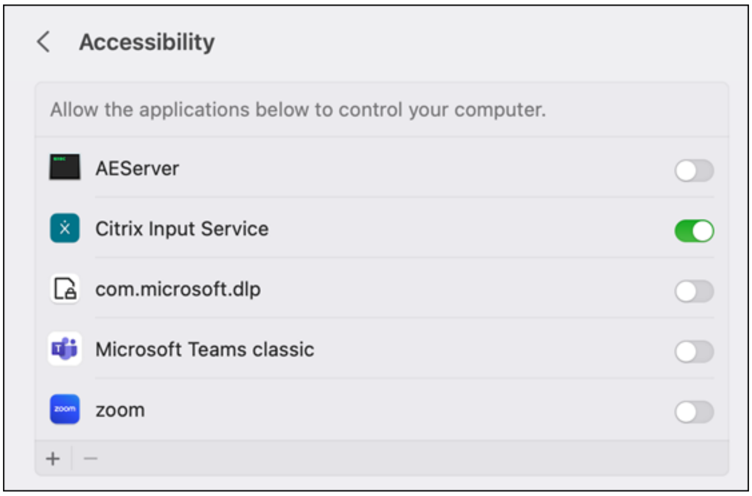


Privacy & Security

Privacy & Security is trying to modify your system settings.

Touch ID or enter your password to allow this.

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



Accessibility

Allow the applications below to control your computer.

- AEServer ○
- Citrix Input Service ●
- com.microsoft.dlp ○
- Microsoft Teams classic ○
- zoom ○

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.

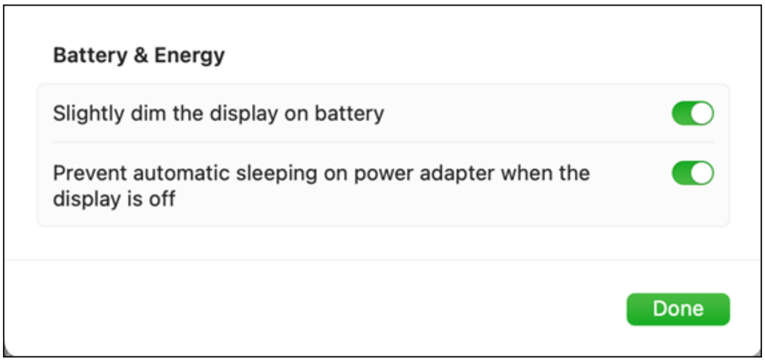
    Generally, this process completes within a few seconds if the network conditions are favorable.

    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.

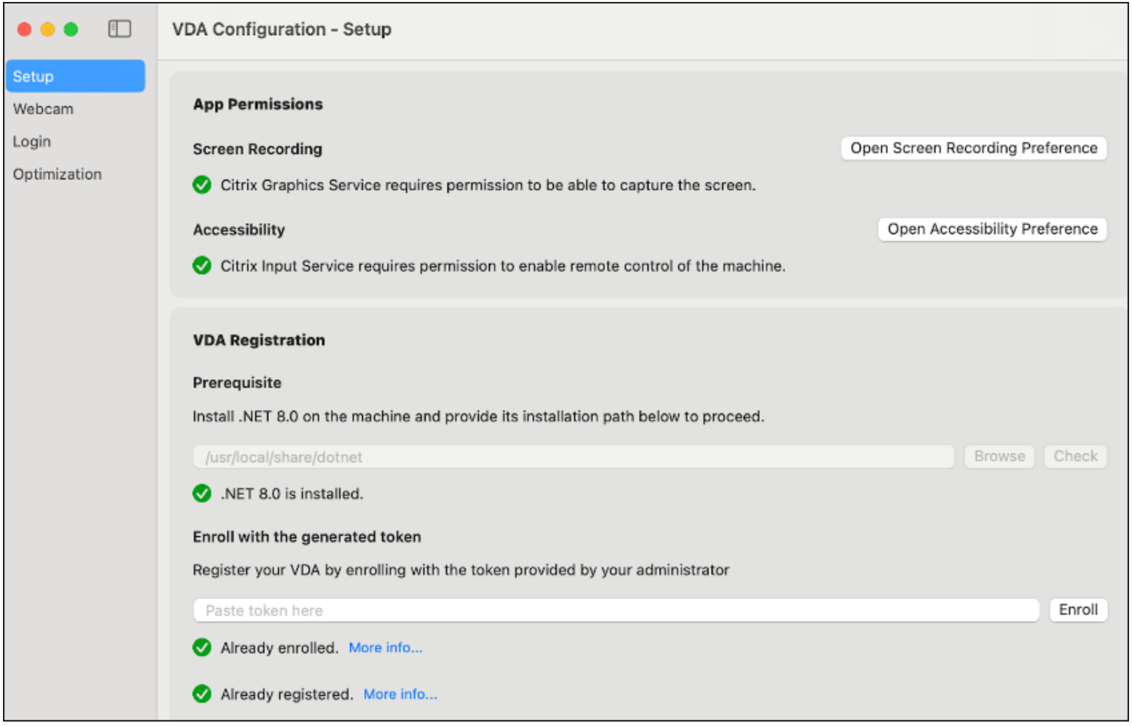


Battery & Energy

Slightly dim the display on battery ●

Prevent automatic sleeping on power adapter when the display is off ●

14. When the VDA is successfully registered, your **Setup** page is as displayed. We have added a **More info** link to the macOS Console application for administrators to access VDA logs when needed.



VDA Configuration - Setup

Setup
Webcam
Login
Optimization

App Permissions

Screen Recording

Open Screen Recording Preference

✓ Citrix Graphics Service requires permission to be able to capture the screen.

Accessibility

Open Accessibility Preference

✓ Citrix Input Service requires permission to enable remote control of the machine.

VDA Registration

Prerequisite

Install .NET 8.0 on the machine and provide its installation path below to proceed.

/usr/local/share/dotnet

✓ .NET 8.0 is installed.

Enroll with the generated token

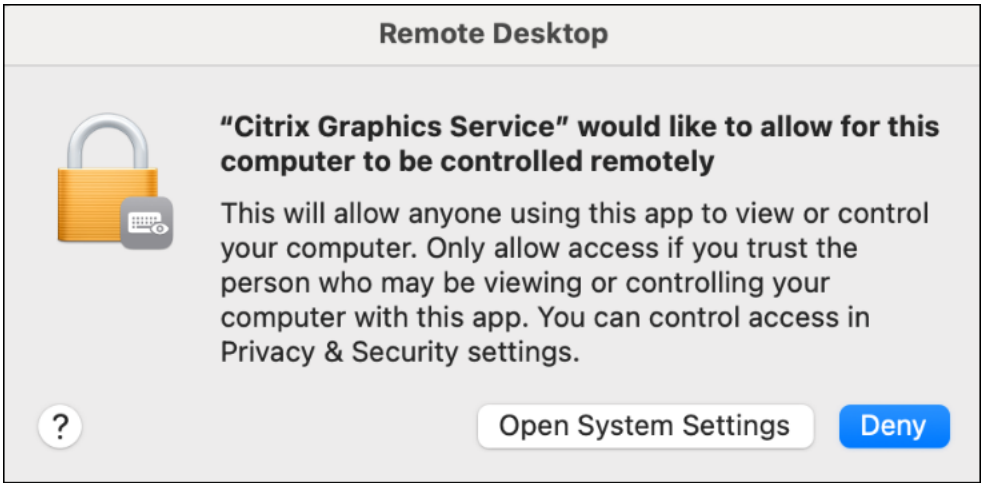
Register your VDA by enrolling with the token provided by your administrator

Paste token here

✓ Already enrolled. More info...

✓ Already registered. More info...

15. When connected first time with Citrix VDA for macOS 25.07 or later, a prompt will appear:



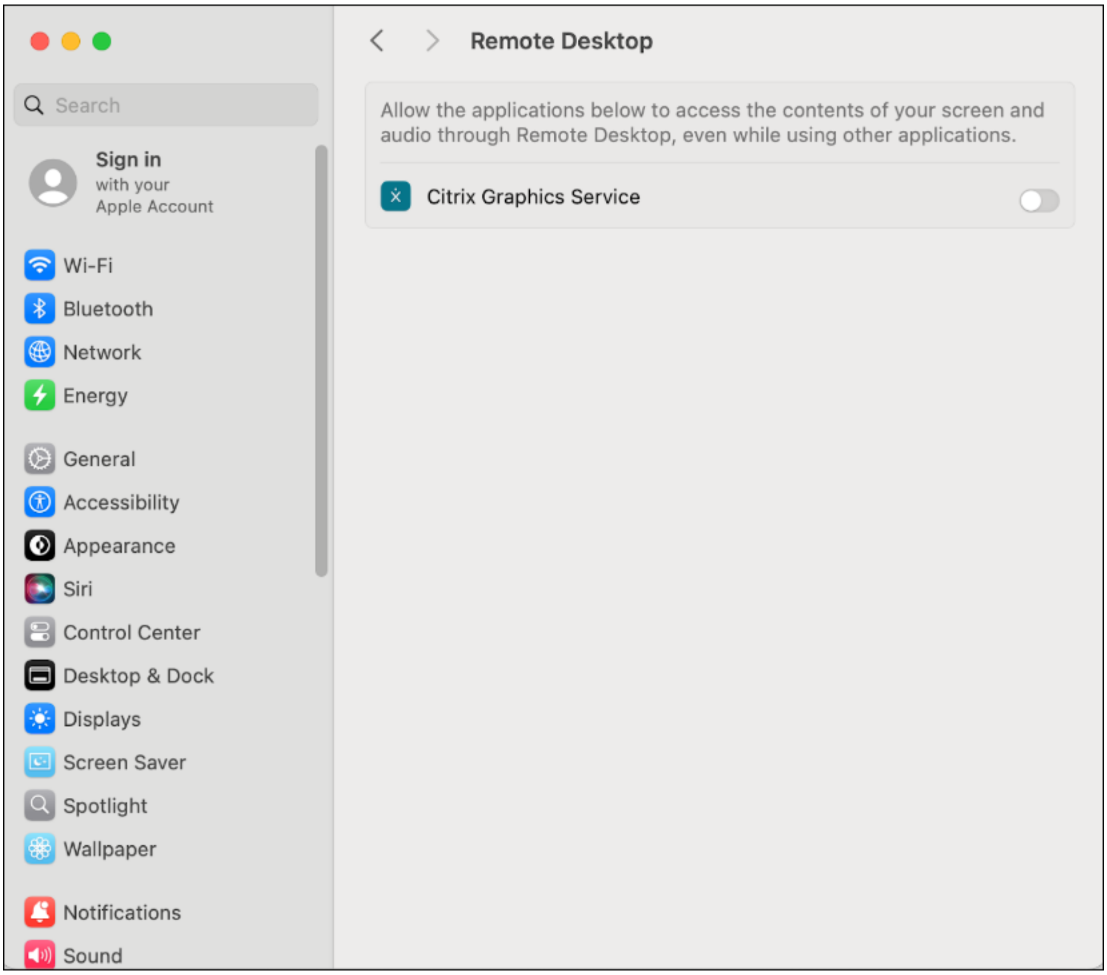
Remote Desktop

"Citrix Graphics Service" would like to allow for this computer to be controlled remotely

This will allow anyone using this app to view or control your computer. Only allow access if you trust the person who may be viewing or controlling your computer with this app. You can control access in Privacy & Security settings.

Although ignoring this prompt will not impact the usage of Citrix VDA for macOS, we recommend suppressing it for an improved user experience by opening the System Settings to grant remote desktop privileges to the Citrix Graphics Service within 'System Settings > Privacy & Security > Remote Desktop'.

> **Note:**
>
> After granted Citrix Graphics Service in Remote Desktop, it also stops the monthly alert from macOS for Citrix Graphics Service.



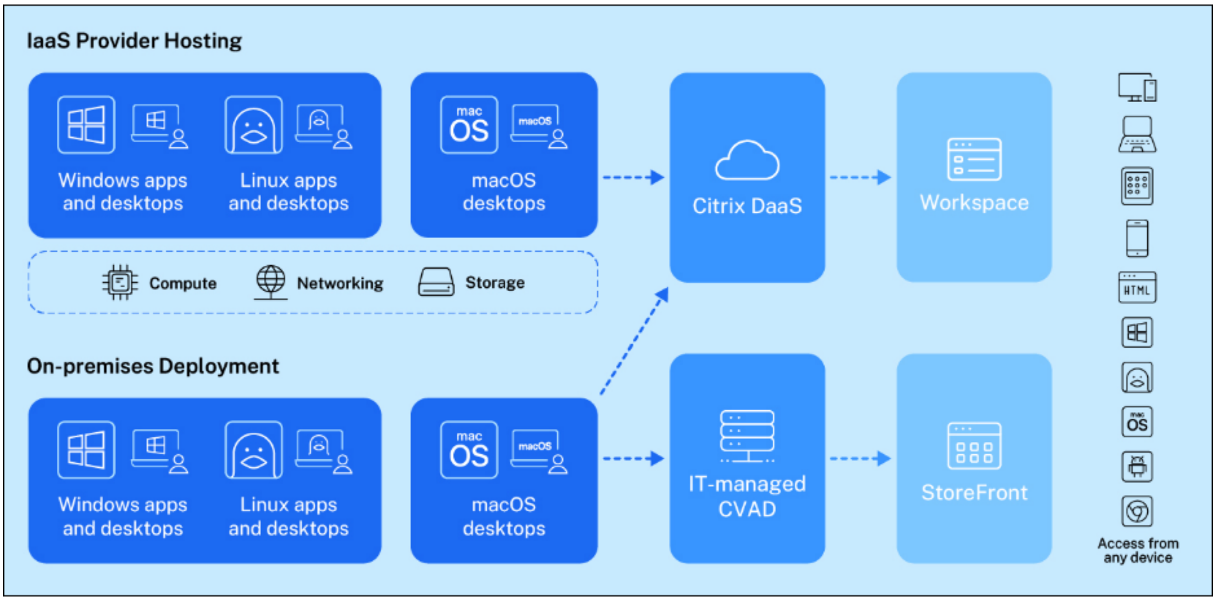
Allow the applications below to access the contents of your screen and audio through Remote Desktop, even while using other applications.

Citrix Graphics Service ○

VDA Deployment Recommendation

August 1, 2025

Citrix VDA for macOS is very flexible regarding deployment scenarios: both Cloud and on-prem environments are supported. We have partnered with leaders in Mac/macOS workload IaaS providers such as MacStadium and AWS EC2 services since Tech Preview of this product, refer below link for more details how to deploy macOS VDA in those environments.



For DaaS customers whose end users need remote access from outside corporate networks to Citrix VDA for macOS deployed on-prem, 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 the Citrix Cloud control plane. The policy is disabled by default. For more information, see Rendezvous V2.

For both DaaS and CVAD customers please refer to below link for a more comprehensive deployment guide about different scenarios include guidelines and tips when you deploy the VDA in IaaS provider such as MacStadium and AWS:
https://community.citrix.com/tech-zone/build/deployment-guides/citrix-mac-vda/

Example using UEM / MDM

August 1, 2025

To deploy Citrix VDA for macOS at scale, streamline the process with a UEM (Unified Endpoint Management) or MDM (Mobile Device Management) tool, which can assist with or automate the entire deployment.

> **Note:**
>
> Microsoft .NET 8.0 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 • Create delivery groups and assign the desktops to users from Citrix DaaS
End User	• Enable the screen recording permission for VDA locally or remotely • 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.

Later in the article, we also provided a quick guide using Workspace ONE UEM.

Deployment with JAMF Pro

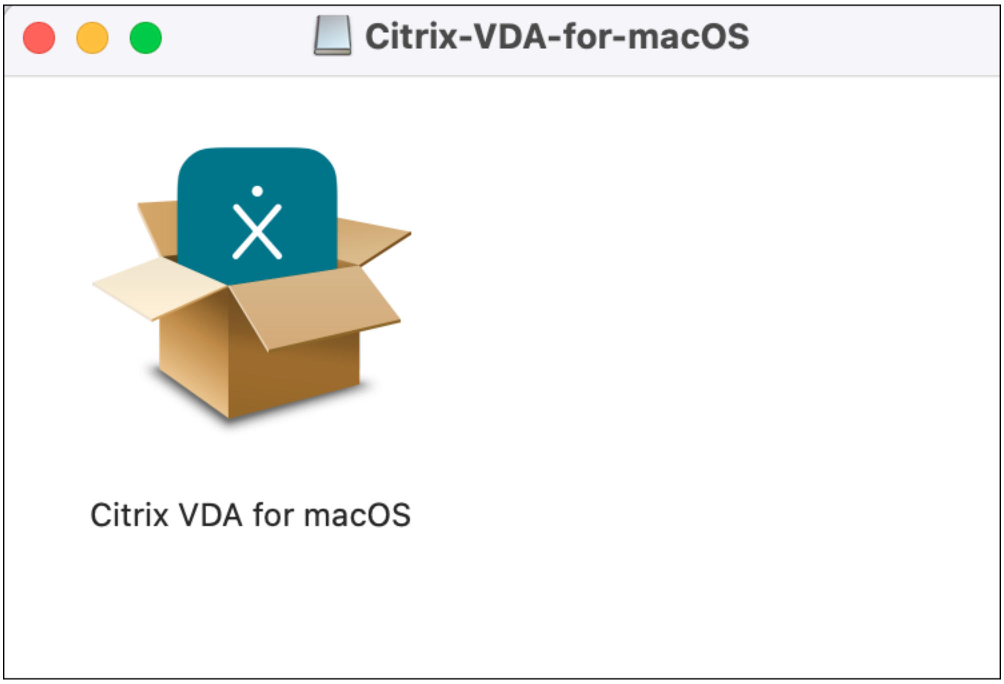
Section 1 - Deploy the virtual delivery agent for macOS package

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.

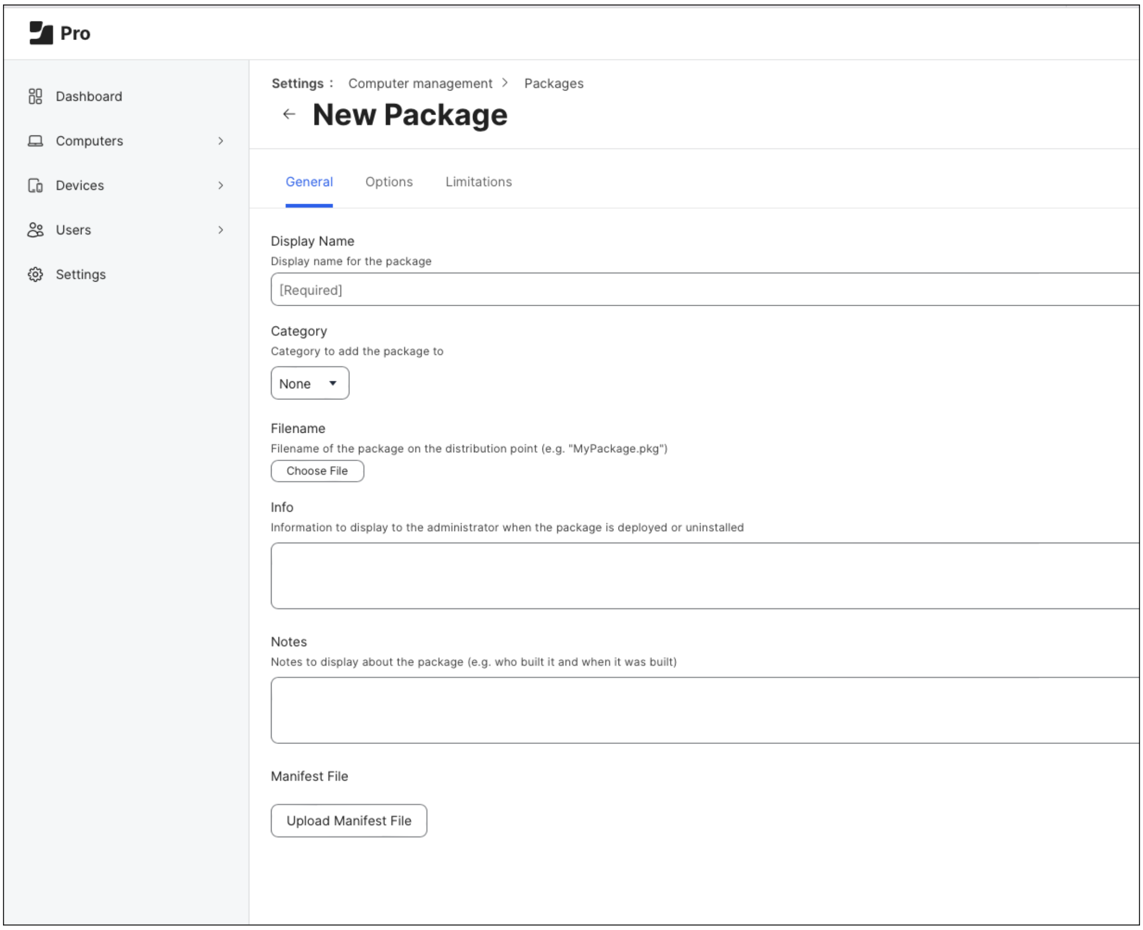
   > **Note:**
   >
   > We will upload this file to the Jamf Pro console later.



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.



Settings : Computer management > Packages

New Package

General Options Limitations

Display Name
Display name for the package
[Required]

Category
Category to add the package to
None

Filename
Filename of the package on the distribution point (e.g. "MyPackage.pkg")
Choose File

Info
Information to display to the administrator when the package is deployed or uninstalled

Notes
Notes to display about the package (e.g. who built it and when it was built)

Manifest File
Upload Manifest File

6. **Save** the package.

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

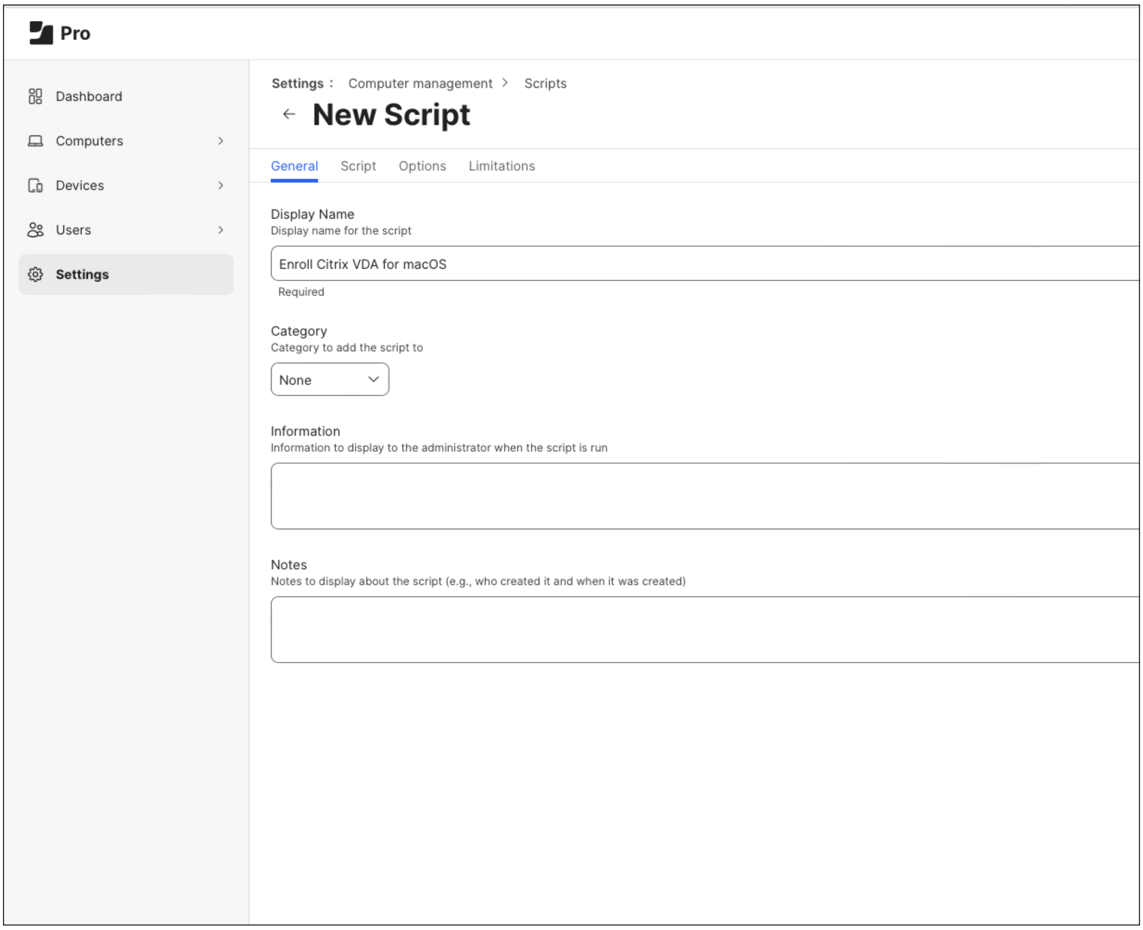
1. Login to the **Jamf Pro** console, and navigate to **Settings** -> **Computer management** -> **Scripts**.
2. Click **New** to add a new script.
3. Enter the following fields for the script.

   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

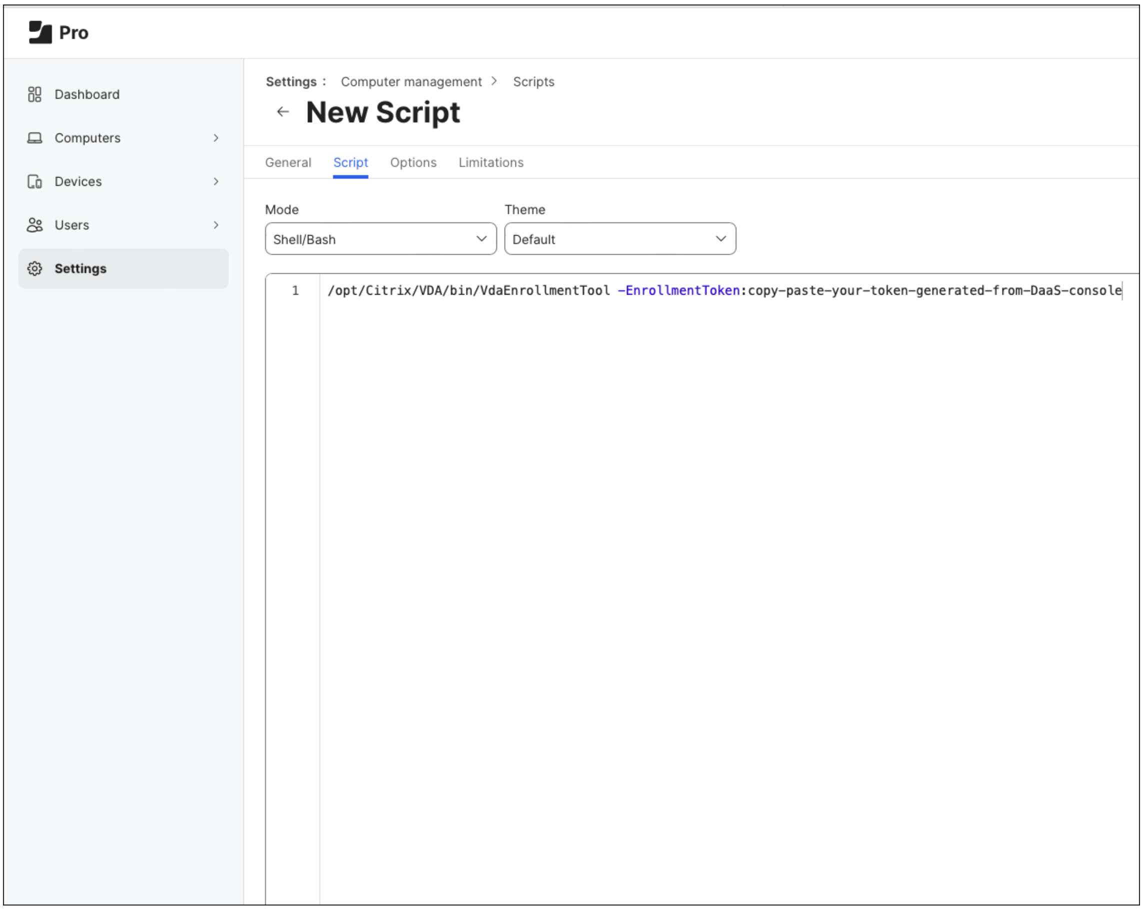


Display Name
Display name for the script
Enroll Citrix VDA for macOS
Required

Category
Category to add the script to
None

Information
Information to display to the administrator when the script is run

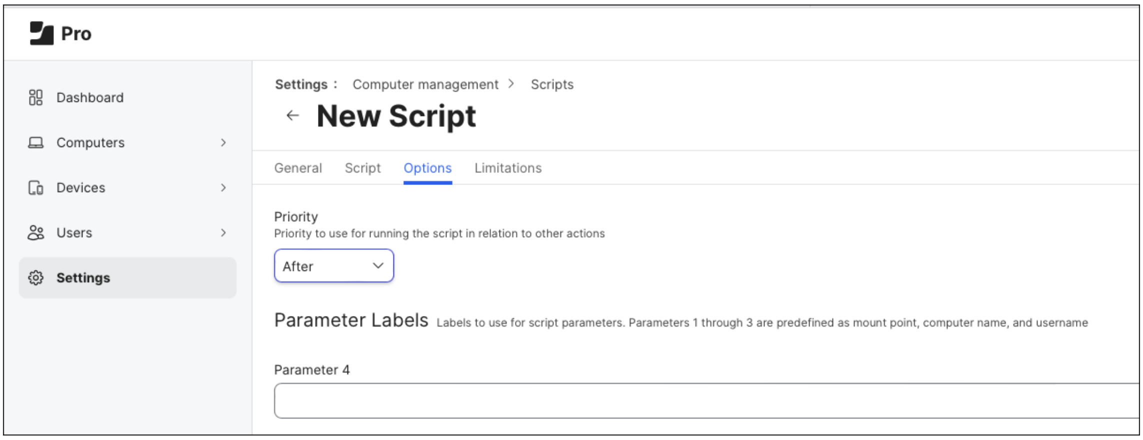
Notes
Notes to display about the script (e.g., who created it and when it was created)



Mode: Shell/Bash

Theme: Default

```
/opt/Citrix/VDA/bin/VdaEnrollmentTool -EnrollmentToken:copy-paste-your-token-generated-from-DaaS-console
```



Priority

Priority to use for running the script in relation to other actions

After

Parameter Labels Labels to use for script parameters. Parameters 1 through 3 are predefined as mount point, computer name, and username

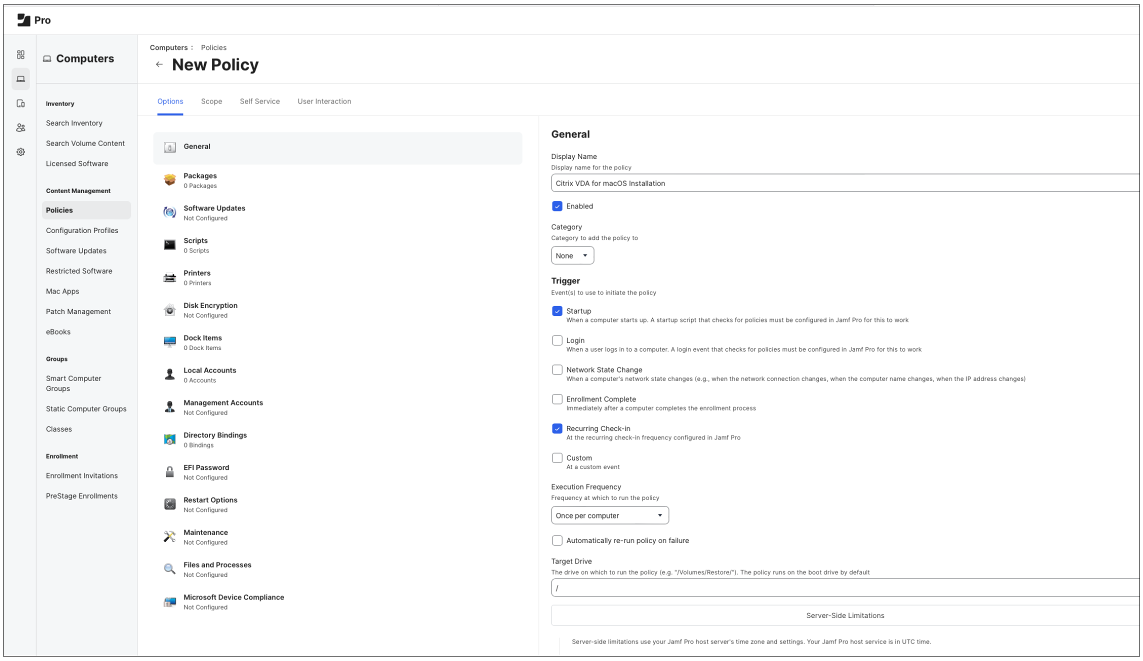
Parameter 4

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.



General

Display Name
Display name for the policy
Citrix VDA for macOS Installation

☑ Enabled

Category
Category to add the policy to
None

Trigger
Event(s) to use to initiate the policy

☑ Startup
When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work

□ Login
When a user logs in to a computer. A login event that checks for policies must be configured in Jamf Pro for this to work

□ Network State Change
When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

□ Enrollment Complete
Immediately after a computer completes the enrollment process

☑ Recurring Check-in
At the recurring check-in frequency configured in Jamf Pro

□ Custom
At a custom event

Execution Frequency
Frequency at which to run the policy
Once per computer

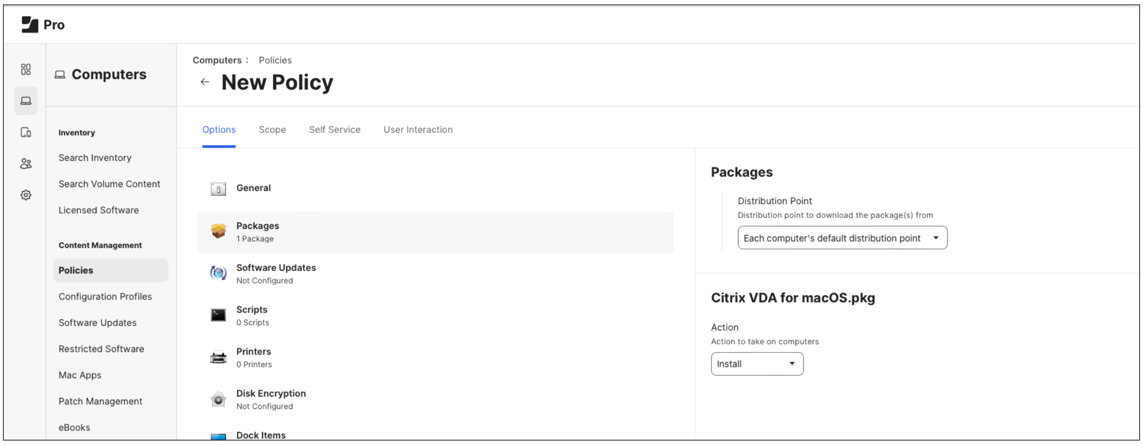
□ Automatically re-run policy on failure

Target Drive
The drive on which to run the policy (e.g. "/Volumes/Restore/"). The policy runs on the boot drive by default
/

Server-Side Limitations

Server-side limitations use your Jamf Pro host server's time zone and settings. Your Jamf Pro host service is in UTC time.

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



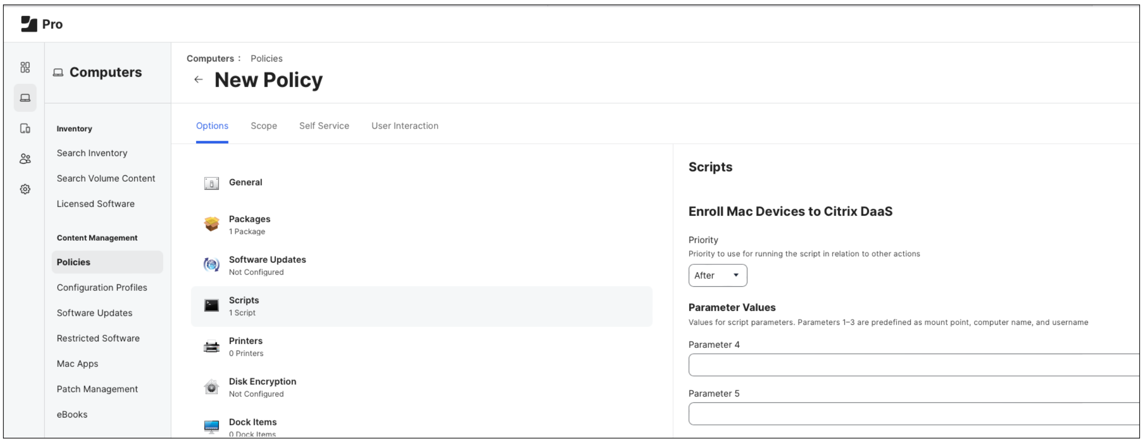
Packages

Distribution Point
Distribution point to download the package(s) from
Each computer's default distribution point

Citrix VDA for macOS.pkg

Action
Action to take on computers
Install

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



Scripts

Enroll Mac Devices to Citrix DaaS

Priority

Priority to use for running the script in relation to other actions

After

Parameter Values

Values for script parameters. Parameters 1–3 are predefined as mount point, computer name, and username

Parameter 4

Parameter 5

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.

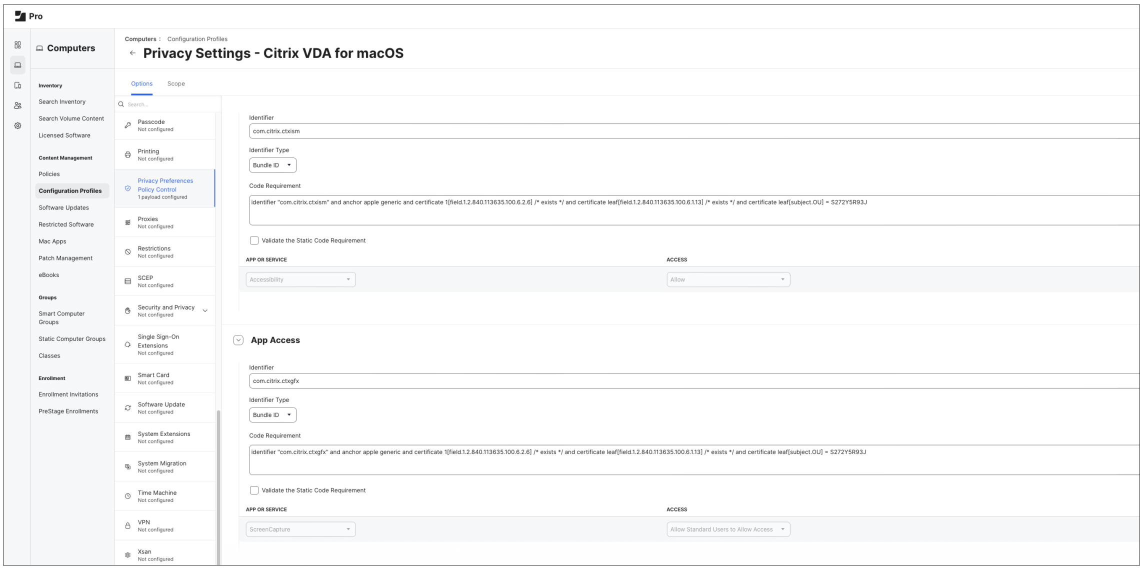
1. Login to the **Jamf Pro** console, and navigate to **Computers** -> **Configuration Profiles**.
2. Click **New** to add a new configuration profile.
3. Enter a display name for the new profile, e.g. **Privacy Settings - Citrix VDA for macOS**.
4. Select **Privacy Preferences Policy Control**.
5. Click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

8. Specify the scope for the configuration profile on your own needs.
9. **Save** the configuration profile.



Computers : Configuration Profiles

Privacy Settings - Citrix VDA for macOS

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

□ Validate the Static Code Requirement

APP OR SERVICE	ACCESS
Accessibility	Allow

App Access

Identifier: com.citrix.ctxgfx

Identifier Type: Bundle ID

Code Requirement: identifier "com.citrix.ctxgfx" 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

□ Validate the Static Code Requirement

APP OR SERVICE	ACCESS
ScreenCapture	Allow Standard Users to Allow Access

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.

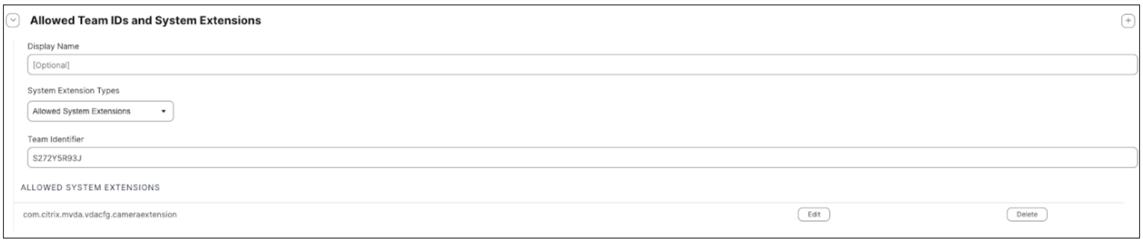
Section 3 (Optional) - Enable webcam redirection

This section describes the steps to enable the webcam redirection.

First, we need to create a configuration profile to allow the webcam system extensions from Citrix.

1. Login to the **Jamf Pro** console, and navigate to **Computers** -> **Configuration Profiles**.
2. Click **New** to add a new configuration profile or update an existing configuration profile.
3. Select **System Extensions**, and click Configure.

