Citrix Workspace™ app for iOS

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Citrix Workspace™ app for iOS 2

About this release 3

Features in Technical Preview 34

Citrix Workspace app for iOS - Preview 41

System requirements and compatibility 42

Install and upgrade 49

Get started 50

Configure Citrix Workspace app 58

Configure Workspace app using Unified Endpoint Management solutions 71

Peripheral devices 86

User Experience 116

Webview for Web and SaaS apps 132

Password management 134

GACS & MDM Support for Session Toolbar Configuration 137

Store configuration 144

Authenticate 150

Secure 186

Session experience 196

Troubleshoot 212

Citrix Workspace app for iOS 227

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace™ app for iOS

September 7, 2025

Citrix Workspace app for iOS is client software available for download from the Apple Store. It enables you to access and run virtual desktops and hosted applications delivered by Citrix Virtual Apps and Desktops.

iOS is the operating system for Apple mobile devices such as iPads and iPhones. Citrix Workspace app for iOS runs on devices using the iOS operating system, such as iPhone X, iPad mini, and iPad Pro.

For detailed information about the features, fixed issues, and known issues, see the About this Release page.

For information about deprecated items, see the Deprecation page.

Language support

Citrix Workspace app for iOS is adapted for use in languages other than English. For a list of languages supported by Citrix Workspace app for iOS, see Language support.

Reference articles

- Tech Brief: Citrix Workspace
- Global App Configuration service
- Workspace user interface (UI)
- Microsoft Teams optimization in Citrix Virtual Apps and Desktops environments
- Citrix Workspace app release timelines

What's new in related products

- Citrix Workspace
- Citrix DaaS
- StoreFront
- Secure Private Access
- Citrix Workspace app for Mac

Legacy documentation

For product releases that have reached End of Life (EOL), see Legacy documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

About this release

September 17, 2026

Learn about new features, enhancements, fixed issues, and known issues.

> **Note:**
>
> - We would love to hear your valuable feedback on this version, which you can provide by navigating to **Settings** > **Report Issue**. Both verbose logs and screenshots can be shared with us from here.
> - Looking for Technical Previews? We have curated a list so that you can find them in one place. Explore our Features in Technical Preview page.

What's new in 26.9.0

Support for OS 27

Citrix Workspace app for iOS now supports iOS/iPadOS 27.

Enhanced anti-screen-capture coverage for multi-window layouts

Anti Screen Capture in App Protection–enabled sessions now extends to floating window mode. Protection is enforced wherever the protected session is presented —full screen, Split View, Slide Over, floating window, and Stage Manager - and is retained in the background and app-switcher snapshot when you switch away from Citrix Workspace app.

Fixed issues in 26.9.0

- Following the upgrade to Citrix Workspace app version 25.9.0.36 on iPads, barcode scans intermittently return incorrect or incomplete data in the Novatek application. [CVADHELP-33376]
- Published app not displayed when Citrix Workspace app is background/fullscreen and launched via Safari. [CVADHELP-33509]
- App protected resource may not launch with Citrix Workspace app for iOS 2511 when the store is added via Web Interface mode. [CVADHELP-31708]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new in 26.7.0

Improved Audio Performance (Playback) over EDT Lossy

Starting with version 2607, Citrix Workspace app for iOS improves in-session audio playback by leveraging EDT Lossy, a UDP-based transport optimized for real-time audio streaming.

Compared with standard EDT and Transmission Control Protocol (TCP), EDT lossy mode provides smoother audio on mobile networks with high latency, variable bandwidth, or packet loss. This update reduces audio stutter and dropouts, providing a more consistent and high-quality listening experience during virtual sessions, media playback, and online meetings.

Scrolling Support for Mouse, Trackpad, and Touch

This feature supports horizontal and diagonal scrolling for the following input methods:

- **Mouse wheel scroll:** Use a physical mouse wheel to scroll vertically and horizontally.
- **Trackpad two-finger pan (Apple and third-party):** Use a two-finger pan gesture to scroll vertically and horizontally.
- **Touch on screen (single-finger scroll):** Use a single finger on an iPhone or iPad screen to scroll vertically and horizontally.

VDA OS detection and keyboard shortcut support

Starting with version 2607, Citrix Workspace™ app for iOS now detects the operating system of the connected VDA and sends appropriate keyboard shortcuts:

- **VDA operating system detection:** Detects whether the connected VDA runs Windows, Linux, or macOS.
- **Automatic input mode for macOS VDA:** When you connect to a macOS VDA, the app switches the input mode to **Scancode**. The app also sends diagnostic data and records a telemetry data point for this setting.
- **Extended keyboard toolbar shortcuts:** Maps common shortcuts to match the Citrix Workspace app for ChromeOS model:
  - Copy (Ctrl+C or Command+C)
  - Paste (Ctrl+V or Command+V)
  - Cut (Ctrl+X or Command+X)
  - Select all (Ctrl+A or Command+A)
  - Undo (Ctrl+Z or Command+Z)
  - Find (Ctrl+F or Command+F)
  - Save (Ctrl+S or Command+S)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved in session toolbar

The session toolbar has been refreshed with a unified design across iPhone and iPad, including updated notch and keypad assets. The toolbar now behaves consistently across iPad orientations, and the interaction between the in-session keyboard and toolbar has been improved to provide a smoother user experience.

Graphic setting auto sync with native iOS setting

Starting with Citrix Workspace app for iOS 2607, the legacy resolution picker under **Settings > Display Options > Resolution** is replaced with simplified, intent-based options that align display scaling with native iOS settings. This makes it easier to achieve DPI matching on external monitors by dynamically adjusting virtual desktop sessions to the connected display's resolution, up to 4K, for optimal clarity and readability. For more information, see Graphic settings auto-synchronization with native iOS settings

Faster and more resilient session launch with parallel EDT and TCP connection attempts

Citrix Workspace app for iOS now improves session launch by attempting EDT and TCP connections in parallel. Previously, session establishment relied on a single transport path at a time, which could increase connection setup time when the preferred path was slow to respond or unavailable. With this enhancement, the app can continue with the transport that becomes available first, helping reduce launch latency and improve connection reliability across varying network conditions.

Deprecation notice

- Starting with version 27.3.0, the **Allow EDT setting** is no longer available in the app UI. Previously, this setting was available at **Settings > Advanced > Adaptive transport settings > Allow EDT**.

  EDT remains available as an administrator-controlled setting. This update simplifies the app experience and provides consistent EDT configuration through administrative policies.

- Starting with version 26.11.0, the **Auto-Configure**, **XenApp Services**, and **Access Gateway** store addition methods will be deprecated. The **Manual Setup** option will be removed. The **Web Interface** option is accordingly moved to the Welcome screen, and renamed to **Add as custom web store**.

For information about deprecated items, see the Deprecation page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues in 26.7.0

- After a period of inactivity, Citrix Workspace app might display the **Get Started** screen. This occurs even if the user is already logged in to a store. [RFIOS-15780]
- When you use Citrix Workspace app for iOS version 2509, session launches might fail with the error message **The session launch ended; either the session was not visible to the user, or the ICA engine did not load properly**. [CVADHELP-31115]
- When you try to launch a published app through Citrix Workspace app with the launch method set to Web Browser, the launch might fail with the error message **Failed to retrieve ICA**. [CVADHELP-33571]
- You might not be able to paste double-byte characters in a VDA session when using Citrix Workspace app for iOS. [CVADHELP-31582]
- On iPad with Citrix Workspace app for iOS 26.3.0, the app might freeze when you enter store credentials, and the enumeration screen might not appear. [CVADHELP-33167]
- When you use an external display in presentation mode, the cursor might stop responding on iPad after local interaction and might not return to the external screen. [CVADHELP-32792]
- You might see the error message **Session Error, Failed to Retrieve ICA** when you launch a protected resource from a store added in Web Interface mode in Citrix Workspace app for iOS 25.11. [CVADHELP-31580]

Known issues in 26.7.0

When you launch a protected session on an iPhone, a white area might appear at the top of the screen, causing the Windows taskbar to disappear. To work around this issue, change the device orientation to landscape. [HDX-108477]

What's new in 26.3.10

This release addresses areas that improve overall performance and stability.

Fixed issues in 26.3.10

- Store addition might fail when Citrix Gateway is connected to the StoreFront through *http*. [CVADHELP-31125]

Known issues in 26.3.10

There are no new known issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new in 26.3.0

Improved Audio Unit Management

Starting with version 26.3.0, Stereo audio handling is refined for improved compatibility with iOS 26. It delivers enhanced stability, clarity, and higher-quality sound performance.

Improved session reconnection experience (Technical Preview)

Starting with version 26.3.0, the following enhancements are made to the Improved session timeout experience (Technical Preview) feature announced in the 25.11.0 release:

- Displaying specific reasons for session timeouts, such as **Device Lock** or **App background**, or **Network disruption**.
- Session Reconnection setting configurable either through GACS by enabling **Manual session reconnect** option found at **Session experience > Connectivity** or through MDM.

IdP Logout on WSP Inactivity Timeout

Starting with version 26.3.0, Citrix Workspace app introduces a setting **Log off identity provider after inactivity timeout** in Workspace portal. This setting allows administrators to log users out of the Identity Provider (such as Microsoft Entra ID) when users sign out from Citrix Workspace app. This feature works with stores which have Multi-factor Authentication (MFA) configured.

EDT Lossy mode support for SecureHDX connections

Starting with version 26.3.0, EDT (Enlightened Data Transport) Lossy mode (unreliable sub-channel) works over SecureHDX (SecureICA 2.0) connections also. Previously, EDT Lossy works only with DTLS-encrypted connections. This enhancement extends unreliable sub-channel support to SecureHDX connections. It improves real-time performance for latency-sensitive protocols such as audio and video when SecureICA 2.0 is enabled. For more information, see EDT Lossy mode now supports SecureHDX

Dynamic keyboard settings support during an active HDX session

Starting with version 26.3.0, keyboard settings changed during an active HDX session take effect immediately. This removes the need for disconnecting and reconnecting the existing session, which has been the case till now.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Always On Tracing (AOT)

Starting with version 26.3.0, Citrix Workspace app for iOS introduces Always On Tracing (AOT), a modern diagnostic framework from Citrix. AOT continuously collects relevant log data across the Citrix Virtual Apps and Desktops (CVAD) environment. It is based on Citrix Diagnostic Facility (CDF) traces and adds component logs to help troubleshoot common issues such as VDA registration failures and app or desktop launch problems. AOT runs automatically in the background and ensures important diagnostic data is available when issues occur, even if you cannot reproduce the problem.

AOT simplifies troubleshooting for IT administrators and Citrix support teams by:

- Automatically capturing session and system logs with no manual steps required.
- Providing easy-to-access, readable logs.
- Enabling self-service diagnostics.
- Reducing dependency on Citrix Support and ensuring faster Mean Time to Resolution (MTTR).
- Making escalation easier with complete diagnostic context.
- Handling logs securely with sensitive data redaction.

For prerequisites and detailed configuration information, see Citrix Always On Tracing documentation.

Enhanced Stability for Menu Bar and Soft Keyboard Functionality

Release 26.3.0 includes the following enhancements, aligned with platform changes in iPadOS 26:

- The app hides the extended keyboard when you change device orientation.
- Keyboard and mouse might not work in a multi-monitor setup if you enable **Extended Display** in **Device Settings > Display & Brightness** and then disable it in **Citrix Workspace app settings**.

Fixed issues in 2603

- When you connect to a Linux VDA using the Citrix Workspace app, the client camera might not be detected or usable, while it works on a Windows VDA. [HDX-97347]
- After you quit Citrix Workspace app while on secondary store page and relaunch it, the primary store's enumeration page opens. [RFIOS-15750]
- You might see "Error code: 403"when you try to add a store URL in Citrix Workspace app for iOS version 25.7.0. [CVADHELP-30678]
- When Floating Window is enabled, the custom resolution setting might not persist after you switch to another app and return to Citrix Workspace app. [HDX-93471]
- Changes you make to Display options in Web Interface mode revert to the default values when you relaunch Citrix Workspace app.[CVADHELP-31436]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You might experience session launch failures after upgrading Citrix Workspace app to version 25.11.0-[CVADHELP-31392]
- You might get the error *The session launch ended; either the session was not visible to the user, or the ICA engine did not load properly* when you launch VDA sessions in Citrix Workspace app version 25.9.0. [CVADHELP-30885]

Known issues in 2603

There are no new known issues.

What's new in 25.11.0

Seamless integration of deviceTRUST® with Citrix Workspace™ app for iOS

Starting with version 25.11.0, Citrix Workspace app for iOS includes deviceTRUST, enhancing security through continuous device posture checks within the session. deviceTRUST is integrated with Citrix Workspace app for unified deployment. For more information, see deviceTRUST.

Key Details:

- **Integrated Functionality:** Starting with release 25.11.0 or later, the deviceTRUST Client Extension is installed by default as part of the Citrix Workspace app for iOS, simplifying deployment and management.
- **Continuous Posture Checks:** This feature enhances security by performing continuous checks on the endpoint device's context and security posture within the session, helping to implement a Zero Trust security model.
- **Compatibility:** The integration is supported on iOS 17, 18 & 26 versions.
- **Administration:** Administrators can use the deviceTRUST console to configure policies and manage device trust settings. For more information on how to configure, see Getting Started for Local

Enhanced On-Screen Keyboard Experience

Starting with version 25.11.0, Citrix enhanced the touch keyboard experience with improvements to the Automatic keyboard display behavior when connecting to Windows Virtual Desktop Agent (VDA) 25.11.0 desktops.

These enhancements improve usability when interacting with input fields and taskbar elements that appear near the bottom of the desktop session while using the on-screen touch keyboard.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved session timeout experience (Technical Preview)

This initiative aims to improve the end-user experience during session timeouts caused by inactivity or network interruptions. Users of both cloud and on-premises stores are provided with an option to reconnect directly from the timeout screen, eliminating the need to relaunch sessions from the client UI.

Key features:

- The timeout screen displays specific reasons for session timeouts, such as **Device went to sleep** or **Network disruption**.
- Users can seamlessly reconnect to the session, whether it is a new session or a continuation of the previous session, based on administrator configuration.
- The solution supports reconnection scenarios where auto reconnect might fail, such as network switches (for example, Wi-Fi to LAN).

> **Note:**
>
> This feature is not currently supported for sessions launched from the browser or for stores added as a Web Interface.

For more information on enabling this administrator-controlled feature, see the HDX documentation for Citrix Virtual Apps and Desktops.

Anti-screen capture and Anti-keylogging support on Custom Web Store

Starting with version 25.11.0, App Protection **Anti-screen capture** and **Anti-keylogging** are now supported on Custom Web Stores.