4. Select **Allowed System Extensions** for **System Extension Types**.
5. Enter **S272Y5R93J** for **Team Identifier**.
   Add the bundle ID com.citrix.mvda.vdacfg.cameraextension under **Allowed System Extensions**.
6. Specify the scope for the configuration profile on your own needs.
7. **Save** the configuration profile.
8. Once the configuration profile is configured, it should look like this.



Allowed Team IDs and System Extensions

Display Name: [Optional]

System Extension Types: Allowed System Extensions

Team Identifier: S272Y5R93J

ALLOWED SYSTEM EXTENSIONS

com.citrix.mvda.vdacfg.cameraextension

Then, we need to create a script to activate the webcam system extension.

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.
   - **Script**: Select Shell/Bash for the mode and enter the following as the content.

     ```
     "/Applications/VDA Configuration.app/Contents/MacOS/VDA
     Configuration"activate-camera-redirection
     ```

   - **Priority**: After
4. Add this script to a new or existing policy and configure the scope accordingly.

Section 4 (Optional) - Enable Single Sign-On while logging in to the session

This section describes the steps to enable Single Sign-On while logging in to the session.

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.
   - **Script**: Select Shell/Bash for the mode and enter the following as the content. Replace the option value according to your own needs. You can check the available options from the Single Sign-On guide.

     ```
     /usr/bin/osascript /opt/Citrix/VDA/bin/ctxsso.scpt -option 1
     -silent
     ```

    - **Priority**: After

4. Add this script to a new or existing policy and configure the scope accordingly.

Section 5 - Allow Screen Recording for Citrix VDA on managed devices

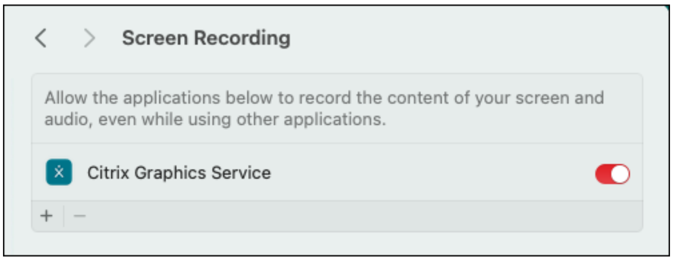
This section describes the steps to allow screen recording for Citrix VDA on the managed devices.

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.

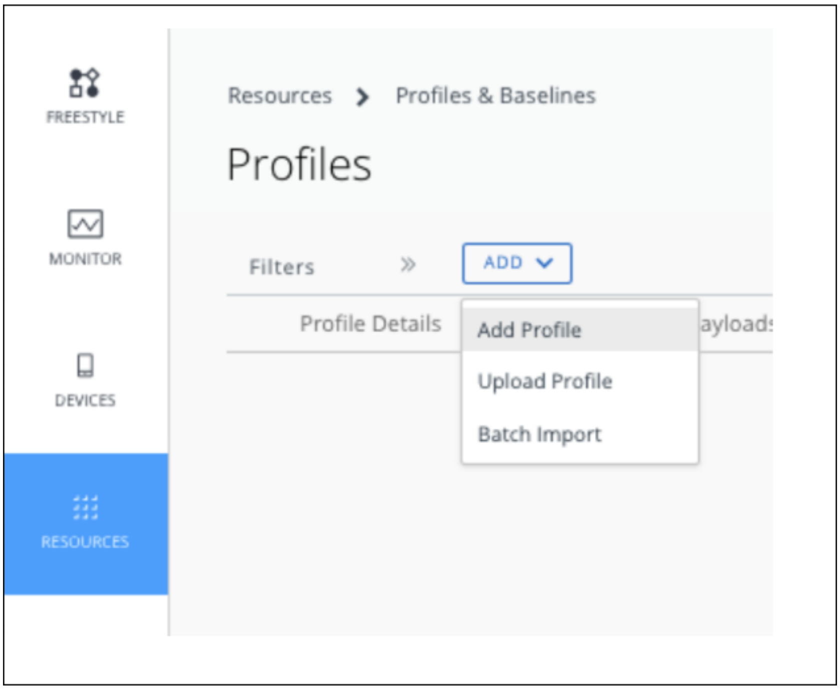


Allow the applications below to record the content of your screen and audio, even while using other applications.

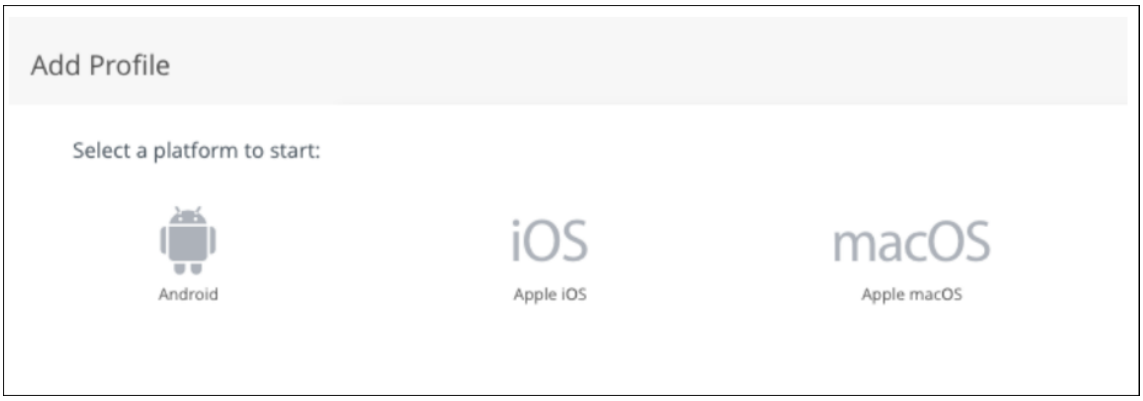
After the permission is properly configured, this target device will be ready for session launches from Citrix Workspace App.

Quick guide using Workspace ONE UEM

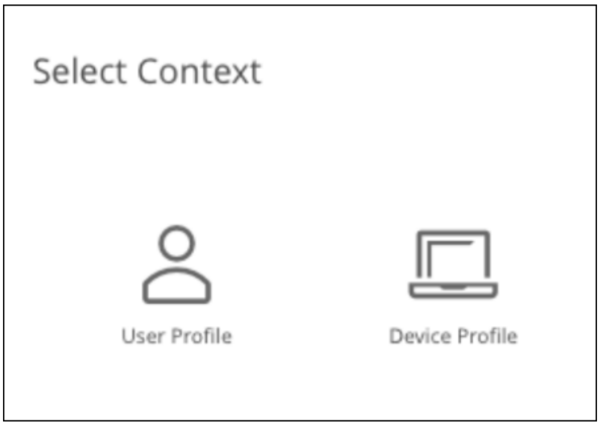
1. Log into the **Workspace UEM** console.
2. Go to **Resources** > **Profile & Baselines** > **Add** > **Add Profile**.



3. Select **macOS**.

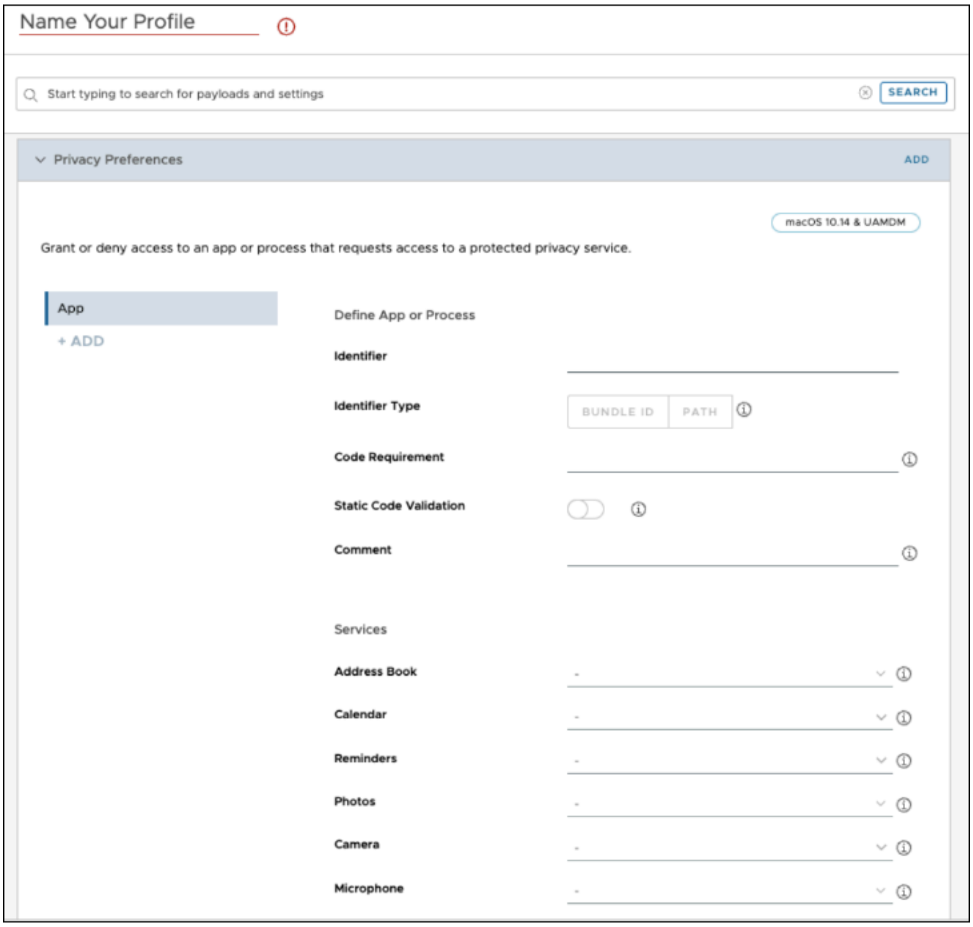


4. Select **Device Profile**.



5. Scroll down to **Privacy Preferences**.

6. Click the **Add Button**.



Grant or deny access to an app or process that requests access to a protected privacy service.

Define App or Process

Identifier:

Identifier Type: BUNDLE ID | PATH

Code Requirement:

Static Code Validation:

Comment:

Services

Address Book: -

Calendar: -

Reminders: -

Photos: -

Camera: -

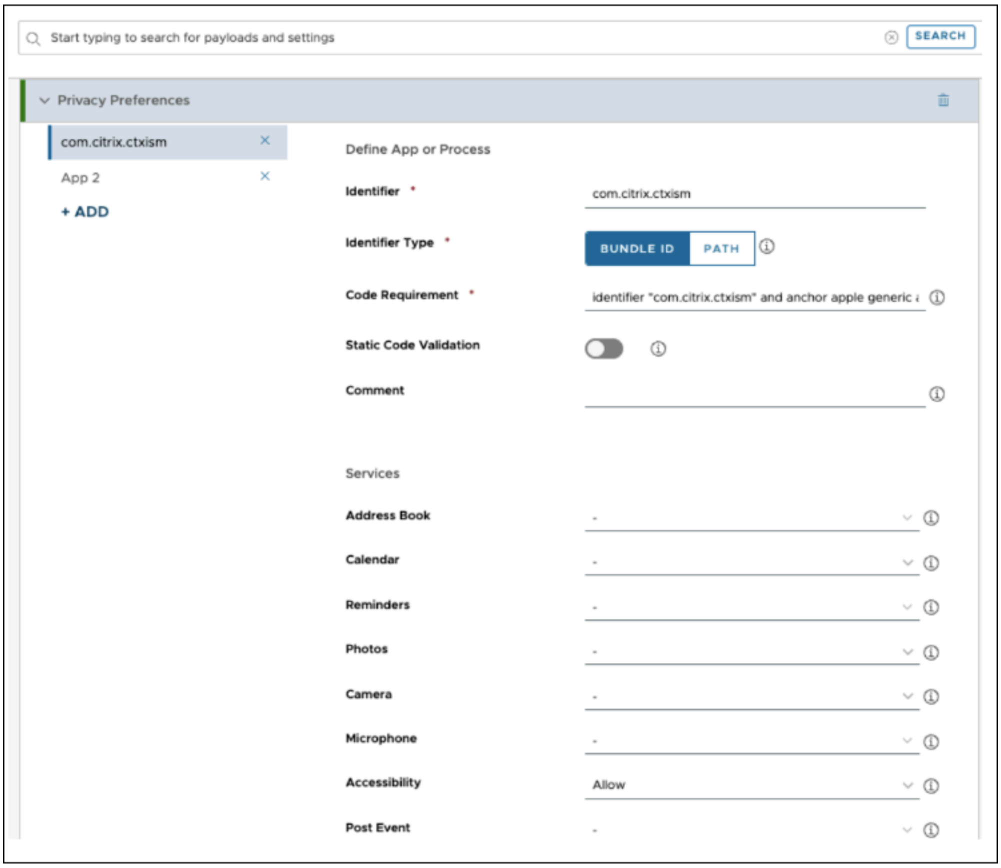
Microphone: -

7. Enter the Identifier: `com.citrix.ctxism`

8. Select **Bundle ID**.

9. Enter the 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

10. Scroll down and set the **Accessibility** to **Allow**.



Define App or Process

Identifier * com.citrix.ctxism

Identifier Type * BUNDLE ID

Code Requirement * identifier "com.citrix.ctxism" and anchor apple generic a

Static Code Validation

Comment

Services

Address Book -

Calendar -

Reminders -

Photos -

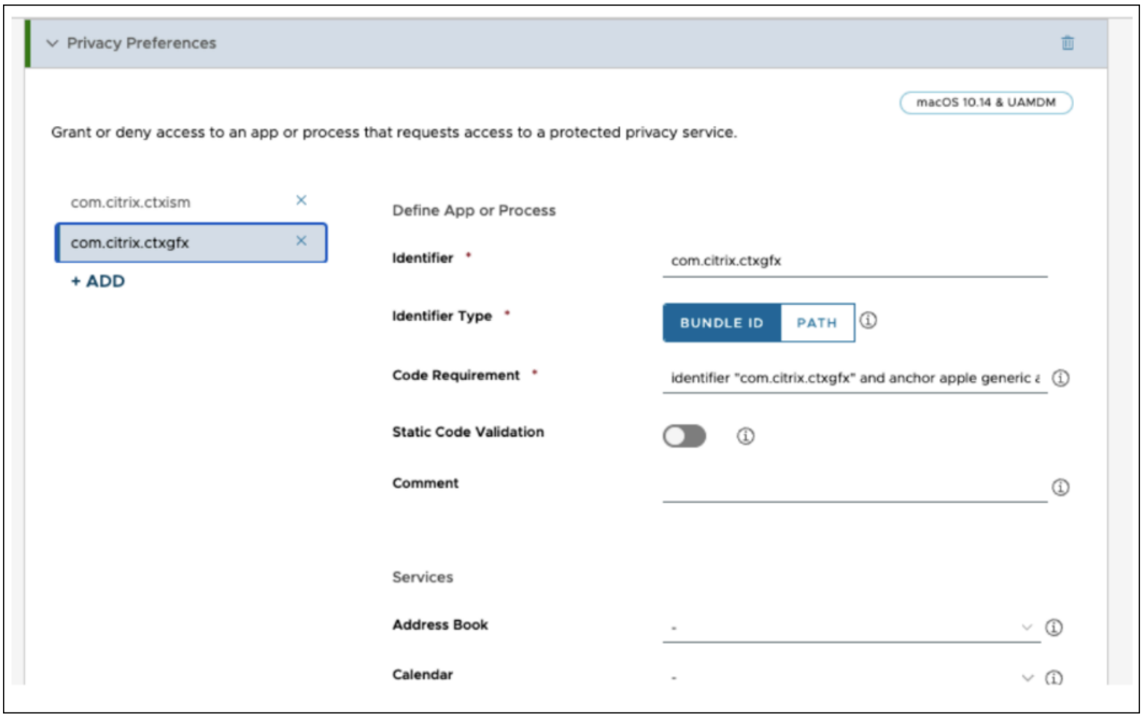
Camera -

Microphone -

Accessibility Allow

Post Event -

11. Click the **+ ADD** adding a second Privacy Preference.
12. Enter the Identifier: `com.citrix.ctxgfx`
13. Select **Bundle ID**.
14. Enter the Code requirement: identifier "com.citrix.ctxgfx" 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



Privacy Preferences

macOS 10.14 & UAMDM

Grant or deny access to an app or process that requests access to a protected privacy service.

com.citrix.ctxism ×

com.citrix.ctxgfx ×

+ ADD

Define App or Process

Identifier * com.citrix.ctxgfx

Identifier Type * BUNDLE ID | PATH

Code Requirement * identifier "com.citrix.ctxgfx" and anchor apple generic a

Static Code Validation

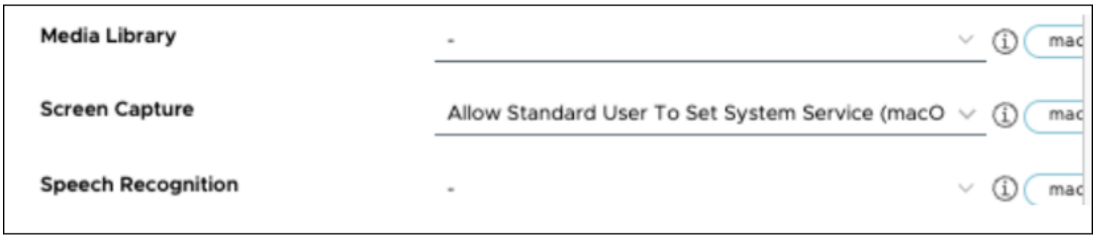
Comment

Services

Address Book -

Calendar -

15. Scroll down and set the Screen Capture to Allow standard User to set system service.



Media Library -

Screen Capture Allow Standard User To Set System Service (macO

Speech Recognition -

16. Press the **Next button** at the bottom right and assign the profile.

Upgrade existing VDAs

August 1, 2025

To upgrade or roll back the existing VDA to a new version, we recommend you to simply use the installer to complete the installation manually or push the new package again through MDM.

You **NEED NOT** uninstall the existing version and perform any enrollment or registration actions.

> **Note:**
>
> .NET runtime is required to upgrade to version 8.0 before VDA installation if the existing VDA version is 24.02 or 23.11.

Uninstall macOS VDA

August 1, 2025

Citrix VDA for macOS can also be removed from macOS completely using following command:

```
sudo /opt/Citrix/VDA/bin/ctxuninstall.sh
```

This operation can be performed either from macOS Terminal App or through your MDM software

Configuration

August 1, 2025

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

- Administration
- Authentication
- General Content Redirection
- Graphics
- Keyboard
- Session

Administration

August 1, 2025

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
- Tools and Utilities
- Session and Account Management

Log Collection

August 1, 2025

Overview

By default, 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
```

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

View or set a single `setlog` value:

```
setlog value <name> [<value>]
```

For example:

```
setlog value log_size 100
```

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

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

  ```
  setlog levels
  ```

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

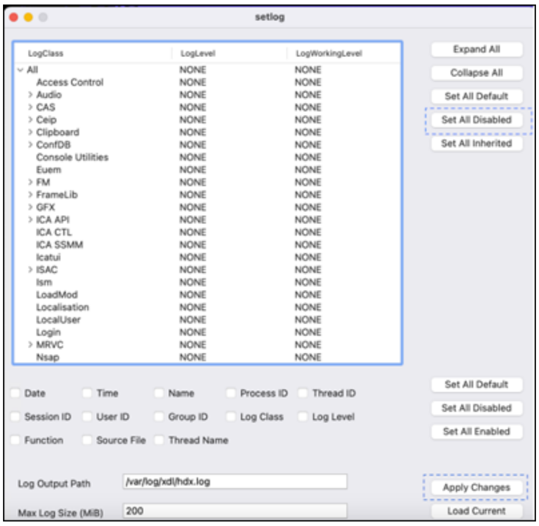
  ```
  setlog level <class> [<level>]
  ```

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.



LogClass	LogLevel	LogWorkingLevel
All	NONE	NONE
Access Control	NONE	NONE
Audio	NONE	NONE
CAS	NONE	NONE
Ceip	NONE	NONE
Clipboard	NONE	NONE
ConfDB	NONE	NONE
Console Utilities	NONE	NONE
Euem	NONE	NONE
FM	NONE	NONE
FrameLib	NONE	NONE
GFX	NONE	NONE
ICA API	NONE	NONE
ICA CTL	NONE	NONE
ICA SSMM	NONE	NONE
Icatui	NONE	NONE
ISAC	NONE	NONE
Ism	NONE	NONE
LoadMod	NONE	NONE
Localisation	NONE	NONE
LocalUser	NONE	NONE
Login	NONE	NONE
MRVC	NONE	NONE
Nsap	NONE	NONE

□ Date □ Time □ Name □ Process ID □ Thread ID
□ Session ID □ User ID □ Group ID □ Log Class □ Log Level
□ Function □ Source File □ Thread Name

Log Output Path: /var/log/xdl/hdx.log
Max Log Size (MiB): 200

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

```
setlog level all error
```

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

LEVEL = true

FUNC = false

FILE = false

TNAME = false
```

- View the current flags:

  ```
  setlog flags
  ```

- View or set a single log flag:

  ```
  setlog flag <flag> [<state>]
  ```

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

```
setlog default
```

> **Important:**
>
> The `ctxlogd` service is configured using the **/var/xdl/.ctxlog** file, which only the root users can create.
>
> **Recommended:**
>
> Avoid granting write permissions to `ctxlogd` configuration for other users. Doing so could allow unauthorized or malicious modifications, negatively impacting server performance and user experience.

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

Tools and Utilities

December 22, 2025

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

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

For additional options, run:

```
sudo xdlcollect.sh -h
```

This command displays more detailed information about usage.

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.

The hdxmonitorlite tool

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

hdxmonitorlite tool is more like a CLI (Command Line Interface) version of HDX™ Monitor that was available in the Windows platform.

With this tool, the administrators can dump important information related to DDC policies configured for the VDA, as well as VDA session information related to network, system configuration etc.

Below are some examples of how to use the tool:

Show help information:

```
sudo /opt/Citrix/VDA/bin/hdxmonitorlite.sh --help
```

Show specific module information:

```
sudo /opt/Citrix/VDA/bin/hdxmonitorlite.sh [module-name] dump
```

Show all modules:

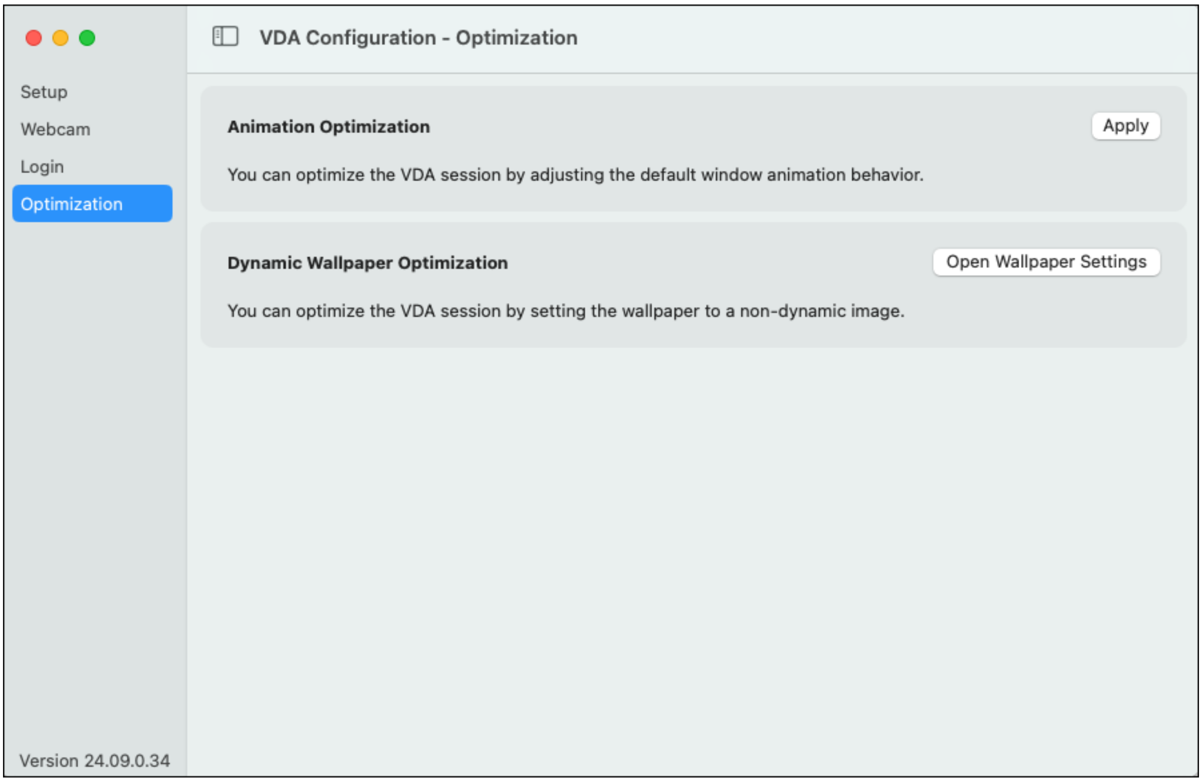
```
sudo /opt/Citrix/VDA/bin/hdxmonitorlite.sh list
```

Show all modules information:

```
sudo /opt/Citrix/VDA/bin/hdxmonitorlite.sh dump
```

ctxoptimizer

The **Citrix Optimizer script** (ctxoptimizer.scpt) enhances Citrix VDA for macOS performance by fine-tuning macOS UI settings to reduce the impact of performance-intensive graphical features, such as animations and dynamic wallpapers.



VDA Configuration - Optimization

Animation Optimization

You can optimize the VDA session by adjusting the default window animation behavior.

Dynamic Wallpaper Optimization

You can optimize the VDA session by setting the wallpaper to a non-dynamic image.

Version 24.09.0.34

The **Animation Optimization** will adjust the animation behavior of Launchpad and Window Minimizer to reduce its impact on Citrix VDA for macOS performance. You can restore the changes by running script:
osascript /opt/Citrix/VDA/bin/ctxoptimizer.scpt -animation disable

Admins can also automate these settings with a script

Examples:

- To enable animation optimizations:

```
osascript /opt/Citrix/VDA/bin/ctxoptimizer.scpt -animation enable
```

- To disable animation optimizations

```
osascript /opt/Citrix/VDA/bin/ctxoptimizer.scpt -animation disable
```

- To change the desktop background:

```
osascript /opt/Citrix/VDA/bin/ctxoptimizer.scpt -wallpaper "/path/to/
image.jpg"
```

- To enable all optimizations with a default background:

```
osascript /opt/Citrix/VDA/bin/ctxoptimizer.scpt -all enable
```

- To enable all optimizations with a specified background:

```
osascript /opt/Citrix/VDA/bin/ctxoptimizer.scpt -all enable -wallpaper
 "/path/to/image.jpg"
```

- To enable animation optimizations silently (ideal for automated environments):

```
osascript /opt/Citrix/VDA/bin/ctxoptimizer.scpt -animation enable -
silent
```

> **Note:**
>
> This script adjusts settings specific to the current user's profile. Do not to run this script with root privileges to avoid unintended system-wide changes.

XDPing

Description

The XDPing tool is a classic CLI tool which automates the process of checking for the causes of common configuration issues in Citrix VDA for macOS.

Depending on how the tool is run, the following checks and information can be displayed:

- The connectivity between the VDA machine and the DDC:
  `sudo -d https://www.ddc.com/`
- Information extracted from the enroll token:
  `sudo xdping -e ~/Citrix VDA for macOS/enroll-token.txt`
- Information and status of the VDA machine:
  `sudo xdping`

Prerequisites

1. Python3 comes pre-installed with macOS.
2. Xcode Command Line tools are installed

How to Use

After installing the VDA, you can run XDPing as follows:

1. Open the **Terminal application**.
2. Execute the command `sudo xdping -h` or `sudo /usr/local/bin/xdping -h` to view the manual page.

If this is the first time you run the XDPing command, it will first create a virtual Python environment in the `/opt/bin/python3/` directory. Subsequently, XDPing will install the XDPing Python package along with its dependencies from the network.

VDA Configuration

Description

VDA Configuration is an application designed to configure your VDA.

After installing VDA, you can find VDA Configuration in the Launchpad of your VDA machine.

You can open it from Launchpad or by running the command `vdaconfig` in the Terminal.

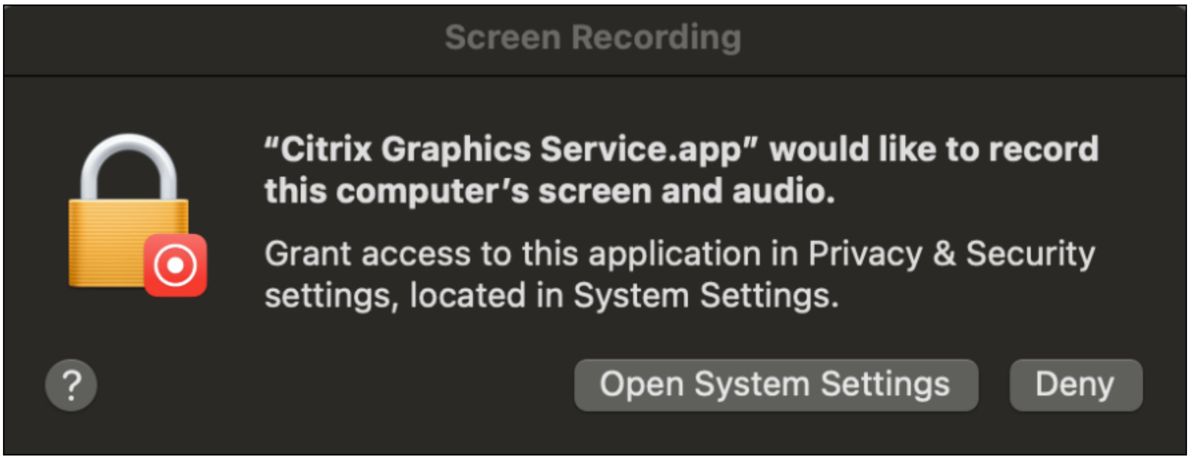
It offers four main types of configuration:

1. Basic Setup Before Using VDA
2. Enable Webcam Redirection
3. Select a Different Login Method
4. Optimize VDA Performance

This document focuses primarily on the basic setup before using VDA. For information on other configurations, please refer to the relevant documentation.

Grant Application Permissions

Before using VDA, you need to grant screen recording and accessibility privileges to it.
For screen recording privilege, a window will automatically appear to request the privilege after installation.



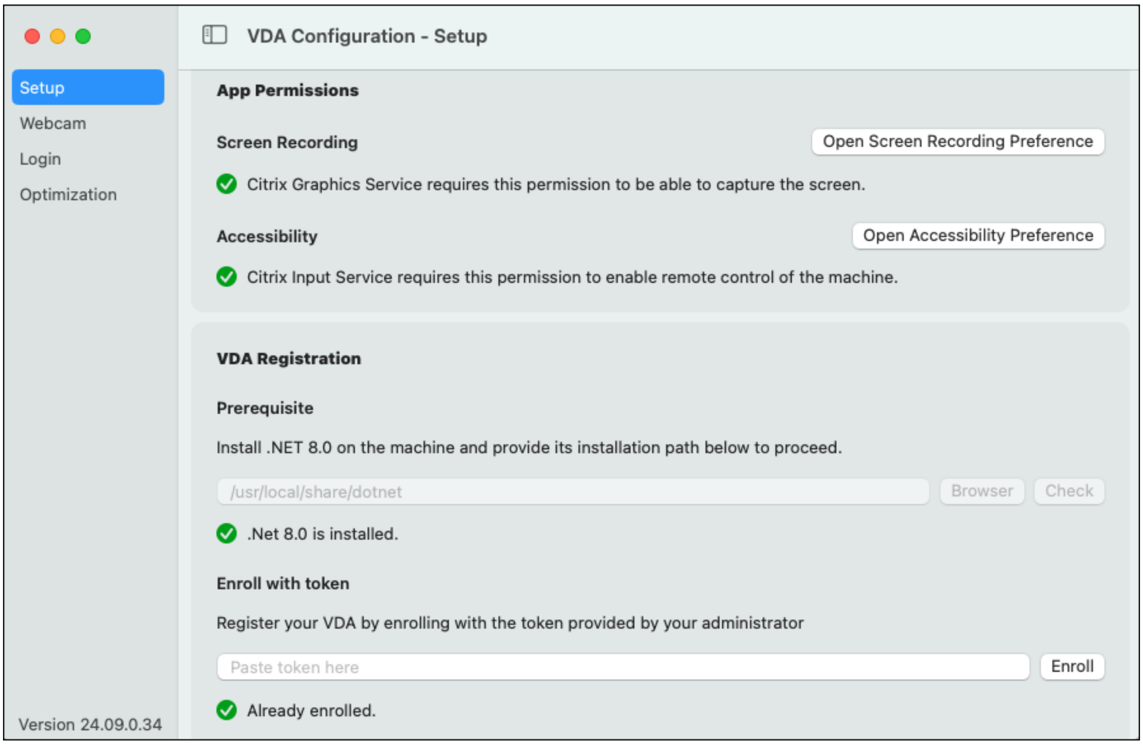
Screen Recording

"Citrix Graphics Service.app" would like to record this computer's screen and audio.

Grant access to this application in Privacy & Security settings, located in System Settings.

You can also grant both privileges manually in VDA Configuration as follows

1. Click the 'Open Screen Recording Preferences'and 'Open Accessibility Preferences'buttons located on the right side of the app permissions panel.



App Permissions

Screen Recording Open Screen Recording Preference

✓ Citrix Graphics Service requires this permission to be able to capture the screen.

Accessibility Open Accessibility Preference

✓ Citrix Input Service requires this permission to enable remote control of the machine.

VDA Registration

Prerequisite

Install .NET 8.0 on the machine and provide its installation path below to proceed.

/usr/local/share/dotnet Browser Check

✓ .Net 8.0 is installed.

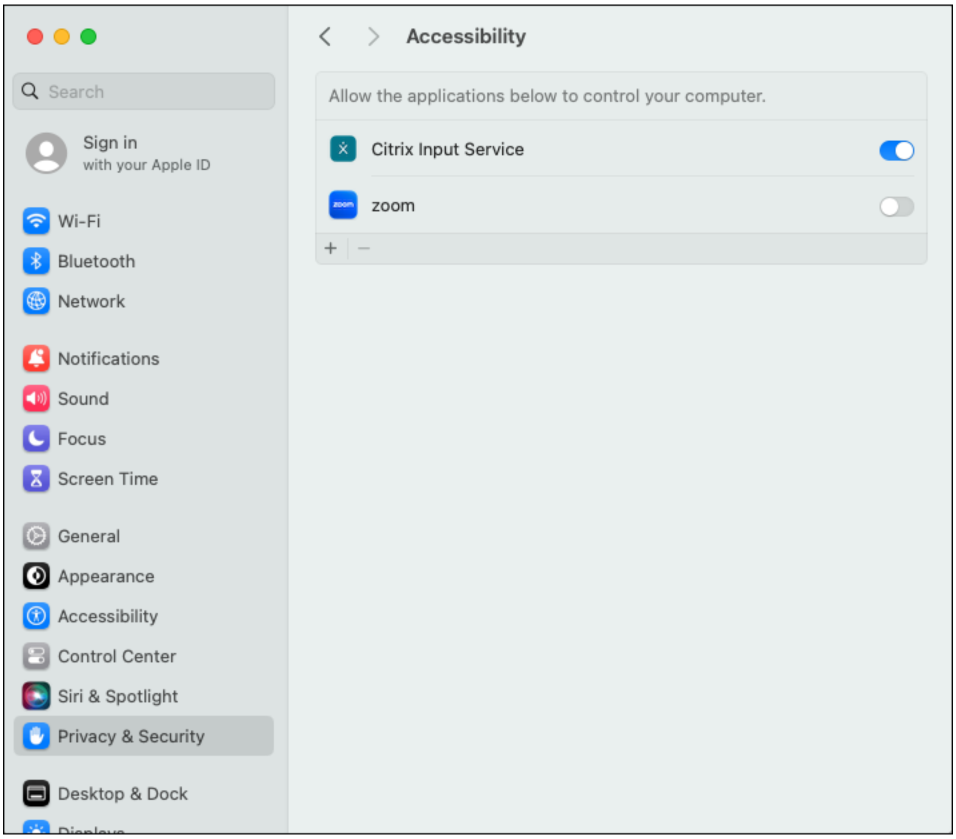
Enroll with token

Register your VDA by enrolling with the token provided by your administrator

Paste token here Enroll

✓ Already enrolled.

2. After clicking the buttons, the System Settings window should open. Approve the requests within this window.

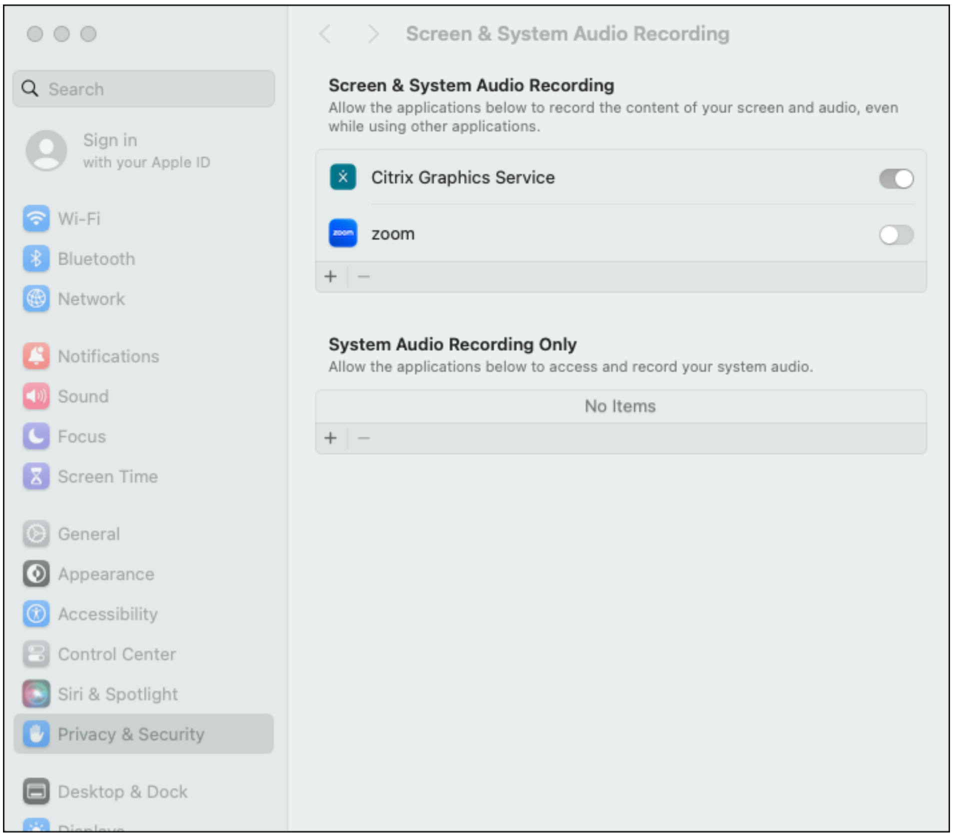


Accessibility

Allow the applications below to control your computer.

Citrix Input Service ●

zoom ○



Screen & System Audio Recording

Screen & System Audio Recording

Allow the applications below to record the content of your screen and audio, even while using other applications.

Citrix Graphics Service ●

zoom ○

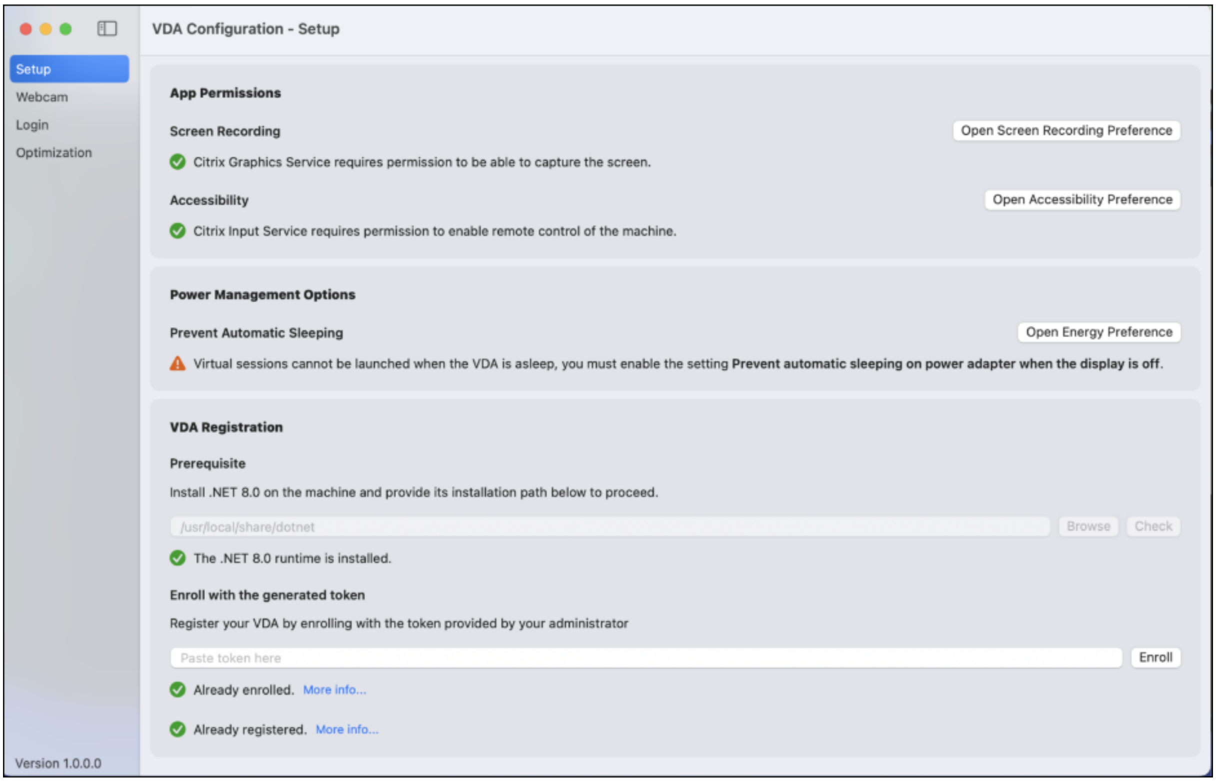
System Audio Recording Only

Allow the applications below to access and record your system audio.