User-agent for Web Interface

Starting with the 25.11.0 version, the user-agent string used during some of the network requests initiated through Web Interface now includes the Citrix Workspace app identifier by default.

Prior to the change the user agent was:

```
Mozilla/5.0 (iPad; CPU OS 18_7 like Mac OS X)AppleWebKit/605.1.15 (
KHTML, like Gecko)Mobile/15E148
```

Post the change the user agent is:

```
Mozilla/5.0 (iPad; CPU OS 18_7 like Mac OS X)AppleWebKit/605.1.15 (
KHTML, like Gecko)Mobile/15E148

CWA/25.11.0 iOS/26.2 X1Class CWACapable 302RedirectionCapable CFNetwork
 Darwin CWA-iPad
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Seamless single sign-on for Entra ID joined VDAs on iOS

Starting with version 25.11.0, Citrix Workspace app for iOS supports seamless single sign-on (SSO) support with Microsoft Entra ID joined VDAs on cloud deployments. Previously, users were prompted for credentials when launching HDX sessions with Microsoft Entra ID joined VDAs because SSO was not available for this scenario. This change provides admins the option to configure SSO- the need to enter credentials at session launch can be omitted, streamlining authentication for organizations using Entra ID as their primary identity provider.

With this feature, users migrating from Active Directory to Entra ID can launch sessions without manual credential entry, delivering an improved and simplified authentication experience. For system compatibility and end-to-end configuration steps, see the Microsoft Entra single sign-on.

Fixed issues in 25.11.0

- You might experience Citrix Workspace app crash while on a Teams call when a USB-C to 3.5mm headphone jack adapter is connected to your device. [HDX-97247]
- You might experience a Citrix Workspace app crash when you access the Visma Web app deployed from SPA. [CVADHELP-29467]
- Citrix Workspace app for iOS might get stuck on the "Fetching your services"dialog after entering store credentials. [CVADHELP-28912]
- You might have experienced issues authenticating with FIDO2 using the system authentication browser on an on-premises store configured with GACS. [CVADHELP-30619]
- You might experience issues when trying to add an account on Citrix Workspace app for iOS 24.9.0 using Derived Credentials. [CVADHELP-27666]
- You might experience inconsistency with Pinch & Zoom functionality in Citrix Workspace app 25.7.2 after upgrading from version 25.3.1. [CVADHELP-29687]
- You might have experienced inconsistent transport when reconnecting EDT sessions after a network disruption in earlier versions of Citrix Workspace app for iOS. The updated version now maintains the last successful protocol, using EDT when available and falling back to TCP only if EDT is not available. [HDX-96848]

Known issues in 25.11.0

There are no new known issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

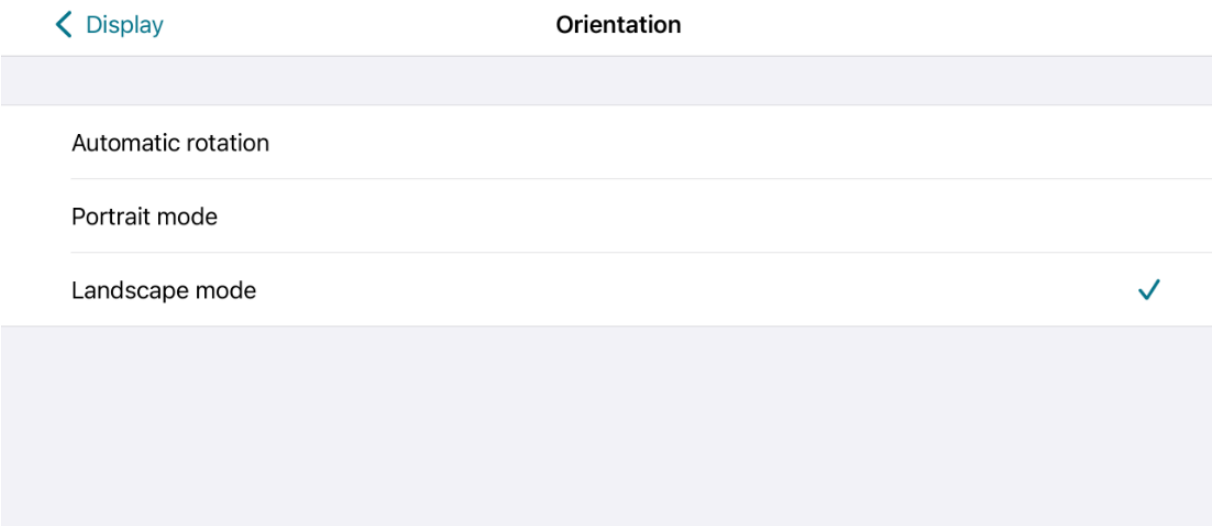
What's new in 25.9.0

Enhanced troubleshooting with Citrix Troubleshoot Connection

Previously, resolving virtual app or desktop launch issues has traditionally required IT support. With the enhanced Citrix Troubleshoot Connection feature, through a revamped UI, Citrix Workspace app enables users to self-remediate and fix launch issues by providing clear error messages and step-by-step recommendations. Users will see the detailed error and a button to fix the issue. You can resolve common problems, such as network issues or unavailable resources, with one-click recovery actions. This reduces your need for IT support and helps you get back to work faster. For more information, see Citrix Troubleshoot Connection.

Support for landscape mode on iPhone

The feature also includes landscape mode support on iPhone for a better troubleshooting experience on your device. This setting allows you to select the orientation of the app for optimal viewing of desktop content and data-intensive screen. With version 2509, the default orientation is **automatic rotation**.



Enhanced desktop launch experience

Starting with version 2509, Citrix Workspace app for iOS ensures an enhanced desktop launch experience. Users experience a seamless, flicker-free transition to the desktop without intermediate screens. The app also eliminates black screens and flickering when resizing or stretching, providing a stable and modern interface. This feature is enabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Improved Caps Lock synchronization for external keyboards

Starting with version 2509, Citrix Workspace app for iOS improves the handling of Caps Lock synchronization when you use external keyboards. The app ensures that the Caps Lock state remains consistent between the iOS client and the Virtual Delivery Agent (VDA), providing seamless typing behavior for you. Switching between local iOS apps and Citrix sessions no longer causes mismatched uppercase or lowercase input.

Audio Device and Volume Sync Improvements

We've enhanced how audio devices and volume are managed in your virtual sessions:

Improved Audio Device Sync: Only your currently selected system audio device is now mapped to the Virtual Delivery Agent (VDA), preventing unnecessary device mapping. The device's actual name is preserved, making it easier to identify within your session.

Enhanced Audio Volume Sync: Speaker volume now syncs one-way from your system to the VDA. Also, you can now adjust microphone gain directly within the VDA, and Citrix Workspace app saves this setting for use in future sessions.

Deprecation notifications of legacy features

Starting with version 26.3.0, Citrix Workspace app for iOS no longer supports the following legacy features. Support is discontinued for the following features:

- Citrix X1 Mouse
- Citrix Casting

For more information, see Citrix Workspace app for iOS deprecation

Fixed issues in 25.9.0

- You might notice that the extended toolbar UI is displayed on iOS 26 devices when the session is switched to windows mode. [HDX-94947]
- You might notice that the soft keyboard disappears on iOS 26 devices when resizing the Citrix Workspace app window. [HDX-93405]
- When launching a session, Citrix Workspace app might not detect certificates present on Yubikey on the session launch screen. [HDX-97210]
- On iPhone devices, you might not be able to log in to the store when using Citrix Workspace app for iOS. [CVADHELP-29188]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- On iPad devices, audio might not be redirected to the 2203 VDA when using Citrix Workspace app for iOS. [CVADHELP-28351]
- When using AirPods with Citrix Workspace app for iOS, you might not hear ringing sounds in a session. [CVADHELP-29065]
- Audio devices connected through a USB-C Hub might not work with Skype in Citrix Workspace app for iOS. [CVADHELP-28497]
- You might notice that the volume of an audio file playing in Windows Media Player inside a session cannot be increased or decreased using the device's volume up or down buttons. [HDX-93089]
- Audio playback might stop after resuming recording through Audacity. [HDX-92378]
- You might notice that Citrix Workspace app crashes when you attempt to sign out of the store while the network connection is turned off. [RFIOS-14795]
- On iPad devices, Citrix Workspace app might crash when connected to an external monitor while a session launch is in progress. [HDX-92002]

Known issues in 25.9.0

- You might experience Citrix Workspace app crash while on a Teams call when a USB-C to 3.5mm headphone jack adapter is connected to your device. [HDX-97247]
- When unlocking the device after it has been locked for some time, you might experience session image truncation. [HDX-96775]

Earlier releases

This section provides information on new features and fixed issues in the earlier releases that we support. For more information on the lifecycle of these releases, see Lifecycle Milestones for Citrix Workspace app and Citrix Receiver.

25.7.2

What's new

Support for iOS 26 Citrix Workspace app for iOS now supports iOS 26. For more information about iOS 26, Refer to the blog iOS26

Enhanced Connection Strength Indicator The connection strength indicator provides real-time insights into your connection quality and helps self-troubleshoot connectivity issues. This capability can be accessed from the toolbar and is enabled by default. From 25.7.2, we have enhanced the indicator, providing visibility in to:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Realtime CPU, Memory, Disk** usage on your local device. Providing user visibility if a depleted performance is a result of strained end point compute
- **Connection history** that provides visibility into the past 15 minutes of activity, indicating whether the connection has been consistently stable or experiencing intermittent drops
- **Real-time recommendation** - Connection Strength Indicator attempts to provide user potential recommendation that can help the user resolve the connection issue before raising a support ticket

For more information, see Enhanced Connection Strength Indicator.

Auto-launch desktops and apps Starting with version 25.7.2, Citrix Workspace app for iOS automatically launches either a desktop or an app tagged with `KEYWORDS: AutoStartPrimaryApp` by administrators in Citrix Studio. This functionality works across both Cloud and On-premises stores. For more information, see Auto-launch desktops and apps

Support iPad and iPhone in Lockdown mode Starting with version 25.7.2, Citrix Workspace app for iOS supports Lockdown Mode on iPad and iPhone. When Lockdown Mode is enabled, certain device functionalities are intentionally limited.

Fixed issues in 25.7.2

There are no new fixed issues.

25.5.10

What's new

This release contains minor bug fixes and Citrix Workspace app for iOS now supports iOS 26.

Fixed issues

There are no fixed issues in this release.

25.5.0

What's new

Enhanced Pointer mode experience Starting with version 25.5.0, Citrix Workspace app for iOS supports scrolling and zooming inside a session when using Pointer mode. In pointer mode, user can

© 1997–2026 Citrix Systems, Inc. All rights reserved.

now:

- Use a two-finger swipe (vertically or horizontally) to scroll in the respective direction.
- Perform zoom on session content by using a two-finger tap and hold, followed by a pinch gesture.

> **Note:**
>
> By default, a two-finger pinch performs local zoom. To perform remote zoom, use a two-finger tap and hold for a few seconds until the message "Remote zoom enabled"appears, then proceed with zooming.

Keyboard Settings Visibility Update Starting with Citrix Workspace app for iOS version 25.5.0, keyboard settings are now visible even when a store is not configured. Previously, the keyboard option in the Citrix Workspace app was only visible after adding a store. In the customer environment, this functionality worked as expected, and synchronization was successful after adding the store. However, the customer has indicated that they cannot add the store to the Citrix Workspace app due to security restrictions.

This update ensures that users who are unable to add a store due to security policies can still access and modify keyboard settings as needed.

Smooth desktop resize experience You might experience black screens or flickering during screen resizing or window mode changes. This feature enhances the user experience by eliminating these issues, providing a smooth and seamless transition when resizing or stretching the screen.

Floating session window support You might experience interruptions or disconnections when switching between apps in a VDA session on mobile devices. This issue is common during multitasking, such as attending meetings or performing MFA authentication. This feature enhances the user experience by ensuring uninterrupted session performance, such as audio and graphics, even when the app is running in the background. It allows users to multitask seamlessly without worrying about session timeouts or losing visibility. This feature provides a more reliable and efficient workflow for devices that do not support Stage Manager.

Limitation This feature works on iOS 18.0 and above

- Multitasking camera might not be supported due to different device chip capabilities.
- Multi-monitor scenarios are not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- You might be unable to authenticate using Azure Multi-Factor authentication. [CVADHELP-28006]
- When Citrix Workspace™ app configuration on iOS, is deployed via Intune. You might notice that multiple stores are displayed even though only one on-prem store is configured to be visible. [CVADHELP-28941]

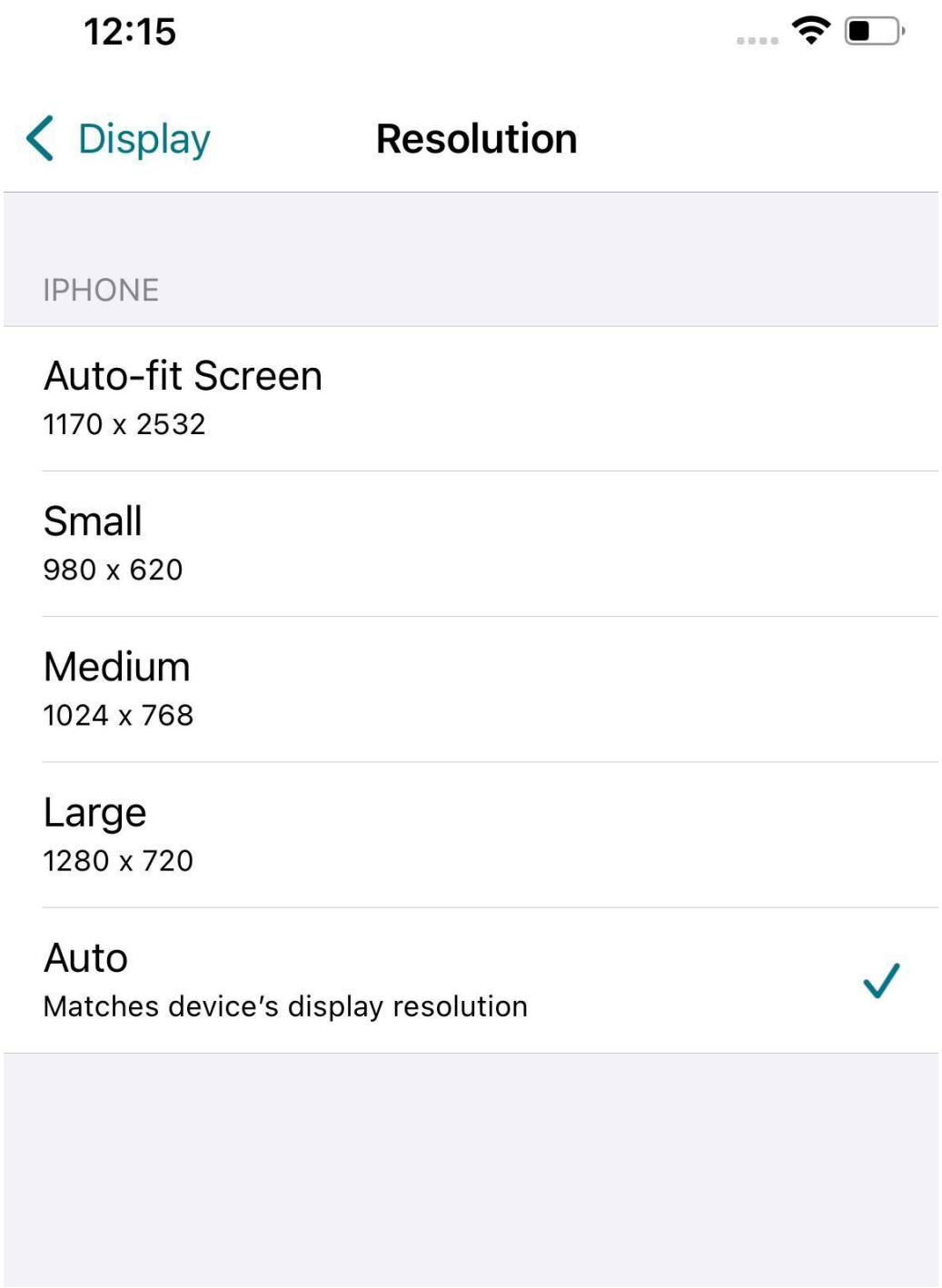
25.3.4

What's new

Enhanced session resolution Starting with version 25.3.4, Citrix Workspace app for iOS introduces enhancements to session resolution, for a more seamless user experience. Defaulting to Auto, the **DPI** settings adjust automatically whenever a user launches a session, enhancing the overall experience.

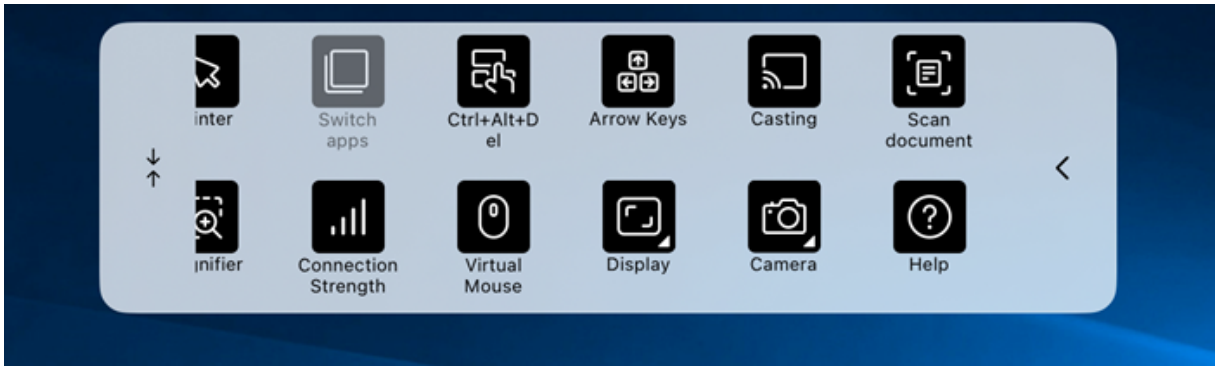
To ensure a consistent and user-friendly experience, virtual desktops now launch in landscape mode by default. This caters to widescreen applications and multitasking needs. This feature is enabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



New In-Session toolbar Starting with version 25.3.4, the new toolbar is enabled by default when there is no admin setting is configured through Global App Configuration service (GACS) and Mobile Device Management (MDM).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Fixed issues

- After upgrading to Citrix Workspace app for iOS version 25.3.4, some users might encounter the following error when attempting to launch sessions:
  The operation couldn't be completed (HDXSDKErrorDomain_Session Error 8). [CVADHELP-28152]
- Some iPad users on VDA 2402 and 2402 CU1 are unable to hear others during calls on apps like Skype or Webex. Impacted users can hear media playback from the session but not the person on the other end. Disconnecting and reconnecting audio may provide a temporary workaround. [CVADHELP-28419]
- You might notice that the pointer in the toolbar gets enabled when the battery icon in the taskbar is clicked in a Windows VDA.
- When a physical mouse is connected on an iPad device, you might notice that the Magnifier and Pointer icons do not automatically toggle off.
- iPadOS: Firebase-Foundation _userInfoForFileAndLine-AppSwitcher.

25.1.2

What's new

This release addresses areas that improve overall performance and stability.

Fixed issues

Citrix Workspace app for iOS might not establish a session when a user is connected to a specified VPN. [HDX-82028]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

25.1.1