No Items

If you do not see the corresponding request, click the + button in the System Settings window and manually select the application located in the /Library/PrivilegedHelperTools/Citrix directory.

Power Management Options button In release 2511, we have added a **Power Management Options** button to allow users to configure sleep prevention settings, preventing VDA devices from entering automatic sleep mode which would make session startup impossible.



VDA Configuration - Setup

App Permissions

Screen Recording

✓ Citrix Graphics Service requires permission to be able to capture the screen.

Accessibility

✓ Citrix Input Service requires permission to enable remote control of the machine.

Power Management Options

Prevent Automatic Sleeping

⚠ Virtual sessions cannot be launched when the VDA is asleep, you must enable the setting **Prevent automatic sleeping on power adapter when the display is off.**

VDA Registration

Prerequisite

Install .NET 8.0 on the machine and provide its installation path below to proceed.

/usr/local/share/dotnet

✓ The .NET 8.0 runtime is installed.

Enroll with the generated token

Register your VDA by enrolling with the token provided by your administrator

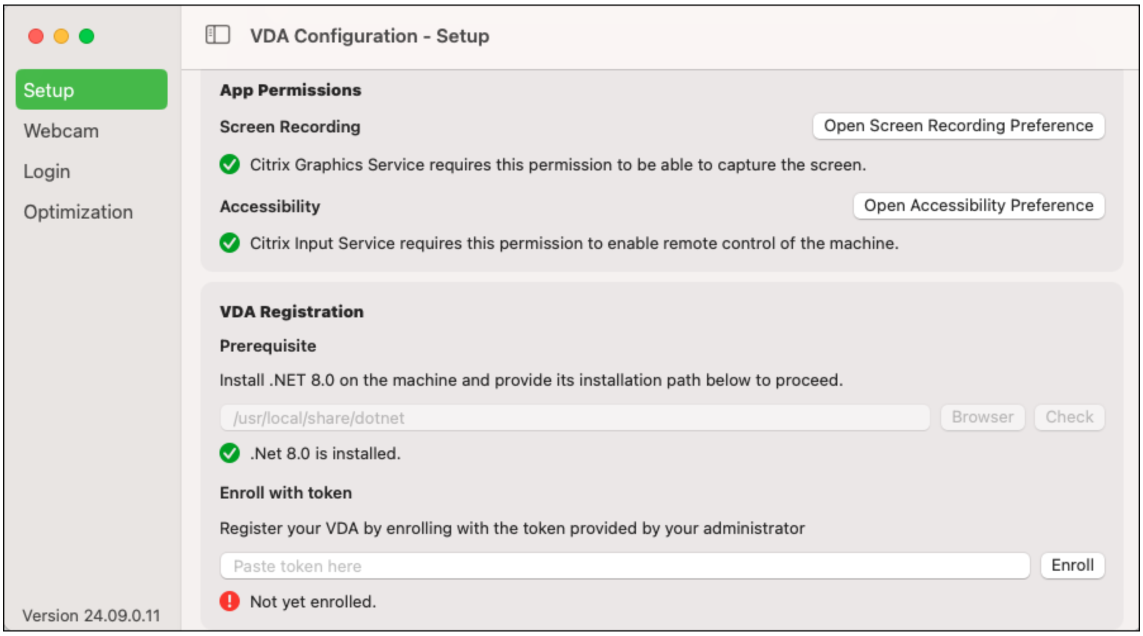
Paste token here

✓ Already enrolled.

✓ Already registered.

Install .NET 8.0 Runtime

1. Download and install .NET Runtime 8.0.
2. Verify the installation by checking its status in VDA Configuration.


Setup
Webcam
Login
Optimization
VDA Configuration - Setup
Open Screen Recording Preference
Open Accessibility Preference
Browser
Check
Paste token here
Enroll

Version 24.09.0.11

App Permissions

Screen Recording

✓ Citrix Graphics Service requires this permission to be able to capture the screen.

Accessibility

✓ Citrix Input Service requires this permission to enable remote control of the machine.

VDA Registration

Prerequisite

Install .NET 8.0 on the machine and provide its installation path below to proceed.

/usr/local/share/dotnet

✓ .Net 8.0 is installed.

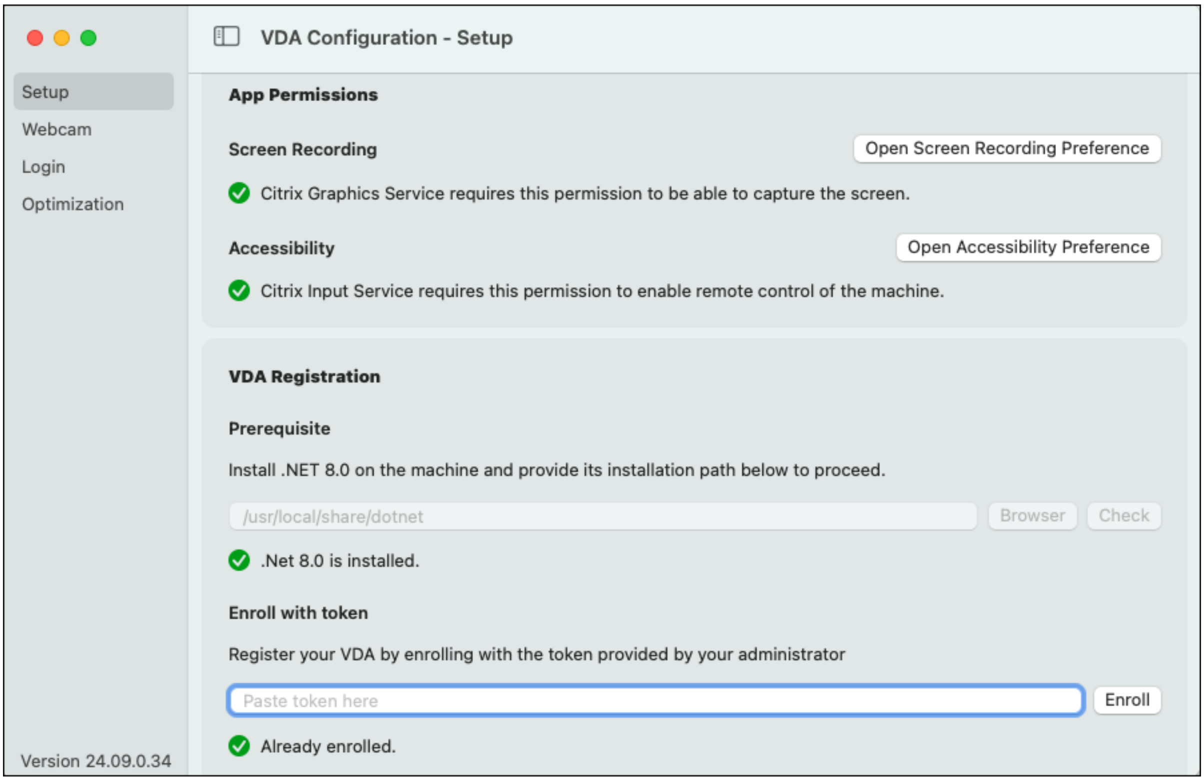
Enroll with token

Register your VDA by enrolling with the token provided by your administrator

! Not yet enrolled.

Enroll with token If you have not yet enrolled, enter your enrollment token in VDA Configuration and click the ‘Enroll’button. This process may take a few moments.

If the enrollment is successful, you will see the following screen. You can now use your VDA.


Setup
Webcam
Login
Optimization
VDA Configuration - Setup
Open Screen Recording Preference
Open Accessibility Preference
Browser
Check
Paste token here
Enroll

Version 24.09.0.34

App Permissions

Screen Recording

✓ Citrix Graphics Service requires this permission to be able to capture the screen.

Accessibility

✓ Citrix Input Service requires this permission to enable remote control of the machine.

VDA Registration

Prerequisite

Install .NET 8.0 on the machine and provide its installation path below to proceed.

/usr/local/share/dotnet

✓ .Net 8.0 is installed.

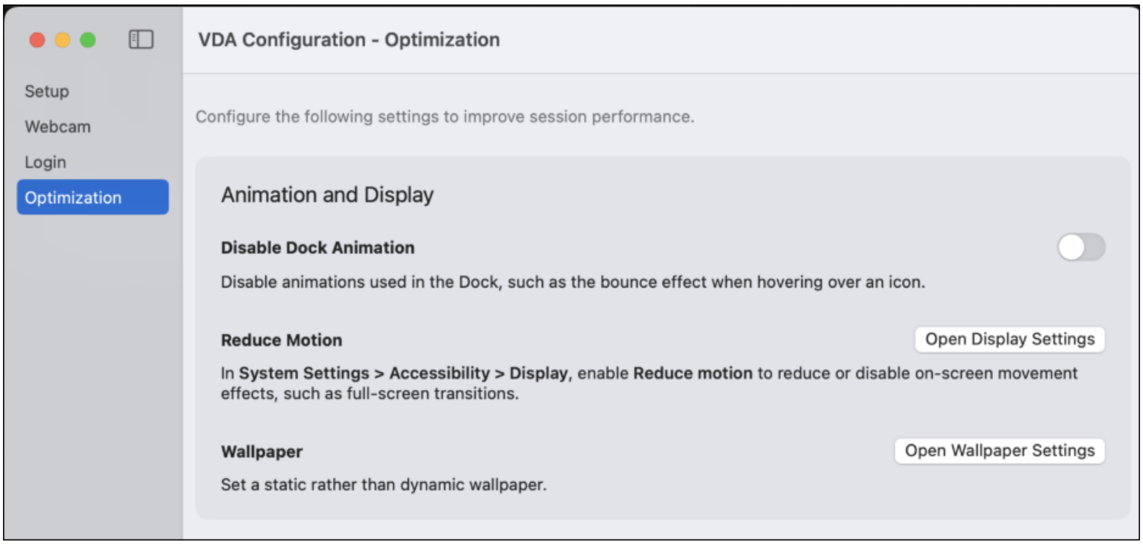
Enroll with token

Register your VDA by enrolling with the token provided by your administrator

✓ Already enrolled.

Optimization Page In release 2511, we have:

- modified the overall page styling.
- added a reduce motion toggle button to improve session performance.



VDA Configuration - Optimization

Configure the following settings to improve session performance.

Animation and Display

Disable Dock Animation

Disable animations used in the Dock, such as the bounce effect when hovering over an icon.

Reduce Motion Open Display Settings

In **System Settings > Accessibility > Display**, enable **Reduce motion** to reduce or disable on-screen movement effects, such as full-screen transitions.

Wallpaper Open Wallpaper Settings

Set a static rather than dynamic wallpaper.

The ctxaudiosession tool

In this 2503 release, we introduced another powerful tool to help administrators diagnostic Audio virtual channel issues, please refer to Audio Diagnostic Tool.

Session and Account Management

December 22, 2025

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

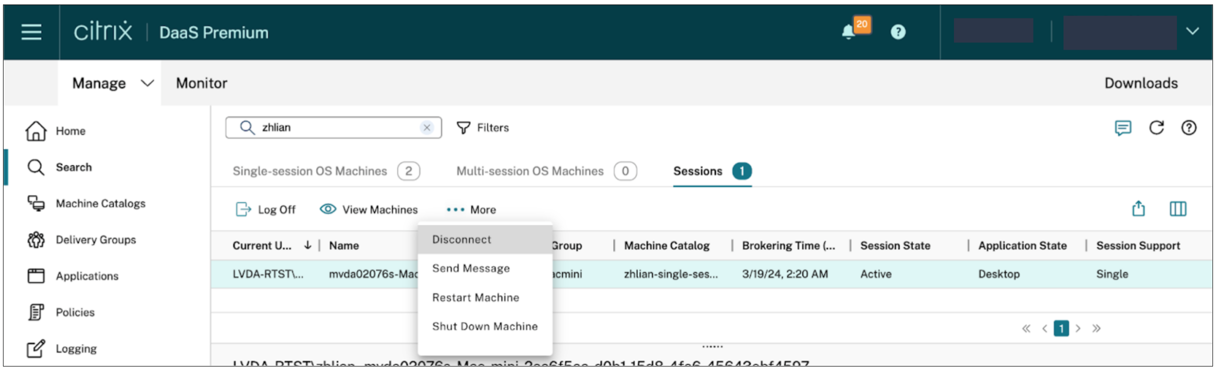
Citrix VDA for macOS does not change or manage user accounts in macOS. End users can log out or switch user accounts inside an active HDX session, which follows default macOS behaviors.

For HDX session, two different operations can be performed:

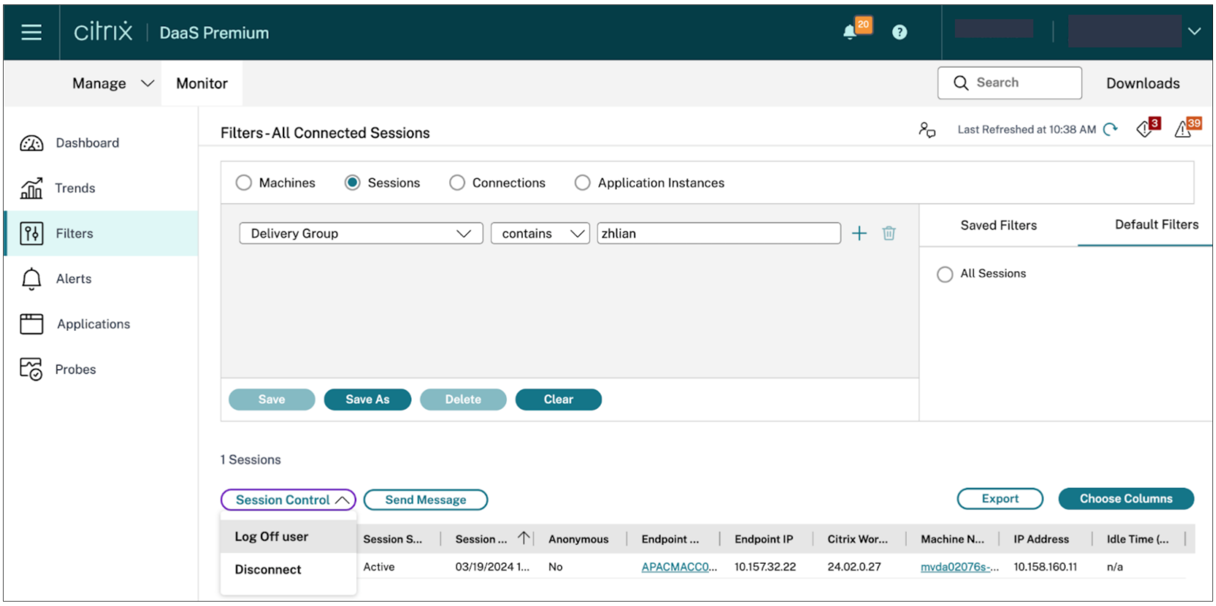
- **Disconnect**: ends the current active connection towards VDA. However, the HDX session for Citrix VDA for macOS is still alive and hence, the session is blocked and can be reused only by the last user connected.
- **Logoff**: terminates the current HDX session and the VDA is able to establish a new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



Current U...	Name	Group	Machine Catalog	Brokering Time (...	Session State	Application State	Session Support
LVDA-RTST\...	mvda02076s-Mac	acmini	zhlian-single-ses...	3/19/24, 2:20 AM	Active	Desktop	Single



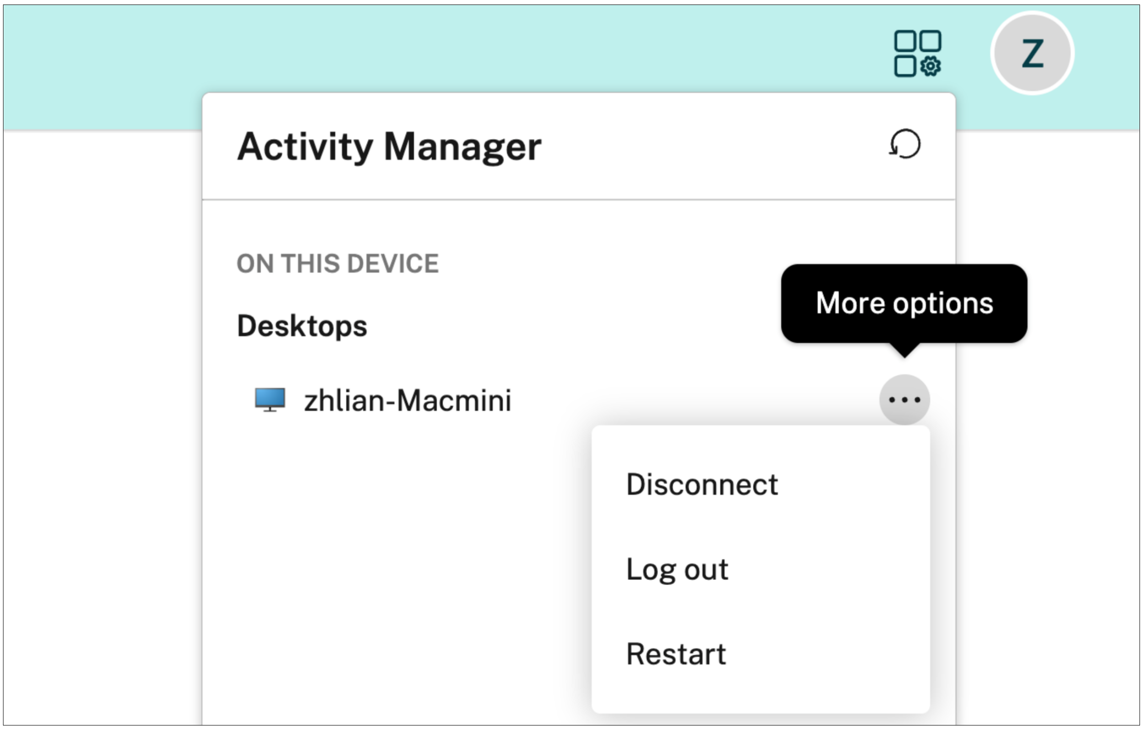
Delivery Group | contains | zhlian

1 Sessions

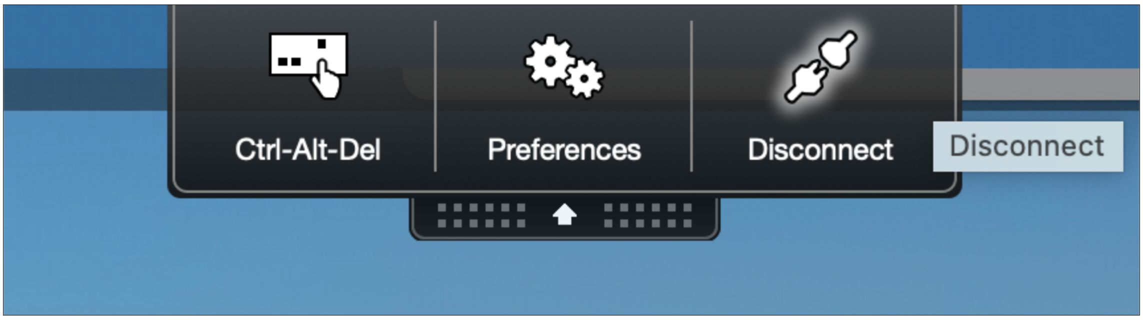
Session S...	Session ...	Anonymous	Endpoint ...	Endpoint IP	Citrix Wor...	Machine N...	IP Address	Idle Time (...
Active	03/19/2024 1...	No	APACMACCO...	10.157.32.22	24.02.0.27	mvda02076s-...	10.158.160.11	n/a

For **end users**, session can be disconnected or logged off in various ways as shown in the following screenshots.:

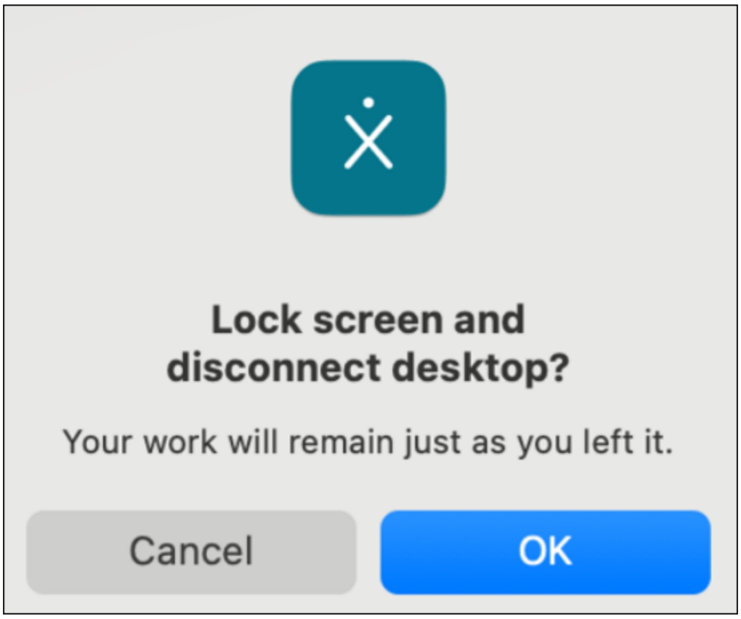
- From the **Activity Manager** at the top right of the **Workspace app** page,



- Pull down the **Workspace app** toolbar, click **Ctrl-Alt-Del** to log-off the HDX session
- Click **Disconnect** to disconnect the session.

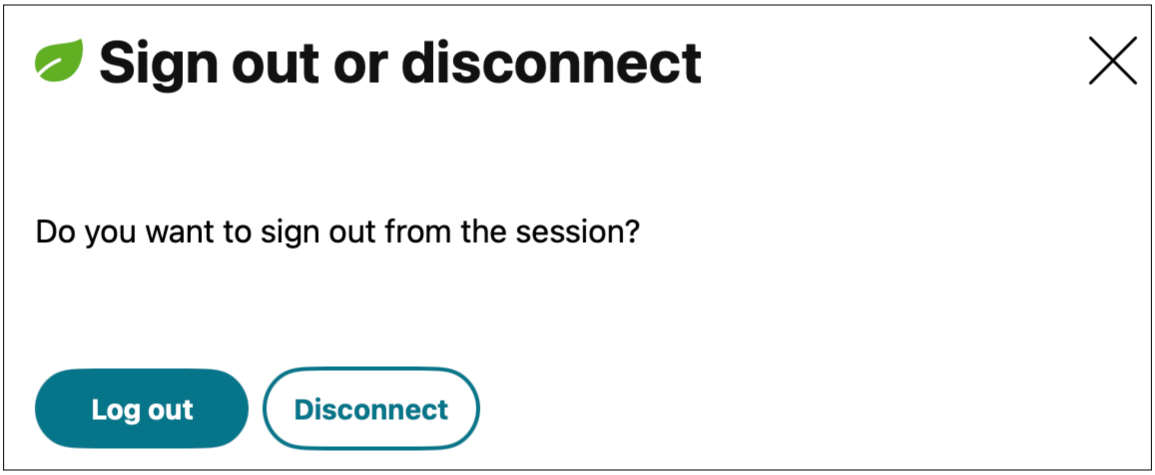


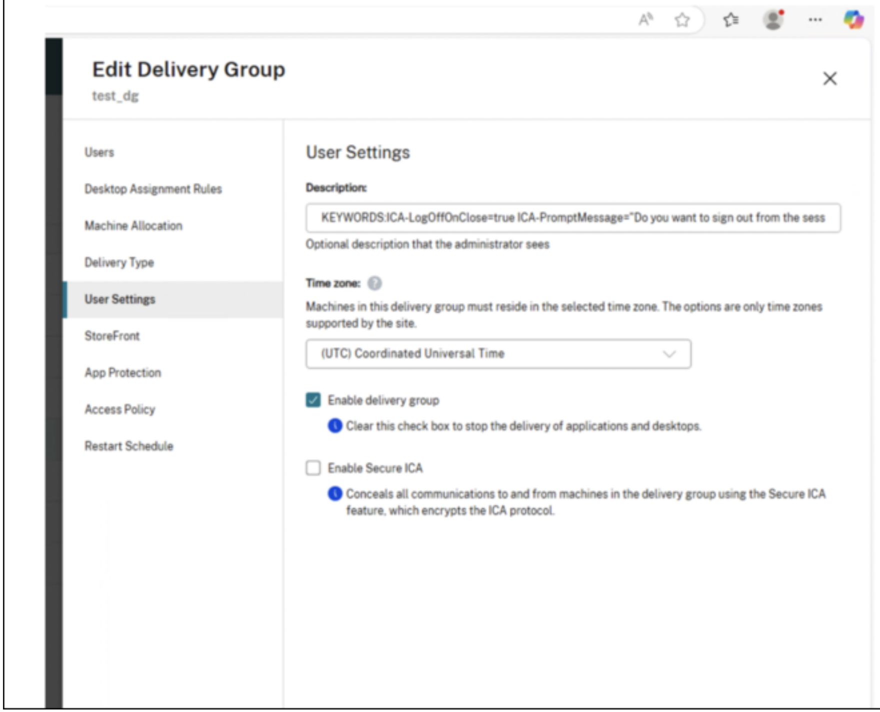
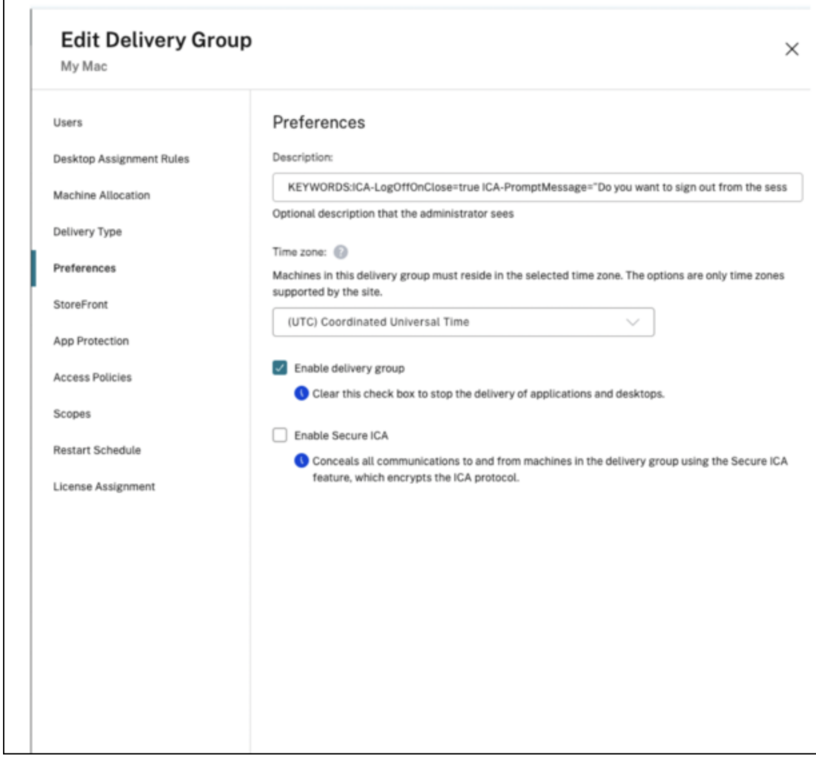
When clicked, you will see below message box reminder.



Lock screen and disconnect desktop?

Your work will remain just as you left it.

> **Note:**
>
> Starting from Citrix Workspace™ app 2505 release, the "Ctrl-Alt-Del"button to sign off session is replaced by options when
> user click "Disconnect"button:
>
> 
>
> Sign out or disconnect
>
> Do you want to sign out from the session?
>
>
>
> To enable this feature, edit the related Delivery Group option by adding the string in related tab.
>
> - for CVAD it is in the "User Settings"
> - for DaaS, it's now in "Preference"
>
> KEYWORDS:`ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to sign out from the session?"ICA-Title="Sign out or disconnect"ICA-Icon=true`

> The above strings are configurable if you want to customize them for end users.
>
> CVAD: Edit Delivery Group --> User Settings
>
> 
>
>
> User Settings
>
> Description:
>
> KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to sign out from the sess
>
> Optional description that the administrator sees
>
> Time zone:
>
> Machines in this delivery group must reside in the selected time zone. The options are only time zones supported by the site.
>
> (UTC) Coordinated Universal Time
>
> ☑ Enable delivery group
>
> Clear this check box to stop the delivery of applications and desktops.
>
> □ Enable Secure ICA
>
> Conceals all communications to and from machines in the delivery group using the Secure ICA feature, which encrypts the ICA protocol.
>
> DaaS: Edit Delivery Group --> Preferences
>
> 
>
>
> Preferences
>
> Description:
>
> KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to sign out from the sess
>
> Optional description that the administrator sees
>
> Time zone:
>
> Machines in this delivery group must reside in the selected time zone. The options are only time zones supported by the site.
>
> (UTC) Coordinated Universal Time
>
> ☑ Enable delivery group
>
> Clear this check box to stop the delivery of applications and desktops.
>
> □ Enable Secure ICA
>
> Conceals all communications to and from machines in the delivery group using the Secure ICA feature, which encrypts the ICA protocol.

Alternatively, an administrator or an end user can run the command `sudo /opt/Citrix/VDA/`

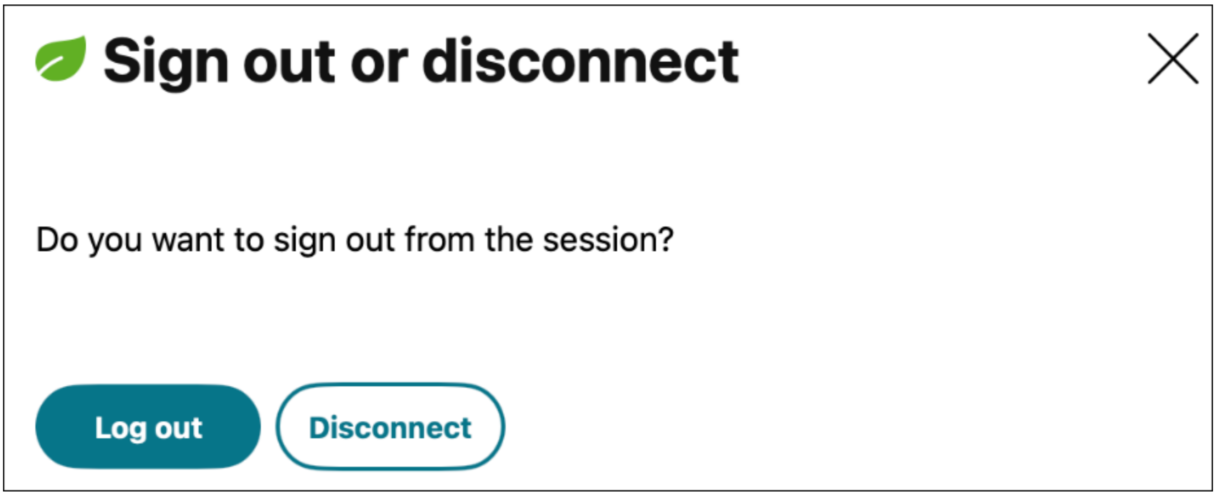
`bin/ctxlogoff` to logoff a session directly from the VDA machine.

Administrators should guide their end users to logoff the session each time after usage if their organization wants to maximize the usage of the 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.

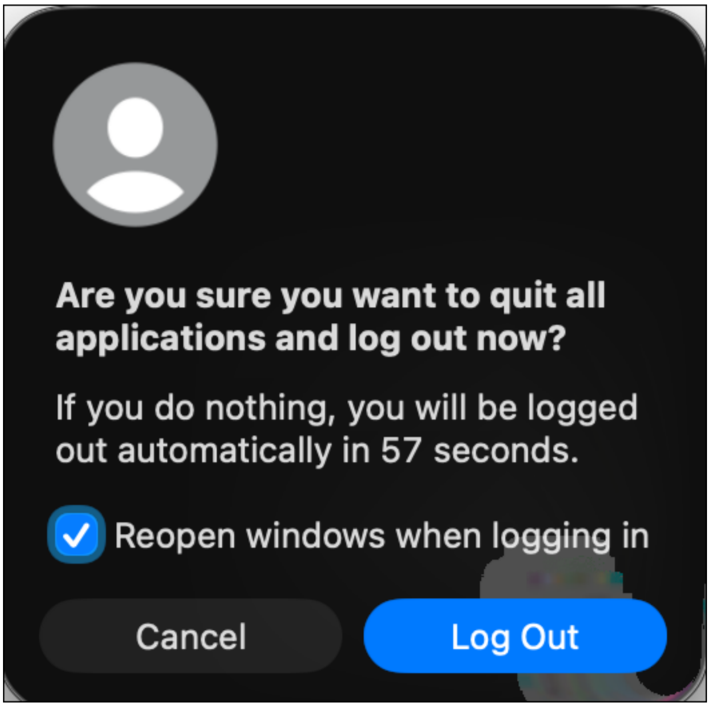
Session Logoff and macOS User Logout Alignment

Citrix VDA for macOS now supports synchronization between HDX session logoff and macOS user logout. When users select Logout from the Workspace app toolbar (see this page for instructions on enabling the Logout option), a macOS logout confirmation dialog is displayed.



Sign out or disconnect

Do you want to sign out from the session?



Are you sure you want to quit all applications and log out now?

If you do nothing, you will be logged out automatically in 57 seconds.

☑ Reopen windows when logging in

Once the macOS logout procedure complete, the HDX session will also be terminated automatically. Alternatively, users can log off the HDX session by directly logging out of the macOS user account within the VDA.

> **Note:**
>
> This feature is disabled by default. To enable it, set the following registry key to 1: `HKLM\System\CurrentControlSet\Control\Citrix\AccessControl\Logoff\LogoffAlignmentOption`
>
> This feature is currently fully supported only in the Citrix Workspace™ app for Mac. For Windows and Linux versions of the Citrix Workspace™ app, HDX session logoff occurs when the macOS user logs out manually within the VDA; however, logging off the HDX session from toolbar may not always trigger a successful macOS user logout.

Authentication

August 1, 2025

To use Citrix VDA for macOS, the administrator can either configure both authentication for Workspace/StoreFront according to Identity Access Management and also macOS user account authentication separately or if the authentication workflow meet the provided capabilities of SSO (Single Sign-On) feature shipped in this release, it can be used.

For more information, see Configure SSO authentication.

SSO Authentication

August 1, 2025

Citrix VDA for macOS now support SSO (Single Sign-on) experience you normally found in Windows and Linux VDA; by authenticated and launching the Citrix VDA for macOS session in Workspace or StoreFront™, you will be taken directly to the macOS user account without the need to input your credential again.

Supported SSO credential types

The SSO experience is provided in conjunction with Citrix control plane DaaS/CVAD components, currently we only support following workflow & credential types.

Workspace/StoreFront authentication type

Citrix Workspace app users should log into their Storefront/Workspace using a username & password pair (or the pair can be retrieved from a device such as Touch ID); Currently, we do not support other types of credentials,e.g., FAS, smart card.

Authentication Method

Your macOS account can be a local account or an Active Directory (AD) account:

- **macOS local account**

  A local account is created and managed directly on the macOS device. If you are using a local account on macOS, SSO will authenticate you using the macOS local account database. Please ensure the local account username and password is configured the same as SF/SF Cloud (username is the short ID without domain prefix)

- **Active Directory (AD) authentication**

  An AD account is managed by Active Directory, a directory service developed by Microsoft for Windows domain networks. If you are using an Active Directory (AD) account, SSO will facilitate authentication through the Active Directory to which the Citrix VDA for macOS device is connected.

> **Note:**
>
> If the same account name exists in both the local and AD account databases, we only support authentication with the local account database.
>
> SSO will not work if you check the **Allow users not in Active Directory to use this delivery group** checkbox while creainge the delivery group.

Limitation

When the Mac device is connected by wifi, it must be connected to a shared network connection, rather than a per-user wifi configuration.

Compatibility

When the Citrix VDA for macOS SSO feature is enabled, your macOS system's default login UI will be replaced with a Citrix VDA for macOS-customized version. We do not support the cases in which the system login process has already been customized by other software including Jamf PRO/Connect. (Refer to the troubleshooting section for instructions on how to determine if your system login process has been customized.)

How to enable SSO

The configuration varies depending on the type of account.

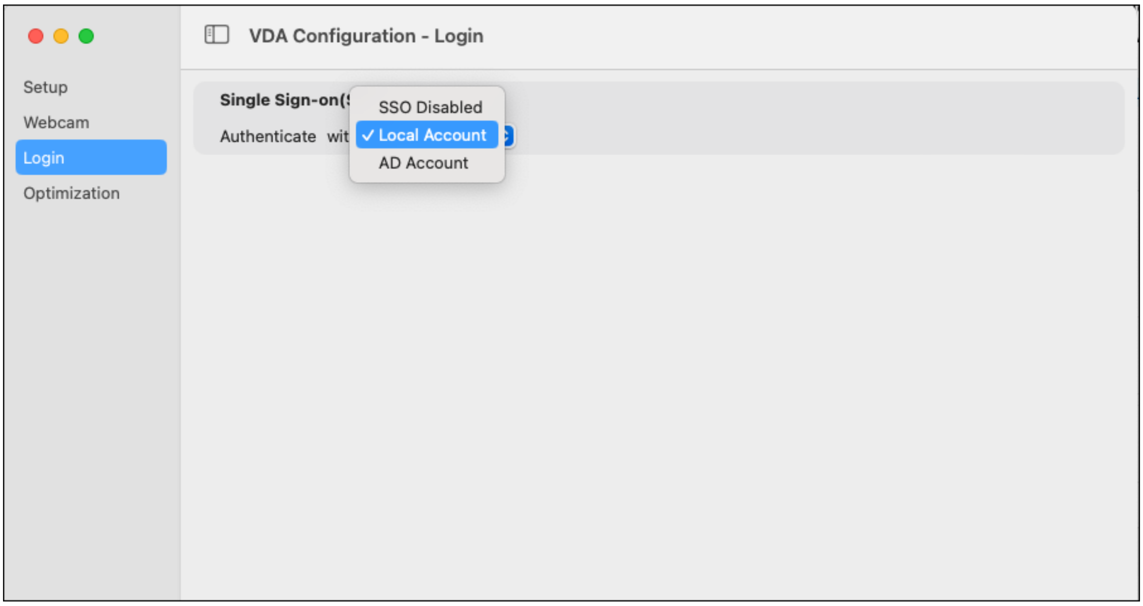
MacOS local authentication Steps

1. Create a **local user account**.

   In macOS System Settings, create a local user account or update an existing one to have the same username and password as the account you use to log into the storefront / workspace. Please refer to Apple's documentation for creating a new local user account or changing an existing user account.

2. **Enable SSO**.

   Enable with VDA Configuration App.


VDA Configuration - Login

Single Sign-on(

Authenticate wit ✓ Local Account

Or run below apple script to enable SSO.

```
sudo osascript /opt/Citrix/VDA/bin/ctxsso.scpt -option 1
```

```
sudo osascript /opt/Citrix/VDA/bin/ctxsso.scpt -option 1 -silent
```

> **Note:**
>
> This mode is particularly useful for scripting and automation purposes

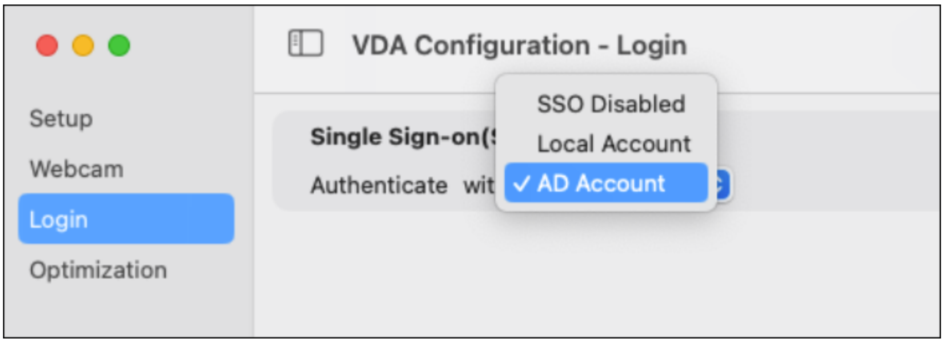
> **Note:**
>
> For local authentication, you need to synchronize local credentials with storefront / workspace credentials manually if password will be changed due to security update needs.

Active Directory (AD) authentication

You must bind your Citrix VDA for macOS machine to the domain where your storefront or workspace account resides.
Steps:

1. Bind your Citrix VDA for macOS device to the domain with macOS's built-in tool, Directory Utility (You can ignore this step if your device has already been connected to the domain). Refer to Apple's documentation Configure domain access in Directory Utility on Mac.

2. **Enable SSO**.
   Enable SSO with VDA Configuration App



VDA Configuration - Login

Single Sign-on(S

Authenticate wit

Or enable SSO function with apple script.