What's new

This release addresses areas that improve overall performance and stability.

> **Important:**
>
> The version 25.1.0 has been rolled back due to stability issues. The new version available is 25.1.1. This means that the latest build 25.1.1 doesn't include the features of version 25.1.0. We are working on a new stable build, which will include all the features of version 25.1.0 along with the necessary fixes.

Fixed issues

Similar to the previous stable build.

25.1.0

What's new

- Enhanced Citrix security with pre-populated user name
- Supports GACS authenticated microservices (On-premises)
- Enhance cross-multi screen experience
- DPI matching
- Default landscape orientation for virtual desktops
- Enhanced secured ICA
- Improved mouse pointer mode

Improved mouse pointer mode Starting with version 25.1.0, Citrix Workspace app for iOS introduces improvements to mouse pointer mode. With this feature, the following enhancements are introduced proving a smoother and more consistent experience:

- The mouse pointer now moves more naturally by using swipe velocity.
- Mouse pointer mode is now available on iPhones, similar to iPads.

> **Note:**
>
> Starting with this release, sessions on iPhones launch in Multitouch Mode by default, allowing you to perform in-session zoom with a pinch gesture. To use client-side (viewport) zoom, Pointer Mode need to be enabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhanced Citrix® security with pre-populated user name Starting with version 25.1.0, you can use Unified Endpoint Management (UEM) to push the user name in a specific format to manage devices. On iOS, Citrix Workspace app reads this configuration, retrieves the user name, and pre-populates it within the authentication prompt, making it read-only. For more information, see Enhanced Citrix security with pre-populated user name.

Supports GACS authenticated microservices (On-premises) Starting with version 25.1.0, Citrix Workspace app for iOS supports Authenticated Microservices, enabling GACS to manage User Groups. This feature offers administrators with enhanced control for on-premises environments. For more information, see Supports GACS authenticated microservices (On-premises).

Enhance cross-multi screen experience Starting with version 25.1.0, Citrix Workspace app for iOS improves the user experience for iPads connected to external monitors or docks. These updates include the ability to distribute applications across multiple screens for improved multitasking. This feature is enabled by default. For more information, see Enhance cross-multi screen experience.

DPI matching The DPI matching feature ensures that the virtual session is rendered according to the DPI of the device. Starting with the 25.1.0 release, a new display setting enhances DPI matching capabilities. For more information, see DPI matching.

Default landscape orientation for virtual desktops Starting with version 25.1.0, Citrix Workspace app enforces landscape orientation by default when launching a virtual desktop on iPhone devices. This ensures an optimal and consistent user experience for widescreen applications and multitasking. For more information, see Default landscape orientation for virtual desktops.

Enhanced secured ICA® Starting with version 25.1.0, the new ICA encryption feature improves security by using modern encryption algorithms. This increases the security posture of our product, and subsequently gives our customers a way to enhance the security posture of their environments in a simple and reliable manner. For more information, see Enhanced secured ICA.

Fixed issues in 25.1.0

There are no new fixed issues in the release.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

24.12.0

What's new

- Launch of in-memory ICA solution
- Fast smart card
- Support for WSUI on-premises using gateway
- Enforcing Citrix access using Citrix Workspace app
- Support for multi-site store failover based on geo-location
- Right option key mapping for Alt key
- Connection Strength Indicator
- Enhanced new customizable toolbar
- Deprecation of operating system iOS 15

Launch of in-memory ICA solution Starting with version 24.12.0, Citrix Workspace app for iOS enhances support for in-memory hybrid launches using the Citrix Workspace launcher. This improvement allows for a more efficient and secure user experience, eliminating the need to download ICA files. For more information, see Launch of In-Memory ICA solution.

Fast smart card Starting with version 24.12.0, Citrix Workspace app for iOS introduces smart card enhancements for improved authentication performance and usability. This update brings significant improvements to smart card support, making the user experience smoother and more efficient. For more information, see Fast smart card.

Support for WSUI on-premises using gateway Starting with version 24.12.0, Citrix Workspace app for iOS supports Web UI for the on-premises store which is behind the gateway as well. The administrator must configure this feature, as it is not enabled by default. For more information, see Support for WSUI on-premises using gateway.

Enforcing Citrix access using Citrix Workspace app

Starting with version 24.12.0, admins can mandate users on iOS devices to access Citrix Workspace exclusively through the native app. When this feature is enabled, users attempting to access the store URL and third-party browsers are automatically redirected to the Citrix Workspace app. This ensures they can take advantage of all the native app's capabilities and enjoy a seamless user experience. For more information, see Enforcing Citrix access using Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for multi-site store failover based on geo-location Starting with version 24.12.0, the multi-store failover handling feature improves multi-store failover handling by running store address checks asynchronously and removing outdated store entries when a new failover store address is detected. For more information, see Support for multi-site store failover based on geo-location.

Right option key mapping for Alt key Starting with version 24.12.0, Citrix Workspace app for iOS introduces an enhancement allowing users to map the right Option key to Alt key in the session. For more information, see Right option key mapping for Alt key.

Connection Strength Indicator Starting with version 24.12.0, Citrix Workspace app for iOS supports the Connection Strength Indicator on the **Desktop Viewer** toolbar. This feature displays a network strength icon that alerts you of network issues. For more information, see Connection Strength Indicator.

Enhanced new customizable toolbar Starting with version 24.12.0, Citrix Workspace app for iOS introduces a new customizable toolbar. The revamped Desktop Viewer toolbar enhances user experience and support by offering greater flexibility. Admins can now tailor the in-session toolbar to meet their organization's needs. External webcam selection is now available in the new toolbar. For more information, see Enhanced new customizable toolbar.

Deprecation of operating system iOS 15 Starting from the 24.12.0 release, support for operating system iOS 15 is deprecated. As an alternative, you can upgrade to the latest available version of iOS. For more information, see Deprecation.

Fixed issues in 24.12.0

- You might be unable to delete a client certificate if it was installed in a store setting that has been deleted. [CVADHELP-26514]
- You might notice that when a user disconnects a session from the sidebar, the session remains active on the secondary monitor. [CVADHELP-26798]
- While opening Citrix Workspace app on iPad and using the next generation UI of StoreFront™ 2402 LTSR, you might encounter an error with the message **Unable to connect to the Server**. [CVADHELP-26319]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

24.10.0

What's new

Feature flag management

Citrix is changing the way it manages feature flags, allowing access to preview features and enabling dynamic management of features in production. To ensure optimal functioning of features which are under feature flags, you need to enable traffic to the URL `features.netscalergateway.net`. For more information, see Feature flag management.

Fixed issues

When multiple apps published from the same VDA are open, clicking the **Switch** button in the session toolbar might not allow users to switch between these apps and might result in no response. [CVADHELP-26404]

24.9.0

What's new

- Support for iOS 18
- Support for Rapid Scan
- Support for sustainability initiative
- Enhanced multi app window management
- Skip enable biometrics prompt
- Fetching GACS endpoints via email, store URL or domain-based discovery API
- Supports GACS authenticated microservices (Cloud)
- Support for App Protection

Support for iOS 18

Citrix Workspace app for iOS now supports iOS 18.

Support for Rapid Scan

Starting with the 24.9.0 version, Citrix Workspace app for iOS supports the Rapid scan feature. You can use this feature to scan multiple documents with an iOS device, and then transfer those scanned documents to a Mac device using the Citrix Workspace app for Mac and iOS.

For more information, see Support for Rapid Scan

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for sustainability initiative

Starting with version 24.9.0, users see a prompt to sign out of their desktop session upon closing a virtual desktop. This feature helps conserve energy by signing out from VMs when not needed. Previously, these sessions remained in a disconnected state, leading to unnecessary energy consumption.

For more information, see Support for sustainability initiative

Enhanced multi-app window management

Starting with version 24.9.0, Citrix Workspace app for iOS supports seamless multi-app window management for iPads connected to external monitors. This feature enhances multitasking and productivity by allowing native multi-app experiences. It can also be enabled when the iPad device is not connected to external monitors.

For more information, see Enhanced multi-app window management

Skip enable biometrics prompt

Previously, end users were prompted to choose whether to use biometrics Touch ID or Face ID for authentication in the Citrix Workspace app. Starting with version 24.9.0, administrators can now skip this prompt, streamlining the login process for users.

When biometrics are enabled, user passwords are securely stored in the keychain and protected by biometric authentication. Upon expiration of the authentication token, users are automatically prompted for biometric verification. If biometrics is not configured on the device, users need to manually enter their credentials when the token expires.

This feature is currently supported only for on-premise stores using LDAP authentication.

For more information, see Skip enable biometrics prompt

Fetching GACS endpoints via email, store URL or domain-based discovery API

Starting with version 24.9.0, admins can configure a web store based on email address, domain, and store URL, allowing the Global App Configuration Service (GACS) to identify and direct users to the appropriate custom web URL. Citrix Workspace app iOS devices can now fetch GACS endpoints using this discovery API, eliminating the need for hardcoded endpoints and reducing unnecessary calls when not configured.

For more information, see Fetching GACS endpoints via email, store URL or domain-based discovery API

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supports GACS authenticated microservices (Cloud)

As of the 24.9.0 release, Citrix Workspace app for iOS support Authenticated Microservices, enabling GACS to manage User Groups for our customers. This provides greater flexibility and control and is currently supported for cloud stores only.

For more information, see Support for GACS Authenticated Microservices (Cloud)

Support for App Protection

Starting with the 24.9.0 version, Citrix Workspace app for iOS supports the App Protection feature.

App Protection is a feature for the Citrix Workspace app that provides enhanced security when using Citrix Virtual Apps and Desktops™ published resources. This feature restricts the ability of clients to be compromised by keylogging and screen capturing malware. App Protection prevents exfiltration of confidential information such as user credentials and sensitive information that is displayed on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

For more information, see Support for App Protection

Fixed issues in 24.9.0

There are no new fixed issues.

24.8.1

What's new

This release addresses areas that improve overall performance and stability.

Fixed issues in 24.8.1

This version addresses areas that improve overall performance and stability.

24.8.0

What's new

This release addresses areas that improve overall performance and stability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues in 24.8.0

- You might not be able to launch a VDA session and login to the virtual desktop successfully in the smart card enabled setup. [CVADHELP-25247]

24.7.0

What's new

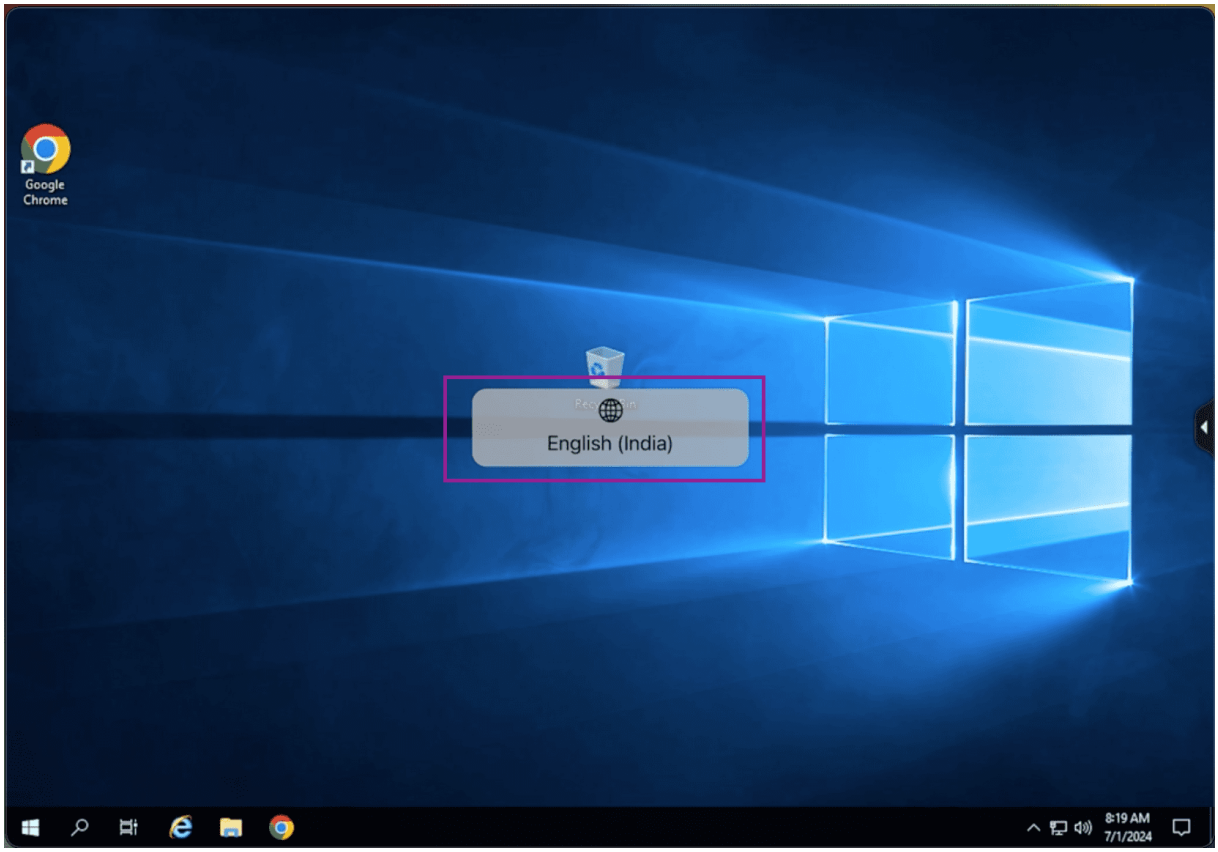
Support for DTLS 1.2 Starting with version 24.7.0, Citrix Workspace app for iOS supports DTLS protocol version 1.2. DTLS 1.2 provides enhancements and improvements over the previous version, which includes robust encryption algorithms, better handshake protocols, and protection against various attacks. This protocol improves overall security.

> **Note:**
>
> If there is any issue with DTLS protocol version 1.2, Citrix Workspace app for iOS seamlessly falls back to the previous supported versions.

For more information, see Support for DTLS 1.2.

Detect and display keyboard language change in the virtual session Starting with the 24.7.0 version, Citrix Workspace app for iOS now automatically detects and displays a message within the virtual session when user switches the keyboard language. When you switch keyboard languages using the globe key in the device keyboard or external keyboard, a message appears on the screen notifying about the current keyboard language. This feature ensures that you're aware of the current keyboard language within the virtual session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information, see Detect and display keyboard language change in the virtual session.

Support for adaptive audio Starting with the 24.7.0, Citrix Workspace app for iOS supports HDX adaptive audio. This feature improves the user experience by providing improved audio quality and low latency.

For more information, see the Audio policy setting article in the Citrix Virtual Apps and Desktops documentation.