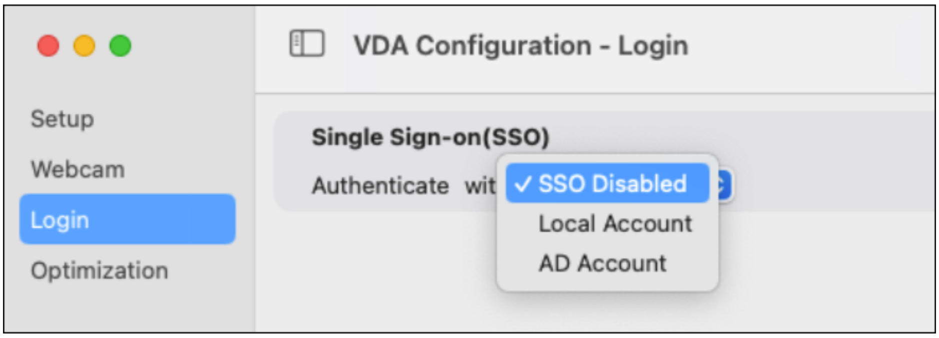
```
sudo osascript /opt/Citrix/VDA/bin/ctxsso.scpt -option 2
```

```
sudo osascript /opt/Citrix/VDA/bin/ctxsso.scpt -option 2 -silent
```

> **Note:**
>
> This mode is particularly useful for scripting and automation purposes.

How to disable SSO

1. Disable SSO with VDA Configuration App



VDA Configuration - Login

Single Sign-on(SSO)

Authenticate wit

Or run below apple script to disable SSO.

```
sudo osascript /opt/Citrix/VDA/bin/ctxsso.scpt -option 0
```

Troubleshooting

1. How to check if you system default login process has been modified.

Run below command in terminal:

```
security authorizationdb read system.login.console
```

Check if string “**loginwindow:login**” exists in output, if not, we do not support this case, as it may already been customized by other software

```
<key>mechanisms</key> <array> <string>builtin:prelogin</string>
<string>builtin:policy-banner</string> <string>loginwindow:login
</string> <string>builtin:login-begin</string> <string>builtin:
reset-password,privileged</string> <string>loginwindow:FDESupport,
privileged</string>
```

</array>

Known Issues

- If your VDA device is connected to multiple networks, registration with the DDC may be lost for a while due to disconnection or logoff.
    - Workaround: Wait for the registration to be ready before launching the session again. After VDA lost registration, it will do registration again immediately, User can try to launch session again after failure.
    - Solution: Maintain a single shared network connection for the Citrix VDA for macOS device.
- If you install Citrix VDA for macOS via terminal (outside of a user session), you may be prompted to manually enter your password upon first login.

General Content Redirection

December 23, 2025

Citrix VDA for macOS general content redirection capabilities follows HDX™ roadmap, in this release, we support

- Clipboard Redirection
    - File Copy and Paste
- Audio Redirection
- Multiple Audio Devices Redirection
- USB Redirection
- Webcam Redirection
- iDevice Redirection
- Smartcard Redirection

Clipboard Redirection

December 22, 2025

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.

File Copy and Paste

Users can copy and paste files between a session and a local client by using the right-click menu or keyboard shortcuts.

Relevant policies

The following clipboard policies are relevant to configuring the feature. For more information about the clipboard policies, see the Policy support list.

- Client clipboard redirection
- Clipboard selection update mode
- Restrict client clipboard write
- Client clipboard write allowed formats
- Restrict session clipboard write
- Session clipboard write allowed formats

> **Note:**
>
> The Limit clipboard client to session transfer size and Limit clipboard session to client transfer size policies control the clipboard buffer size rather than the size of the transferred files. For more information about supported policies, see the Policy support list.

Limitations

- Cut is not supported. Requests to cut a file are treated as copy operations.
- Drag and drop is not supported.
- File copy and paste must be performed sequentially. A new file copy and paste can only begin once the previous operation has finished.

Clipboard redirection bandwidth limit

This setting specifies the maximum allowed bandwidth (kbps) for data transfer between the session and the local clipboards.

Clipboard redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for data transfer between the session and the local clipboards, as a percentage of the total session bandwidth.

Limit clipboard client to session transfer size

This setting specifies the maximum size of clipboard data that a single copy-and-paste operation can transfer from a client device to a virtual session.

To limit the clipboard transfer size, enable the Limit clipboard client to session transfer size setting. Then, in the Size Limit field, enter a value in kilobytes to define the size of data transfer between the local clipboard and a session.

By default, this setting is disabled.

Limit clipboard session to client transfer size

This setting specifies the maximum size of clipboard data that a single copy-and-paste operation can transfer from a virtual session to a client device.

To limit the clipboard transfer size, enable the Limit clipboard session to client transfer size setting. Then, in the Size Limit field, enter a value in kilobytes to define the size of data transfer between a session and the local clipboard.

By default, this setting is disabled.

Restrict client clipboard write AND Client clipboard write allowed formats

Enabling the two settings lets you allow specific data formats to be copied and pasted from the session to the client (writing to the client).

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_UNICODETEXT
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_HTML
- CFX_FILE
- CFX_RICHTEXT

Restrict session clipboard write AND Session clipboard write allowed formats

Enabling the two settings lets you allow specific data formats to be copied and pasted from the client to the session (writing to the session).

The following clipboard formats are system defined:

- CF_TEXT
- CF_BITMAP

- CF_METAFILEPICT
- CF_SYLK
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_UNICODETEXT
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_HTML
- CFX_FILE
- CFX_RICHTEXT

Audio Redirection

August 1, 2025

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

Support for Audio volume synchronization

Starting from release 2507, macOS VDA now supports synchronization of audio volume between the VDA and your audio devices. You can now adjust the volume using the VDA audio volume slider and have the same volume on your device and this also applies to the other way around. This feature is enabled by default.

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 Citrix VDA for macOS 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 Citrix VDA for macOS:

```
/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 version 2212 and higher
- 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.

USB Redirection

September 10, 2025

Overview

USB devices are shared between the Citrix Workspace™ app and the Citrix VDA for macOS desktop. When a USB device is redirected to the desktop, you can use the USB device as if it were locally connected.

> **Note:**
>
> We recommend using USB device redirection when the network latency is lower than 100 milliseconds. Do not use USB device redirection when the network latency is higher than 200 milliseconds.

USB device redirection includes two main areas of functionality:

- Citrix USB session module (CtxHDX)
- Citrix USB service module (CtxUSB)

Citrix USB session module

The Citrix USB session module acts as a communication bridge between the USB service module and Citrix Workspace app. All USB data transfers between the Citrix VDA for macOS and Citrix Workspace app are encapsulated by the Citrix ICA® USB protocol.

Citrix USB service module

The Citrix USB service module manages all operations on USB devices, for example, attach or detach USB devices.

How USB device redirection works

Typically, if a USB device is redirected successfully to the Citrix VDA for macOS, one or more device nodes are created in the system and attached in macOS USB host controller. Sometimes, however, the redirected device isn't usable for an active Citrix VDA for macOS session. USB devices rely on drivers to function properly and some devices require special drivers. If drivers aren't provided, the redirected USB devices are inaccessible to the active Citrix VDA for macOS session. To make sure of USB device connectivity, install the drivers and configure the system properly.

The Citrix VDA for macOS supports a list of USB devices that are successfully redirected from the client.

Supported USB devices

> **Note:**
>
> We have added support for USB 3.0 ports. You can insert USB 3.0 devices into USB 3.0 ports on a client device.

The following devices class has been verified to support this version of the Citrix VDA for macOS. Other devices might be freely used, with unexpected results:

- USB mass storage device
  - Supported File System format: Mac OS Extended, ExFAT, MS-DOS(FAT) and NTFS, whereas NTFS is read-only on a Mac.
- HID Device
  - The following device has tested with Citrix VDA for macOS：Wacom Pen Tablet CTL-472
- Audio / Video Device
  - Webcam Device and Audio Device currently is not supported in Citrix VDA for macOS USB redirection. We suggest using the optimized Webcam Redirection and Audio Redirection Features for these devices.

Configuration

Set USB device redirection policies

A Citrix policy controls whether USB device redirection is enabled or disabled. The type of device can also be specified using a Delivery Controller™ policy. When configuring USB device redirection for the Citrix VDA for macOS, configure the following policy and rules:

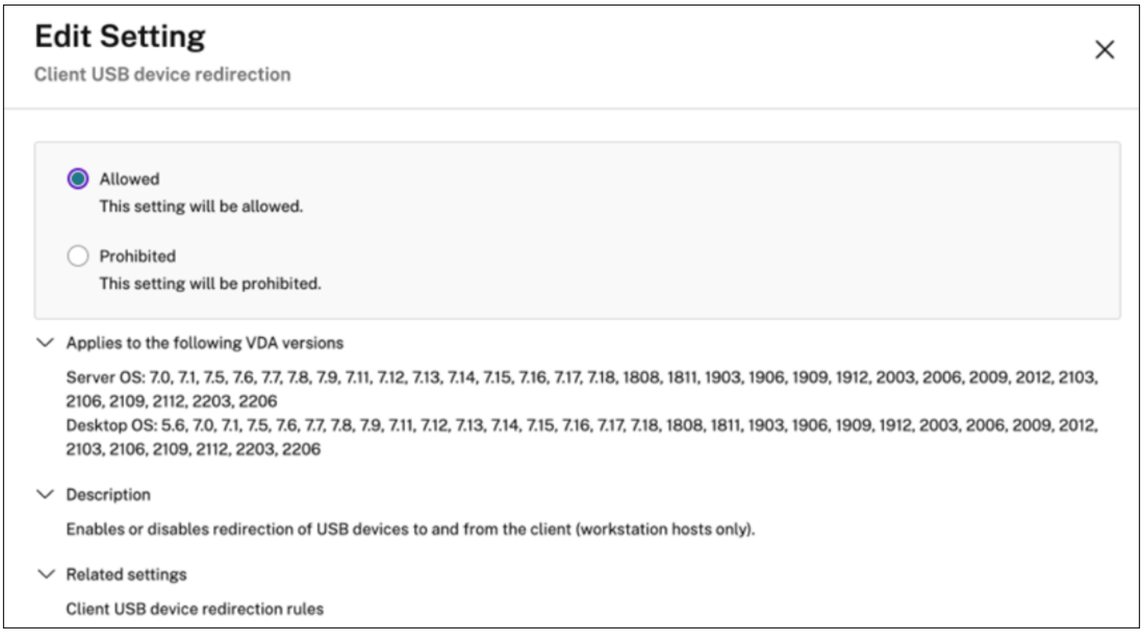
- Client USB device redirection policy
- Client USB device redirection rules

Enable USB device redirection

In Citrix Studio, enable (or disable) USB device redirection from the client (for workstation hosts only).

In the **Edit Setting** dialog:

1. Select **Allowed**.
2. Click **OK**.



Edit Setting

Client USB device redirection

● Allowed
This setting will be allowed.

○ Prohibited
This setting will be prohibited.

Applies to the following VDA versions

Server OS: 7.0, 7.1, 7.5, 7.6, 7.7, 7.8, 7.9, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 1808, 1811, 1903, 1906, 1909, 1912, 2003, 2006, 2009, 2012, 2103, 2106, 2109, 2112, 2203, 2206
Desktop OS: 5.6, 7.0, 7.1, 7.5, 7.6, 7.7, 7.8, 7.9, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 1808, 1811, 1903, 1906, 1909, 1912, 2003, 2006, 2009, 2012, 2103, 2106, 2109, 2112, 2203, 2206

Description

Enables or disables redirection of USB devices to and from the client (workstation hosts only).

Related settings

Client USB device redirection rules

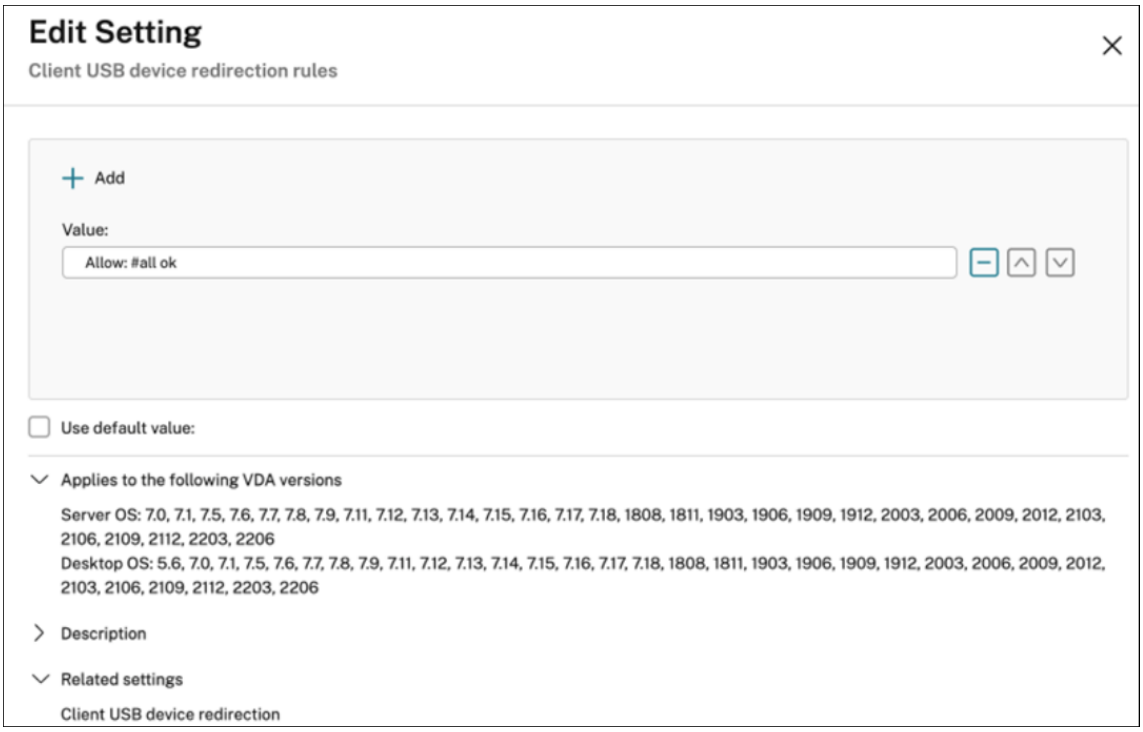
Set USB device redirection rules

After enabling the USB redirection policy, set the redirection rules using Citrix Studio by specifying which devices are allowed (or denied) on the Citrix VDA for macOS.

In the **Client USB device redirection rules** dialog:

1. Click **New** to add a redirection rule, or click 1. Edit to review an existing rule.

   After creating (or editing) a rule, click **OK**.



Edit Setting

Client USB device redirection rules

Value:

Allow: #all ok

□ Use default value:

Applies to the following VDA versions

Server OS: 7.0, 7.1, 7.5, 7.6, 7.7, 7.8, 7.9, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 1808, 1811, 1903, 1906, 1909, 1912, 2003, 2006, 2009, 2012, 2103, 2106, 2109, 2112, 2203, 2206

Desktop OS: 5.6, 7.0, 7.1, 7.5, 7.6, 7.7, 7.8, 7.9, 7.11, 7.12, 7.13, 7.14, 7.15, 7.16, 7.17, 7.18, 1808, 1811, 1903, 1906, 1909, 1912, 2003, 2006, 2009, 2012, 2103, 2106, 2109, 2112, 2203, 2206

Related settings

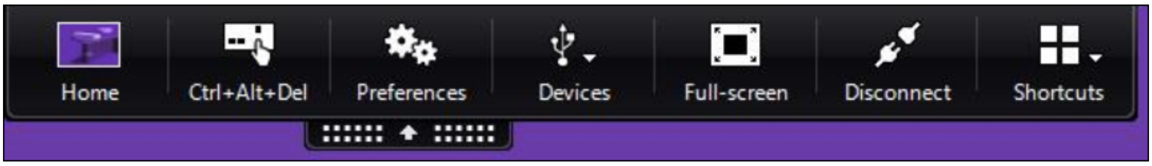
Client USB device redirection

For more information on configuring USB redirection, see the Citrix Generic USB Redirection Configuration Guide.

Troubleshoot USB device redirection issues

Use the information in this section to troubleshoot various issues that you might come across when using the Citrix VDA for macOS.

No devices in the toolbar of Citrix Workspace app Sometimes, you might not be able to see devices listed in the toolbar of Citrix Workspace app, which indicates that no USB redirection is taking place.



If you come across the issue, verify the following:

- The policy is configured to allow USB device redirection.
- The Citrix USB service module is running.

If the policy is not set correctly, refer the Set USB device redirection policies to set it correctly.

Redirection failure when USB devices are visible in the toolbar of Citrix Workspace app, but are labeled "policy restricted" When the issue occurs, do the following:

- Configure the Citrix VDA for macOS policy to enable redirection.
- Check whether any additional policy restrictions are configured in the registry of Citrix Workspace app. Check **DeviceRules** in the registry path to make sure that the device isn't denied access by this setting:

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB`

A USB Mass Storage device is redirected successfully, but I can't write data to it in my session Check if the file system is NTFS. NTFS is read-only in macOS.

USB Device Session Isolation

Citrix VDA for macOS only supports a single ICA session that is used at the same time. However, with Apple's built-in VNC client, we can launch two or more sessions with different user accounts.

For instance, one ICA session for user A and two VNC sessions for user B and user C. USB redirection doesn't support USB device session isolation currently.

Webcam Redirection

August 1, 2025

Overview

Users of video conferencing etc. applications running in VDA for macOS sessions can now use their webcams with HDX™ webcam video compression capability. The feature is enabled by configuration through the "VDA Configuration"app installed with VDA.
HDX webcam video compression is also called Optimized webcam mode. This type of webcam video compression sends the H.264 video directly to the video conferencing application running in the virtual session. HDX webcam video compression uses the multimedia framework technology that is part of the client operating system to intercept video from capture devices, transcode, and compress it.
When a session is launched, the Workspace app in the client handles the webcam requests from VDA. The client then sends the video only to the server that can display it properly. The server leverages the camera extension of macOS system to process webcam streams, and its integration gives you the

same experience on your desktop. Workspace app compresses the video to save bandwidth and provide better resiliency on WAN scenarios.

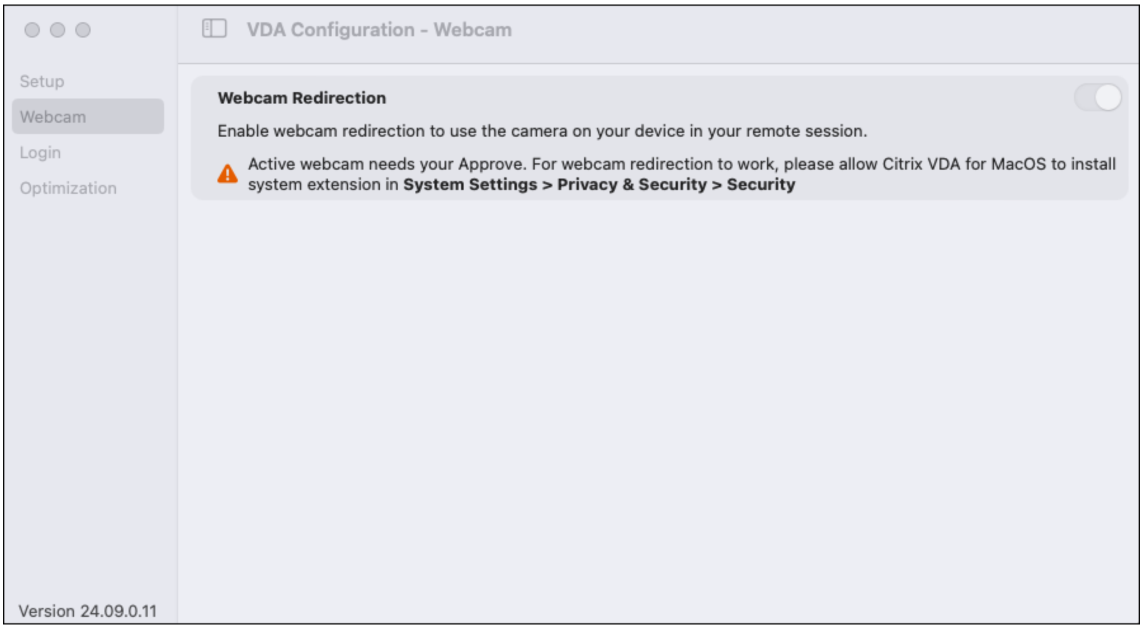
We also support plug-and-play capability for webcam redirection, simplifying the user experience. Webcams are automatically detected and configured for use within virtual sessions, removing the need for manual configuration or session reconnections. Multiple webcam devices in one client can be also redirected to the Citrix® virtual sessions.

Besides these, multiple resolutions of the peripheral camera are supported to redirect as the resolutions of Citrix HDX Webcam. Users are able to choose the suitable camera resolution whenever they would like to.

Configuration

To use Webcam Redirection, complete the following configuration:
Activate camera extension to make webcam available.
Open "VDA Configuration"App: find the App in Applications or Launchpad to open
Navigate to the tab "Webcam"
Click the toggle to activate camera extension, as shown in the screenshots below (Click the toggle in active mode will deactivate the camera extension)

- For macOS versions earlier than 15:



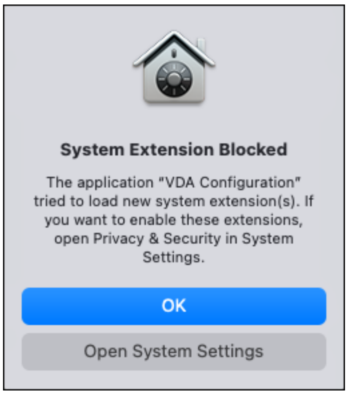
Webcam Redirection

Enable webcam redirection to use the camera on your device in your remote session.

Active webcam needs your Approve. For webcam redirection to work, please allow Citrix VDA for MacOS to install system extension in **System Settings > Privacy & Security > Security**

Version 24.09.0.11

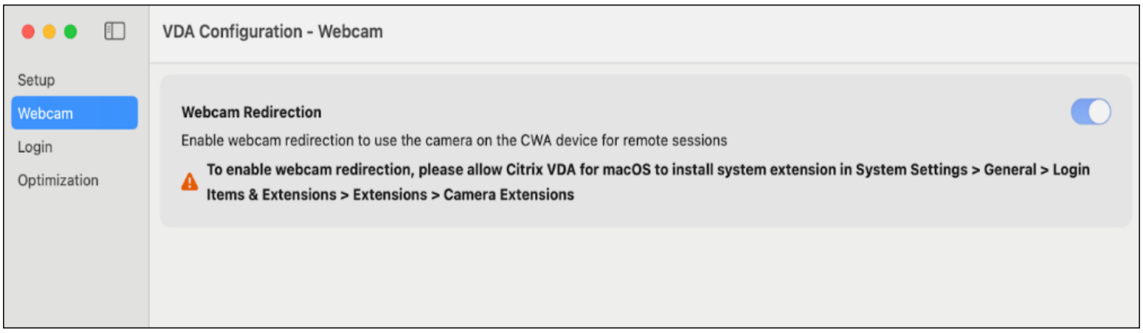
1. Click **Open System Settings** to navigate to system setting page:



System Extension Blocked

The application "VDA Configuration" tried to load new system extension(s). If you want to enable these extensions, open Privacy & Security in System Settings.

- For macOS versions 15 and later:



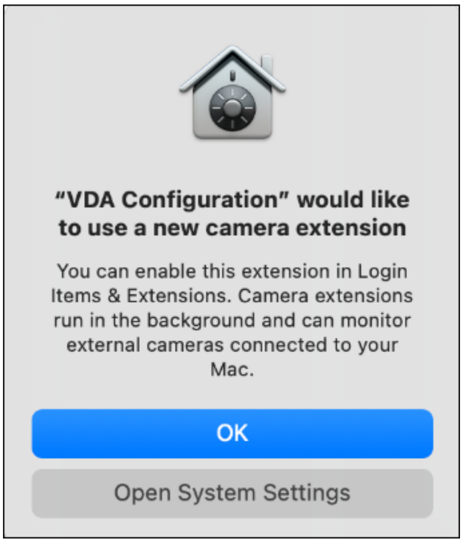
VDA Configuration - Webcam

Webcam Redirection

Enable webcam redirection to use the camera on the CWA device for remote sessions

⚠ To enable webcam redirection, please allow Citrix VDA for macOS to install system extension in System Settings > General > Login Items & Extensions > Extensions > Camera Extensions

1. Click **Open System Settings** to navigate to system setting page:

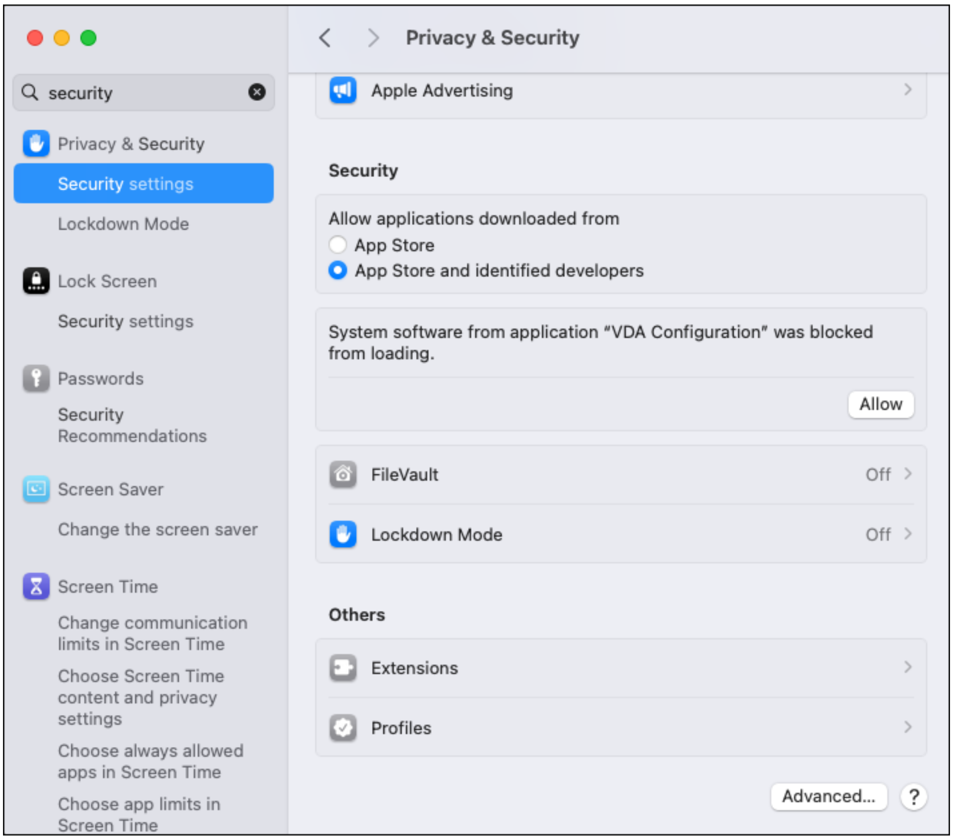


"VDA Configuration" would like to use a new camera extension

You can enable this extension in Login Items & Extensions. Camera extensions run in the background and can monitor external cameras connected to your Mac.

1. Click **Allow** so that Citrix VDA for macOS can load system extension for webcam redirection.

   For macOS versions earlier than 15, you can also manually navigate to Privacy & Security and Security:



Security

Allow applications downloaded from
○ App Store
● App Store and identified developers

System software from application "VDA Configuration" was blocked from loading.

Allow

FileVault Off

Lockdown Mode Off

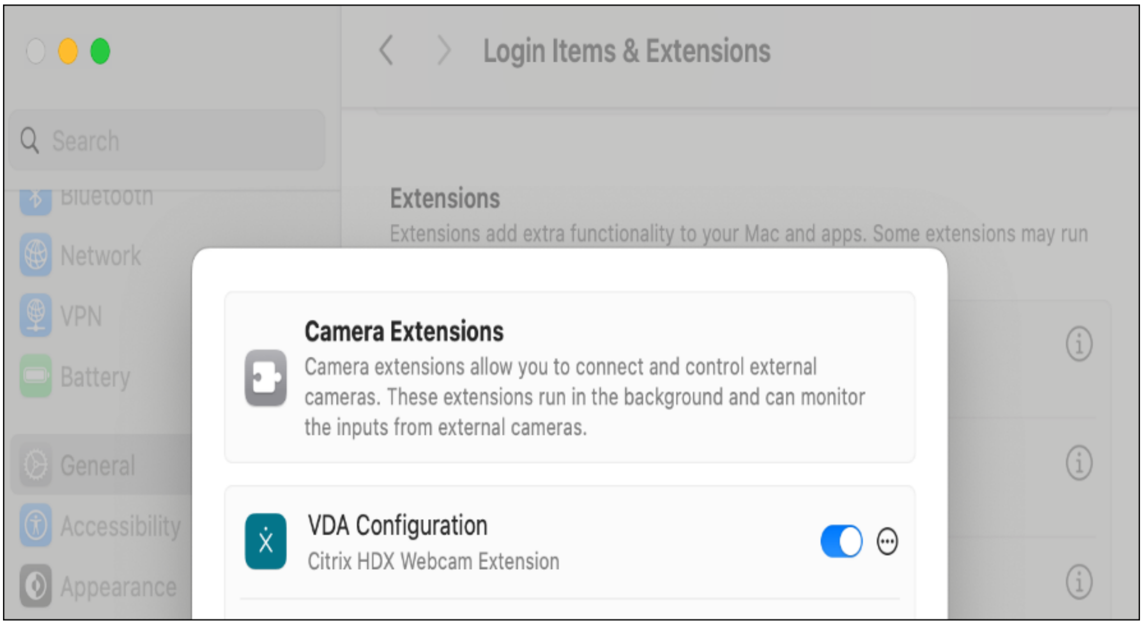
Others

Extensions

Profiles

Advanced… ?

For macOS versions 15 and later, you also manually navigate to **General**, **Login Items & Extensions** and then **Camera Extensions**.

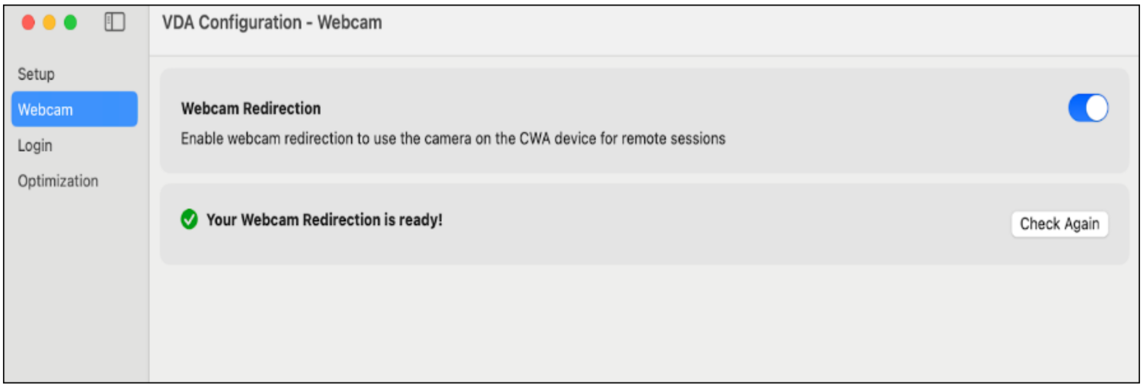


Camera Extensions

Camera extensions allow you to connect and control external cameras. These extensions run in the background and can monitor the inputs from external cameras.

VDA Configuration
Citrix HDX Webcam Extension

2. Now the configuration is successful as shown below.



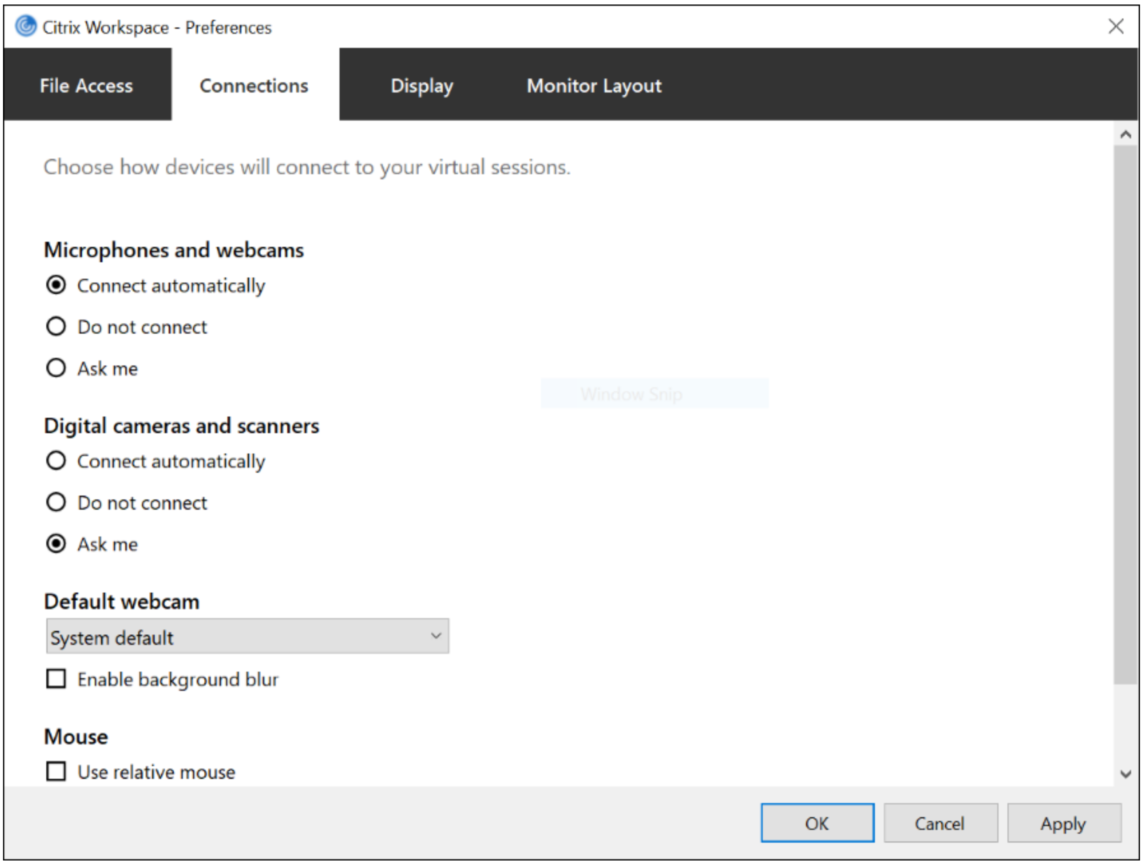
VDA Configuration - Webcam

Webcam Redirection

Enable webcam redirection to use the camera on the CWA device for remote sessions

✓ Your Webcam Redirection is ready!

3. Ensure webcam access is allowed when you connect to a VDA session, and then the redirected Citrix HDX webcams can be used. For example, with Citrix Workspace™ app for Windows, you can configure it to Connect automatically to use webcams.



Choose how devices will connect to your virtual sessions.

Microphones and webcams

● Connect automatically

○ Do not connect

○ Ask me

Digital cameras and scanners

○ Connect automatically

○ Do not connect

● Ask me

Default webcam

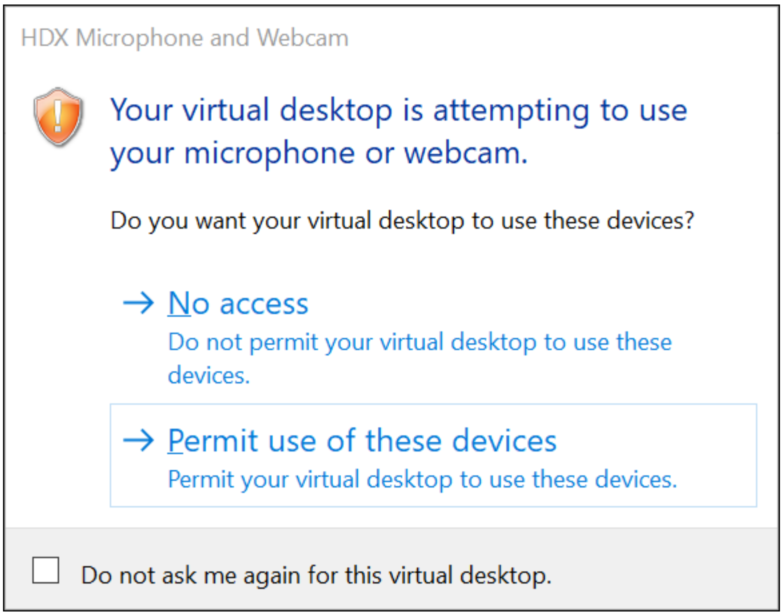
System default

□ Enable background blur

Mouse

□ Use relative mouse

Or select "Ask me"and allow it each time



HDX Microphone and Webcam

Your virtual desktop is attempting to use your microphone or webcam.

Do you want your virtual desktop to use these devices?

→ No access
Do not permit your virtual desktop to use these devices.

→ Permit use of these devices
Permit your virtual desktop to use these devices.

□ Do not ask me again for this virtual desktop.

Limitation

- Webcam shall in general support H.264 codec to be used, check the related CWA documents for requirements.

Troubleshooting

If webcam redirection can't work as expected, follow these steps in sequence to resolve the issue:

Step 1: Verify Camera Extension Status

1. Open Terminal App and execute the following command:

   ```
   systemextensionsctl list | grep com.citrix.mvda.vdacfg.cameraextension
   ```

2. Review the output, it will show the current camera extension status managed by macOS system, which is corresponding to the Citrix HDX Webcam Extension.
   If the status is activated enabled, proceed to Step 2:

   ```
   S272Y5R93J com.citrix.mvda.vdacfg.cameraextension (1.2.0.1/1.2.0.1)
   Citrix HDX Webcam Extension [activated enabled]
   ```

   If the status is activated waiting for user, you must approve the request in System Settings:

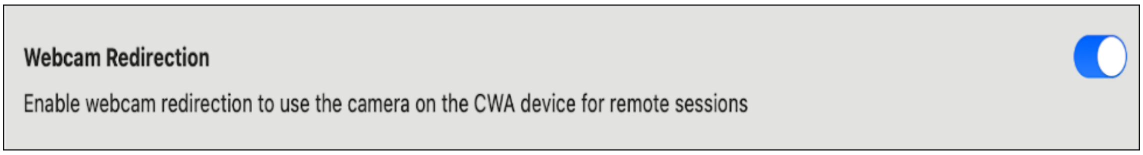
   - For macOS 15 and later: Navigate to System Settings > General > Login Items & Extensions > Extensions > Camera Extensions.

- For earlier versions of macOS: Navigate to System Settings > Privacy & Security > Security.

```
S272Y5R93J com.citrix.mvda.vdacfg.cameraextension (1.2.0.1/1.2.0.1)
Citrix HDX Webcam Extension [activated waiting for user]
```

If nothing is found, open the **VDA Configuration** App and navigate to the Webcam tab. If Webcam Redirection is not activated, we recommend you to activate it.

If it is already activated, the webcam extension will be automatically updated to the new version.



Webcam Redirection

Enable webcam redirection to use the camera on the CWA device for remote sessions

3. If you have an active Citrix HDX session, disconnect it and reconnect.

Step 2: Verify Camera Extension Process Status

1. Open Terminal App and execute the following command:

```
ps -ef | grep "com.citrix.mvda.vdacfg.cameraextension"
```

2. If there is a process running, go to Step3.
   If no process is running, since the process is managed by the macOS system, you have to open the "VDA Configuration"App and switch to the Webcam tab, disable Webcam Redirection to deactivate the camera extension and enable it again, and then check the process status by running the command above.

Step 3: Confirm Camera Status

1. Navigate to System Settings -> General -> About -> System Report…-> Camera, or use the following command to retrieve camera details:

```
system_profiler SPCameraDataType
```

2. Verify if a camera with a name starting with "HDX -"is listed:
   If the HDX camera is listed: Proceed to Step 4.
   If the HDX camera is not listed: Reconnect the current Citrix HDX session.

Step 4: Ensure Application and Webcam Interaction

1. If you can not see the redirected webcam in one application:

   - Quit and restart the application.

    - If the issue persists, restart macOS (some applications may require this step).

2. If the webcam is detected but no video is displayed in your apps:

    - Disconnect the current session and connect it again.

Printing redirection

August 1, 2025

Printing redirection enables users to easily print documents and other files from within their macOS VDA desktops to printers connected to their local machines. Citrix PDF Universal Printer driver is introduced from now on to enable Printing redirection.

The Citrix PDF Universal Printer driver supports creating Citrix PDF Printer when a user logon to macOS VDA desktop. When the user opens documents to print and selects the Citrix PDF Printer option, the driver converts the file to PDF and transfers the PDF to the local device. The PDF is then opened for viewing and printing from a locally attached printer.

The PDF printer can be enabled, configured, and set as default using a Citrix Policy. The Citrix PDF Printer option is available to users of the Citrix Workspace™ app for Windows, Linux, MacOS, Chrome, and HTML5.

Configuration

To utilize the Citrix PDF printer in addition to the default PDF printing capabilities of Citrix Workspace app, configure the following policies in Citrix Studio:

- Client Printer Redirection: Ensure this policy is set to Allowed (enabled by default).
- Auto-create PDF Universal Printer: Set this policy to Enabled (disabled by default).
- Auto-create client printers: Set this policy to Auto-create all client printers.
  Refer to policy support list for details on how those policies are applied.

> **Note:**
>
> For PostScript files, we recommend converting them to PDF format before printing with the Citrix PDF printer.

Troubleshooting

1. Check Citrix DDC Policies

- Verify that the Citrix DDC policies listed in the Configuration section are properly configured by the command in Terminal App:
  `sudo hdxmonitor print dump`

2. Printer Not Created in Session

   - If the policies are configured but the printer is not created in the session, check if the `cupsd` service is functioning correctly by running the following command:
     `sudo launchctl list org.cups.cupsd`

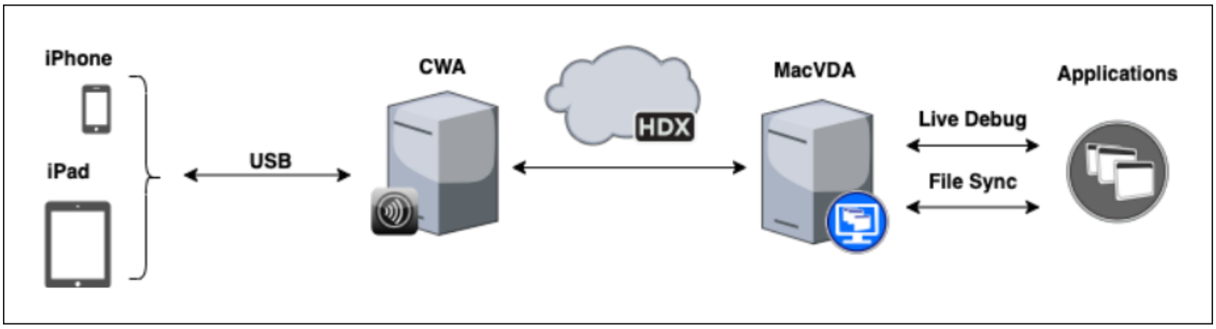
3. Printer Created But Unable to Print

   - If the printer is created in the session but cannot print files, ensure that the printer on the client side is functioning correctly.

iDevice Redirection with Citrix Virtual Delivery Agent for macOS

August 1, 2025

For Apple application developers, now iPhones and iPads can be redirected to macOS VDA from Citrix Workspace app. This will enable developers to debug and troubleshoot apps on physical devices, providing a valuable addition to use Xcode provided simulators.



System Requirements

- macOS: 14.6 or later
- macOS VDA: CR2507 or later
- Citrix Workspace™ app
- Windows: version 2402 LTSR or later CR

Releases

- Mac: 2505
- iDevice (iPhone, iPad) Requirements
- iOS - 17.6.1 and later
- iPadOS - 17.7.3 and later

Supported iDevice functionalities

With iPhone/iPad redirection, we have verified the following typical functionalities:

- Manage and sync with iOS/iPadOS device.
- Retrieving iOS/iPadOS syslogs and viewing / filtering them in macOS VDA.
- Live debugging of applications on the redirected iDevice.

Network Latency Recommendations

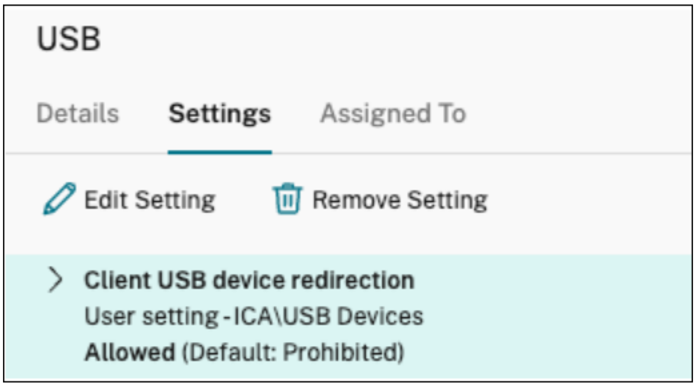
We support a wide range of network latency as long as remote desktop can be connected, but for optimal performance to run the iPhone/iPad redirection,

- Network round-trip time should ideally be around 60ms for the live debugging function to work smoothly, high latency could potentially impact usability
- HDX™ Adaptive transport(UDP) is the preferred transport protocol over TCP based on the performance test results too.

Detailed performance data under various network conditions can be found in the last section of this article.

Configuration

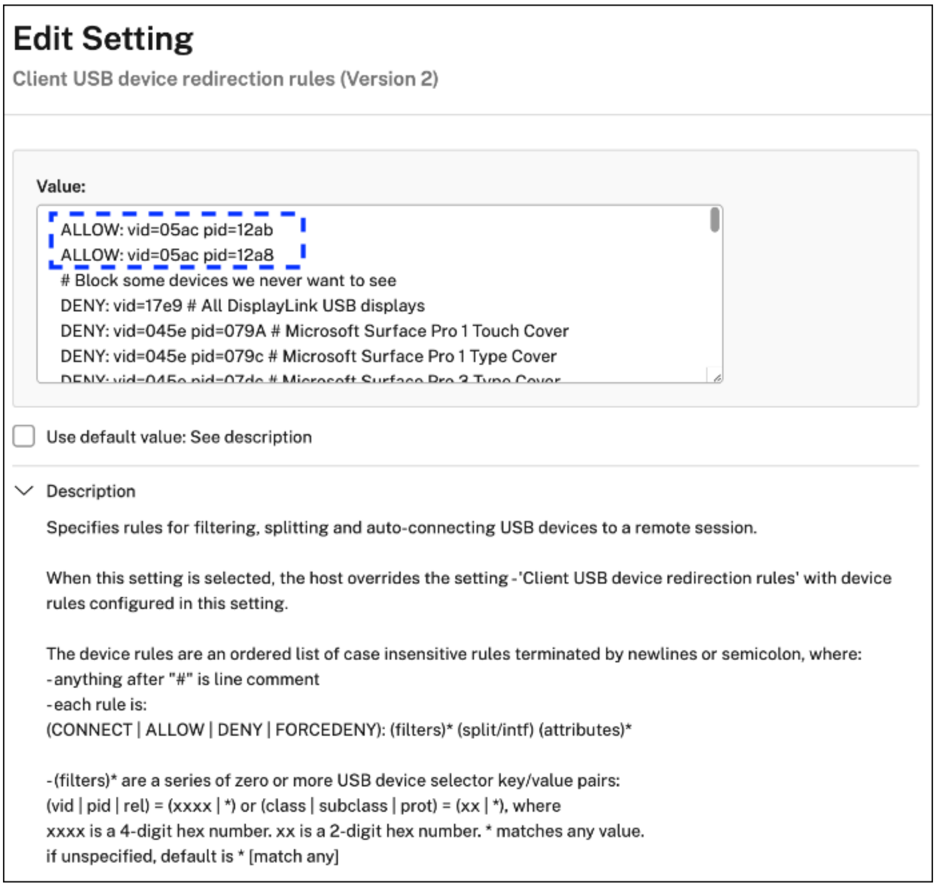
- The Citrix Studio USB redirection DDC policy must be enabled.



USB

Client USB device redirection
User setting - ICA\USB Devices
Allowed (Default: Prohibited)

- Set the "Client USB device redirection rule (Version 2)"to allow iDevice to be redirected.



Edit Setting

Client USB device redirection rules (Version 2)

Value:

```
ALLOW: vid=05ac pid=12ab
ALLOW: vid=05ac pid=12a8
# Block some devices we never want to see
DENY: vid=17e9 # All DisplayLink USB displays
DENY: vid=045e pid=079A # Microsoft Surface Pro 1 Touch Cover
DENY: vid=045e pid=079c # Microsoft Surface Pro 1 Type Cover
DENY: vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
```

□ Use default value: See description

Description

Specifies rules for filtering, splitting and auto-connecting USB devices to a remote session.

When this setting is selected, the host overrides the setting -'Client USB device redirection rules' with device rules configured in this setting.

The device rules are an ordered list of case insensitive rules terminated by newlines or semicolon, where:
-anything after "#" is line comment
-each rule is:
(CONNECT | ALLOW | DENY | FORCEDENY): (filters)* (split/intf) (attributes)*

-(filters)* are a series of zero or more USB device selector key/value pairs:
(vid | pid | rel) = (xxxx | *) or (class | subclass | prot) = (xx | *), where
xxxx is a 4-digit hex number. xx is a 2-digit hex number. * matches any value.
if unspecified, default is * [match any]

In the DDC policy, there are two types of USB rules:

- Client USB device redirection rules
- Client USB device redirection rules (Version 2)

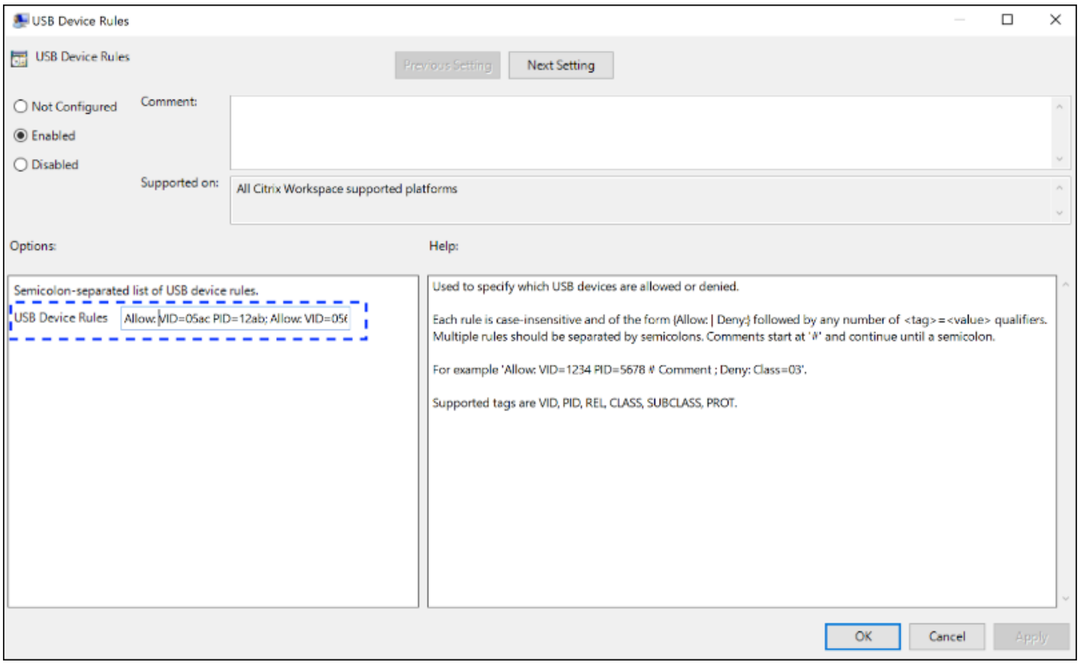
Please use Version 2, as it offers enhanced device control capabilities.
After adding the new VID/PID entries, the configuration will be complete.
Client USB device redirection rules V2 specifies rules for filtering, splitting, and auto-connecting USB devices to a remote session. When this setting is selected, the host overrides the Client USB device redirection rules setting with the device rules configured in this setting. For more information, see USB Device Redirection

> **Note:**
>
> iDevice redirection can also work with the original "Client USB device redirection rules."In that case, you must edit the CWA local file to enable CWA to redirect iPhone and iPad devices from the USB virtual channel on the clients.
>
> 1. Open the search bar by pressing the Windows key and S key, then type "gpedit".

2. Go to Local Computer Policy -> Computer Configuration -> Administrative Templates -> Citrix Components -> Citrix Workspace -> Remote client devices -> Generic USB Remoting.

3. Change the USB Device Rules to "Enabled"and add the iPad/iPhone Vendor ID (vid) and Product ID (pid) to the USB rules, as shown in the example below.

```
Allow: VID=05ac PID=12ab; Allow: VID=05ac PID=12a8
```



○ Not Configured
● Enabled
○ Disabled

Supported on: All Citrix Workspace supported platforms

Semicolon-separated list of USB device rules.

USB Device Rules: Allow: VID=05ac PID=12ab; Allow: VID=05(

Used to specify which USB devices are allowed or denied.

Each rule is case-insensitive and of the form {Allow: | Deny:} followed by any number of <tag>=<value> qualifiers. Multiple rules should be separated by semicolons. Comments start at '#' and continue until a semicolon.

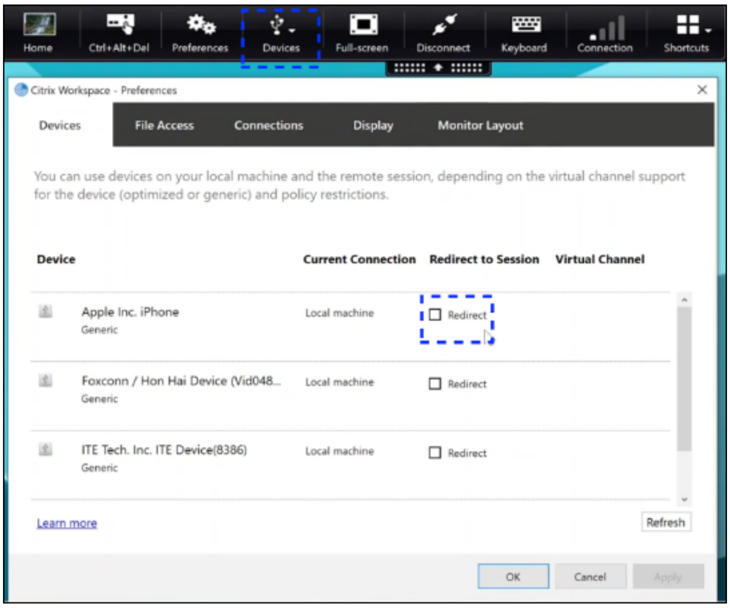
For example 'Allow: VID=1234 PID=5678 # Comment ; Deny: Class=03'.

Supported tags are VID, PID, REL, CLASS, SUBCLASS, PROT.

VID: 05ac, PID: 12ab means iPad
VID: 05ac, PID: 12a8 means iPhone

Redirect the iDevices in Citrix Workspace app

For example, select the "Apple Inc. iPhone"device by clicking on the "Device"button within the CWA Collection Bar.



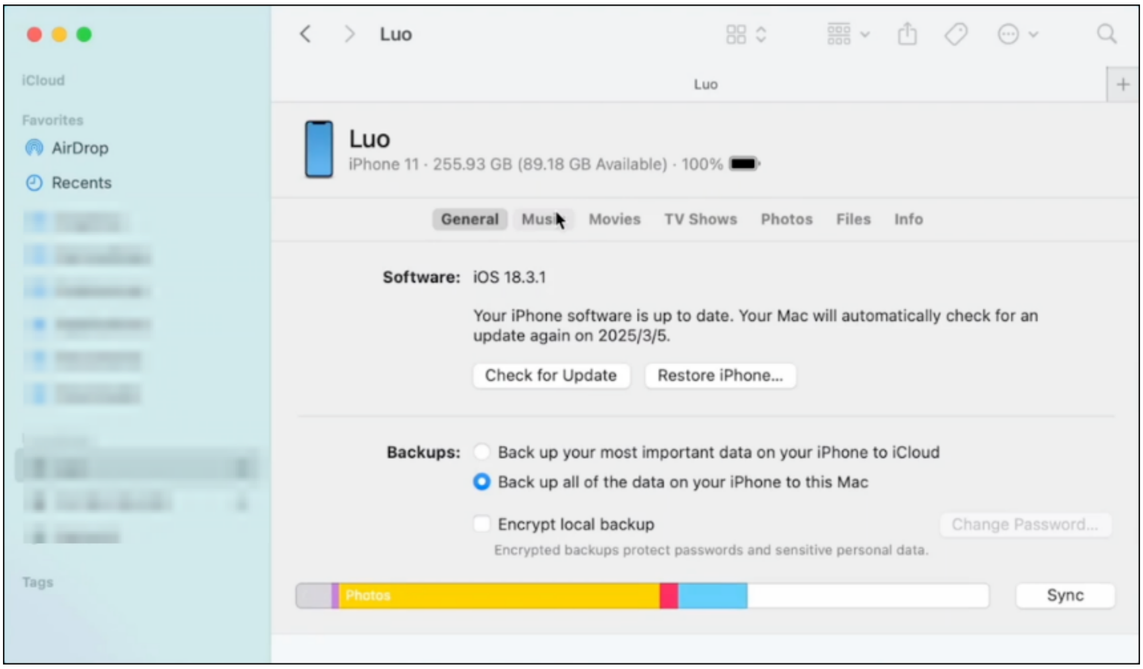
Citrix Workspace - Preferences

You can use devices on your local machine and the remote session, depending on the virtual channel support for the device (optimized or generic) and policy restrictions.

Device	Current Connection	Redirect to Session	Virtual Channel
Apple Inc. iPhone Generic	Local machine	☐ Redirect	
Foxconn / Hon Hai Device (Vid048... Generic	Local machine	☐ Redirect	
ITE Tech. Inc. ITE Device(8386) Generic	Local machine	☐ Redirect	

Examples of using iDevice Redirection Feature

- Manage or sync iOS device



Luo

iPhone 11 · 255.93 GB (89.18 GB Available) · 100%

Software: iOS 18.3.1

Your iPhone software is up to date. Your Mac will automatically check for an update again on 2025/3/5.

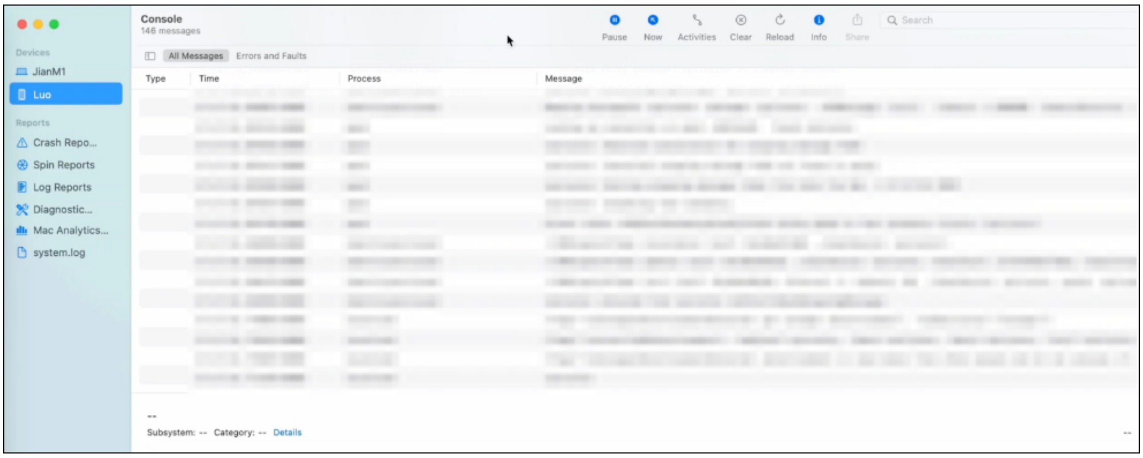
Backups: ○ Back up your most important data on your iPhone to iCloud

● Back up all of the data on your iPhone to this Mac

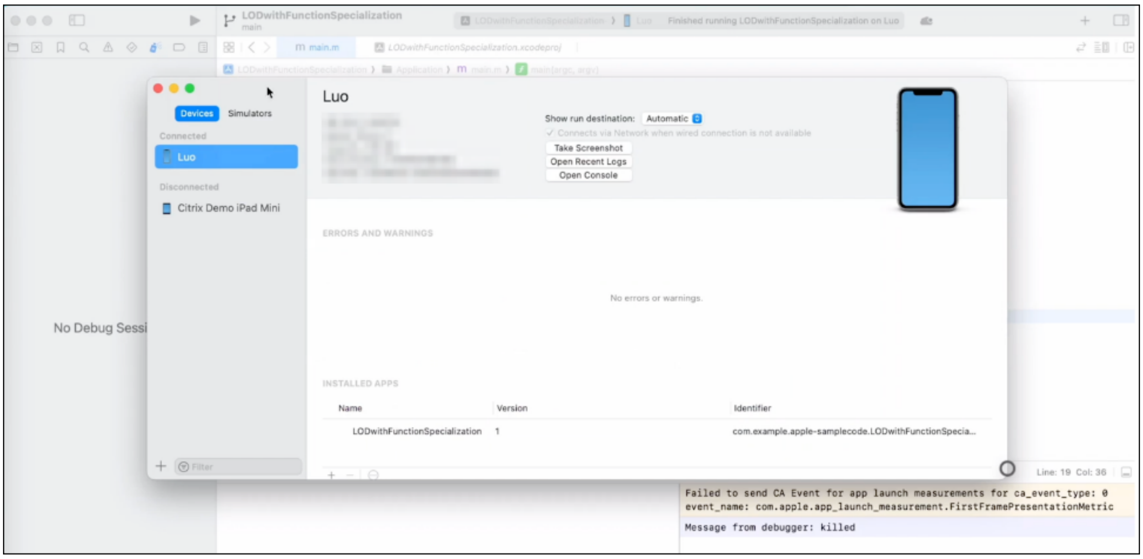
☐ Encrypt local backup

Encrypted backups protect passwords and sensitive personal data.

- Retrieving iOS syslogs and viewing / filtering them in macOS VDA



- Debugging is available for applications on the redirected iOS device

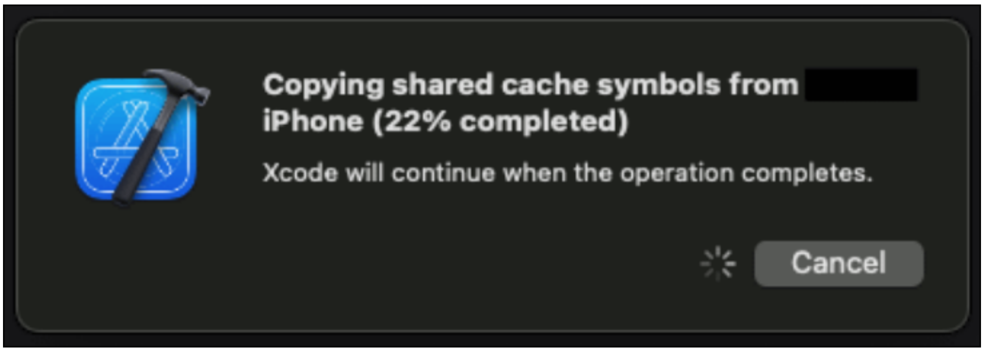


Name	Version	Identifier
LODwithFunctionSpecialization	1	com.example.apple-samplecode.LODwithFunctionSpecia...

```
Failed to send CA Event for app launch measurements for ca_event_type: 0
event_name: com.apple.app_launch_measurement.FirstFramePresentationMetric
Message from debugger: killed
```

Tips for optimization iOS / iPadOS shared caches symbols sync for iDevice living debugging.

When debugging an iDevice with Xcode for the first time, Xcode copies shared cache symbols for the device. This is a one-time job, but the symbol file size is typically large, around 4 GB. macOS VDA also supports copying the symbols file from the remote iDevice to Xcode running in macOS VDA. Because the symbols file is large, the file copying time can take around 30 minutes.

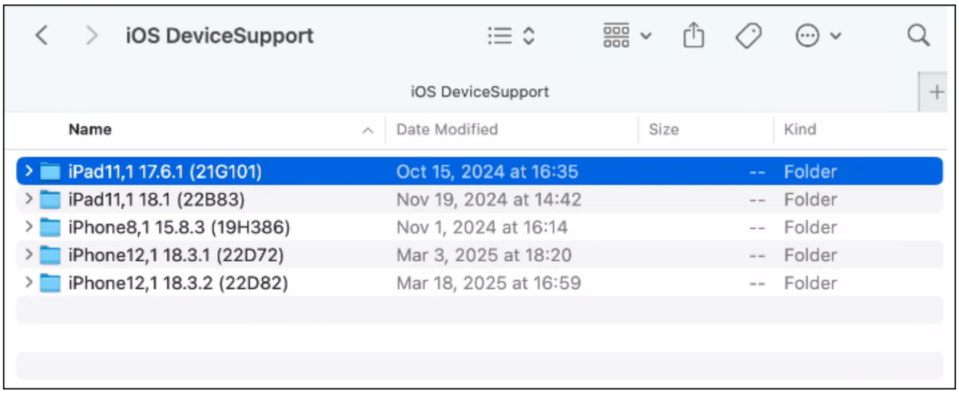


Copying shared cache symbols from [redacted] iPhone (22% completed)

Xcode will continue when the operation completes.

One optimization is to manually copy the shared cache into the Xcode folder in advance to bypass the file syncing in Xcode.
If you have connected the iDevice locally:

1. Open the local Xcode folder: ~/`Library`/`Developer`/`Xcode`/`iOS DeviceSupport`.



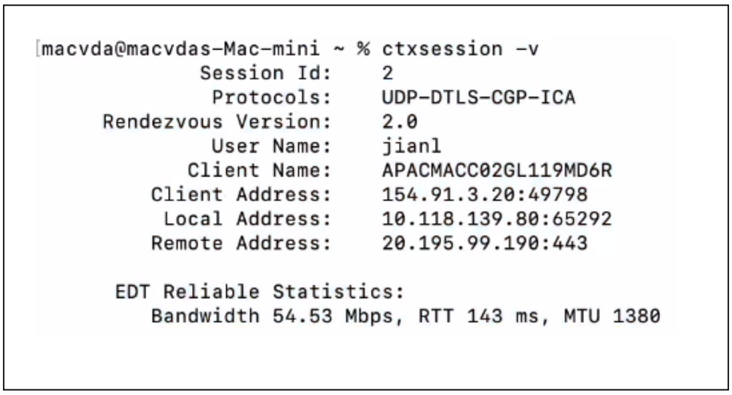
Name	Date Modified	Size	Kind
iPad11,1 17.6.1 (21G101)	Oct 15, 2024 at 16:35	--	Folder
iPad11,1 18.1 (22B83)	Nov 19, 2024 at 14:42	--	Folder
iPhone8,1 15.8.3 (19H386)	Nov 1, 2024 at 16:14	--	Folder
iPhone12,1 18.3.1 (22D72)	Mar 3, 2025 at 18:20	--	Folder
iPhone12,1 18.3.2 (22D82)	Mar 18, 2025 at 16:59	--	Folder

2. Copy the shared caches symbols file into macOS VDA under the same Xcode folder via network file sharing.

iDevice Redirection Performance Considerations

The performance of iDevice redirection relies more on network round-trip time (latency) and depends on USB Redirection feature (USB Virtual Channel capability). Network bandwidth in this case, has limited impact.

The network RTT can be retrieved by executing the "ctxsession -v"command from the Citrix Virtual Delivery Agent for macOS.



```
[macvda@macvdas-Mac-mini ~ % ctxsession -v
             Session Id:    2
              Protocols:    UDP-DTLS-CGP-ICA
     Rendezvous Version:    2.0
              User Name:    jianl
            Client Name:    APACMACC02GL119MD6R
         Client Address:    154.91.3.20:49798
          Local Address:    10.118.139.80:65292
         Remote Address:    20.195.99.190:443

      EDT Reliable Statistics:
         Bandwidth 54.53 Mbps, RTT 143 ms, MTU 1380
```

The table below displays the estimated time delays for various device actions based on Round Trip Time (RTT).

UDP Connections

Device Action	RTT ~5ms	RTT ~30ms	RTT ~60ms	RTT ~90ms	RTT ~120ms
Show device info in macOS Finder	15s	30s	55s	80s	100s
Collect device syslog	1.5s	3s	7s	11s	16s
Sync/Deploy 100m file	60s	100s	160s	220s	270s
XCode live debugging w/ breakpoint	31s	85s	150s	250s	480s

TCP Connection

Device Action	RTT ~5ms	RTT ~30ms	RTT ~60ms	RTT ~90ms	RTT ~120ms
Show device info in macOS Finder	12s	30s	55s	85s	106s
Collect device syslog	1.5s	4s	7s	13s	17s
Sync/Deploy 100m file	60s	145s	240s	340s	450s
XCode live debugging w/ breakpoint	40s	85s	150s	250s	480s

Smartcard Redirection

December 23, 2025

Overview

This feature enables secure authentication using smart card within HDX sessions on macOS, providing security through hardware-based authentication tokens. The implementation supports both traditional smart card authentication and modern FIDO2 passwordless authentication protocols.

Capabilities

- Smart card authentication
  - Leverages physical smart card devices for strong authentication.
- FIDO2 passwordless authentication
  - Support FIDO2 protocol standards for passwordless authentication.

Configuration and Prerequisites

- USB redirection policy
  - To use this feature, USB redirection policy must be enabled. Additionally, smart card devices must be allowed through USB redirection rules.
- macOS device pairing
  - Smart card devices must be paired with specific macOS user accounts.

Steps to use smart card for macOS login in HDX session

Pre-requisites

Make sure USB redirection policy is enabled and the smart card device is allowed through USB redirection rules. Make sure the smart card is paired with the specified macOS user account.

1. **Insert smart card:** Insert the smart card device into the client machine.
2. **Launch HDX session:** Launch an HDX session to a macOS endpoint and wait for the login window to appear.
3. **Redirect smart card:** In the CWA (Citrix Workspace App) toolbar, select Devices -> [smart card device name] to redirect the smart card to the HDX session.
4. **Authenticate:** Enter the smart card PIN in the macOS login window to complete the authentication and login to macOS.

> **Note:**
>
> SSO feature should be disabled when user use smart card for macOS login in HDX session.

Graphics

December 23, 2025

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

- Automatic DPI Scaling
- Configure Graphics
- Multi Monitor Support
- Thinwire Progressive Display
- HDX Screen Sharing
- Selective build to lossless

High DPI

August 1, 2025

The Citrix VDA for macOS supports High DPI with automatic DPI scaling. When you open a virtual desktop session, the DPI scale 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 **High DPI for Citrix Workspace™**.
    - In Citrix Workspace App for Windows, it”™s enabled by default. For more information about configuring High DPI for Citrix Workspace App for Windows, see DPI scaling.
    - By default, High DPI is not enabled in Citrix Workspace App for Mac. See the guide for instructions on how to enable it.
    - In Citrix Workspace App for Linux, High DPI is not enabled by default. Please refer to the guide for instructions on how to enable it.
- 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.

Limitation

- Currently, the High DPI feature supports scale factors of 1 and 2 in the client. For Example: 100% and 200%.
- Each monitor in the client must have a minimum resolution of 2560x1440; otherwise, High DPI will not work.

Graphics Configuration and Fine-Tuning

August 1, 2025

This section describes the Citrix VDA for macOS 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 Citrix VDA for macOS.

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**

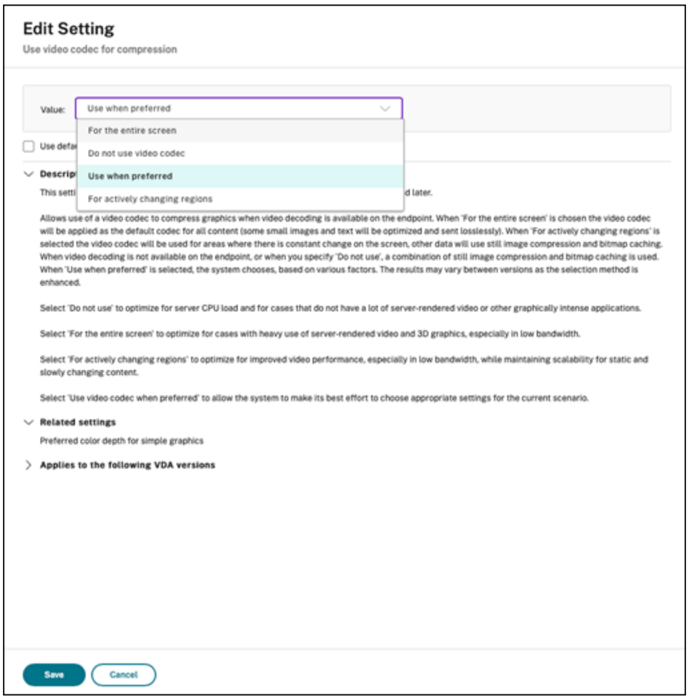
  The adaptive display technology in Thinwire identifies moving images (video, 3D in motion).

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.



Edit Setting

Use video codec for compression

Value: Use when preferred

For the entire screen

Do not use video codec

Use when preferred

For actively changing regions

□ Use defa

Descrip

This setti d later.

Allows use of a video codec to compress graphics when video decoding is available on the endpoint. When 'For the entire screen' is chosen the video codec will be applied as the default codec for all content (some small images and text will be optimized and sent losslessly). When 'For actively changing regions' is selected the video codec will be used for areas where there is constant change on the screen, other data will use still image compression and bitmap caching. When video decoding is not available on the endpoint, or when you specify 'Do not use', a combination of still image compression and bitmap caching is used. When 'Use when preferred' is selected, the system chooses, based on various factors. The results may vary between versions as the selection method is enhanced.

Select 'Do not use' to optimize for server CPU load and for cases that do not have a lot of server-rendered video or other graphically intense applications.

Select 'For the entire screen' to optimize for cases with heavy use of server-rendered video and 3D graphics, especially in low bandwidth.

Select 'For actively changing regions' to optimize for improved video performance, especially in low bandwidth, while maintaining scalability for static and slowly changing content.

Select 'Use video codec when preferred' to allow the system to make its best effort to choose appropriate settings for the current scenario.

Related settings

Preferred color depth for simple graphics

Applies to the following VDA versions

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

August 1, 2025

Overview

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

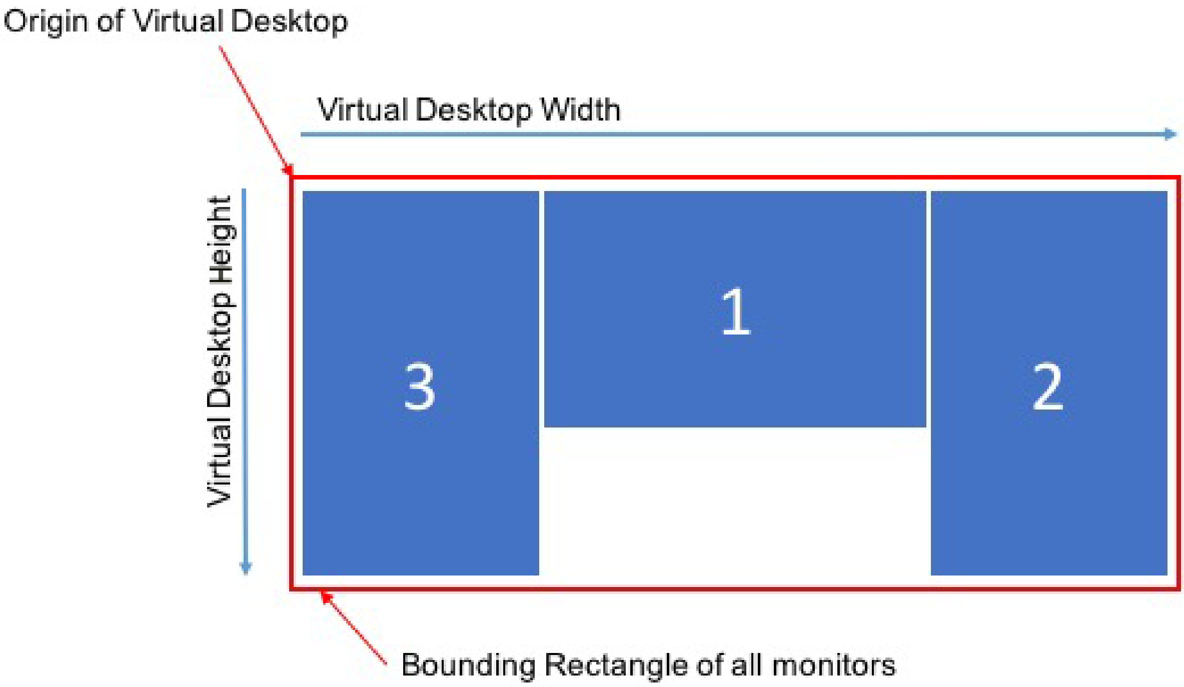
This section tells you how to configure a Citrix VDA for macOS for different monitor resolutions and layouts.

Virtual session desktop

Citrix VDA for macOS 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.

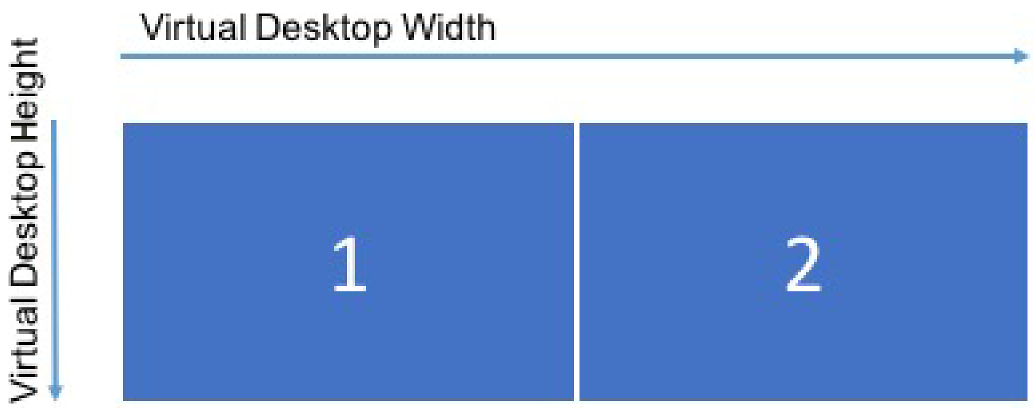
This calculation is important for the following reasons:

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

Allowing for different client monitor configurations

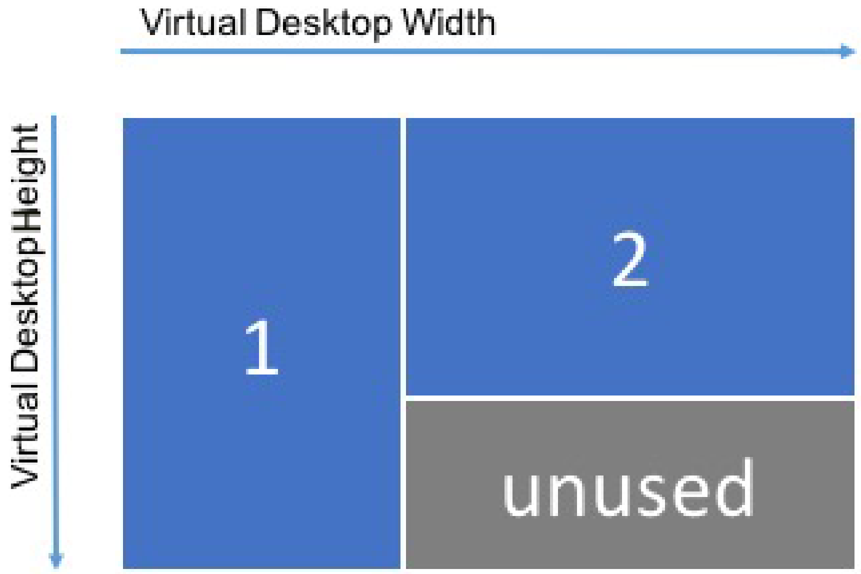
Knowing the maximum size of the virtual desktop for your client monitor configurations allow you to configure the Citrix VDA for macOS to be flexible in terms of client monitor configurations.

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 Citrix VDA for macOS 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 Citrix VDA for macOS virtual desktop to a size of 4160×2560.

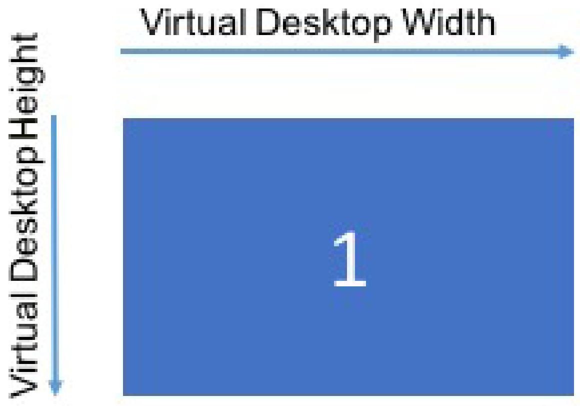
For the greatest flexibility in a multi-monitor configuration, find the smallest bounding rectangle of all monitor layouts you want to support. For configurations with two 2560×1600 monitors, the possible layouts include:

- **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 Citrix VDA for macOS

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:

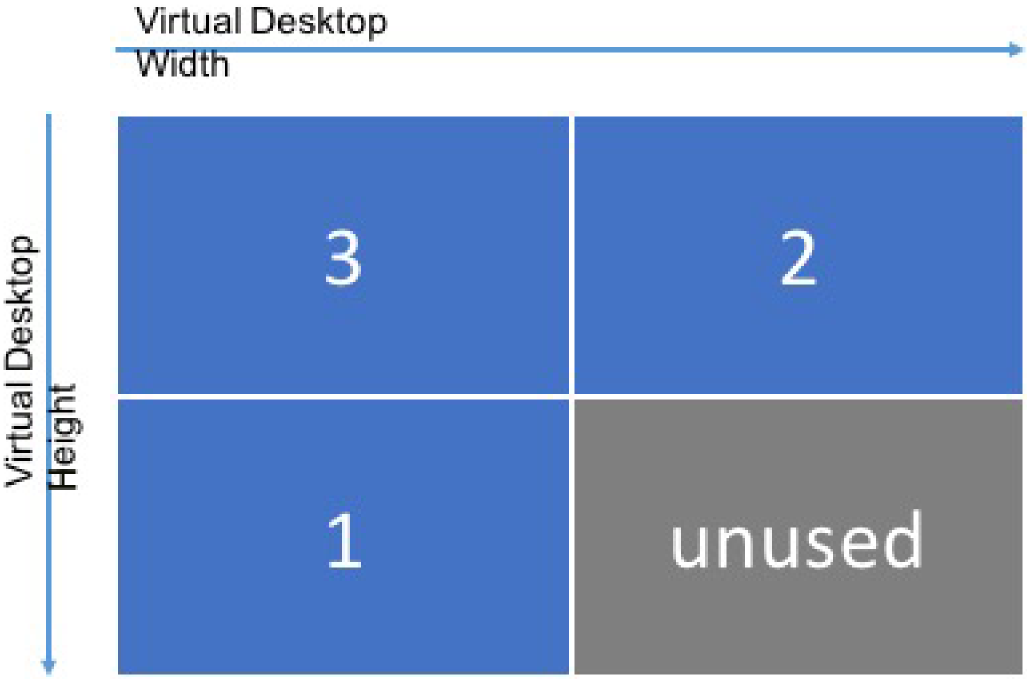
- **M** is the amount of memory used for session graphics.
- **X** is the width of the virtual session desktop.

- **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 Citrix VDA for macOS 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 Citrix VDA for macOS 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 Citrix VDA for macOS multi-monitor configuration

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

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
```

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
```

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
```

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

Thinwire Progressive Display

August 1, 2025

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.