Support for configuring Citrix Workspace app settings through UEM Previously, you can only configure the store URL in the Citrix Workspace app using the Unified Endpoint Management (UEM).

Starting with the 24.7.0 version, you can also configure the Citrix Workspace app settings on the managed devices using any UEM solution that is deployed in your infrastructure.

> **Note:**
>
> As an administrator, if you have an option of configuring the Citrix Workspace app settings using UEM and Global App Configuration service (GACS), UEM settings take precedence over GACS.

For more information, see Support for configuring Citrix Workspace app settings through UEM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Technical Preview

- Support for authentication using FIDO2 when connecting to an on-premises store
- Support for multiple audio devices
- Support for App Protection

For a complete list of Technical Preview features, see the Features in Technical Preview page.

Fixed issues in 24.7.0

- Citrix Workspace app for iOS NetScaler® store users might be unable to sign in to the new UI if Secure Private Access is enabled with clientless VPN (cVPN) policies. (RFIOS-13733)

24.6.0

What's new

This release addresses areas that improve overall performance and stability.

Fixed issues in 24.6.0

- You might notice that the trackpad on the magic keyboard is not functioning properly in the virtual session on an iPad pro M4 device. For more information, see Citrix Knowledge Center article - CTX677048. [HDX-66083]
- When you capture an image using the device camera from the virtual app session, you might notice that the captured image appears upside down. [CVADHELP-25448]
- When using Skype in a virtual session, you might notice that the screen freezes when you close Citrix Workspace app and reconnect to the session. [CVADHELP-25480]

24.5.0

What's new

Support for authentication using FIDO2 when connecting to a cloud store Starting with the 24.5.0 version, users can authenticate to Citrix Workspace app using FIDO2-based password-less authentication when connecting to a cloud store. FIDO2 offers a seamless authentication method, allowing enterprise employees to access apps and desktops within virtual sessions without the need to enter user name or password. This feature supports both roaming (USB only) and platform authenticators (PIN code, Touch ID, and Face ID only). This feature is enabled by default. For more information, see Support for authentication using FIDO2 when connecting to a cloud store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> FIDO2 authentication is supported with the Chrome custom tabs by default. If you are interested in using FIDO2 authentication with WebView, register your interest by email at ios_ear_support@cloud.com.

Support for document scanner Starting with the 2405 version, Citrix Workspace app for iOS supports the document scanner feature. With this feature, you can now scan and save multiple documents, all within the desktop session. This feature is enabled by default. For more information, see Support for document scanner.

Technical Preview

- Support for single sign-on for Microsoft Entra ID joined VMs
- Support for enforcing biometric authentication to access Citrix Workspace app

For a complete list of Technical Preview features, see the Features in Technical Preview page.

Fixed issues

- You might notice that when using the barcode scanner in the virtual session, the text can't be scanned correctly. [HDX-63675]

24.4.0

What's new

This release addresses areas that improve overall performance and stability.

Deprecation announcement of the TLS 1.0 and TLS 1.1 protocols Citrix is planning to deprecate the support for TLS 1.0 and TLS 1.1 protocols in the future releases. The alternative protocol is TLS 1.2 or TLS 1.3. For more information, see Deprecation.

Fixed issues

- When you open the device camera from the virtual app session, the Citrix Workspace app for iOS might close unexpectedly. [CVADHELP-24825]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

24.3.5

What's new

Support for the Twocanoes smart card utility reader Starting with the 24.3.5 version, Citrix Workspace app for iOS supports the Twocanoes smartcard utility readers. For more information about the supported smart card readers and configuration details, see Smart Cards.

> **Note:**
>
> The Twocanoes smart card utility USB-C reader is supported for both Citrix Workspace app login and virtual session login. However, the Twocanoes smart card utility Bluetooth reader is supported only for Citrix Workspace app login and not for virtual session login.

Support for configuring device name through UEM Starting with the 24.3.5 version, Citrix Workspace app for iOS enables administrators to assign and identify device names based on user groups through Unified Endpoint Management (UEM). For more information, see Support for configuring device name through UEM.

Technical Preview

- Support for configuring Citrix Workspace app settings through UEM

For more information on this Technical Preview, see Features in Technical Preview.

Fixed issues

This version addresses areas that improve overall performance and stability.

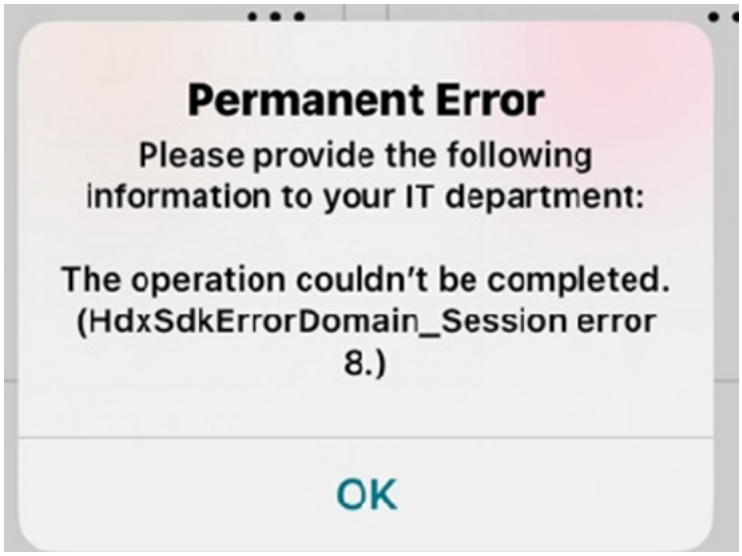
Known issues

Known issues in 25.7.2

- Session launches may fail with the following error when the iOS device is connected to a dock:

  "Permanent error. Please provide the following information to your IT department. The operation could not be completed. (HdxSdkErrorDomain_session error 8.)"

© 1997–2026 Citrix Systems, Inc. All rights reserved.



This issue occurs if Citrix Workspace app is launched while the device is already connected to the dock. As a workaround, Launch Citrix Workspace app first, then connect the dock to the device and launch the session. A fix is planned for release version 25.9.0 (expected end of October).

- While iOS version 26 will support Windowed mode, from this release Citrix Workspace app for iOS is restricted to a single window. This means only one session can be active at a time, and if users attempt to open another window, they will be switched to the currently active session.
- Lockdown Mode restricts certain web-based features when enabled on your iPad or iPhone as mentioned below.
    - Lockdown Mode simplifies rich media content display.
    - You might also encounter limited authentication flows or have restricted network operations.

Known issues in 25.5.0

There are no new known issues.

Known issues in 25.1.0

The toolbar menu does not expand when clicking the new toolbar notch on an external monitor. [HDX-81673]

Known issues in 24.12.0

Fast smart card does not currently support Elliptic Curve Cryptography (ECC) smart cards. [RFIOS-14497]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issues in 24.9.0

There are no new known issues.

Known issues in 24.8.1

There are no new known issues.

Known issues in 24.8.0

There are no new known issues.

Known issues in 24.7.0

There are no new known issues.

Known issues in 24.5.0

You might notice that the trackpad on the magic keyboard is not functioning properly in the virtual session on an iPad pro M4 device. As a workaround, you can use a external mouse (either wired USB type-C connector or Bluetooth) to navigate the screen in the virtual session. [HDX-66083]

Known issues in 24.1.0

After upgrading Citrix Workspace app for iOS to version 24.1.0, the keyboard input using the virtual keyboard in the session might fail for applications based on Oracle Java Web Start software. [CVADHELP-24645]

Known issues in 24.10.0

There are no new known issues.

Limitations

- We recommend that you use **Control + C** and **Control + V** keys on the soft keyboard of your device to copy and paste. **Command + C** and **Command + V** keys on an external keyboard might not work. [HDX-32431]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Attempts to launch an app by tapping the ICA file in the download manager fail when using the Safari web browser.
  To ensure a successful app launches from Safari, make sure the latest version of Citrix Workspace app or Citrix Receiver for iOS (but not both) is present on the device. [RFIOS-5502]
- After migrating to Citrix Workspace from StoreFront, the screen flickers momentarily while tapping the **Next** button on the Pendo guide.
- While starting web and SaaS apps from within the Citrix Workspace app, if the app uses Google IdP and requires the user to sign in then the authentication will fail with the error message "Access Denied". [RFIOS-11904]

Deprecation

For information about deprecated items, see the Deprecation page.

Features in Technical Preview

August 28, 2026

Features in Technical Preview are available to use in non-production or limited production environments, and to give customers an opportunity to share feedback. Citrix® does not accept support cases for features in technical preview but welcomes feedback for improving them. Citrix might act on feedback based on its severity, criticality, and importance.

Interested in trying a Technical Preview feature? Send an email to citrixappios@citrix.com and let us know which feature you would like to evaluate.

List of features in Technical Preview

Title	Available from version
Derived credentials and Apple Token Extension support	26.7.0
Improved session reconnection experience	26.3.0
Support for single sign-on for Microsoft Entra ID-joined VMs	24.5.0
Support for configuring Citrix Workspace app settings through UEM	24.3.5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Title	Available from version
Add multiple stores using Unified Endpoint Management (UEM)	23.9.0
Delete multiple stores using Unified Endpoint Management (UEM))	23.9.0
Enhanced web store experience	23.8.0
Support for an enhanced Single sign-on (SSO) experience for web and SaaS apps	23.3.0

Derived credentials and Apple Token Extension support

Citrix Workspace app for iOS 26.7.0 supports Apple Token Extension (CryptoTokenKit) in both the app and active HDX sessions. This enables a third-party derived-credential application on the device to supply digital certificates for following usecases:

- **Citrix Gateway or StoreFront authentication**: Authenticates users to the Citrix environment using a derived certificate, without a physical smart card reader.
- **Virtual app and desktop logon**: The user principal name is read from the certificate and passed to the VDA at launch, so the session signs on without prompting again.
- **In-session cryptographic redirection**: Extends credentials into the HDX session so virtualized apps (for example, browsers, mail clients, PDF signing tools, and enterprise apps) can make cryptographic requests through the client token extension.

A derived credential is a client certificate issued to a mobile device after identity proofing with an existing PIV or CAC card during enrollment. It provides smart-card-equivalent assurance on devices without card readers.

Improved session reconnection experience

Starting with version 26.3.0, the following enhancements are made to the Improved session timeout experience (Technical Preview) feature announced in the 25.11.0 release:

- Displaying specific reasons for session timeouts, such as **Device Lock** or **App background**, or **Network disruption**.
- Session Reconnection setting configurable either through GACS by enabling **Manual session reconnect** option found at **Session experience > Connectivity** or through MDM.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System and infrastructure requirements

Component	Requirement
Client OS	iOS or iPadOS 17.0 or later
Citrix client	Citrix Workspace app for iOS 26.7.0 or later
Virtual Delivery Agent	Citrix VDA for Windows, with smart card redirection policies enabled
Third-party provider	Enrolled credential app implementing an iOS CryptoTokenKit token extension
Infrastructure	Citrix Gateway or StoreFront configured for client-certificate authentication
Certificate	Must contain a UPN in the Subject Alternative Name (SAN) for session logon and in-session use

This feature is enabled per customer. Contact Citrix Support to enable it for your stores.

Configuration steps

1. Install the derived-credential provider app and complete enrollment.
2. In Citrix Workspace app, go to **Settings** > **Derived Credentials**, and enable **Use Derived Credentials**.
3. Add the store. If client-certificate authentication is configured, Citrix Workspace app presents the available credential.
4. Launch a desktop or app and authorize when prompted.

Administrators can lock this setting through the MDM advanced-settings policy.

Support for single sign-on for Microsoft Entra ID joined VMs

Technical Preview from 24.5.0 version	Enablement form	Feedback form

Starting with the 24.5.0 version, Citrix Workspace app for iOS supports users signing in to Azure AD-joined VM devices using single sign-on authentication. You need to provide Microsoft credentials when signing in to an Azure AD-joined VM device for the first time. For subsequent sign-ins, credentials are not required until the token expires.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - If the user does not use **WKwebview** for authentication, the credentials must be entered for the first time.
> - This feature is applicable only for cloud stores.

Add multiple stores using Unified Endpoint Management (UEM)

Technical Preview from 23.12.0 version	Enablement form	Feedback form

Admins can use Unified Endpoint Management solutions to configure and add multiple stores for managed iOS devices. The details for each store can be added to an XML file. This XML file can then be uploaded while configuring the app configuration policy.

> **Note:**
>
> The XML file must be in a key-value format.

Configuration key	Value type	Description
url	String	The store URL. For example, example.cloud.com
storeType (optional)	Integer	If set to **1**, users can view the native or the default store loading. If set to **2**, users can view the store inside a web interface.
displayName (optional)	String	The name of the store.
restrict_user_store_modification (optional)	Boolean	If set to **true**, users can't modify that is, add, delete, or edit the store. If set to **false**, users can modify that is, add, delete, or edit the store.

> **Important**
>
> - If the **restrict_user_store_modification** flag is set to **true**, all the existing stores are deleted before adding a new UEM configured store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

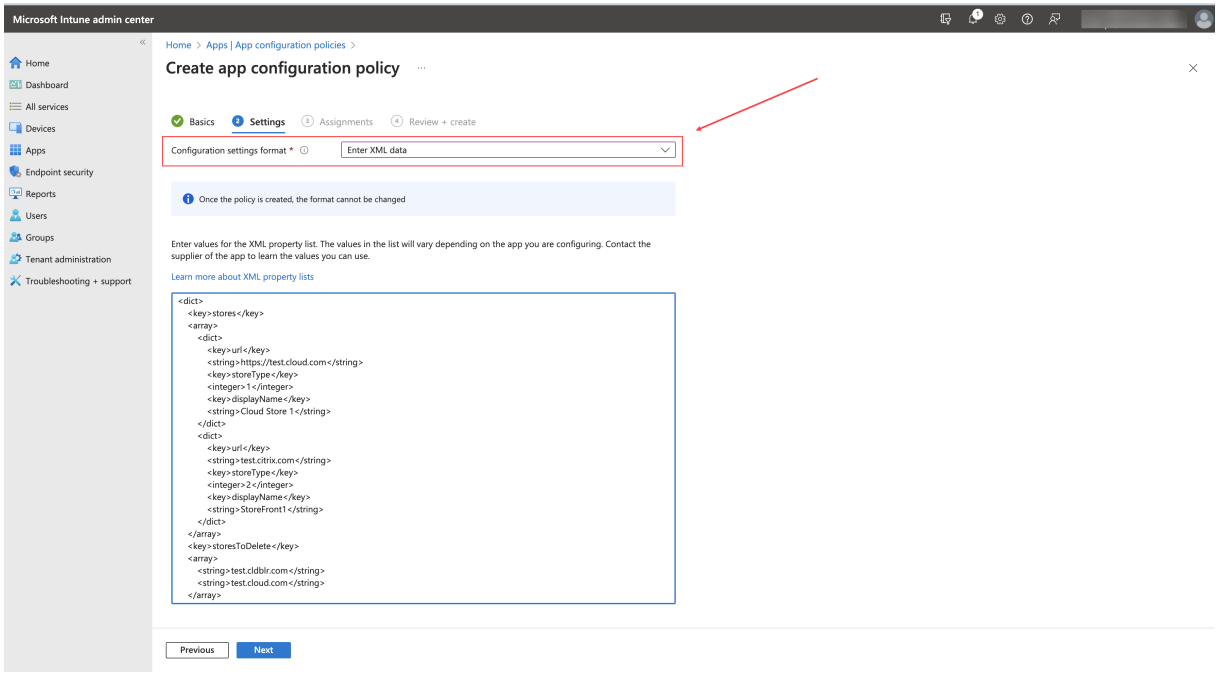
> • If storeType is not provided, the default interface is treated as native.

Sample XML Configuration to add stores Refer to this sample XML file for more information.

```
<dict>
    <key>stores</key>
    <array>
        <dict>
            <key>url</key>
            <string>test.cloud.com</string>
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>Cloud Store </string>
        </dict>
        <dict>
            <key>url</key>
            <string>test.citrix.com</string>
            <key>storeType</key>
            <integer>2</integer>
            <key>displayName</key>
            <string>StoreFront</string>
        </dict>
    </array>
        <key>restrict_user_store_modification</key>
    <true/>
</dict>
```

Once the XML file is ready with the store configuration, admins can upload the file to the **Create app configuration policy** page. For example, in Microsoft Intune, admins need to select **Enter xml data** option from the **Configuration settings format** dropdown.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Delete multiple stores using Unified Endpoint Management (UEM)

Technical Preview from 23.12.0 version	Enablement form	Feedback form

Admins need to add a list of stores to be deleted to an XML file with the key name **storesToDelete** to delete one or more stores.

Sample XML configuration to delete stores Refer to this sample XML file for more information.

```
<dict>
    <key>storesToDelete</key>
<array>
    <string>test.cldblr.com</string>
    <string>test.onprem.com</string>
</array>
</dict>
```

The following is a sample XML configuration file containing configuration for addition and deletion of stores.

```
    <dict>
    <key>stores</key>
    <array>
        <dict>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                <key>url</key>
                <string>test.cloud.com</string>
                <key>storeType</key>
                <integer>1</integer>
                <key>displayName</key>
                <string>Cloud Store </string>
            </dict>
            <dict>
                <key>url</key>
                <string>test.citrix.com</string>
                <key>storeType</key>
                <integer>2</integer>
                <key>displayName</key>
                <string>StoreFront</string>
            </dict>
        </array>
        <key>storesToDelete</key>
        <array>
            <string>test.cldblr.com</string>
            <string>test.onprem.com</string>
        </array>
        <key>restrict_user_store_modification</key>
        <true/>
    </dict>
```

Enhanced web store experience

Technical Preview from 23.8.0 version	Enablement form	Feedback form

End users can now stay signed-in to a web interface store until they sign out or the session times out. End users can also access the settings option without signing out of the current store. Click the ellipses icon to access the following options:

- **Settings**: Use this option to add and manage your stores.
- **Sign Out**: Use this option to sign out of your current web interface store.

Support for an enhanced Single sign-on (SSO) experience for web and SaaS apps

Technical Preview from 22.3.5 version	Enablement form	Feedback form

This feature simplifies the configuration of SSO for internal web apps and SaaS apps while using third-party identity providers (IdPs). The enhanced SSO experience reduces the entire process to a few

© 1997–2026 Citrix Systems, Inc. All rights reserved.

commands. It eliminates the mandatory prerequisite to configure Citrix Secure Private Access™ in the IdP chain to set up SSO. It also improves the user experience, provided the same IdP is used for authentication to both the Workspace app and the particular web or SaaS app being launched.

Technical Preview to General Availability (GA)

Service or feature	General availability version
Support for enforcing biometric authentication to access Citrix Workspace app	24.9.0
Support for rapid scan	24.9.0
Support for app protection	24.9.0
Support for authentication using FIDO2 when connecting to an on-premises store	24.9.0
Support for multiple audio devices	24.9.0
Support for adaptive audio	24.5.0
Support for Accessibility and VoiceOver	24.9.0
External Webcam support	24.9.0
Support for configuring Citrix Workspace app settings through UEM	24.7.0
Support for document scanner	24.5.0
Support for FIDO2-based authentication	23.9.0
Support for Apple's native non-mirror mode	23.3.0

Citrix Workspace app for iOS - Preview

September 17, 2026

The upcoming version of the Citrix Workspace app for iOS is 26.11.0, tentatively available in November 2026.

For information on installation, see the Install page.

For information about installing Early Access Release (EAR) builds from TestFlight, please see our blog.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can provide Early Access Release feedback through email at ios_ear_support@citrix.com.

> **Note:**
>
> This is an Early Access Build shared for the purpose of testing or validation with the intent to make organizations ready for the upcoming release and is NOT advised to be deployed in production environments.

System requirements and compatibility

February 16, 2026

Citrix Workspace™ app for iOS needs to be updated to the latest version that is available in the Apple Store to avail customer support.

Supported operating systems

Citrix Workspace app for iOS supports the following operating systems:

- iOS 26 and iPadOS 26.
- iOS 18 and iPadOS 18.
- iOS 17 and iPadOS 17.

At any point in time, Citrix® supports only the latest and the previous two iOS operating systems (N, N-1, and N-2) only.

Server requirements

Verify if you've installed all the latest hotfixes for your servers.

- For connections to virtual desktops and apps, Citrix Workspace app supports Citrix StoreFront and Web Interface.

  StoreFront:

  - StoreFront 3.6 or later (recommended). Citrix Workspace app has been validated with the latest version of StoreFront; previous supported versions include StoreFront 2.6 or later.

    Provides direct access to StoreFront stores. Citrix Workspace app also supports prior versions of StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> With XenApp and XenDesktop 7.8, Citrix introduced support for the Framehawk virtual channel and 3D Pro. This functionality was extended to Citrix Workspace app.

- StoreFront configured with a Workspace for website.

  Provides access to StoreFront stores from a Safari web browser. Users must manually open the ICA file using the browser. For the limitations of this deployment, see the StoreFront documentation.

Web Interface:

- Web Interface 5.4 with Web Interface sites
- Web Interface 5.4 with XenApp and XenDesktop sites
- Web Interface on Citrix Gateway (browser-based access only using Safari)

  Enable the rewrite policies provided by Citrix Gateway.

- **Citrix Virtual Apps and Desktops™**, **XenApp**, and **XenDesktop** (any of the following products):
  - Citrix Virtual Apps and Desktops 7 1808 or later
  - Citrix XenDesktop 7.x or later
  - Citrix XenApp 7.5 or later

Connections, certificates, and authentication

For connections to StoreFront, Citrix Workspace app supports the following authentication methods:

	Workspace for Web using browsers	StoreFront Services site (native)	StoreFront XenApp and XenDesktop Site (native)	Citrix Gateway to Workspace for Web (browser)	Citrix Gateway to StoreFront Services site (native)
Anonymous	Yes	Yes			
Domain	Yes	Yes	Yes	Yes*	Yes*
Domain pass-through	Yes	Yes	Yes		
Security token				Yes*	Yes*

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	Workspace for Web using browsers	StoreFront Services site (native)	StoreFront XenApp and XenDesktop Site (native)	Citrix Gateway to Workspace for Web (browser)	Citrix Gateway to StoreFront Services site (native)
Two-factor authentication (domain with security token)				Yes*	Yes*
SMS				Yes*	No
Smart card		Yes		Yes*	Yes*
User certificate				Yes (Citrix Gateway plug-in)	Yes (Citrix Gateway plug-in)

*Available only for:

- Workspace for websites.
- Deployments that include Citrix Gateway, with or without installing the associated plug-in on the device.

For connections to the Web Interface 5.4, Citrix Workspace app supports the following authentication methods:

> **Note:**
>
> Web Interface uses the term Explicit to represent domain and security token authentication.

	Web Interface (browsers)	Web Interface XenApp and XenDesktop® Site	Citrix Gateway to Web Interface (browser)	Citrix Gateway to Web Interface XenApp and XenDesktop Site
Anonymous	Yes			
Domain	Yes	Yes	Yes*	
Domain pass-through	Yes			
Security token			Yes*	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	Web Interface (browsers)	Web Interface XenApp and XenDesktop® Site	Citrix Gateway to Web Interface (browser)	Citrix Gateway to Web Interface XenApp and XenDesktop Site
Two-factor authentication (domain with security token)			Yes*	
SMS			Yes*	
Smart card				
User certificate			Yes (Require Citrix Gateway plug-in)	

Certificates

Private (self-signed) certificates You can successfully access Citrix resources using Citrix Workspace app:

- when a private certificate is installed on the remote gateway.
- when the root certificate for the organization's certificate authority is installed on the device.

> **Note:**
>
> When the remote gateway's certificate cannot be verified upon connection, an untrusted certificate warning appears. This issue is because the root certificate isn't included in the local keystore. If a user chooses to continue through the warning, a list of applications is displayed; however, applications fail to start.

Manually installed certificate In iOS 10.3 and later, a certificate included in a profile that you install manually isn't automatically trusted for SSL. To trust manually installed certificate profiles in iOS:

1. Make sure you've installed the certificate profile on the device.
2. Go to **Settings** > **General** > **About** > **Certificate Trust Settings**.

   Each root that has been installed through a profile appears under **Enable Full Trust For Root Certificates**.
3. You can toggle trust on or off for each root.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Import root certificates on iPad and iPhone devices Obtain the root certificate of the certificate issuer and email it to an email account configured on your device. When clicking the attachment, you're asked to import the root certificate.

Wildcard certificates Wildcard certificates are used in place of individual server certificates for any server within the same domain. Citrix Workspace app supports wildcard certificates.

Intermediate certificates and Citrix Gateway When your certificate chain includes an intermediate certificate, the intermediate certificate must be appended to the Citrix Gateway (or Access Gateway) server certificate. Also, for Access Gateway installations, see Install, link, and update certificates that match your requirement in Citrix ADC documentation.

RSA SecurID authentication is supported for Secure Gateway configurations (through the Web Interface only) and all supported Access Gateway configurations.

Citrix Workspace app supports all authentication methods supported by Access Gateway.

Joint Server Certificate Validation Policy Releases of Citrix Workspace app have a stricter validation policy for server certificates.

> **Important**
>
> Before installing Citrix Workspace app, confirm that the certificates at the server or gateway are correctly configured as described here. Connections might fail if:
>
> - the server or gateway configuration includes a wrong root certificate
> - the server or gateway configuration does not include all intermediate certificates
> - the server or gateway configuration includes an expired or otherwise invalid intermediate certificate
> - the server or gateway configuration includes a cross-signed intermediate certificate