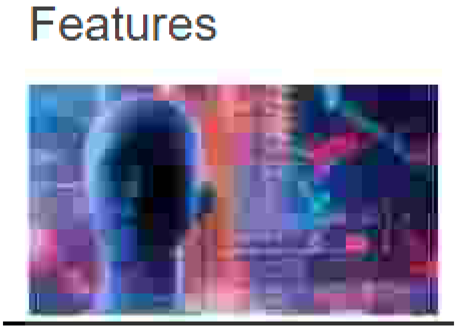
You were able to use policy settings to reduce bandwidth consumption by configuring the session to **Low** visual quality.

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

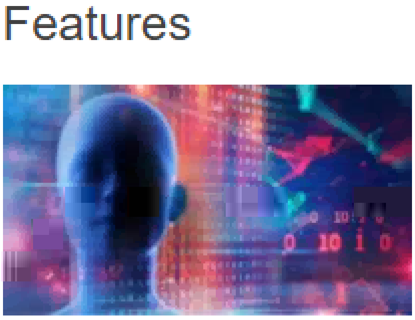
- Available bandwidth falls below 2 Mbps.
- Network latency exceeds 200 ms.

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
```

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
```

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
```

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

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

Selective Build to Lossless

macOS VDA support Intelligent Build to lossless (IBTL)

The general roadmap for Citrix HDX™ Graphics is working towards one consolidated intelligent graphics mode that is adaptable and suitable for all workloads and all circumstances.

IBTL (Intelligent build to lossless) is one of the steps we have been taking in that direction. With Intelligent Build-to-lossless, the Citrix graphics encoder decides based on screen activity and other metrics whether to switch one or more monitors into build-to-lossless.

Other monitors will continue to be encoded using the bandwidth efficient and high quality Thinwire+ encoder. If the screen activity ceases, the affected monitors will automatically be switched back to Thinwire+ encoding. No longer does the admin need to decide whether to use build-to-lossless for a particular workload, the decision is now made in real-time based on what the user is doing.

H265 support

Apple Silicon built-in H.265 (HEVC) encoder delivers superior performance with significantly higher compression efficiency for each frame compared to earlier codecs.

When used in macOS VDA, it enables substantially higher frame rates while simultaneously reducing bandwidth consumption, making it ideal for high-quality remote desktop experiences over constrained network connections. H.265 will be the default video codec for macOS VDA if the Citrix Workspace app side supports it.

Feature toggle

The codec policy "Use video codec for compression"can be leveraged to toggle between different graphic codec features. Setting this policy to "Use when preferred"enables the IBTL feature, which is also the default configuration.

> **Note:**
>
> Related policy settings might affect whether IBTL takes effect:
>
> *OptimizeFor3dWorkload = off (Default value is disabled), enable it will enable full screen H264. VisualQuality !=BuildToLossless (Default value is medium), select BuildToLossless will enable BuildToLossless.*

Related registry configuration at VDA side (for administrator reference):

- Disable IBTL:

  ```
  sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet
  \Control\Citrix\Thinwire"-t "REG_DWORD"-v "DisableSB2L"-d "0
  x00001"--force
  ```

- Enable indicator to monitor if IBTL feature works:

  ```
  sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet
  \Control\Citrix\Thinwire"-t "REG_DWORD"-v "SB2LIndicatorLocation"
  -d "0x00001"--force
  ```

Conditions IBTL is “engaged”or “disenaged”:

- Large transient graphics workload (by default, more than 75% of the surface).
- Frame processing time is too high (by default, 2.5x more than ideal frame time, only after bandwidth optimizations have been toggled off).
- Network connection with MacVDA is poor (Input FPS is stabilized and more than min_fps && Output FPS significantly less than Input FPS and there is a significant portion of the screen that is changing (> 25%)).
- IBTL exit: the input FPS is lower than configured minimum FPS for more than 10 seconds.

HDX™ Screen Sharing

August 1, 2025

Overview

Citrix VDA for macOS has the (HDX Screen Sharing) capability so you can share the screen of your macOS desktop to other session users (could be Windows or Linux VDA users on their respective virtual desktops) by generate secure screen sharing code & pass to others, so he/she could assist the session live; alternatively, Citrix VDA for macOS also allow you to assist/access others screen once you had acquired the code been generated in similar process; keyboard and mouse control is also part of the HDX Screen Sharing capabilities.

System requirements

- Install Qt 5 framework.

To align the unified user experience crossing all VDA regarding HDX Screen Sharing, you need install Qt framework, the minimal compatible version is Qt 5 (rev. 5.15.13 or later) ; install Qt 5 can be performed using, for example, homebrew by run following command:

brew install qt@5

- There must be network connectivity between the VDA hosting the session and the machines connecting to the shared sessions. Network port requirements are based on ICA ports in use (TCP/UDP 1494 or 2598) and the Screen sharing policy configuration (TCP 52525 to 52625 by default).

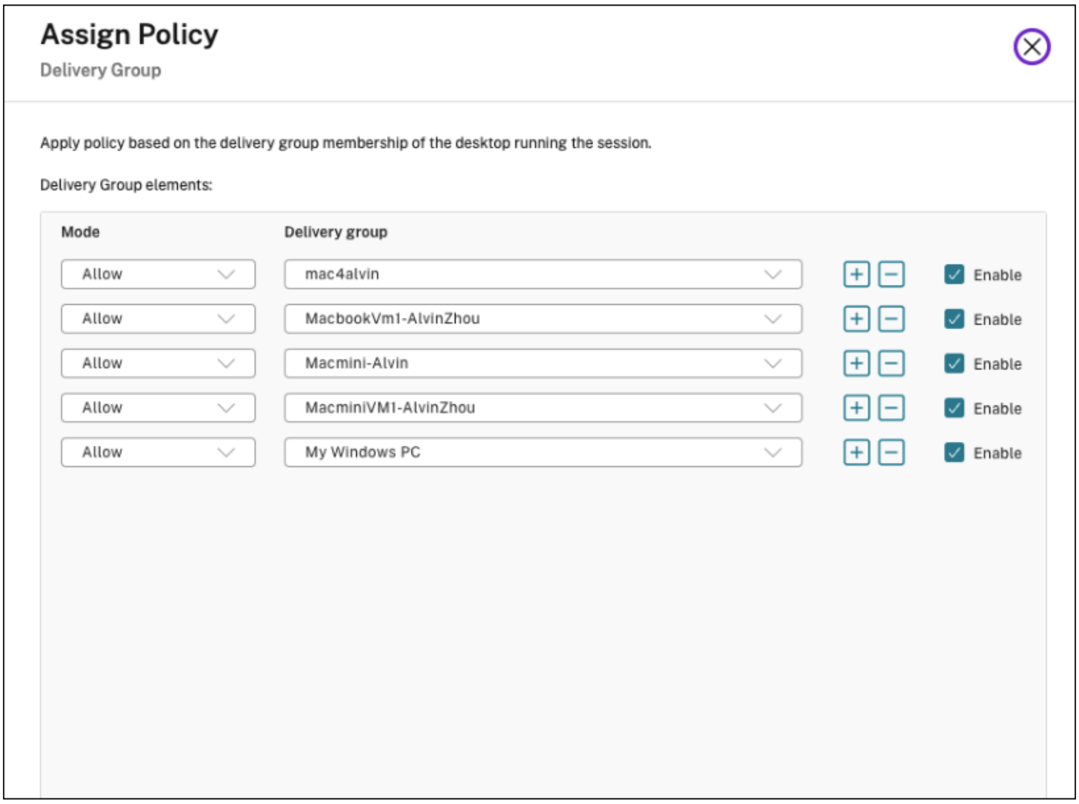
Configuration

1. Enable HDX Screen Sharing

   HDX screen sharing feature is disabled by default for security & privacy reasons. To enable it, complete the following settings:

   a) Enable the "Screen Sharing" policy in DaaS Console or CVAD Web Studio, the policy shall be configured for both "sharee" and "sharer" for sessions involved as below picture indicated.

   b) Allow TCP ports 52525–52625 inbound/outbound in your firewall. Refer Screen Sharing for more details.



Assign Policy

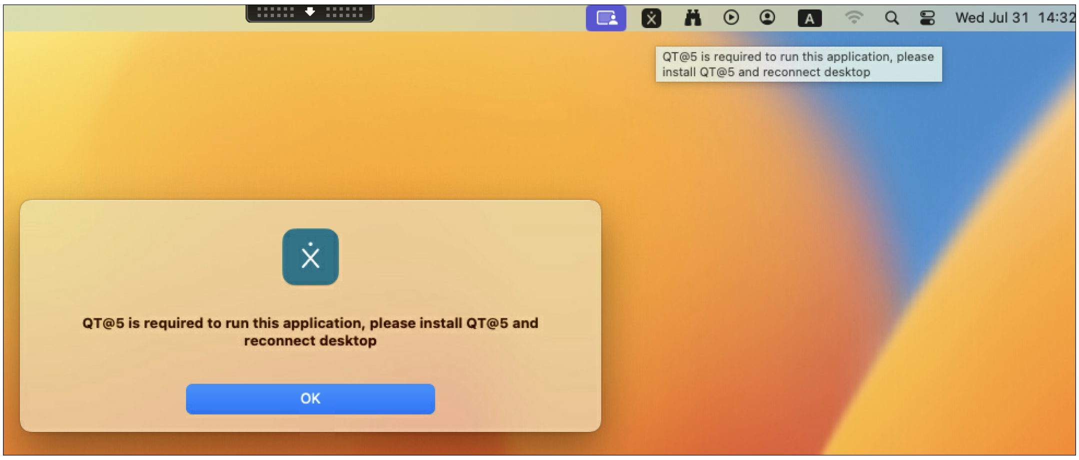
Delivery Group

Apply policy based on the delivery group membership of the desktop running the session.

Delivery Group elements:

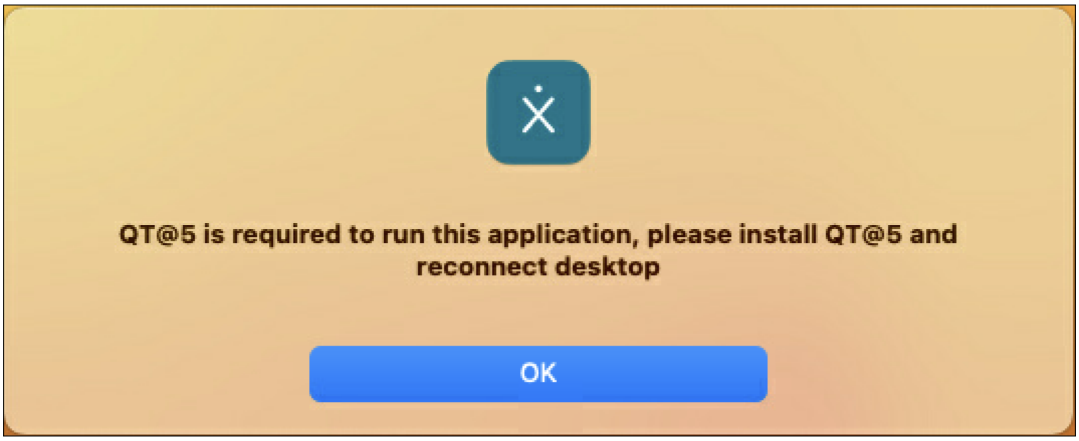
Mode	Delivery group		
Allow	mac4alvin	⊞ ⊟	☑ Enable
Allow	MacbookVm1-AlvinZhou	⊞ ⊟	☑ Enable
Allow	Macmini-Alvin	⊞ ⊟	☑ Enable
Allow	MacminiVM1-AlvinZhou	⊞ ⊟	☑ Enable
Allow	My Windows PC	⊞ ⊟	☑ Enable

When you enabled HDX Screen Sharing without install correctly Qt 5, when click the Screen Sharing icon in status as indicated.



QT@5 is required to run this application, please install QT@5 and reconnect desktop

QT@5 is required to run this application, please install QT@5 and reconnect desktop

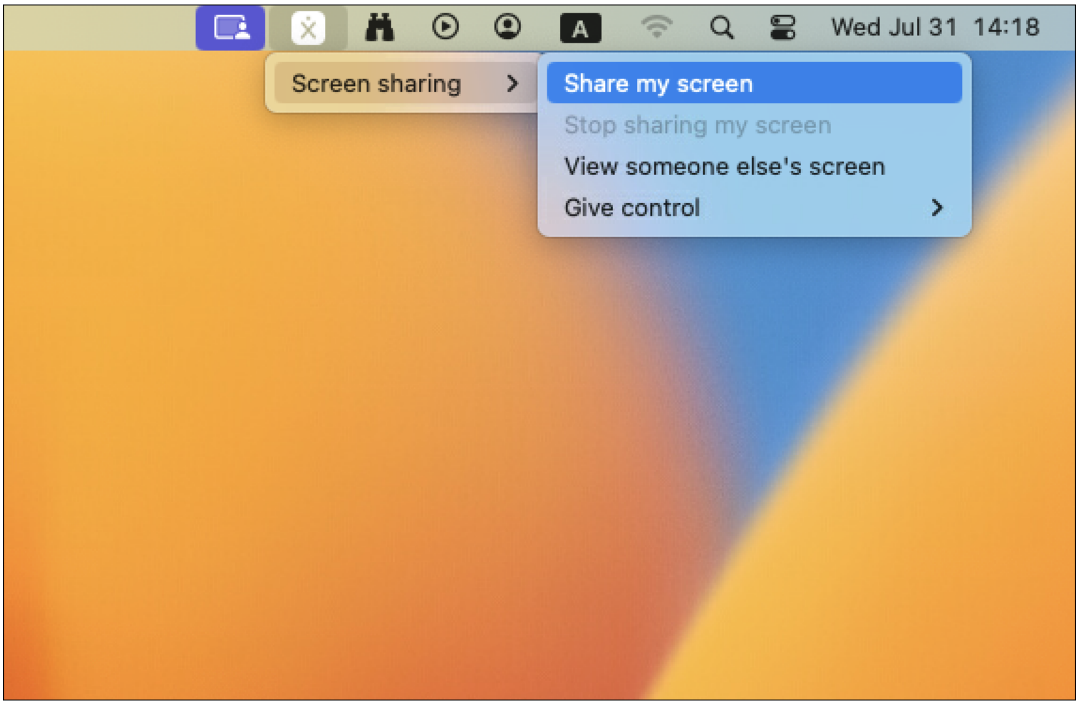


QT@5 is required to run this application, please install QT@5 and reconnect desktop

The following example walks you through the procedure of sharing a screen and viewing someone else's screen.

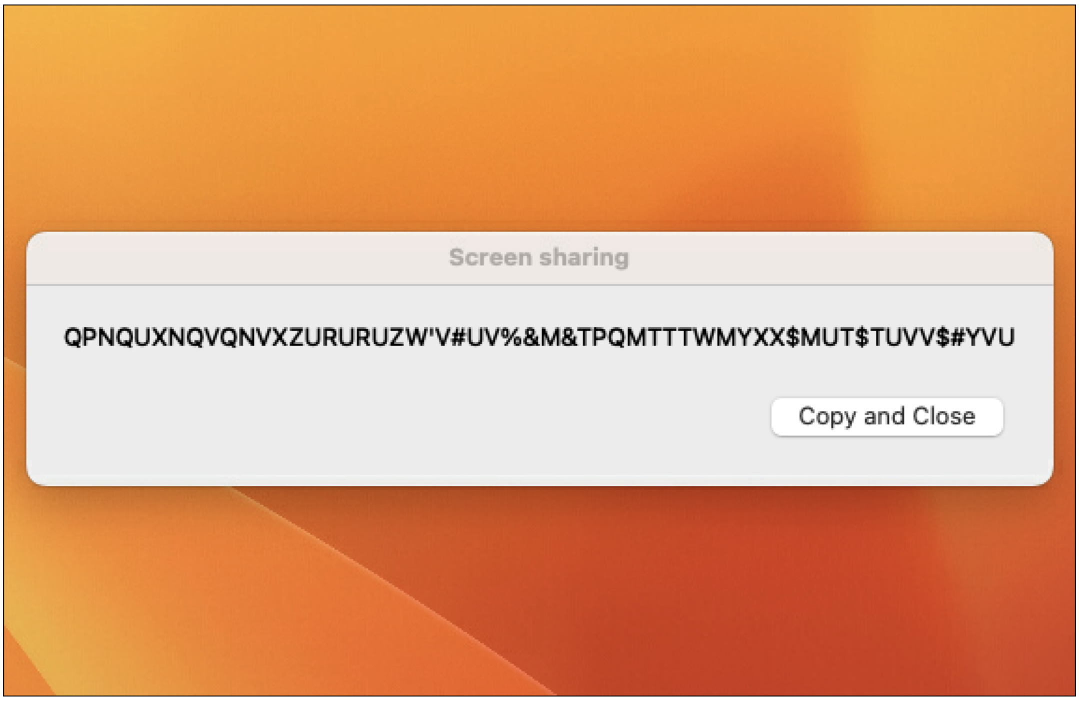
2. To share a screen.

   a) In the status bar of your virtual desktop, click the following system tray icon and select **Screen sharing > Share my screen**.



b) Click **Copy and Close**.

The current screen sharing code persists until you stop and restart sharing your screen.

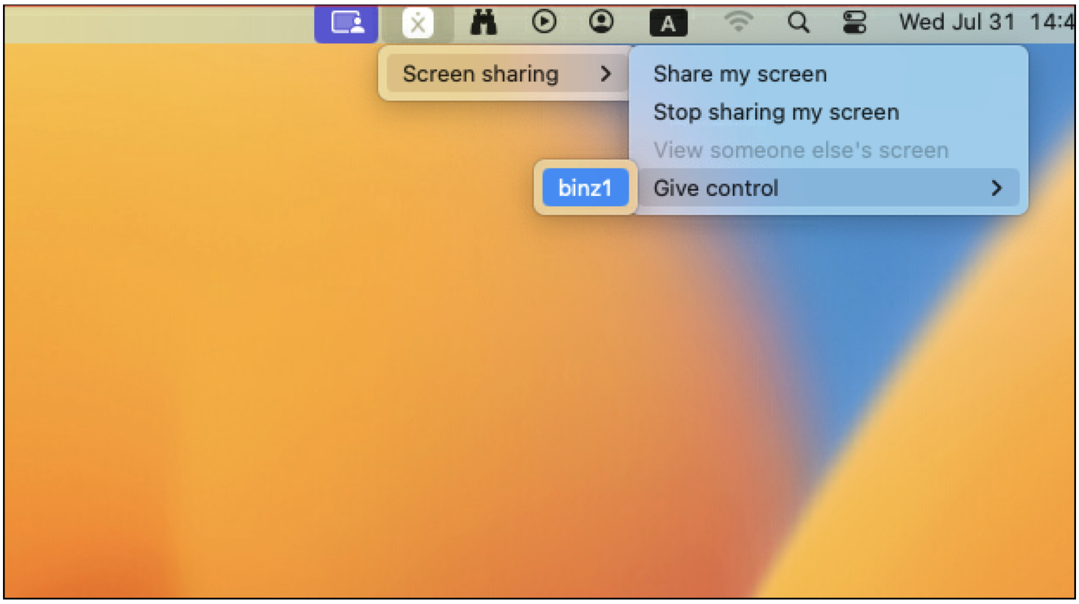


```
QPNQUXNQVQNVXZURURUZW'V#UV%&M&TPQMTTTWMYXX$MUT$TUVV$#YVU
```

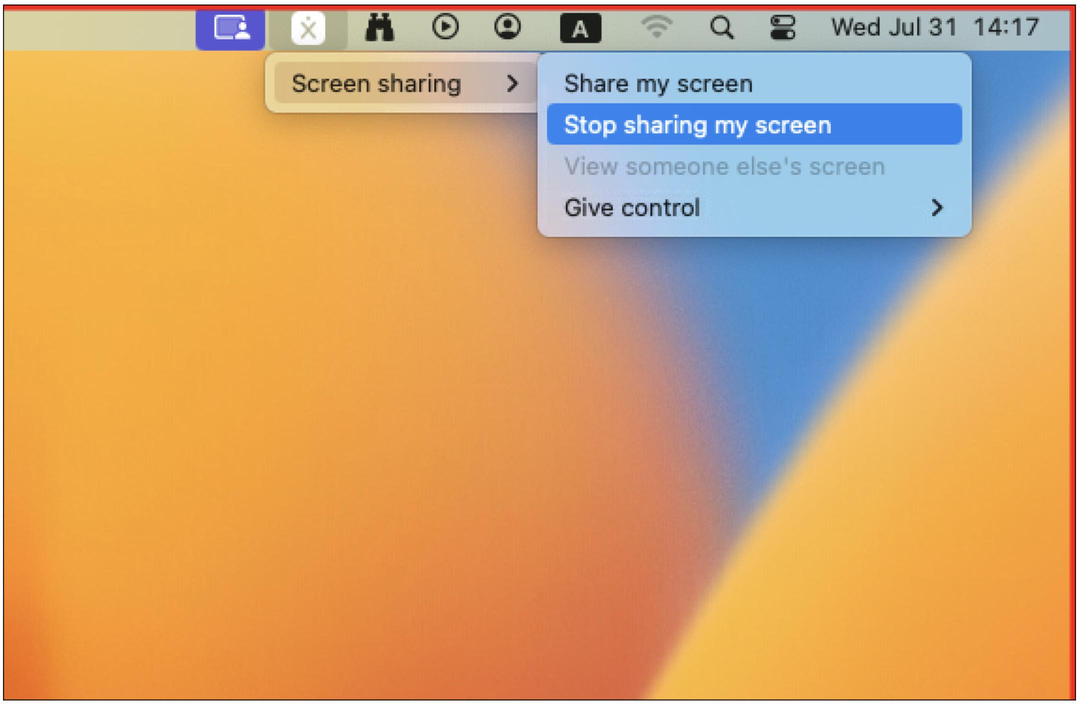
> **Note:**
>
> While you are sharing your screen, there is a red border around it, indicating that sharing is in progress.

c) Share the copied code with session users on other virtual desktops that you want to share your screen with.

d) To let a viewer control your screen, select **Give control** and then the viewer's name. To stop giving control, clear the viewer's name.

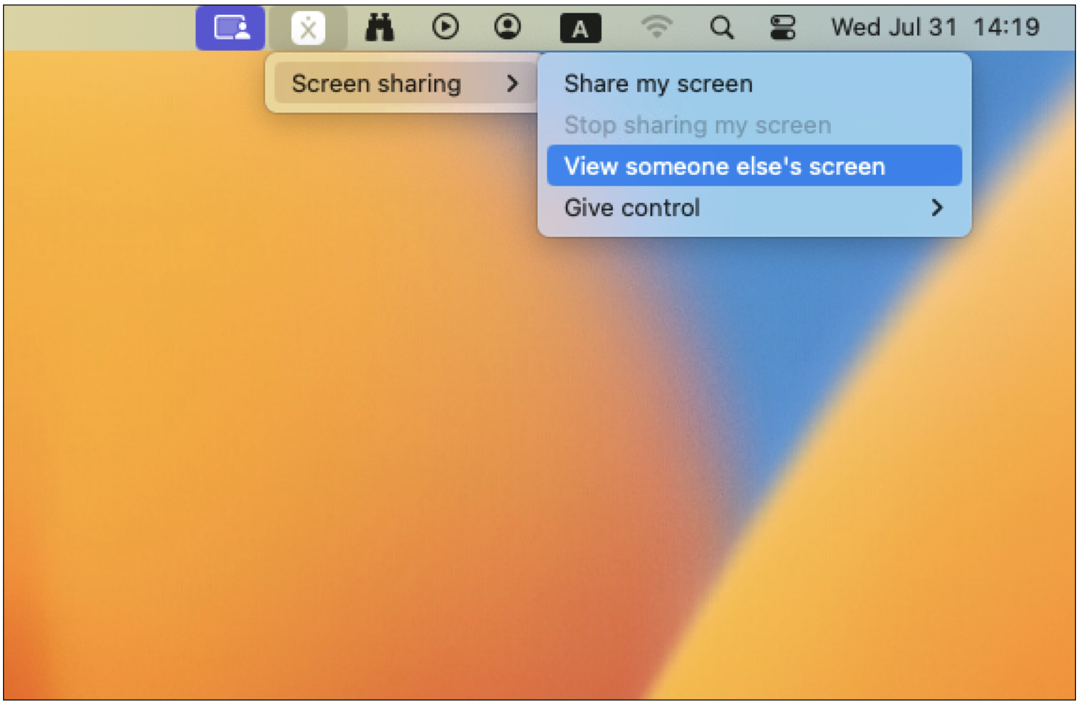


e) To stop sharing your screen, select Stop sharing my screen.

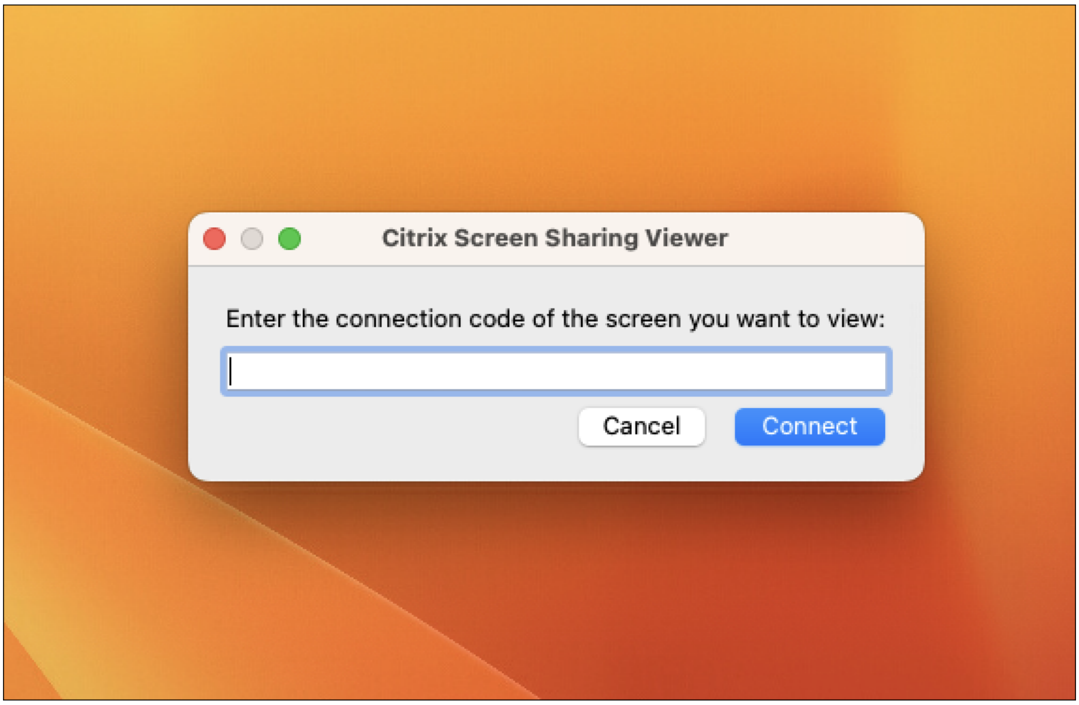


3. To view someone else's screen.

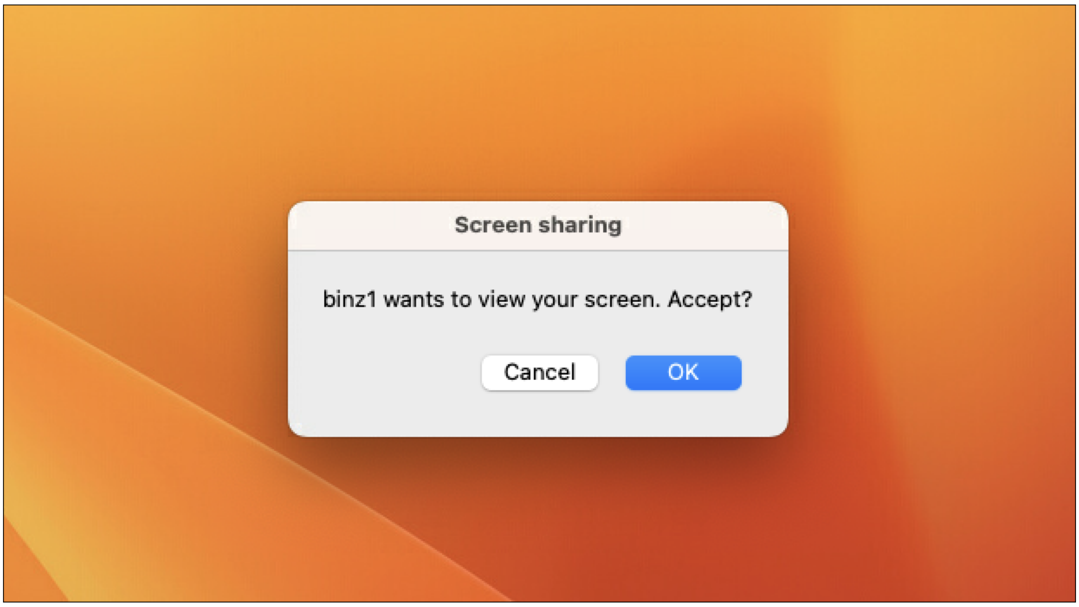
a) In the status bar of your virtual desktop, click the screen sharing icon and select View someone else's screen.



b) Enter the connection code of the screen that you want to view and then click Connect.


Citrix Screen Sharing Viewer
Enter the connection code of the screen you want to view:
Cancel
Connect

c) Wait for the screen sharer to accept your request. For example:

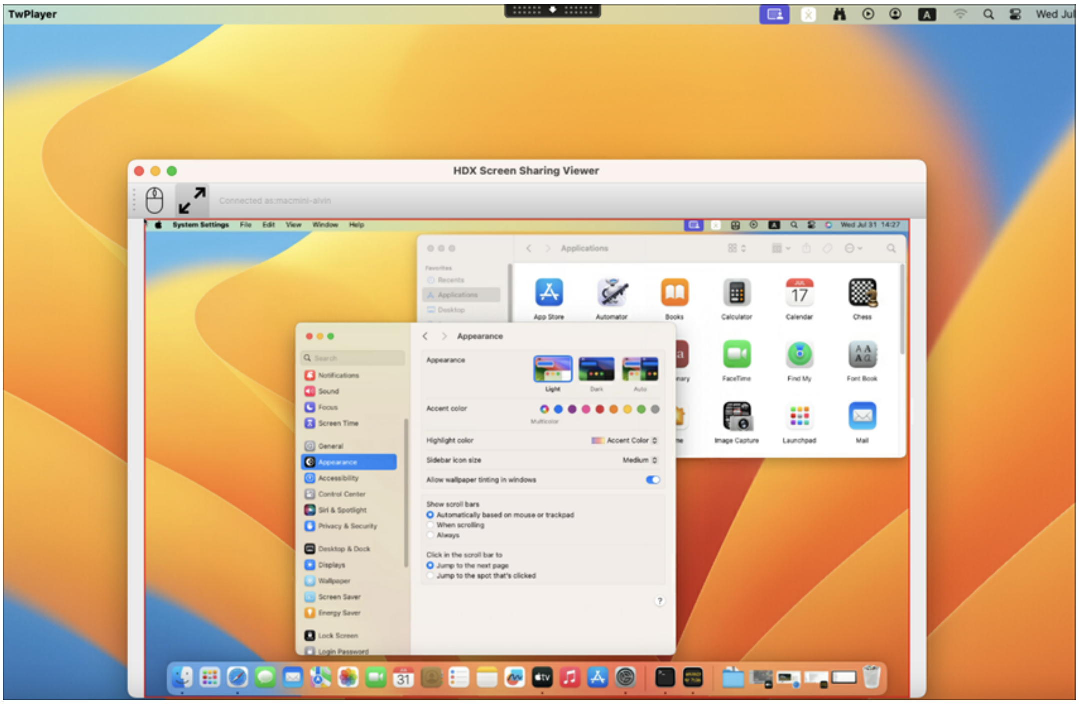


Screen sharing

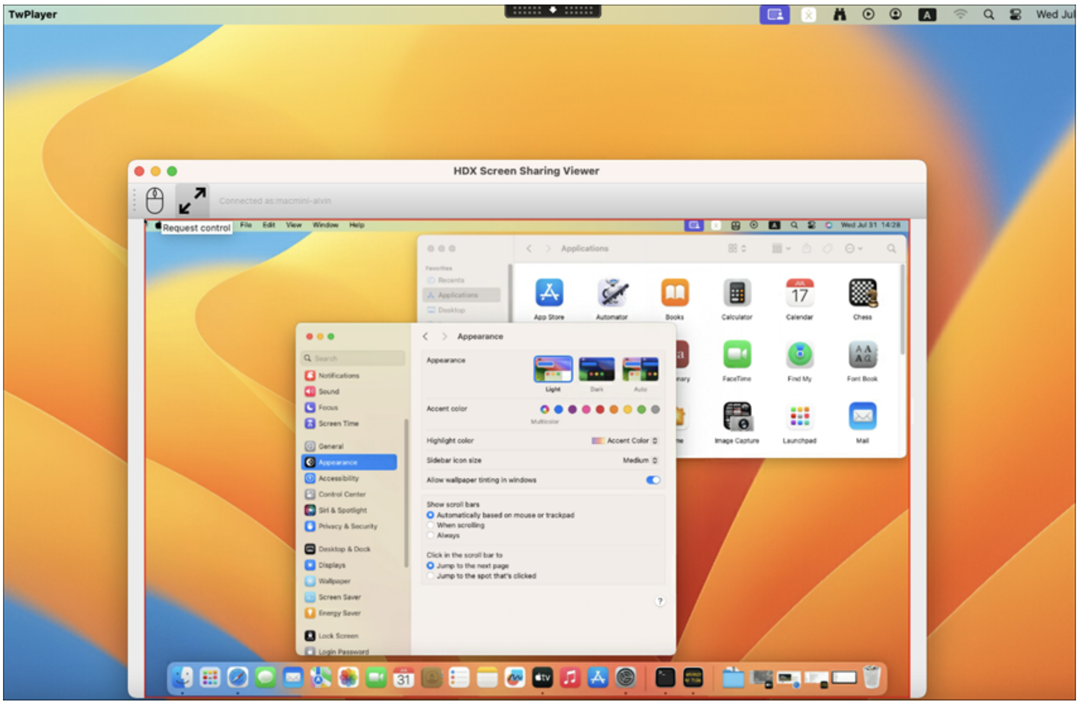
binz1 wants to view your screen. Accept?

> **Note:**
>
> On the sharer side, the MacOS system issues a notification of your request.
>
> If the sharer does not accept your request within 30 seconds, your request expires and a prompt appears.

a) After the screen sharer accepts your request by clicking OK, the shared screen appears in your Desktop Viewer. You are connected as a viewer with an automatically assigned user name.

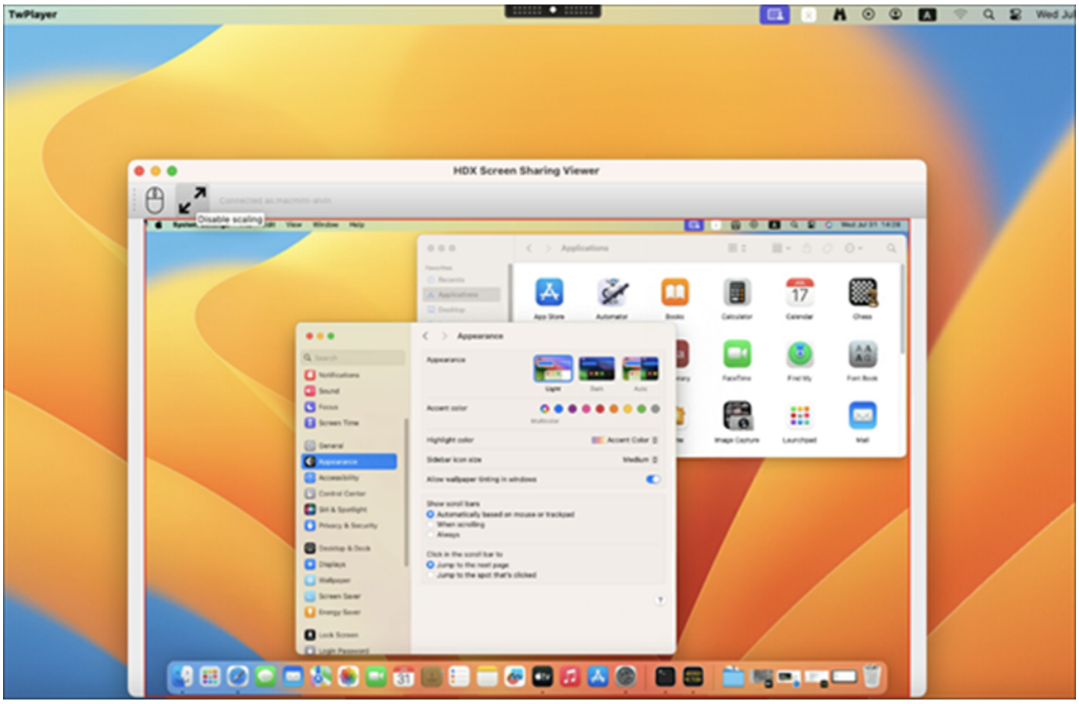


b) To request control over the shared screen, click the mouse icon in the upper left corner. Click the mouse icon again to release control over the shared screen.



> **Note:**
>
> If the sharer does not accept your request within 30 seconds, your request expires.
>
> Only one viewer is allowed to control a shared screen at a time.

c) To disable display scaling or scale to the window size, click the icon next to the mouse icon.



Considerations

The screen sharing feature does not support the H.265 video codec.

Users of desktop sessions can share their session screens with up to 10 viewers by default. The maximum number of viewers is configurable through `ctxreg update -k "HKLM\System\CurrentControlSet\Control\Citrix\Thinwire"-v "ScreenSharingViewerMaxNum"-d <hex_value>`.

When the maximum number is reached, a prompt appears when users try to accept extra connection requests.

> **Note:**
>
> The ScreenSharing Icon is shown as a menubar icon on the top right, the system would hide the last icon if there's not enough space on the menu bar when resizing the cwa viewer to a small one. To reveal the icon, it is recommended to resize the viewer to maximum and move the ScreenSharing icon to the right most by holding "Command"and then drag the icon to the right most, thus the ScreenSharing icon would be the last icon to be hidden if resolution decreased.

Keyboard

In this section, we give you details on

- Dynamic Keyboard Layout Synchronization
- Keyboard Layout Synchronization
- Keyboard Input Mode
- Support Mouse Button

Dynamic Keyboard Layout Synchronization

August 1, 2025

Previously, the keyboard layouts on the Citrix VDA for macOS 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

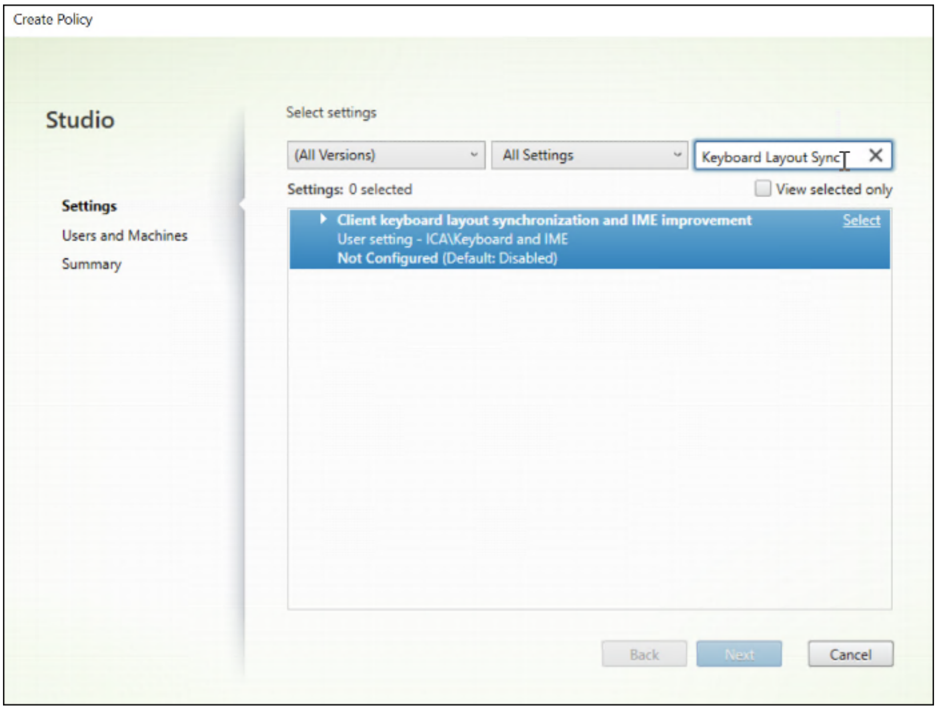
Group Policy

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 Citrix VDA for macOS apply to all sessions on that VDA.

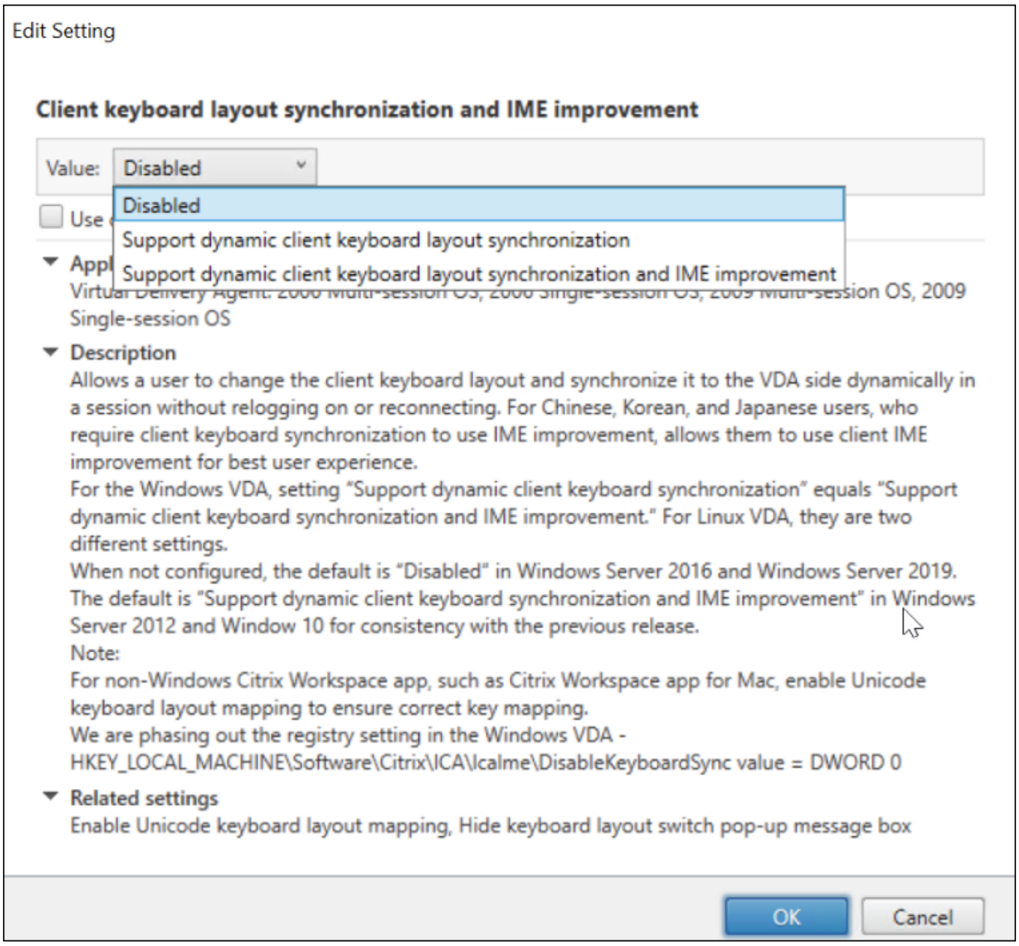
Set the **Client Keyboard Layout Sync** and **IME Improvement policy** to enable or disable the dynamic keyboard layout synchronization feature:

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**.



Edit Setting

Client keyboard layout synchronization and IME improvement

Value: Disabled

- Disabled
- Support dynamic client keyboard layout synchronization
- Support dynamic client keyboard layout synchronization and IME improvement

□ Use

Appl

Virtual Delivery Agent: 2006 Multi-session OS, 2006 Single-session OS, 2009 Multi-session OS, 2009 Single-session OS

Description

Allows a user to change the client keyboard layout and synchronize it to the VDA side dynamically in a session without relogging on or reconnecting. For Chinese, Korean, and Japanese users, who require client keyboard synchronization to use IME improvement, allows them to use client IME improvement for best user experience.

For the Windows VDA, setting "Support dynamic client keyboard synchronization" equals "Support dynamic client keyboard synchronization and IME improvement." For Linux VDA, they are two different settings.

When not configured, the default is "Disabled" in Windows Server 2016 and Windows Server 2019. The default is "Support dynamic client keyboard synchronization and IME improvement" in Windows Server 2012 and Window 10 for consistency with the previous release.

Note:

For non-Windows Citrix Workspace app, such as Citrix Workspace app for Mac, enable Unicode keyboard layout mapping to ensure correct key mapping.

We are phasing out the registry setting in the Windows VDA - HKEY_LOCAL_MACHINE\Software\Citrix\ICA\Icalme\DisableKeyboardSync value = DWORD 0

Related settings

Enable Unicode keyboard layout mapping, Hide keyboard layout switch pop-up message box

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 Citrix VDA for macOS.

Registry Setting

To enable dynamic keyboard layout Sync without Citrix Policy listed above enabled, set **KeyboardSyncMode** to **2** under the key `HKLM\Software\Citrix\VirtualDesktopAgent\mac\kbime` by ctxreg

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

August 1, 2025

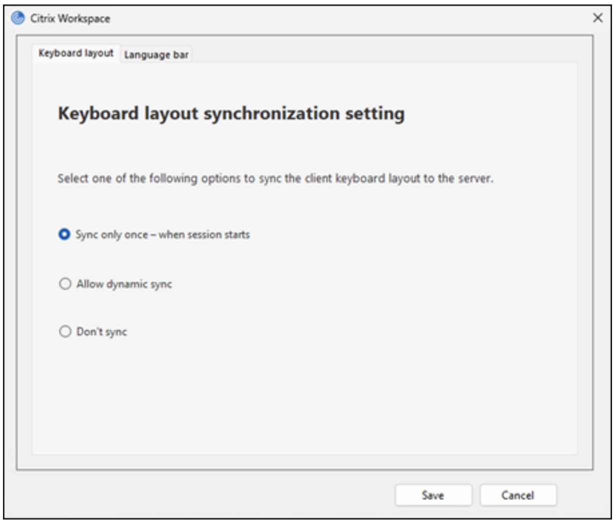
Keyboard layout synchronization enables users to have the same keyboard layout on the Citrix VDA for macOS and the client device, to guarantee the input experience.

As of the Citrix VDA for macOS Version, Citrix has added support for synchronizing client-side keyboard layout to Citrix VDA for macOS 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.



Keyboard layout synchronization setting

Select one of the following options to sync the client keyboard layout to the server.

● Sync only once – when session starts

○ Allow dynamic sync

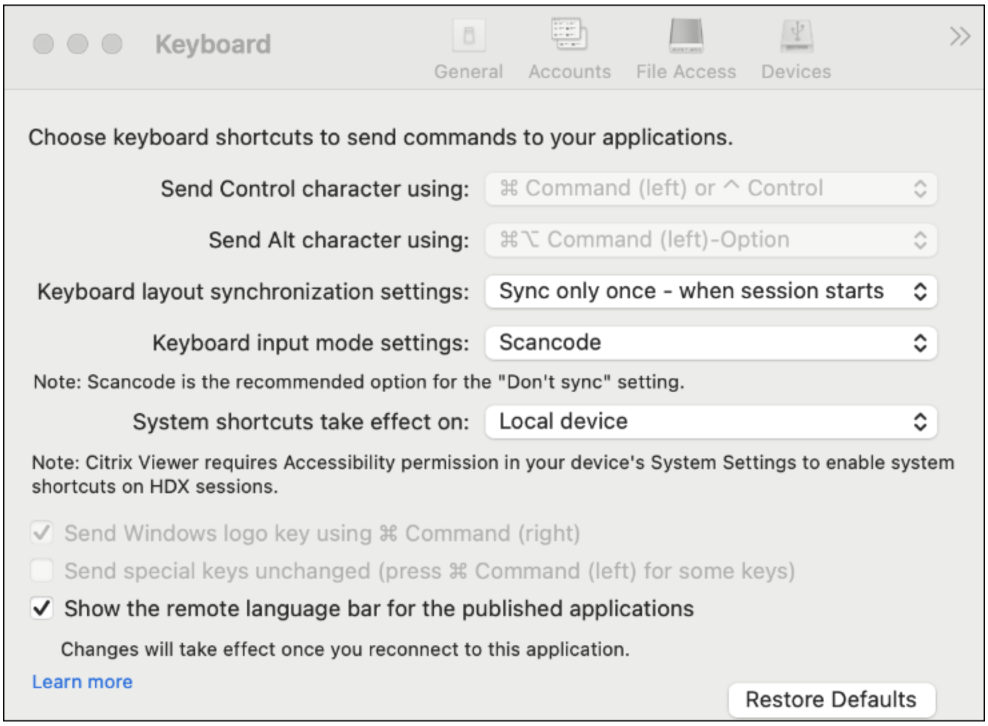
○ Don't sync

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

Citrix Workspace App for macOS

1. Open **Citrix Workspace App Preferences**.

2. Select **Keyboard**.



Choose keyboard shortcuts to send commands to your applications.

Send Control character using: ⌘ Command (left) or ^ Control

Send Alt character using: ⌘⌥ Command (left)-Option

Keyboard layout synchronization settings: Sync only once - when session starts

Keyboard input mode settings: Scancode

Note: Scancode is the recommended option for the "Don't sync" setting.

System shortcuts take effect on: Local device

Note: Citrix Viewer requires Accessibility permission in your device's System Settings to enable system shortcuts on HDX sessions.

☑ Send Windows logo key using ⌘ Command (right)

□ Send special keys unchanged (press ⌘ Command (left) for some keys)

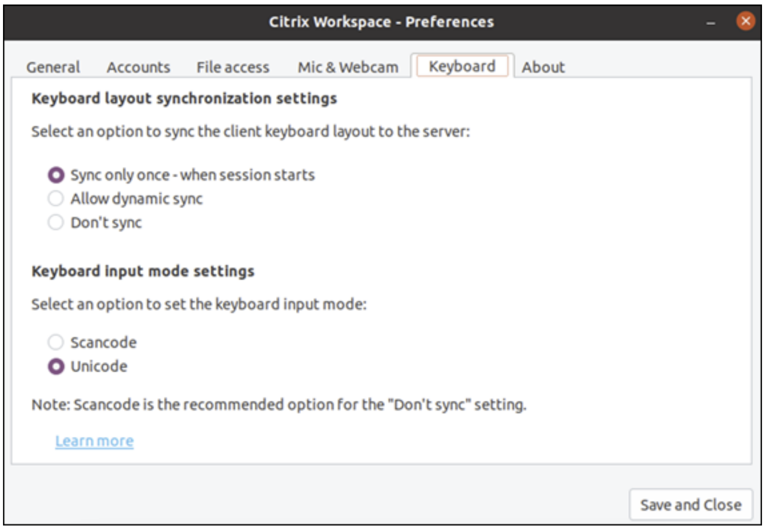
☑ Show the remote language bar for the published applications

Changes will take effect once you reconnect to this application.

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**.



Keyboard layout synchronization settings

Select an option to sync the client keyboard layout to the server:

● Sync only once - when session starts
○ Allow dynamic sync
○ Don't sync

Keyboard input mode settings

Select an option to set the keyboard input mode:

○ Scancode
● Unicode

Note: Scancode is the recommended option for the "Don't sync" setting.

Learn more

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

Keyboard Input Mode

August 1, 2025

Citrix VDA for macOS 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.

Although Citrix has added support for both Scancode and Unicode in Citrix VDA for macOS, **Scancode Mode** is more recommended for better user experience with shortcuts passthrough.

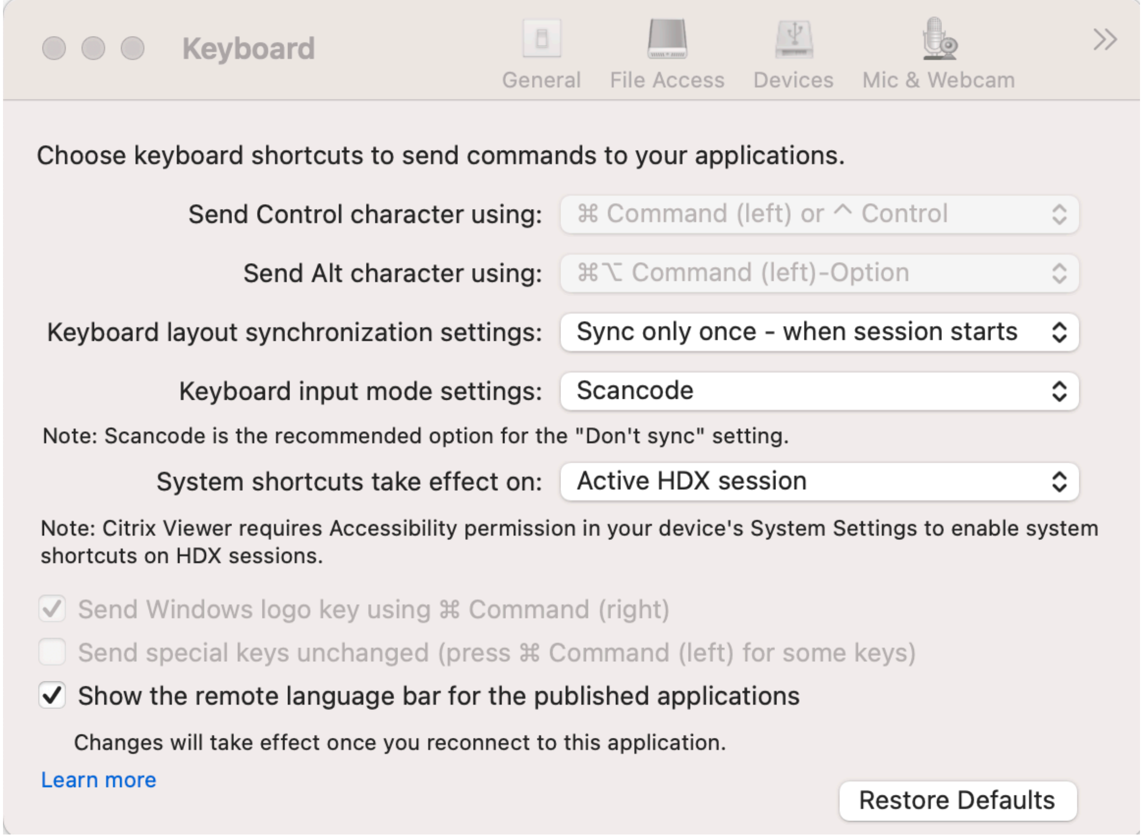
Configuration from Citrix Workspace™ App

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**.



Choose keyboard shortcuts to send commands to your applications.

Send Control character using: ⌘ Command (left) or ^ Control

Send Alt character using: ⌘⌥ Command (left)-Option

Keyboard layout synchronization settings: Sync only once - when session starts

Keyboard input mode settings: Scancode

Note: Scancode is the recommended option for the "Don't sync" setting.

System shortcuts take effect on: Active HDX session

Note: Citrix Viewer requires Accessibility permission in your device's System Settings to enable system shortcuts on HDX sessions.

☑ Send Windows logo key using ⌘ Command (right)

□ Send special keys unchanged (press ⌘ Command (left) for some keys)

☑ Show the remote language bar for the published applications

Changes will take effect once you reconnect to this application.

Learn more

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 **Active HDX™ Session** 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 Citrix VDA for macOS sessions. See Workspace App for Mac

Support mouse side buttons

August 1, 2025

Overview

Some mouse devices have two side buttons that can be clicked by thumb.

They are recognized as 'button 4'and 'button 5'if connected to a Mac device.

In remote Citrix VDA for macOS sessions, these two buttons are now supported, they also work as 'button 4'and 'button 5', some applications can utilize these buttons by default, check those applications' manual for how-to.

The mouse side buttons offer more functionality for users, enhancing productivity and streamlining interactions.

In Citrix VDA for macOS sessions, these buttons can be customized to support various tasks, within the hosting macOS system.

Features

Location: Side buttons are usually on the left side of the mouse, accessible by the thumb.

Functionality: Depends on application support, these buttons can be configured to perform specific actions to navigate backward or forward in a web browser, run macros, or trigger custom commands.

Example like:

Basic Navigation

Back and Forward Navigation:

Also known as the fourth and fifth button, most commonly configured to move forward and backward in the web browsers.

Back Button:

Navigate to the previous page or item within supported applications.

Forward Button:

Move to the next page or item in supported applications.

Custom Commands

Application-Specific Functions
Users can assign custom commands to side buttons for applications running within Citrix VDA for macOS, such as opening files or running specific tasks.

Audio

December 23, 2025

- Loss tolerant mode for audio
- Audio Quality Enhancer
- Audio Diagnostic Tool

Loss tolerant mode for audio

December 22, 2025

Starting with the 2411 version, loss tolerant mode supports audio.

This feature enhances the user experience for real-time streaming and improves audio quality over EDT when users are connecting through a network with latency and packet loss.

For more information about the loss tolerant mode and EDT, see Additional information in the Citrix Virtual Apps and Desktops documentation.

Loss tolerant mode for audio is enabled by default. If disabled or to re-enable, complete the following steps:

1. Enable HDX adaptive transport (EDT).
2. Enable loss tolerant mode for audio.

Client requirements and settings

The following are the minimum Citrix Workspace™ app versions that support loss tolerant mode:

- Citrix Workspace app for Windows 2309
- Citrix Workspace app for Linux 2311
- Citrix Workspace app for Mac 2311

In addition, please note the following:

- (Optional) For direct connections between Citrix Workspace app and VDA, enabling DTLS on VDAs is required.
- (Optional) For remote connections, loss tolerant mode must also be supported on the Citrix Gateway Service or NetScaler Gateway.

> **Note:**
>
> The following audio transport options are available over UDP:
>
> - Audio over UDP
> - HDX™ Adaptive Transport (Enlightened Data Transport)
>
> For MacVDA, we only support EDT Audio which is also UDP based but built-in capability.

Audio Quality Enhancer (AQE)

February 9, 2026

Audio Quality Enhancer for EDT loss tolerant mode

Starting with the 2507 version, audio quality enhancer is enabled by default for adaptive audio over EDT loss tolerant mode for audio.

Audio quality enhancer maintains clear audio during brief network disruptions. This feature adapts to the network conditions to ensure consistent audio performance during playback and recording.

> **Note:**
>
> Adaptive audio must be enabled for this feature to work.

Audio Quality Enhancer for reliable transport (preview)

Starting with 2507 in Tech Preview, audio quality enhancer is also available for connections over reliable transport (i.e. TCP and EDT-Reliable). Under poor network conditions, both audio playback and recording will have a smoother experience with reduced latency.

To enable the feature, complete the following steps

1. Enable the feature on the Mac VDA.

   Run the following command in the terminal:

   ```
   sudo /opt/Citrix/VDA/bin/ctxreg create -k "HKLM\System\CurrentControlSet
   \Control\Citrix\VirtualChannels\Audio"-v "fAlwaysUseSpeexJitterBuffer
   "-t REG_DWORD -d 0 –force
   ```

2. Enable the feature on Citrix Workspace app for Mac.

   Run the following command in the terminal:

   ```
   defaults write com.citrix.receiver.nomas AlwaysUseSpeexJitterBuffer
    -bool NO
   ```

To disable the feature, complete the following steps

1. Disable the feature on the Mac VDA.

   ```
   Run the following command in the terminal:
   ```

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

2. Disable the feature on Citrix Workspace app for Mac.

   Run the following command in the terminal:

   ```
   defaults write com.citrix.receiver.nomas AlwaysUseSpeexJitterBuffer
    -bool YES
   ```

> **Note:**
>
> - Adaptive audio must be enabled for this feature to work.
> - This feature is disabled by default in Tech Preview (over reliable transport).
> - This feature must be enabled on both VDA and CWA.
> - This feature is supported with Citrix Workspace app for Mac version 2508 and later.

Audio diagnostic command line tool

August 1, 2025

The audio diagnostic command line tool on the VDA can be used to query session data related to audio policies, configuration, and data transport.

Usage

1. Open a command prompt and run `ctxaudiosession` from the `/opt/Citrix/VDA/bin` folder.
   - Running the tool will display all active ICA® session(s) audio information and devices redirection status for the current user.

Output

The tool outputs various configuration settings that can help diagnose audio-related issues within a session.

Section	Description
Warning	Audio service warning messages for device statuses, transport type, audio codec, etc.
State Information	Audio state, version, codecs, transport applied to the current session(s), etc.
Policy Settings	Audio policies applied to the current session(s).
Local Settings	Audio related configuration stored in the registry or local settings.

Section	Description
Capabilities	Audio capabilities results between the CWA and VDA.
Sounds Devices	Device names, their roles, and their running statuses in the session(s).

Session

December 23, 2025

In this section, we give you details on

- Proxy PAC File Support
- Session Reliability
- Rendezvous V2
- Supportability Service
- Shield v2
- Auto Client Reconnect

Rendezvous V2

August 1, 2025

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 Citrix VDA for macOS.

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.

How to disable Rendevous V2

1. 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`

> **Note:**
>
> - Rendezvous V2 must be configured in context of using Citrix DaaS and when Citrix Gateway Service (Cloud Gateway Services:https://docs.citrix.com/en-us/citrix-gateway-service/get-started-with-citrix-gateway-service) is used for HDX session broking etc.
> - To register and enroll Citrix VDA for macOS, the default VDA's behavior is to connect to the Citrix Gateway Service regardless Rendezvous V2 is enabled or not.

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

August 1, 2025

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:

- 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
   ```