When validating a server certificate, Citrix Workspace app now uses **all** the certificates supplied by the server (or gateway) when validating the server certificate. As in previous releases, Citrix Workspace app then also checks that the certificates are trusted. If the certificates aren't trusted, the connection fails.

This policy is stricter than the certificate policy in web browsers. Many web browsers include a large set of root certificates that they trust.

The server (or gateway) must be configured with the correct set of certificates. An incorrect set of certificates might cause Citrix Workspace app connections to fail.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Suppose that a gateway is configured with these valid certificates. This configuration is recommended for customers who require stricter validation, by determining exactly which root certificate is used by Citrix Workspace app:

- Example Server Certificate
- Example Intermediate Certificate
- Example Root Certificate

Then, Citrix Workspace app checks if all these certificates are valid. Citrix Workspace app also validates if **Example Root Certificate** is already trusted.

> **Notes:**
>
> - If Citrix Workspace app does not trust **Example Root Certificate**, the connection fails.
> - Some certificate authorities have more than one root certificate. If you require a stricter validation, make sure that your configuration uses the appropriate root certificate.

For example, there're currently two certificates:

- DigiCert or GTE CyberTrust Global Root
- DigiCert Baltimore Root or Baltimore CyberTrust Root

These certificates can validate the same server certificates. On some user devices, both root certificates are available. On other devices, only one is available (**DigiCert Baltimore Root** or **Baltimore CyberTrust Root**).

If you configure **GTE CyberTrust Global Root** at the gateway, Citrix Workspace app connections on those user devices fails. Consult the certificate authority's documentation to determine which root certificate has to be used. Also note that root certificates eventually expire, as do all certificates.

Then, Citrix Workspace app uses these two certificates. The app searches for a root certificate on the user device. If the app finds one that validates correctly, and is also trusted (such as **Example Root Certificate**), the connection succeeds. Otherwise, the connection fails.

This configuration supplies the intermediate certificate that Citrix Workspace app needs, but also allows Citrix Workspace app to choose any valid, trusted, root certificate.

Now suppose that a gateway is configured with these certificates:

- Example Server Certificate
- Example Intermediate Certificate
- Wrong Root Certificate

A web browser might ignore the wrong root certificate. However, Citrix Workspace app doesn't ignore the wrong root certificate, and the connection fails.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Some certificate authorities use more than one intermediate certificate. In this case, the gateway is normally configured with all the intermediate certificates (but not the root certificate) such as:

- Example Server Certificate
- Example Intermediate Certificate 1
- Example Intermediate Certificate 2

> **Important**
>
> Some certificate authorities use a cross-signed intermediate certificate. Such certificates are intended for situations where there're more than one root certificate and an earlier root certificate is still in use at the same time as a later root certificate. In such cases, at least two intermediate certificates exist.

For example, the earlier root certificate **Class 3 Public Primary Certification Authority** has the corresponding cross-signed intermediate certificate **Verisign Class 3 Public Primary Certification Authority - G5**. However, a corresponding later root certificate **Verisign Class 3 Public Primary Certification Authority - G5** is also available, which replaces **Class 3 Public Primary Certification Authority**. The later root certificate does not use a cross-signed intermediate certificate.

> **Note:**
>
> The cross-signed intermediate certificate and the root certificate have the same Subject name (Issued To), but the cross-signed intermediate certificate has a different Issuer name (Issued By). The Issuer name distinguishes the cross-signed intermediate certificate from an ordinary intermediate certificate (such **Example Intermediate Certificate 2**).

This configuration, omitting the root certificate and the cross-signed intermediate certificate, is normally recommended:

- Example Server Certificate
- Example Intermediate Certificate

Avoid configuring the gateway to use the cross-signed intermediate certificate, as Citrix Workspace app selects the earlier root certificate:

- Example Server Certificate
- Example Intermediate Certificate
- Example Cross-signed Intermediate Certificate [not recommended]

It isn't recommended to configure the gateway with only the server certificate:

- Example Server Certificate

In such cases, if Citrix Workspace app can't locate all the intermediate certificates, the connection fails.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System requirements for Microsoft Entra SSO

The following are the system requirements for using Microsoft Entra SSO:

- Control plane: Citrix DaaS
  - Citrix Cloud Commercial (US, EU, and APS)
  - Citrix Cloud Japan
- User portal: Citrix Workspace
- Virtual Delivery Agent (VDA)
  - Windows: version 2507 or newer
- Citrix Workspace app
  - iOS: version 2511 or newer
- Session host OS:
  - Windows 11, version 24H2 with 2025-09 Cumulative Updates for Windows 11 (KB5065789) or later installed (build 26100.6725)

Considerations

- Microsoft Entra single sign-on is only supported when accessing Citrix Workspace through Citrix Workspace app. If users access Citrix Workspace through a web browser, single sign-on will not work.
- Auto Client Reconnect is not supported when Microsoft Entra single sign-on is used to log into the session. This feature is automatically disabled when this logon method is used. Session Reliability is still available for automatic reconnection in case of network disruptions.
- When a virtual desktop is locked, the default behavior is to display the Windows lock screen. Depending on your authentication requirements, you might need to change the session lock behavior. For more information, see Session lock behavior.

Install and upgrade

September 7, 2025

You can download or upgrade to the latest version of Citrix Workspace app the Apple Store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- First-time users can download Citrix Workspace app from the Apple Store and install it on their device.
- Existing users can upgrade to the latest version of Citrix Workspace app from the Apple Store.

For information on configuring Citrix Workspace app, refer to the Configure section.

For information about the features available in Citrix Workspace app for iOS, see Citrix Workspace app feature matrix.

Get started

September 13, 2025

Setup

Citrix Workspace app for iOS supports the configuration of Web Interface for your Citrix Virtual Apps deployment. There are two types of Web Interface sites:

- XenApp and XenDesktop® Sites
- Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) Sites.

Web Interface sites enable client devices to connect to the server farm. Authentication between Citrix Workspace app for iOS and a Web Interface site can be handled using various solutions, including Citrix Secure Web Gateway.

Also, you can configure StoreFront to provide authentication and resource delivery services for Citrix Workspace app. The configuration enables you to create centralized enterprise stores to deliver desktops, applications, and other resources to users.

For more information about configuring connections, including videos, blogs, and a support forum, see http://community.citrix.com.

Before your users access applications hosted in your Citrix Virtual Apps and Desktops and Citrix DaaS deployment, configure the following components in your deployment as described here.

- When publishing applications on your farms or sites, consider the following options to enhance the experience for users accessing those applications through StoreFront stores.
    - Verify to include meaningful descriptions for published applications because these descriptions are visible to users in Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You can emphasize published applications for your mobile device users. You can list the applications under the Featured list. To populate this list on Citrix Workspace app, edit the properties of applications that are published on your servers. You can now append the KEYWORDS: Featured string to the value of the **Application description** field.
- The screen-to-fit mode adjusts the application to the screen size of mobile devices. To enable this mode, edit the properties of applications that are published on your servers and append the KEYWORDS: mobile string to the value of the Application description field. This keyword also activates the auto-scroll feature for the application.
- To automatically subscribe all users of a store to an application, append the KEYWORDS: Auto string to the description when you publish the application in Citrix Virtual Apps. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application.

- If the Web Interface of your Citrix Virtual Apps and Desktops and Citrix DaaS™ deployment does not have a site, create one. The name of the site and how you create it depends on the version of Web Interface you've installed.

Manual setup

In general, when Citrix Workspace app connects to Citrix Gateway, Citrix Workspace app tries to locate a XenApp and XenDesktop Site or Citrix Virtual Apps website after authenticating. If no site is detected, Citrix Workspace app for iOS displays an error. To avoid this situation, you can configure an account manually so Citrix Workspace app for iOS can connect to Citrix Gateway.

1. Tap the **Accounts** icon > **Accounts Screen** > **Plus Sign (+)**. The New Account screen appears.
2. In the top right corner of the screen, tap the icon to the left of **Options** and tap **Manual setup**. Other fields appear on the screen.
3. In the **Address** field, type the secure URL of the site or Citrix Gateway (for example, `agee.mycompany.com`).
4. Select one of the following connection options. The other fields on the screen change, depending on your selection.

    - **Web Interface** - Select for Citrix Workspace app to display a Citrix Virtual Apps website similar to a Web browser. This UI is also known as Web View.
    - **XenApp Services** - Select for Citrix Workspace app for iOS to locate a specific XenApp and XenDesktop Site for which authentication through the Citrix Gateway isn't configured. In the additional options that appear on this screen, provide site logon credentials.
        - <StoreFront FQDN>: If there are many stores, a list is presented and the user can choose the store to add.
        - <StoreFront FQDN>/citrix/<Store Name>: This option adds the StoreFront store <Store Name>.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- <StoreFront FQDN>/citrix/PnAgent/config.xml: This option adds the default legacy PNAgent store.
- <StoreFront FQDN>/citrix/<Store Name>/PnAgent/config.xml: This option adds the legacy PNAgent store associated with <Store Name>.

- Citrix Gateway - Select for Citrix Workspace app for iOS to connect to a XenApp and XenDesktop Site through a specific Citrix Gateway. In the additional options on this screen, select the server edition and its logon credentials, including whether it requires a security token for authentication.

5. For certificate security, use the setting in the Ignore certificate warnings field to determine whether you want to connect to the server even if it has an invalid, self-signed, or expired certificate. The default setting is OFF.