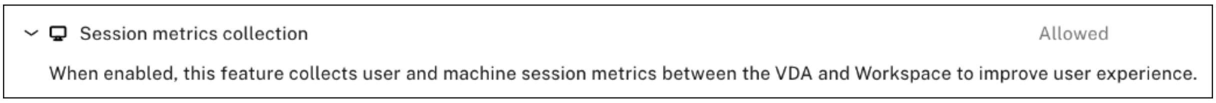
   If there is no TCP listener on the session reliability port, enable the listener by running the following command.

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

Supportability Service

August 1, 2025

When connecting to Citrix VDA for macOS from Citrix Workspace App, anonymous diagnostic information is collected and available to assist further troubleshooting and/or improve end user experience, to disable the supportability data collection or understand more about what has been collected, please follow below procedures:
The supportability data collection is enabled by default, you can stop data point collection by:



Session metrics collection — Allowed

When enabled, this feature collects user and machine session metrics between the VDA and Workspace to improve user experience.

- Prohibit policy "Session metrics collection"in Web Studio

To enable supportability data collection, please allow DDC policy “Session metrics collection” again.

For more details and background regarding supportability service, see Policy Default Settings

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 Citrix VDA for macOS
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
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

Data Point	Key Name	Description
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 values mean 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"}
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"}

Data Point	Key Name	Description
Active keyboard layout	VDAKeyboardLayout	The input source name that getting active in a session, including the ones that dynamically Synced in

Auto Client Reconnect (ACR)

August 1, 2025

Overview

Allowing automatic client reconnection (ACR), so users can resume their session where they were interrupted when the connection was broken. Automatic reconnection detects broken connections and then reconnects the users to their sessions.

Policy Settings

This release implements to support the following policies for Auto Client Reconnect:

- Auto client reconnect
- Auto client reconnect authentication
    - by default ACR authentication is not required. In this case, for Citrix VDA for macOS, Single Sign On(SSO) feature must be enabled, see SSO Authentication.
- Auto client reconnect timeout
- Reconnect UI transparency level

For more policy details, see Auto Client Reconnect.

HDX™ Direct

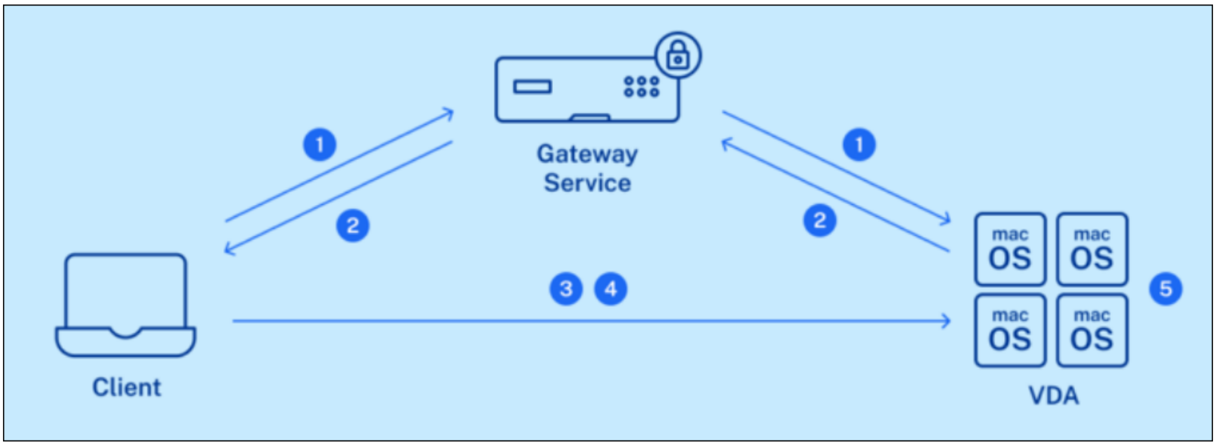
August 1, 2025

Overview

When accessing macOS VDA from within an enterprise's intranet or externally with Citrix Workspace™ app, HDX Direct allows client (CWA) devices to establish a secure and direct connection with the VDA bypassing Citrix Gateway Service or NetScaler® Gateway. When direct communication can be established. It can help organizations achieve the following advantages:

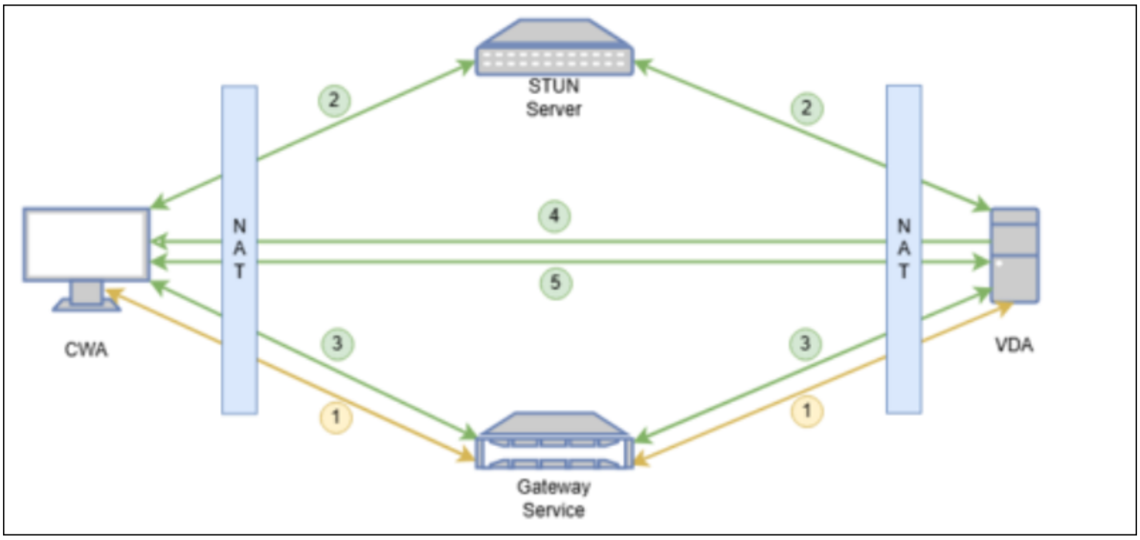
- Reducing bandwidth consumption by establishing a secure and direct user session traffic between VDA and Client.
- Adding resiliency to the session when CGS (Citrix Gateway Service) goes down.
- Improving session performance by avoiding connecting through an intermediary.

How HDX Direct works for internal client



1. CWA establishes an HDX session to VDA through the Gateway Service.
2. Both CWA and VDA send STUN requests to STUN servers to discover their public IPs and Ports. And STUN server responses to CWA and VDA with their corresponding public IPs and ports.
3. CWA and VDA exchange their public IPs and ports through existing HDX sessions.
4. VDA sends UDP packets to the CWA's public IP and port.
5. After receiving UDP packets from VDA, CWA establishes a direct DTLS connection with VDA and the session is transferred to the new connection.

How HDX Direct works for client outside intranet



1. CWA establishes an HDX session to VDA through the Gateway Service.
2. Both CWA and VDA send STUN requests to STUN servers to discover their public IPs and Ports. And STUN server responses to CWA and 1. VDA with their corresponding public IPs and ports.
3. CWA and VDA exchange their public IPs and ports through existing HDX sessions.
4. VDA sends UDP packets to the CWA's public IP and port.
5. After receiving UDP packets from VDA, CWA establishes a direct DTLS connection with VDA and the session is transferred to the new connection.

STUN protocol is a protocol widely used for identifying an endpoint's IP address and port allocated by a NAT. Once the initial connection is established, Hdx-Direct public IP discovery is triggered on both CWA and VDA. This involves the endpoints communicating to STUN server using STUN protocol and finding their corresponding public IP addresses. The following image depicts such communication:

STUN Server User can configure local registry to specify STUN Servers which can be used by MacVDA.

Num	Reg Path	Reg Key	Comments
1	HKLM\Software\Citrix\HdxDirect	StunServers	Use “;”to separate multiple STUN Servers.
2	HKLM\System\CurrentControlSet\Control\Citrix\Wds\icawd\HdxDirect	CitrixStunServers	Used to identify if a specified STUN server is hosted by Citrix and use “;”to separate multiple STUN Servers.

If user does not configure STUN Servers in local registry, below default STUN Servers are used by MacVDA.

STUN Server Address	Port	Host by Citrix
stun.l.google.com	19302	No
stun.cloud.com	3478	Yes
stun-azure.nssvctesting.net	3478	Yes
stun-aws.citrixngsk8sdev.net	3478	Yes
stunserver.stunprotocol.org	3478	No

Configuration

HDX Direct is disabled by default. To enable this feature, you can configure the Citrix DDC policies below, please also refer to macOS VDA policy support list for details:

- HDX Direct: enable or disable this feature.
- HDX Direct mode: configure if HDX Direct is available for internal clients or for both internal and external clients. For HDX Direct support in this release, both modes are supported, but it's available for internal clients only.

Validation

To check whether a HDX session is working with HDX Direct, run the `/opt/Citrix/VDA/bin/ctxsession -v` command in the terminal.

If HDX Direct is working from an internal client, HDX Direct State shows `Connected - Internal` .

If HDX Direct is working from an external client, HDX Direct State shows `Connected - External` .

Troubleshooting

If Citrix DDC policies are configured, but HDX session doesn't work with HDX Direct, check if the policies are applied to the current macOS VDA by the tool hdxmonitor:

```
sudo hdxmonitor network dump
```

The result will show if HDX Direct is applied or not.

Once confirmed, HDX Direct will work in the next new HDX connection. Go to the policy support list for more information on HDX Direct policies.

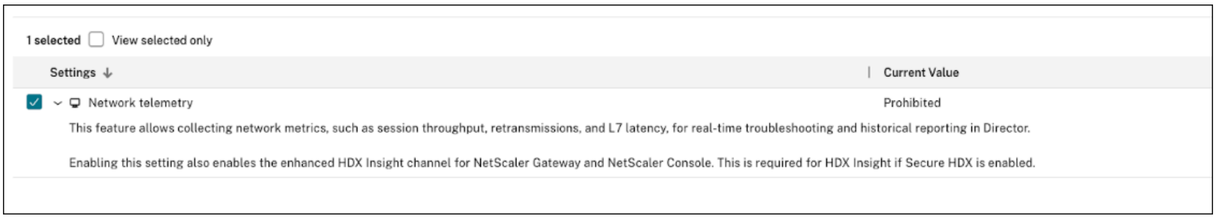
> **Note:**
>
> Hdx-Direct for external users is only available with EDT (UDP) as the transport protocol. Therefore, Adaptive Transport must be enabled.

HDX™ Insight support

August 1, 2025

macOS VDA now supports secure HDX which is the end-to-end encrypted solution for ICA traffic, when enabled, HDX Insight capability & Smart Control (e.g. Configure ICA Access Profile) feature from NetScaler is also supported through in-band CGP protocol.

Please toggle the new policy named "Network telemetry"to turn on/off this feature. Default value for this policy is "Prohibited".



1 selected □ View selected only

Settings ↓	Current Value
☑ ⌄ Network telemetry This feature allows collecting network metrics, such as session throughput, retransmissions, and L7 latency, for real-time troubleshooting and historical reporting in Director. Enabling this setting also enables the enhanced HDX Insight channel for NetScaler Gateway and NetScaler Console. This is required for HDX Insight if Secure HDX is enabled.	Prohibited

Shield v2

December 22, 2025

Overview

MacVDA support Shield V2 feature. Compared to Shield V1, Shield V2 is connector-less, cloud-connector doesn't participate into the work-flow. And Shield V2 support:

1. Session launch when Daas or Workspace outage
2. New session launch type "Connection Lease"
3. Offline mode MacVDA desktop access

Policy Setting

- Daas should open shield related feature-toggles to support shield v2 connection leasing type session launch
- Citrix Workspace shield feature setting to download and update related cache files.
- No policy setting for Shield V2 feature of MacVDA

Some local registry settings in clxmtp service:

```
create -k "HKLM\Software\Citrix\ClxMtpService" -t "REG_DWORD" -v "
    ClxMtpSvcEnabled" -d "0x00000001" --force
create -k "HKLM\Software\Citrix\ClxMtpService" -t "REG_DWORD" -v "
    ClxMtpValidationBypass" -d "0x00000001" --force
create -k "HKLM\Software\Citrix\ClxMtpService" -t "REG_DWORD" -v "
    ClxMtpFsmLogLevel" -d "0x00000003" --force
create -k "HKLM\Software\Citrix\ClxMtpService" -t "REG_DWORD" -v "
    ClxMtpTimeoutInMilliSeconds" -d "0x00002710" --force
```

Requirements and limitations

Management Plane

- Supported in all editions of Citrix DaaS with Citrix Workspace.
- Not supported for Citrix Workspace with site aggregation to on-premises Virtual Apps and Desktops.
- Not supported when on-premises Citrix Gateway is used as an ICA Proxy. (Using Citrix Gateway Service as a Workspace authentication method is supported.)

User device requirements

Minimum supported Citrix Workspace app versions:

- Citrix Workspace app for Windows 2106
- Citrix Workspace app for Linux 2106
- Citrix Workspace app for Mac 2106
- Citrix Workspace app for Android 22.2.0
- Citrix Workspace app for iOS 22.4.5
- Citrix Workspace app for ChromeOS 2301

For users who access their apps and desktops using browsers:

- Citrix Workspace app 2109 for Windows at a minimum. Supported with Google Chrome and Microsoft Edge.
- Citrix Workspace app for Mac version 2112 at a minimum for use with Google Chrome.
- Citrix Workspace app for Windows (Store) is not supported.

If using connectorless VDAs:

- Citrix MacVDA 2511 release.

Security

December 23, 2025

- Lock Screen Support
- Secure ICA 2.0
- Session watermark

Secure ICA 2.0

August 1, 2025

macOS VDA support Secure ICA 2.0

The Secure ICA 2.0 Feature evolves from the original Secure ICA. The main drawback of the original Secure ICA was its susceptibility to MITM attacks, which Secure ICA 2.0 addresses. In addition, the up-to-date Advanced Encryption Standard (AES) cipher is used. One key aspect of Secure ICA 2.0 vs. network-level encryption (TLS or DTLS) is the ability to provide true end-to-end encryption (E2EE) between the Citrix Workspace App (CWA) and the VDA. This means that no intermediate network elements (including the Citrix Gateway) are able to decrypt the ICA traffic.

Phase	Algorithm
key exchange	ECDHE
authentication	RSA

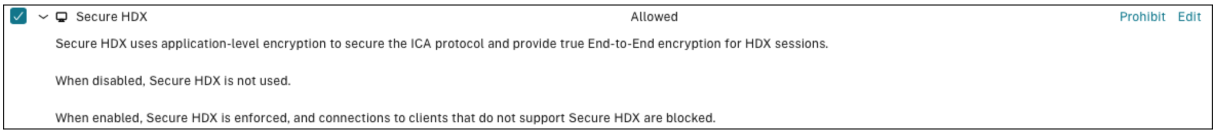
Phase	Algorithm
session cipher	AES-256
cipher-block dependency and additional options	GCM
message authentication	SHA256

Network encryption consideration

Network level encryption and Secure ICA 2.0 are complementary: customers can choose to enable both simultaneously.

Feature toggle/Group policy

The feature toggle **Secure HDX** policy, is designed to turn on/off this feature.



☑ Secure HDX Allowed

Secure HDX uses application-level encryption to secure the ICA protocol and provide true End-to-End encryption for HDX sessions.

When disabled, Secure HDX is not used.

When enabled, Secure HDX is enforced, and connections to clients that do not support Secure HDX are blocked.

Backward compatibility & limitation

Capability negotiation is performed during the ICA® initialization phase, so this feature is compatible with old versions; macOS VDA does not support "Shield"at the moment, so currently we support "non-Shield"scenarios. In "non-Shield"mode, VDA self-signed certificate is provided to CWA via a trusted path, while in "Shield"mode, VDA self-signed certificate is provided to CWA via CLXMTP protocol.

Lock Screen Support

August 1, 2025

Lock Screen is a built-in macOS security feature that automatically secures the system during periods of inactivity.

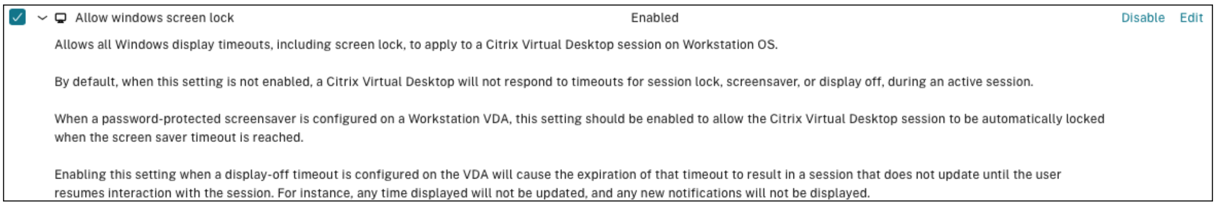
Users can customize various aspects of this behavior, including activating the screen saver or turning off the display after user-defined timeout intervals. These settings are essential for maintaining security and protecting privacy.

Lock Screen is turned off by default as the design of VDA encourages continuity of rendering session traffic.

Now with this feature, we”™re providing these capabilities:

- Screen saver can be activated, keyboard and mouse can exit screen saver
- Password authentication after returning from screen saver

Feature toggle a policy named *“AllowWindowsScreenLock”* to turn on/off. The default value for this policy is *“Disabled”*.



☑ Allow windows screen lock | Enabled | Disable Edit

Allows all Windows display timeouts, including screen lock, to apply to a Citrix Virtual Desktop session on Workstation OS.

By default, when this setting is not enabled, a Citrix Virtual Desktop will not respond to timeouts for session lock, screensaver, or display off, during an active session.

When a password-protected screensaver is configured on a Workstation VDA, this setting should be enabled to allow the Citrix Virtual Desktop session to be automatically locked when the screen saver timeout is reached.

Enabling this setting when a display-off timeout is configured on the VDA will cause the expiration of that timeout to result in a session that does not update until the user resumes interaction with the session. For instance, any time displayed will not be updated, and any new notifications will not be displayed.

Limitations

- Display off is not supported; we instead use display off timeout values to trigger the screen saver.
- Changes to system Lock Screen settings require a session disconnect and reconnect to take effect.

Session watermark

December 22, 2025

Overview

Session watermarks are a crucial security feature designed to deter and track data theft. This is achieved by embedding traceable information, such as user ID, date and time, or session ID, directly into the visual display of the session desktop.

Enabling this feature may increase network bandwidth and CPU usage. We recommend you configure and test the session watermark on different hardware devices for optimal settings before rolling out in large scale - to achieve better user experience, don’t enable more than two watermark text items.

Enable session watermark

When you enable this setting, the session display has an opaque textual watermark displaying session-specific information.

The other watermark settings depend on this one being enabled. Session watermark is disabled by default.

Include client IP address

When you enable this setting, the session displays the current client IP address as a watermark.

By default, Include client IP address is disabled.

Include connection time

When you enable this setting, the session watermark displays a connect time. The format is **yyyy/mm/dd hh:mm**. The time displayed is based on the system clock and time zone.

By default, Include connection time is disabled.

Include logon user name

When you enable this setting, the session displays the current logon user name as a watermark. We recommend that the user name is a maximum of 20 characters.

By default, Include logon user name is enabled.

Include VDA host name

When you enable this setting, the session displays the VDA host name of the current ICA session as a watermark.

By default, Include VDA host name is enabled.

Include VDA IP address

When you enable this setting, the session displays the VDA IP address of the current ICA session as a watermark.

By default, the VDA IP address is disabled.

Session watermark style

This setting controls whether you display a single watermark text label or multiple labels. Choose Multiple or Single from the Value drop-down menu.

Multiple displays up to five watermark labels in the session. One in the center and four in the corners.

Single displays a single watermark label in the center of the session.

By default, the Session watermark style is Multiple.

Custom watermark text

This setting lets you apply custom text (for example, the corporate name) to display in the session watermark. When you configure a non-empty string, it displays the text in a new line appending other information enabled in the watermark.

The watermark custom text is limited to 25 Unicode characters. If you configure a longer string, it is truncated to 25 characters.

> **Note:**
>
> There is no default text.

You can add more customization using custom tags in the text.

As a result, the maximum number of characters in the custom text will be increased to 1024.

The available tags for watermark settings are described in the following table:

Tag	Description	Example
<font=value>	Allows you to change the font of watermark text. The value is the name of a font available on the VDA.	<font=Courier New>
<fontzoom=value>	Allows you to set the percentage of the font zoom factor. The value is 200 for 200% zoom on watermark text.	<fontzoom=200>
<position=value>	Allows you to change the position of the watermark text. The values are center, topleft, topright, bottomleft, and bottomright. This tag is only applicable with single style.	<position=topright>

Tag	Description	Example
<rotation=value>	Allows you to rotate watermark text. The value is specified in degree and the range is from -360 and 360.	<rotation=45>
<style=value>	Allows you to change the display style. This tag overrides the Session watermark style policy.	<style=single>

The following watermark styles are available:

- Single style - one single watermark text label appears at the center of the session. You can use the position tag to change the location.
- Multiple style –up to five watermark labels appear in the session - one in the center and one in each corner.
- Tile - Multiple labels appear in the session. Watermark text is placed equally across the entire screen.

The available tags for changing watermark text are described in the following table:

Tag	Description
	The IP address of the endpoint.
	The date the session was established.
	The domain name of the logged-in user account.
	The machine name of the VDA.
	Creates an extra line.
	The IP address of the VDA.
	The time the session was established.
	The name of the user.

- The Watermark custom text policy takes effect only when the Enable session watermark policy is enabled. Its default value is Disabled.
- If you use the tags for changing watermark text, all other session watermark policies, except Enable session watermark, are ignored. If you use the tags for watermark text settings, you can use all other watermark policies.

Watermark transparency

You can specify watermark opacity from 0 through 100. The larger the value specified, the more opaque the watermark.

> **Note:**
>
> By default, the value is 17.

To adjust the user experience, use the Session Watermark policy settings to configure the placement and watermark appearance on the screen.

> **Note:**
>
> If a user presses the **Print Screen** key to capture the screen, the screen captured at the VDA side doesn't include the watermarks. We recommend that you take measures to avoid the captured image being copied.

Policy Support List

December 23, 2025

Configure Citrix® policies to control user access and session environments. Citrix policies are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of users, devices, or connection types. Each policy can contain multiple settings. You can use the following tool with Citrix policies:

- **Web Studio**. If you are a Citrix administrator without permission to manage group policy, use Web Studio to create policies for your site. Policies that are created using Web Studio are stored in the site database, and the updates are pushed to the VDA either when that VDA registers with the broker or when a user connects to that VDA.

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
ICA keep alives	SendICAKeepAlives	computer	ICA \ Keep Alive	Do not send ICA keep alive messages (0)	reboot
ICA keep alive-time-out	ICAKeepAliveTimeout	computer	ICA \ Keep Alive	60 seconds	reboot
ICA® listener port number	IcaListenerPortNumber	computer	ICA	1494	reboot
HDX™ Adaptive Transport	HDXoverUDP	computer	ICA	Preferred (2)	reboot
Rendezvous protocol	RendezvousProtocol	computer	ICA	Prohibited	reboot
Session reliability connections	AcceptSessionReliabilityConnections	computer	ICA \ Session Reliability	Allowed (1)	reboot

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Session reliability port number	SessionReliabilityPort	computer	ICA\ Session Reliability	2598	reboot
Session reliability timeout	SessionReliabilityTimeout	computer	ICA\ Session Reliability	180s	reboot
Auto Client Reconnect	AllowAutoClientReconnect	computer	ICA\ Auto Client Reconnect	Allowed (1)	reboot
Reconnection UI transparency level	ReconnectionUiTransparencyLevel	computer	ICA\ Auto Client Reconnect	80%	reboot
Client audio redirection	AllowAudioRedirection	user	Audio	Allowed (1)	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Client microphone redirection	AllowMicrophoneRedir	user	Audio	Allowed (1)	new connection
Client clipboard redirection	AllowClipboardRedir	user	Clipboard	Allowed (1)	new connection
Target minimum frame rate	TargetedMinimumFramesPerSecond	user	ThinWire	10 fps	new connection
Target frame rate	FramesPerSecond	user	ThinWire	30 fps	new connection
Visual quality	VisualQuality	user	ThinWire	Medium (3)	new connection
Use video codec for compression	VideoCodec	user	ThinWire	Use when preferred (3)	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Allow visually lossless compression	AllowVisuallyLosslessCompression	user	ThinWire	Disabled (0)	new connection
Preferred color depth for simple graphics	PreferredColorDepth	user	ThinWire	24 bits per pixel(1)	new connection
ICA round trip calculation	IcaRoundTripCheckEnabled	user	ICA\End User Monitoring	Enabled (1)	new connection
ICA round trip calculation internal	IcaRoundTripCheckPeriod	user	ICA\End User Monitoring	15	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
ICA round trip calculations for idle connections	IcaRoundTripCheckWhenIdle	user	ICA\End User Monitoring	Disabled (0)	new connection
Session idle timer	EnableSessionIdleTimer	user	Session Timers	Enabled (1)	new connection
Session idle timer interval	SessionIdleTimerInterval	user	Session Timers	1440 minutes	new connection
Disconnected session timer	EnableSessionDisconnectTimer	user	Session Timers	Disabled (0)	new connection
Disconnected session timer interval	SessionDisconnectTimerPeriod	user	Session Timers	1440 minutes	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Client keyboard synchronization land IME improvement	ClientKeyboardLayoutSyncAndIME	User	Keyboard & IME	Disabled (0)	new connection
Overall session bandwidth limit	LimitUSBBw	User	ICA\Bandwidth	0	new connection
Audio redirection bandwidth limit	LimitAudioBw	User	ICA\Bandwidth	0	new connection
Audio redirection bandwidth limit percent	LimitAudioBwPercent	User	ICA\Bandwidth	0	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Client USB device redirection bandwidth limit	LimitUSBBw	User	ICA\Bandwidth	0	new connection
Client USB device redirection bandwidth percent	LimitUSBBwPercent	User	ICA\Bandwidth	0	new connection
Clipboard redirection bandwidth limit	LimitClipbdBW	User	ICA\Bandwidth	0	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Client USB device redirection rules	USBDeviceRules	User	USB	0	new connection
Clipboard redirection bandwidth limit percent	LimitClipbBWPercent	User	ICA\Bandwidth	0	new connection
Client USB device redirection	AllowUSBRedir	User	USB	Prohibited (0)	new connection
Screen sharing	ScreenSharing	User	Screen Sharing	Disabled (0)	new connection
Loss tolerant mode for audio	LossTolerantAudio	User	Audio	Disabled (0)	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Auto client reconnect timeout	ACRTimeout	computer	ICA \ Auto Client Reconnect	120s	new connection
Auto client reconnect authentication	ACRRequireAuth	computer	ICA \ Auto Client Reconnect	Do not require authentication	new connection
Clipboard selection update mode	ClipboardSelectionUpdateMode	user	Clipboard	Selections are updated on both client and host	new connection
Restrict client clipboard write	RestrictClientClipboardWrite	user	Clipboard	False	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Restrict session clipboard write	RestrictSessionClipboardWrite	user	Clipboard	false	new connection
Client clipboard write allowed formats	ClientClipboardWriteAllowedFormats	user	Clipboard	“\0”	new connection
Session clipboard write allowed formats	SessionClipboardWriteAllowedFormats	user	Clipboard	“\0”	new connection
Auto-create client printers	AutoCreateClientPrinters	user	Printer	All(3)	new connection
Auto-create generic universal printers	AutoCreateGenericUPDPrinter	user	Printer	Disabled (0)	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect							
Auto-create PDF Universal Printer	AutoCreatePDFPrinter	user	Printer	Disabled (0)	new connection							
Hdx Direct	HDXDirect	computer	HdxDirect	Prohibited (0)	new connection							
Hdx Direct Mode	HDXDirectMode	computer	HdxDirect	internal only	new connection							
Client Printer Redirection	AllowPrinterRedir	user	Printer	Enabled (1)	new connection							
Client USB device redirection rules (Version 2)	USBDeviceRulesV2	user	USB	“	Client USB device redirection rules (Version 2)	USBDeviceRulesV2	user	USB	“\0”	new connection	”	new connection
Secure HDX	SecureHDX	computer	SecureHDX	Disabled (0)	new connection							

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Network Telemetry	EnableGatewayStatusMonitoring	computer	Virtual Delivery Agent Settings \ Monitoring	Prohibited (0)	new connection/reconnect
Allow windows screen lock	AllowWindowsScreenLock	computer	Graphics	Disabled (0)	new connection
Enable session watermark	EnableSessionWatermark	user	Session Watermark	Disabled	new connection
Include client IP address	IncludeClientIPAddress	user	Session Watermark	Disabled	new connection
Include connection time	IncludeConnectTime	user	Session Watermark	Disabled	new connection

Citrix Policy	Key name	Type	Module	Default Value	When takes Effect
Include logon user name	IncludeLogonUsername	user	Session Watermark	Enabled	new connection
Include VDA host name	IncludeVDAHostName	user	Session Watermark	Enabled	new connection
Include VDA IP address	IncludeVDAIPAddress	user	Session Watermark	Disabled	new connection
Watermark custom text	WatermarkCustomText	user	Session Watermark	N/A	new connection
Session watermark style	WatermarkStyle	user	Session Watermark	Multiple	new connection
Watermark transparency	WatermarkTransparency	user	Session Watermark	17	new connection

> **Note:**
>
> For Client clipboard write allowed formats, currently, the release includes support for the following formats: CF_UNICODETEXT, CF_DIB
>
> For Session clipboard write allowed formats, currently, the release includes support for the following formats: CF_TEXT, CF_UNICODETEXT, CF_BITMAP, CF_DIB, CF_DIBV5

Known Issues

September 7, 2025

In this section, we provide details on

- Limitations
- Troubleshooting Guide

Limitations

January 19, 2026

Citrix Graphics Service:

When deploying Citrix VDA for macOS on macOS 15 or later, you may encounter a new prompt to allow **Citrix Graphics Services** even if the service has been allowed before.

This prompt will happen every month for each user. For macOS VDA 25.07 or later user, you can suppress this by following the step-15 in Use the Installer of Citrix VDA for macOS.

It will not impact Citrix VDA for macOS to function even when it is ignored but however, for better user experience, we recommend enterprise administrator to suppress this prompt by running or automating the following command in terminal for each user (make sure you have Full Disk Access to the Terminal app before running the command).

For a user, who has never encountered this prompt:

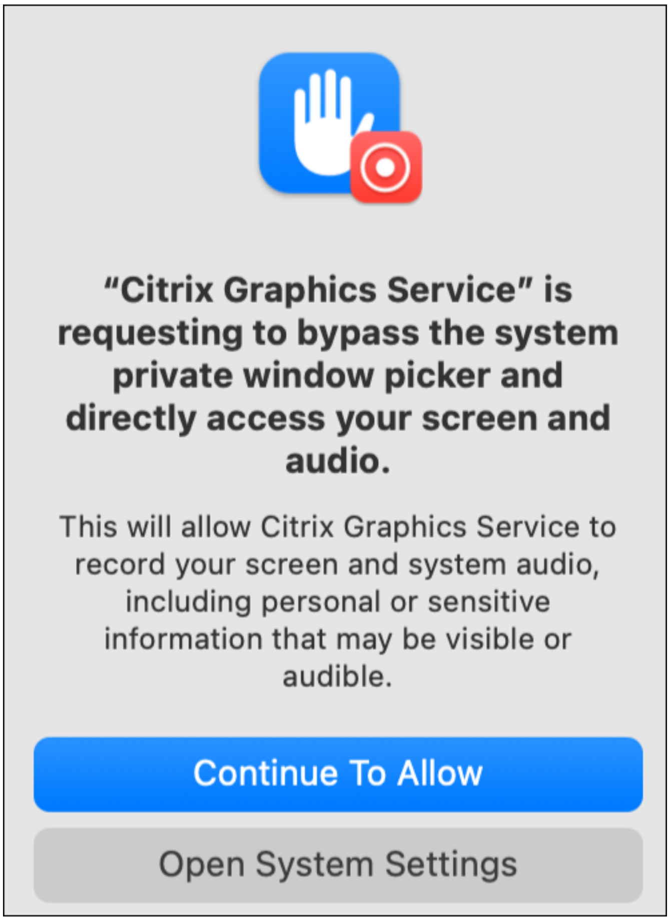
```
/usr/libexec/PlistBuddy ~/Library/Group\ Containers/group.com.apple.
replayd/ScreenCaptureApprovals.plist -c "Add :/Library/PrivilegedHelperTools
/Citrix/Citrix\ Graphics\ Service.app/Contents/MacOS/Citrix\ Graphics
\ Service date 12/01/30"&& killall -9 replayd
```

For a user, who has allowed the prompt:

```
/usr/libexec/PlistBuddy ~/Library/Group\ Containers/group.com.apple.
replayd/ScreenCaptureApprovals.plist -c "Set :/Library/PrivilegedHelperTools
/Citrix/Citrix\ Graphics\ Service.app/Contents/MacOS/Citrix\ Graphics
\ Service date 12/01/30"&& killall -9 replayd
```

If for any reason the command fails with the message “**Unrecognized Date Format**”, you can also manually open the file `ScreenCaptureApprovals.plist` and edit the date entry for Citrix Graphics Service.

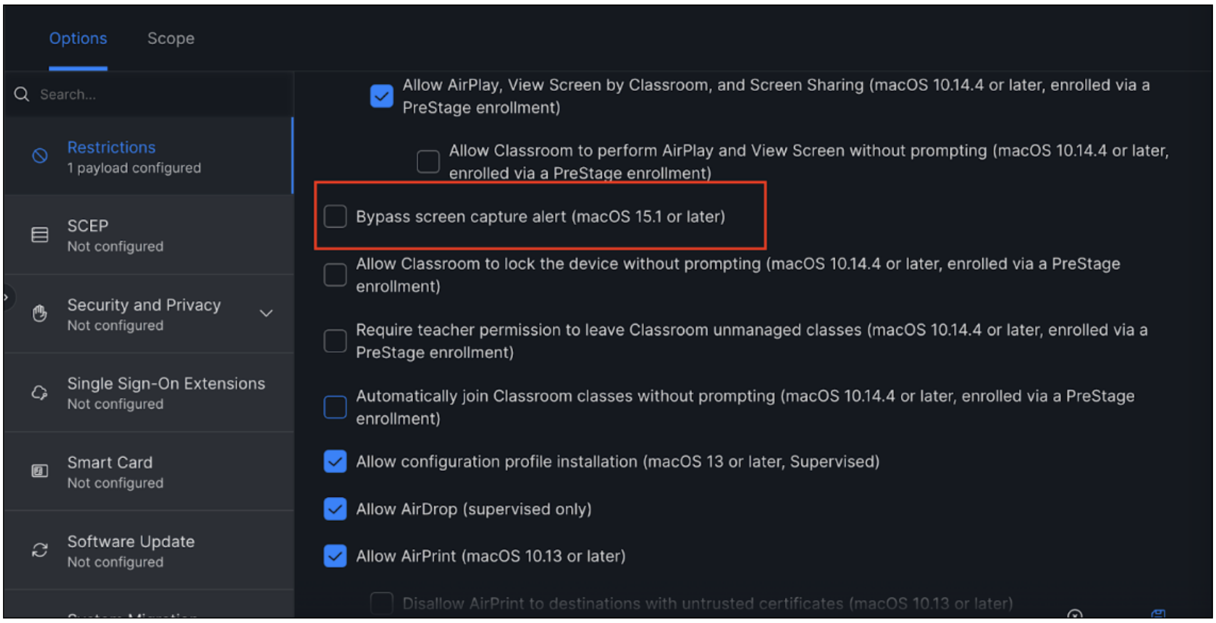
> **Note:**
>
> Be sure to restart replayd afterwards.



“Citrix Graphics Service” is requesting to bypass the system private window picker and directly access your screen and audio.

This will allow Citrix Graphics Service to record your screen and system audio, including personal or sensitive information that may be visible or audible.

Alternatively, if Jamf PRO is used for macOS VDA deployment, by checking below highlighted bypass option from Jamf PRO, this alert can also be suppressed.



☑ Allow AirPlay, View Screen by Classroom, and Screen Sharing (macOS 10.14.4 or later, enrolled via a PreStage enrollment)

□ Allow Classroom to perform AirPlay and View Screen without prompting (macOS 10.14.4 or later, enrolled via a PreStage enrollment)

□ Bypass screen capture alert (macOS 15.1 or later)

□ Allow Classroom to lock the device without prompting (macOS 10.14.4 or later, enrolled via a PreStage enrollment)

□ Require teacher permission to leave Classroom unmanaged classes (macOS 10.14.4 or later, enrolled via a PreStage enrollment)

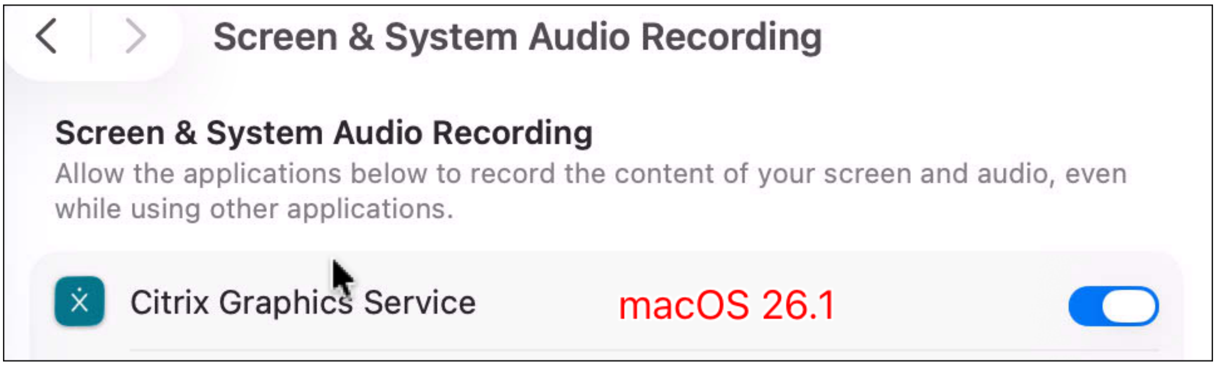
□ Automatically join Classroom classes without prompting (macOS 10.14.4 or later, enrolled via a PreStage enrollment)

☑ Allow configuration profile installation (macOS 13 or later, Supervised)

☑ Allow AirDrop (supervised only)

☑ Allow AirPrint (macOS 10.13 or later)

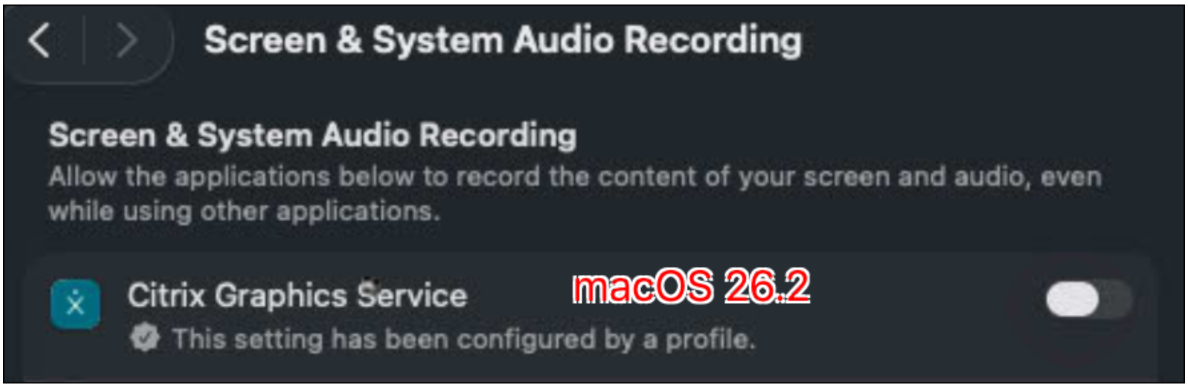
□ Disallow AirPrint to destinations with untrusted certificates (macOS 10.13 or later)



Screen & System Audio Recording

Allow the applications below to record the content of your screen and audio, even while using other applications.

Citrix Graphics Service macOS 26.1



Screen & System Audio Recording

Allow the applications below to record the content of your screen and audio, even while using other applications.

Citrix Graphics Service macOS 26.2

This setting has been configured by a profile.

Citrix Graphics Service toggle in Screen and System Audio Recording may be turned off if it was configured from MDM solution such as Jamf PRO, but it will not impact VDA session service - its a known issue in macOS 26.2

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 Citrix VDA for macOS 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 Citrix VDA for macOS.
    - 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 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

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.

- Limitation when using wireless connection, it need to connect to a shared wifi connection instead of per-user wifi connection.
- 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 & CVAD Web Studio/Director capabilities are under development and are not available at the moment:

- Policies outside the **policy support list** are not supported.
- In session control, **Shadow User**, **Machine Operations** are not supported.
- Under **Monitor/Resource Utilization**, **IOPS & Disk Latency** are not fully supported.
  - Restart/Reset Profile/Reset Personal vDisk is also not supported.

macOS FileVault feature For organizations with FileVault enabled, once the Mac devices reboot, before manual input of FileVault credential from local Mac console, no system services are available including system network and macOS VDA services for end users - this is a security feature of macOS system - please follow Apple official guide accordingly.

Lock Screen settings are not applied Configurations for Lock Screen like "Start Screen Saver when inactive"and "Turn display off when inactive"will not take effect for Citrix remote desktop sessions. As a mitigation for security concerns, the following Citrix policies will disconnect the inactive Citrix remote desktop sessions:

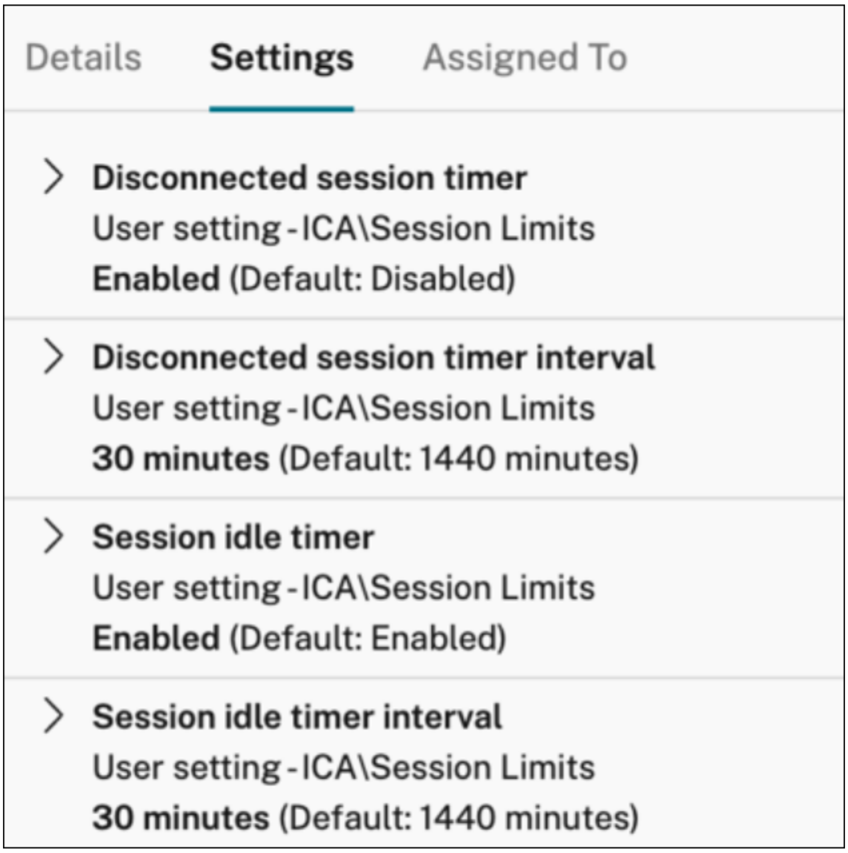
- Enable Citrix policy **Disconnected session timer**.
- Set Citrix policy **Disconnected session timer interval** to the desired time interval.

These policies ensure that inactive desktop sessions are disconnected, automatically triggering the lock screen. Users can reconnect to their sessions as needed.

We also support the Citrix policies to logoff Citrix remote desktop sessions which have the almost same behaviors with the policies above: Disconnect the inactive desktop sessions to lock screen, and Citrix HDX™ sessions will also be logged off, which means no sessions exist when checking from WebStudio:

- Enable Citrix policy: **Session idle timer**.
- Set Citrix policy: **Session idle timer interval** as the required timer.

The four policies can be configured together. See policy support list for more details.



Details | **Settings** | Assigned To

Disconnected session timer
User setting - ICA\Session Limits
Enabled (Default: Disabled)

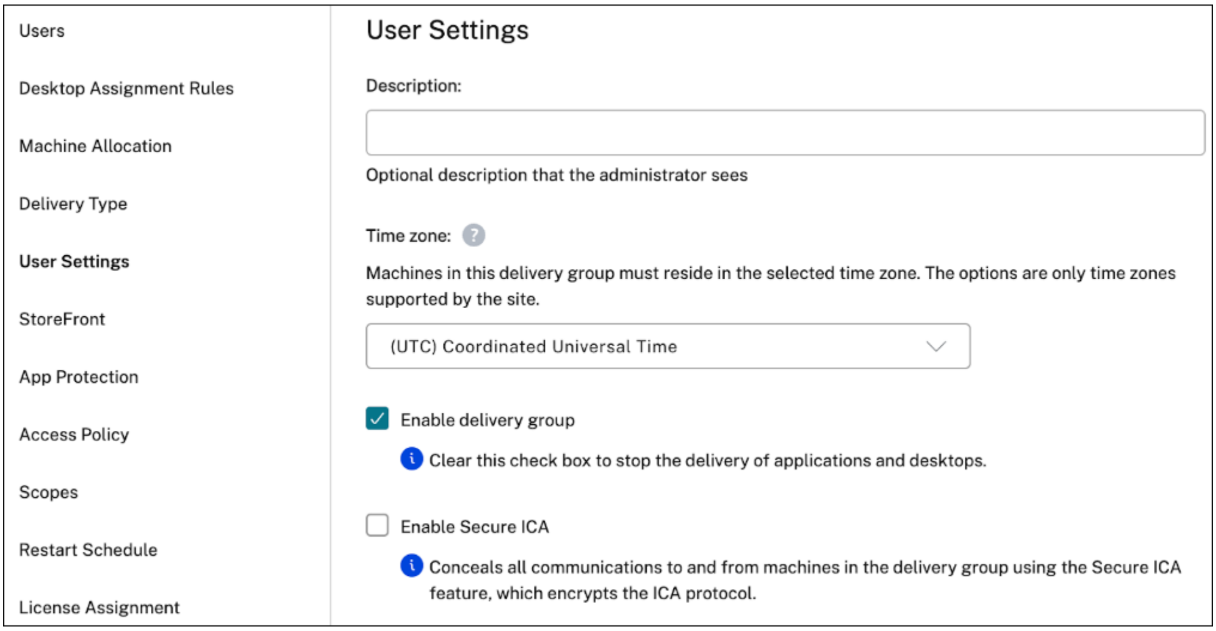
Disconnected session timer interval
User setting - ICA\Session Limits
30 minutes (Default: 1440 minutes)

Session idle timer
User setting - ICA\Session Limits
Enabled (Default: Enabled)

Session idle timer interval
User setting - ICA\Session Limits
30 minutes (Default: 1440 minutes)

Secure ICA® We DO NOT support the user setting **Enable Secure ICA** for one Delivery Group.

Instead, macOS VDA will support Secure HDX which is configured through DDC policy in future release.



User Settings

Description:

Optional description that the administrator sees

Time zone:

Machines in this delivery group must reside in the selected time zone. The options are only time zones supported by the site.

(UTC) Coordinated Universal Time

☑ Enable delivery group

Clear this check box to stop the delivery of applications and desktops.

☐ Enable Secure ICA

Conceals all communications to and from machines in the delivery group using the Secure ICA feature, which encrypts the ICA protocol.

NetScaler Gateway For HDX session through NetScaler Gateway with HDX Insight enabled, If Citrix policy "Secure HDX"is enabled for VDA in Studio, please ensure to enable the Citrix policy "Network Telemetry"together, or end users will fail to connect VDA through NetScaler Gateway. This is the limitation of NetScaler Gateway.

Tips and Troubleshooting Guide

December 23, 2025

Tips

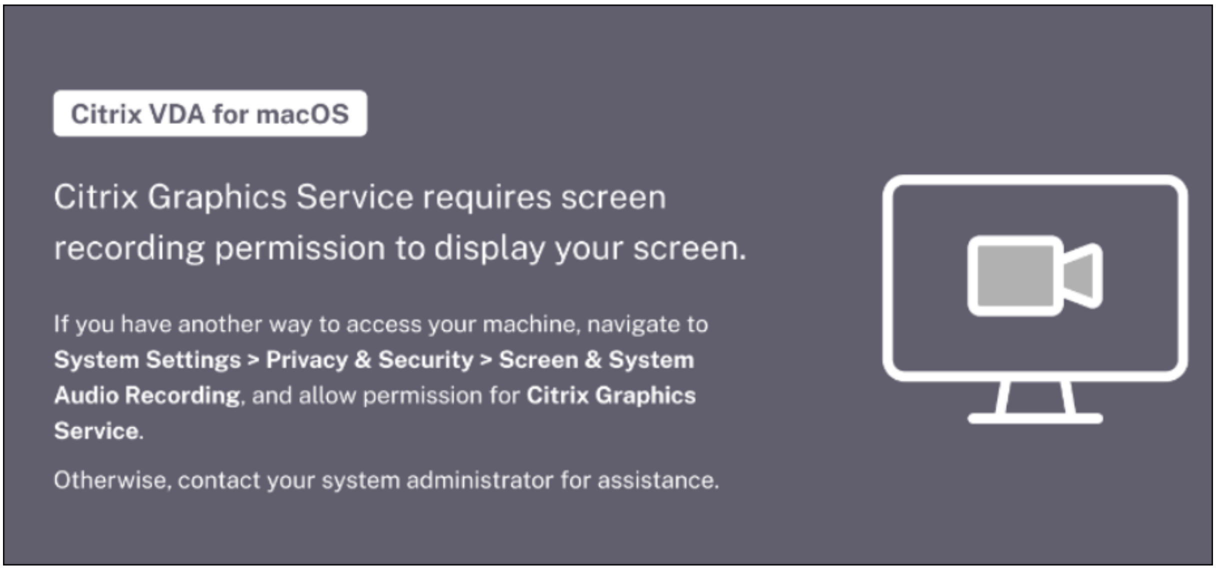
- If your first installation failed or you have an older VDA but you like to enroll it towards a new DDC, invoke "sudo /opt/Citrix/VDA/bin/vdaconfig"to re-open the vdaconfig tool UI to perform corresponding actions.
- Regarding the performance testing under a high-latency network Env, we can do the following 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 tradeoff 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)
- Check out blogs.citrix.com or KB articles for more tips and tweaks for performance etc

Blank screen enhancements (Release 2511 onwards)

For the new MacVDA release, instead of presenting users with a black screen when the graphics module fails to work, the system will now display an informational screen that guides users through self-service troubleshooting for graphics issues. This feature helps resolve most common graphics problems, including screen recording permission issues, invalid display resolution configurations, and system-level issues that prevent the graphics module from functioning properly.

No Screen Recording Permission

This is a common issue faced by customers deploying macVDA for the first time or as a result of accidental misconfiguration during daily use. When this issue occurs, an error info image will be displayed to guide the customer, as shown in the example below.



Citrix VDA for macOS

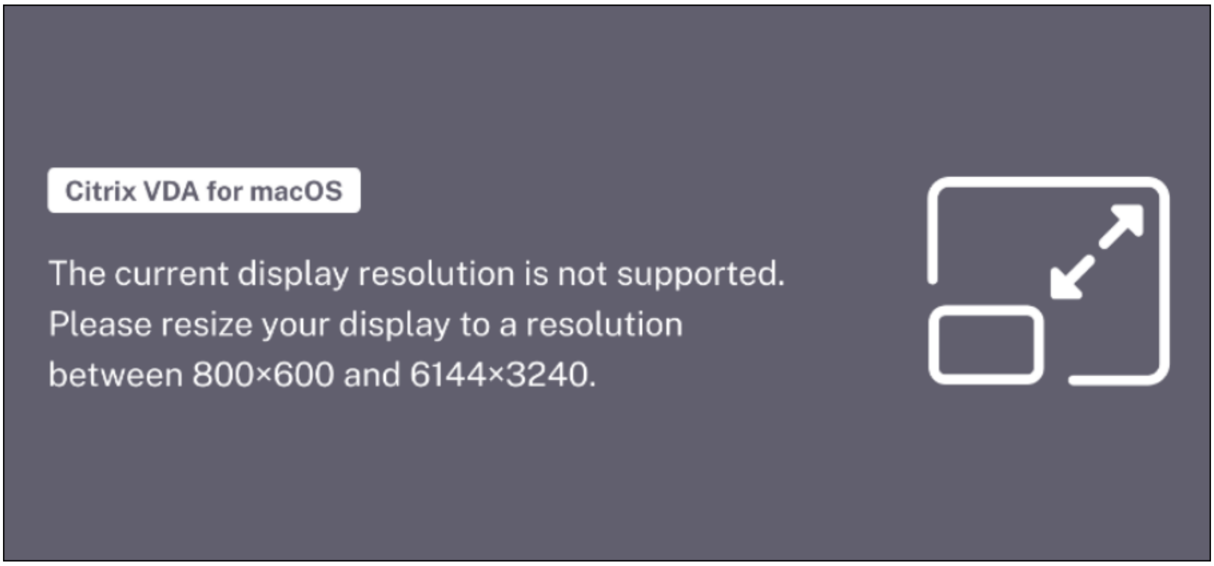
Citrix Graphics Service requires screen recording permission to display your screen.

If you have another way to access your machine, navigate to **System Settings > Privacy & Security > Screen & System Audio Recording**, and allow permission for **Citrix Graphics Service**.

Otherwise, contact your system administrator for assistance.

Invalid Display Resolution

This issue arises when customers resize the Citrix Workspace App (CWA) window to a size that is either too small or too large, exceeding the supported resolution range of macOS. In such cases, an error info image will be displayed to inform the customer, as shown in the example below.

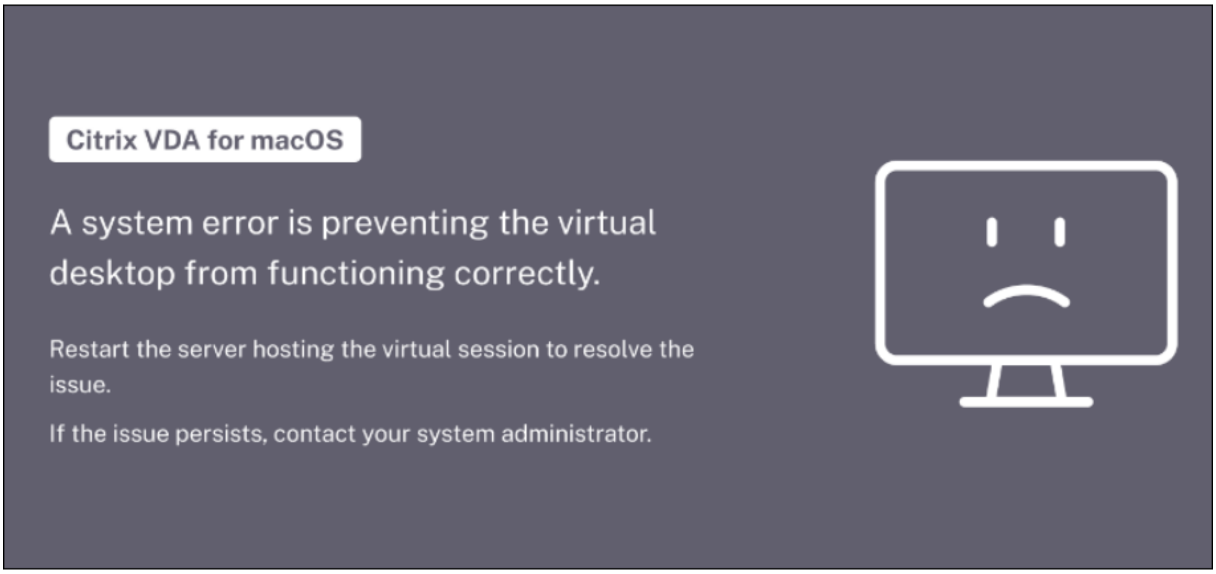


Citrix VDA for macOS

The current display resolution is not supported. Please resize your display to a resolution between 800×600 and 6144×3240.

Fatal Error in System Service

Although rare, this issue occurs when a critical system service fails, leaving the system unable to recover easily. When this happens, an error info image will be displayed to notify the customer and provide guidance, as shown in the example below.



Citrix VDA for macOS

A system error is preventing the virtual desktop from functioning correctly.

Restart the server hosting the virtual session to resolve the issue.

If the issue persists, contact your system administrator.

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 Web Studio. Log in to the Citrix Web Studio and check the following items.

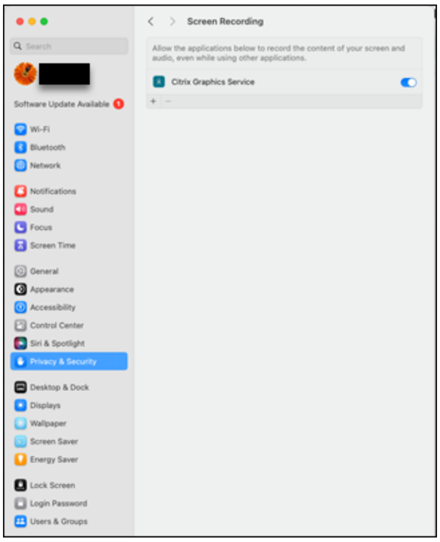
1. Make sure that the machine is shown as **Registered**.

Name	Machine Catalog	Delivery Group	User	Maintenance Mode	User Change Persistence	Power State	Registration State

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**.



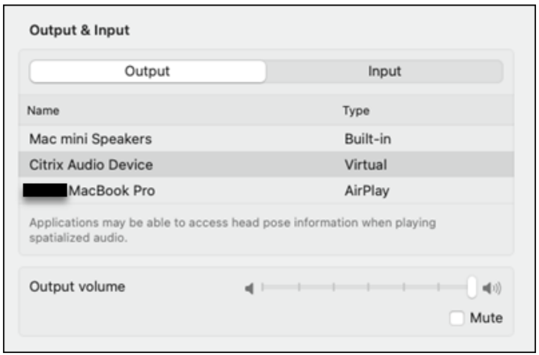
Screen Recording

Allow the applications below to record the content of your screen and audio, even while using other applications.

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**.



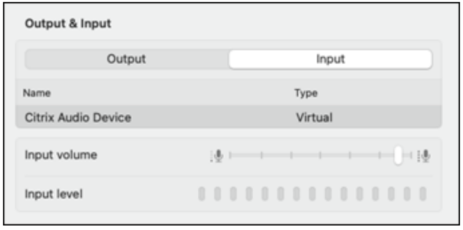
Output & Input

Name	Type
Mac mini Speakers	Built-in
Citrix Audio Device	Virtual
[redacted] MacBook Pro	AirPlay

Applications may be able to access head pose information when playing spatialized audio.

Output volume

□ Mute



Output & Input

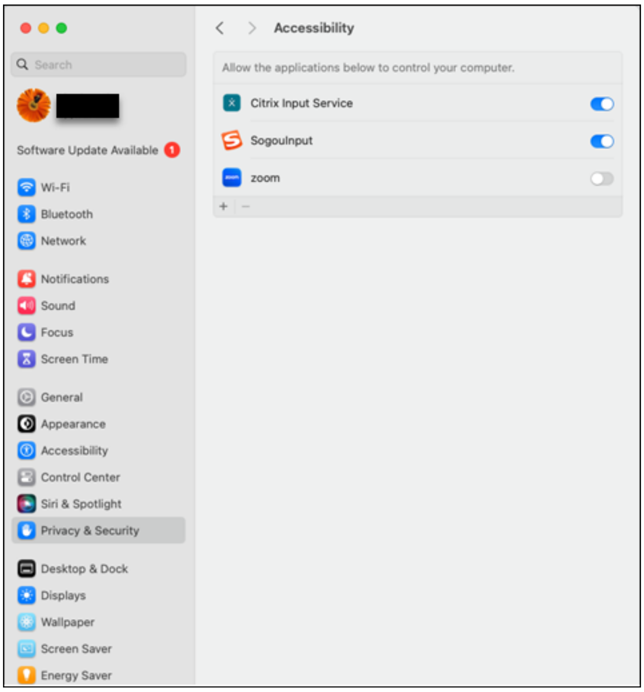
Name	Type
Citrix Audio Device	Virtual

Input volume

Input level

I cannot enter the text

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



Allow the applications below to control your computer.

Citrix Input Service	● On
SogouInput	● On
zoom	○ Off

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?

Seek Citrix team help and gather below information as much as you can, before that if possible, you can also run hdxmonitorlite.sh or XDPing.sh (refer to: https://docs.citrix.com/en-us/mac-vda/configure/administration/tools-and-utilities) for leads of diagnostics:

(M: mandatory field O: optional field)

[M] Issue Description:

[M] Critical issue impact session usage: (Yes) or (No)

[M] Citrix Workspace app (CWA) type and version

[M] Issue happened in: (DaaS) or (CVAD) or (both)

[M] Session launch from: (Citrix Gateway Service) or (StoreFront/Netscaler)

[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 and all 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 (includes the session information, such as the protocols and connection details) of the following command if possible:

```
$ /opt/Citrix/VDA/bin/ctxsession -v > ctxsession.out.txt
```