   Important: If you do enable this option, make sure you're connecting to the correct server. Citrix® strongly recommends that all servers have a valid certificate to protect user devices from online security attacks. A secure server uses an SSL certificate issued from a certificate authority. Citrix does not support self-signed certificates and does not recommend by-passing the certificate security.
6. Tap Save.
7. Type your user name and password (or token, if you selected two-factor authentication), and then tap Log On. The Citrix Workspace app for iOS screen appears, in which you can access your desktops and add and open your apps.

StoreFront

> **Important:**
>
> - When using StoreFront, Citrix Workspace app for iOS supports Citrix Access Gateway Enterprise Edition versions from 9.3, and Citrix Gateway versions through 13.
> - Citrix Workspace app for iOS supports only XenApp and XenDesktop Sites on Web Interface.
> - Citrix Workspace app for iOS supports launching sessions from Workspace for Web, as long as the web browser works with Workspace for Web. If launches do not occur, configure your account through Citrix Workspace app for iOS directly. Users must manually open the ICA file using the browser Open in Workspace function. For the limitations of this deployment, see the StoreFront documentation.

With StoreFront, the stores you create consist of services that provide authentication and resource delivery infrastructure for Citrix Workspace app for iOS. Create stores that count and sum up desktops and applications from the following:

- Citrix Virtual Apps and Desktops and Citrix DaaS sites
- Citrix Virtual Apps farms

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Install and configure StoreFront. For details, see the StoreFront product documentation. For administrators who need more control, Citrix provides a template you can use to create a download site for Citrix Workspace app for iOS.
2. Configure stores for StoreFront as you do for other Citrix Virtual Apps and Desktops and Citrix DaaS applications. No special configuration is needed for mobile devices. For details, see User Access Options in the StoreFront section of Product Documentation. For mobile devices, use either of these methods:

    - Provisioning files. You can provide users with provisioning files (.cr) that has connection details for their stores. After installation, users open the file on the device to configure Citrix Workspace app for iOS automatically. By default, Workspace for websites offer users a provisioning file for the single store for which the site is configured. Alternatively, you can use the Citrix StoreFront management console to generate provisioning files for single or many stores that you can manually distribute to your users.
    - Manual configuration. You can directly inform users of the Citrix Gateway or store URLs to access their desktops and applications. For connections through Citrix Gateway, users must also know the product edition and required authentication method. After installation, users type these details into Citrix Workspace app, which tries to verify the connection and, if successful, prompts users to sign in.
    - Automatic configuration. Tap **Add Account** on the Welcome screen and type the URL of the StoreFront server in the address field. The configuration of the account happens automatically while the account is added.

To configure Citrix Gateway

If you have users who connect from outside the internal network, configure authentication through Citrix Gateway. For example, users who connect using the Internet from a remote location.

- When using StoreFront, Citrix Workspace app for iOS supports Citrix Access Gateway Enterprise Edition versions from 9.3, and Citrix Gateway versions through 13.

Web Interface

To configure the Web Interface site, users with iPhone and iPad devices can launch applications through your Web Interface site and the built-in Safari browser on the mobile device. Configure the Web Interface site the same as you do for other Citrix Virtual Apps applications. If no XenApp and XenDesktop Site is configured for the mobile device, Citrix Workspace app for iOS automatically uses your Web Interface site. No special configuration is needed for mobile devices.

The built-in Safari browser supports Web Interface 5.x.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To launch applications on the iOS device

On the mobile device, users can log on to the Web Interface site using their normal logon and password.

Automatic provision for mobile devices

In StoreFront, use the **Export Multi-Store Provisioning File** and **Export Provisioning File** tasks to generate files containing connection details for stores, including any Citrix Gateway deployments and beacons configured for the stores. Make these files available to users to enable them to configure Citrix Workspace app for iOS automatically with details of the stores. Users can also obtain Citrix Workspace app for iOS provisioning files from Workspace for websites.

> **Important:**
>
> In many server deployments, use only one server at a time to modify the configuration of the server group. Verify if the Citrix StoreFront management console isn't running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile. Select the Stores node in the left pane of the Citrix StoreFront management console.
2. To generate a provisioning file containing details for multiple stores, in the Actions pane, click Export Multi-Store Provisioning File and select the stores to include in the file.
3. Click Export and Save the provisioning file with a `.cr` extension to a suitable location on your network.

User access information

You must provide users with the Citrix Workspace app for iOS account information they need to access their hosted their applications, desktops, and data. You can provide this information by:

- Configuring email-based account discovery
- Providing users with a provisioning file
- Providing users with account information to enter manually

Configure email-based account discovery

You can configure Citrix Workspace app for iOS to use email-based account discovery. When configured, users enter their email address rather than a server URL during initial Citrix Workspace app for iOS installation and configuration. Citrix Workspace app determines the Access Gateway or StoreFront

© 1997–2026 Citrix Systems, Inc. All rights reserved.

server, or Endpoint Management virtual appliance that are associated with the email address that is based on Domain Name System (DNS) Service (SRV) records and then prompts the user to log on to access their hosted applications, desktops, and data.

> **Note:**
>
> Email-based account discovery isn't supported if Citrix Workspace app for iOS is connecting to a Web Interface deployment.

Add DNS Service Location (SRV) record to enable email-based discovery During initial configuration, Citrix Workspace app can contact Active Directory Domain Name System (DNS) servers to obtain details of the stores available for users. This means that users do not need to know the access details for their stores when they install and configure Citrix Workspace app for iOS. Instead, users enter their email addresses and Citrix Workspace app contacts the DNS server. You can gather the domain details from the email address.

To enable Citrix Workspace app to locate available stores that are based on the users' email addresses:

- configure Service Location (SRV) locator resource records for Access Gateway.
- configure the StoreFront or AppController connections on your DNS server.

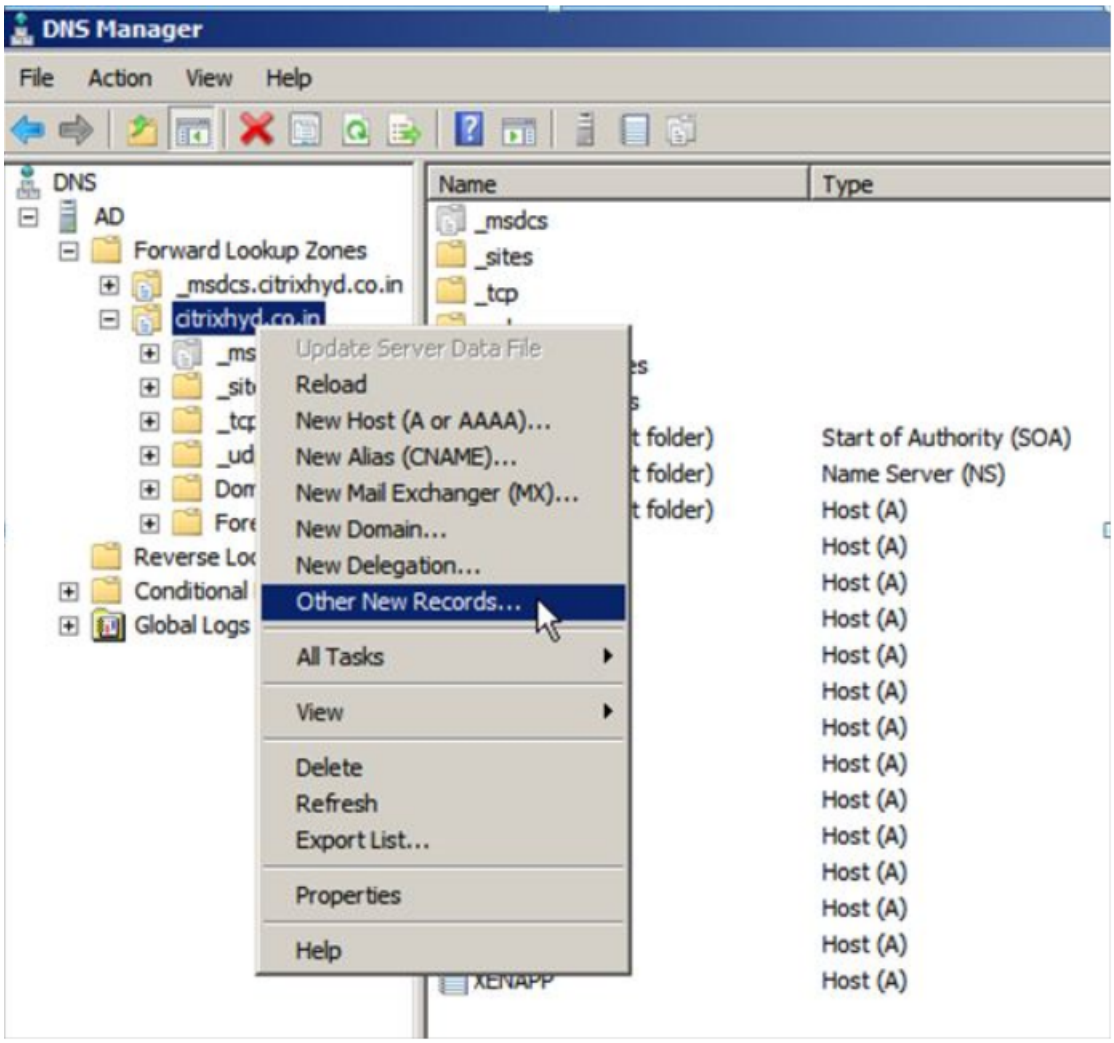
You must install a valid server certificate on the Access Gateway appliance and the StoreFront or AppController server to enable email-based account discovery. The full chain to the root certificate must also be valid. For the best user experience, install either a certificate with:

- a Subject
- a Subject Alternative Name entry of *discoverReceiver.domain*.
- a wildcard certificate for the domain containing your users' email accounts.

To allow users to configure Citrix Workspace app for iOS by using an email address, add an SRV record to your DNS zone as follows:

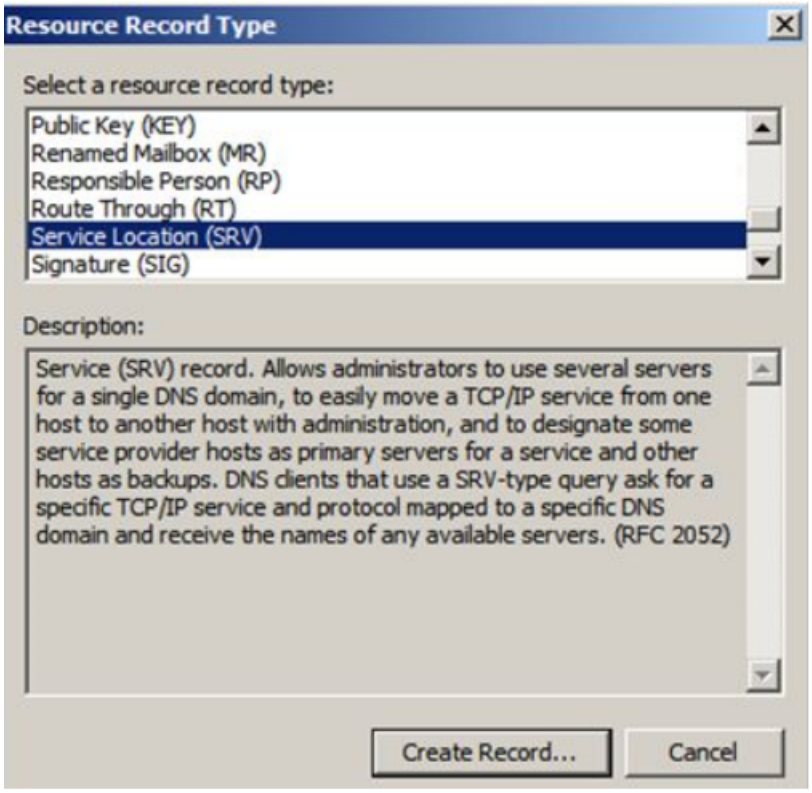
1. Log in to your DNS server.
2. In DNS, right-click your Forward Lookup Zone.
3. Click **Other New Records.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. The **Resource Record Type** dialog box appears.
5. Under **Select a resource record type**, select **Service Location (SRV).**
6. Select **Create Record.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. The Properties dialog box appears.
8. Select the **Service Location** tab.
9. Under **Service**, enter the host value _citrixreceiver.
10. Under **Protocol**, enter the value _tcp.
11. Under **Host offering this service**, specify the fully qualified domain name (FQDN) and port for your Access Gateway appliance (to support both local and remote users) or the StoreFront or AppController server (to support users on the local network only).
12. Click OK.

> **Note:**
>
> Your StoreFront FQDN must be unique and different from the Access Gateway virtual server FQDN. Using the same FQDN for StoreFront and the Access Gateway virtual server isn't supported. Citrix Workspace app requires a unique StoreFront FQDN address that is only resolvable from user devices that are connected to the internal network. If not, Citrix Workspace app users can't use email-based account discovery.

Provide users with a provisioning file

You can use StoreFront to create provisioning files containing connection details for accounts. You make these files available to your users to enable them to configure Citrix Workspace app for iOS automatically. After installing Citrix Workspace app for iOS, users simply open the `.cr` file on the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

device to configure Citrix Workspace app for iOS. If you configure Workspace for websites, users can also obtain Citrix Workspace app for iOS provisioning files from those sites.

For more information, see the StoreFront documentation.

Provide users with account information to enter manually

If providing users with account details to enter manually, ensure you distribute the following information to enable them to connect to their hosted desktops successfully:

- The StoreFront URL or XenApp and XenDesktop Site hosting resources; for example: `servername.company.com`.
- For access using Citrix Gateway, provide the Citrix Gateway address and the required authentication method.

When a user enters the details for a new account, Citrix Workspace app tries to verify the connection. If successful, Citrix Workspace app for iOS prompts the user to log on to the account.

Configure Citrix Workspace app

May 15, 2026

This article lists tasks that help you configure Citrix Workspace app for iOS.

Auto-launch desktops and apps

Starting with version 25.7.2, you can now experience the automatic launching of either desktop or application.

> **Note:**
>
> The mobile platforms support the launch of only one resource at a time. Marking multiple resources for auto-launch might lead to unexpected behavior.

How to configure

To ensure a core application launch automatically in Citrix Workspace, administrators must append the string `KEYWORDS: AutoStartPrimaryApp` to the application description. After it is configured, the application will start automatically for all users.

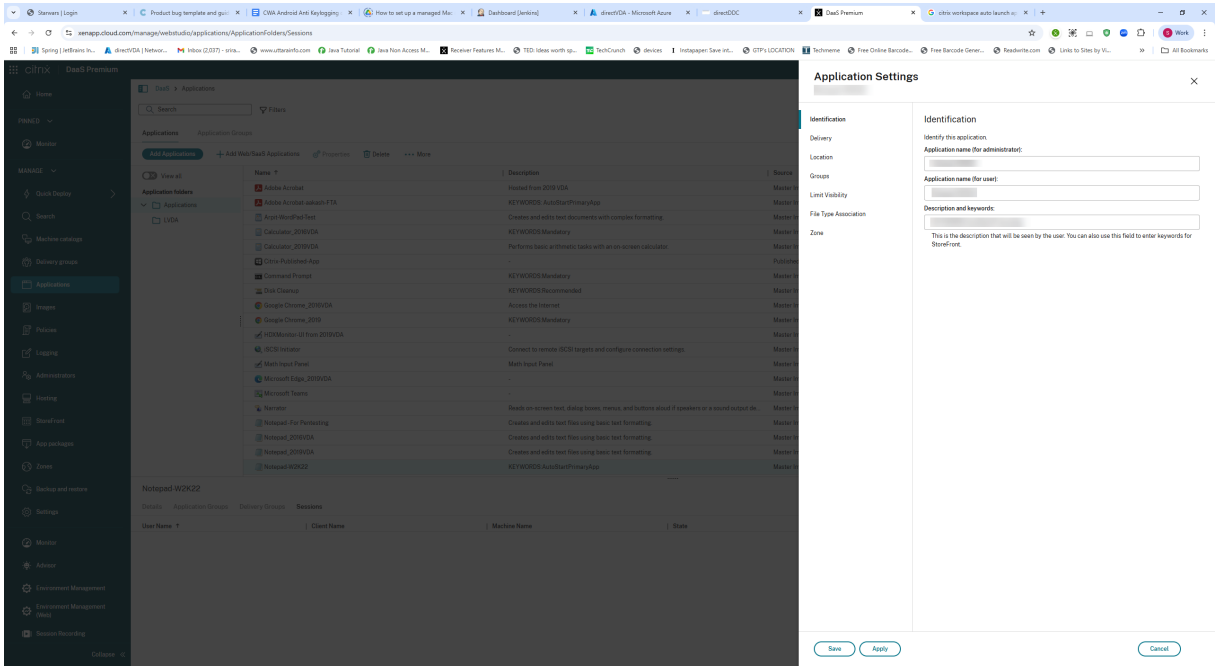
The following steps are for administrators:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Open the management console:**
   Launch Citrix Studio or your organization's Citrix management portal. Sign in with an account that has permissions to edit published applications.
2. **Locate the application:**
   Go to **Applications** and select the application you want to configure for auto-launch (for example, Notepad).
3. **Edit application properties:**
   Select the application, then choose **Edit** or **Properties**. Locate the **Description** field.
4. **Append the auto-start keyword:**
   Add a space at the end of the description, then append the following keyword:

   ```
   KEYWORDS:AutoStartPrimaryApp
   ```

5. **Save the changes:**
   Click **OK**, **Save**, or **Update** to apply the changes.



Enhanced audio quality with real-time Echo Cancellation

Starting with version 25.3.0, Citrix Workspace app for iOS introduces the Echo Cancellation feature, delivering crystal-clear audio on mobile devices. This feature actively eliminates echoes in real-time, ensuring smooth and uninterrupted communication during virtual meetings and calls. It enhances productivity, reduces disruptions, and provides a superior user experience, even in challenging mobile network conditions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supports GACS authenticated microservices (On-premises)

Starting with version 25.1.0, Citrix Workspace app for iOS supports Authenticated Microservices, enabling GACS to manage User Groups. This feature offers administrators with enhanced control for on-premises environments. For more information, see Manage settings for user group using configuration profile.

Fetching GACS endpoints via email, store URL or domain-based discovery API

Starting with the 24.9.0 release, admins can configure a web store based on email address, domain, and store URL, allowing the Global App Configuration service (GACS) to identify and direct users to the appropriate custom web URL. Citrix Workspace app iOS devices can now fetch GACS endpoints using this discovery API, eliminating the need for hardcoded endpoints and reducing unnecessary calls when not configured. This update benefits both cloud and on-premise stores, and users can configure web stores directly through the store URL, with the option to add custom web stores using GACS. For more information, see Global App Configuration service channel support.

Supports GACS authenticated microservices (Cloud)

As of the 24.9.0 release, Citrix Workspace app for iOS support Authenticated Microservices, enabling GACS to manage User Groups for our customers. This provides greater flexibility and control and is currently supported for cloud stores only. For more information, see Manage settings for user group using configuration profile (Preview).

Feature flag management

Feature flags are used to dynamically enable or disable features. If an issue occurs with Citrix Workspace app in production, the affected feature can be disabled even after the feature has been shipped.

No configuration is required to enable traffic for feature management, unless a firewall or proxy is blocking outbound traffic. In such cases, you must enable traffic to specific URLs or IP addresses based on your policy requirements.

Enable traffic for feature flag management

From Citrix Workspace app version 24.10.0 onwards:

To ensure optimal functionality and access to preview features, you must enable traffic to the following URL:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `features.netscalergateway.net`

> **Note:**
>
> Starting January 2025, Citrix Workspace app versions below 24.10.0 no longer support preceding features. After this date, this section becomes irrelevant as versions 24.10.0 or higher have these features enabled. To avoid issues, upgrade to Citrix Workspace app Version 24.10.0 or higher. Additionally, ensure that the `features.netscalergateway.net` setting is enabled. Failure to do so might result in issues with version 24.10.0 or higher.

Inactivity timeout for Citrix Workspace app

Admins can specify the amount of idle time that is allowed. After the time-out value, an authentication prompt appears.

The inactivity timeout value can be set starting from 1 minute to 24 hours. By default, the inactivity timeout isn't configured. Admins can configure the inactivityTimeoutInMinutesMobile property by using a PowerShell module. Click Download PowerShell modules for Citrix Workspace app configuration to download the PowerShell modules for Citrix Workspace app configuration.

When you've reached the specified time-out value, the end-user experience is as follows depending on the authentication type configured:

- After the inactivity timeout, you'll receive a prompt to provide biometric authentication to access the Citrix Workspace app again.
- If you can cancel the biometric authentication prompt, the following message appears:

  Citrix Workspace app is locked.

  You must authenticate to continue to use the Workspace app.

If the passcode is not configured on the iOS, you have to sign in with credentials after the inactivity timeout.

> **Note:**
>
> This feature is applicable for customers on Workspace (Cloud) only.

Customer Experience Improvement Program (CEIP)

What is the Citrix Customer Experience Improvement Program (CEIP) for Citrix Workspace app?

The Citrix Customer Experience Improvement Program (CEIP) collects configuration and usage data from the Citrix Workspace app and automatically sends it to Citrix Analytics. This data enables Citrix to

© 1997–2026 Citrix Systems, Inc. All rights reserved.

analyze the performance and enhance the quality, functionality, and performance of the Citrix Workspace app, optimize resource allocation for product development, and support service levels through effective staffing and infrastructure investment.

All data is used and analyzed solely in aggregate form, ensuring that no individual user or device is singled out or specifically analyzed. Citrix does not collect any Personally Identifiable Information (PII) through CEIP, and all data collection is in accordance with relevant industry data privacy and security standards.

Tools used to gather CEIP Data

Citrix Workspace app for iOS uses Citrix Analytics and Google Firebase to collect the CEIP data.

Data collected

The specific CEIP data elements collected by Citrix Analytics and Google Firebase are:

Session information and session launch method	Citrix stores and store configuration	Auth type and authentication configuration	ICA® connections
HDX™ session launch	Store app session	WebView action open	WebView action copy
WebView action share	Workspace app review	Connection status, connection error, connection center usage	External display
Socket status	Session duration	HDX over UDP	Session launch time
Device information	Device model info	Send usage statistics	App language, Workspace app language
Keyboard language	Citrix store type	Citrix store combination	Store protocol type
Store count	HDX UDP status	RSA token installations	

Which users is CEIP data collected from?

The Citrix Workspace app collects the CEIP data via Citrix Analytics that is configured to include users from all regions. However, CEIP data collected through Citrix Analytics includes user data from the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

European Union (EU), European Economic Area (EEA), Switzerland, and the United Kingdom (UK), whereas Google Firebase excludes users located in these regions. To ensure this functionality is in place, please update to the most recent version.

Can users and administrators disable CEIP data collection?

CEIP data collection can be fully disabled in all jurisdictions as per the below configuration.

Starting with version 2205, you can stop sending CEIP data (with the exception of two data elements, as specified in the note below) by following these steps:

1. Open Citrix Workspace app for iOS.
2. Tap **Home** > **Settings**.
3. Navigate to the **General** section, turn off **Send Usage Statistics**.

Additional information

Citrix handles your data in accordance with the terms of your contract with Citrix. The data is protected as specified in the Citrix Services Security Exhibit. For more information, see the Citrix Trust Center.

Citrix uses Google Firebase to collect certain data from Citrix Workspace app as part of CEIP. Review how Google handles data collected for Google Firebase.

> **Note:**
>
> Google Firebase excludes data collection for users in the European Union (EU), European Economic Area (EEA), Switzerland, and the United Kingdom (UK).

Known limitations

- On VDA 7.18 and earlier, casting to a workspace hub requires the desktop or other resource you're using to have the h.264 full-screen policy enabled and the legacy graphics policy to be disabled.

Session sharing

If users log off from a Citrix Workspace app account, they can still disconnect or log off from remote sessions.

- **Disconnect**: Ends the connection on this device, but your session keeps running on the server—you can reconnect later and continue where you left off. The user can then start another device, launch Citrix Workspace app for iOS, and reconnect to the last state before the user discon-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nects from the iOS device. This option allows users to reconnect from one device to another device and resume working in running applications.

- **Log off**: Logs off from the account and closes the Windows application. It also logs off from the Citrix Virtual Apps and Desktops, and Citrix DaaS server. This option allows users to disconnect from the server and log off from the account. When they launch Citrix Workspace app for iOS again, it opens in the default state.

Cloud stores

You can access the web, SaaS apps, and websites hosted by your organization regardless of your access location. This feature is available only for customers on cloud stores.

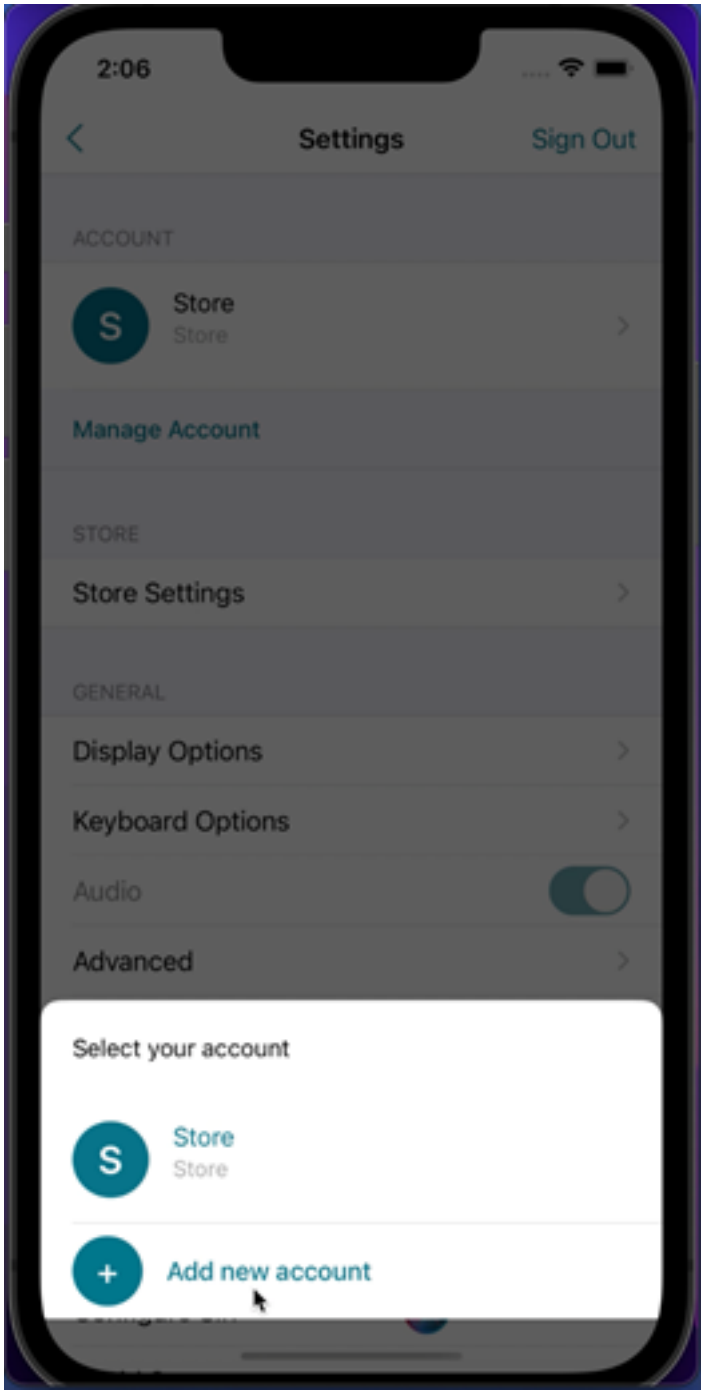
Support for multiple cloud stores

Starting with the 24.1.0 release, you can add multiple cloud store accounts to the Citrix Workspace app for iOS and iPadOS. Now, it's easy for end users to add and switch between multiple stores. This feature improves the user experience when accessing multiple stores.

To add another account, do the following steps:

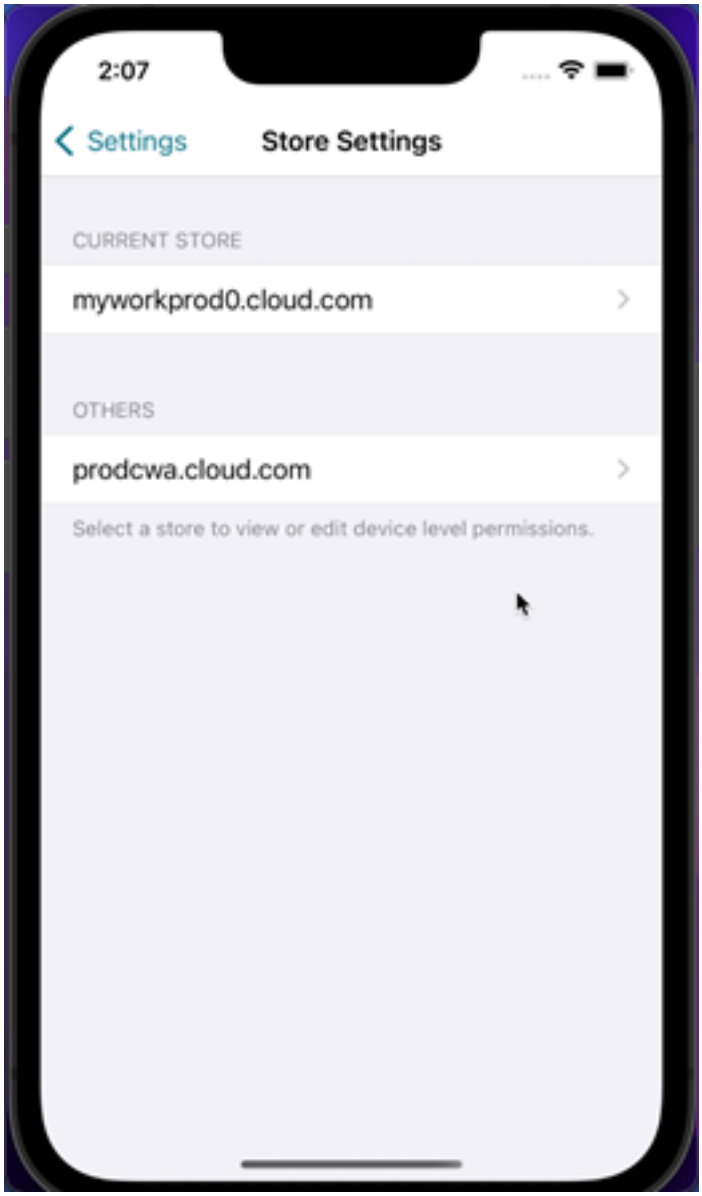
1. Navigate to **Settings > Manage Account**. A dialog appears at the bottom of the screen with a list of your accounts.
2. Tap **Add new account**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Type the URL or email address provided by your IT administrator. To optionally use a smart card to log on, tap **Use smart card**.
4. Tap **Continue**. The **Sign in** dialog appears with fields for your user name, password, domain, and passcode.
5. Type the information. For more information about the fields, contact your IT administrator.
6. Tap **Sign in**. Your new account is now set up.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Auto-populate store URL

Starting with the 23.2.0 version, when you're accessing the rebranded Citrix Workspace app for iOS, you can choose to auto-populate the store URL. This capability reduces manual intervention and provides quick access to the app. For more information about app personalization, see App Personalization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for deleting multiple stores at once

Starting with the 24.2.0 version, Citrix Workspace app for iOS supports the selection of multiple stores and deleting them. This feature improves the user experience while working with multiple stores. This feature is enabled by default.

To delete multiple stores at once from the **Stores** screen, do the following steps:

1. On the **Stores** screen, tap **Select**.
2. Select stores to delete. To delete all the stores, tap **Select All**.
3. Tap **Delete**.

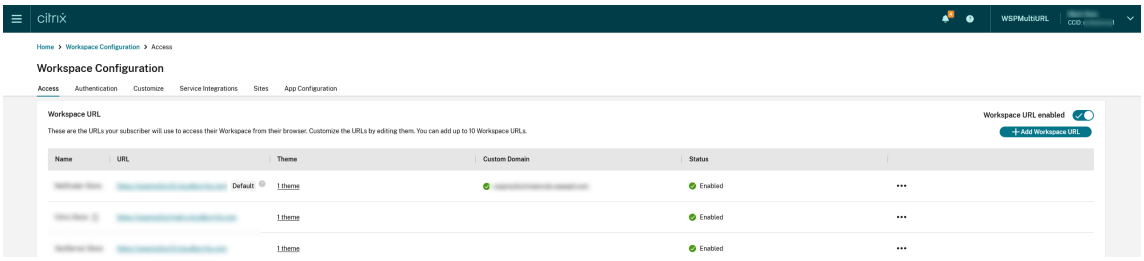
Support for administrator to restrict the user from changing the store name

Previously, users were able to change the store name by using the **Edit Account** option.

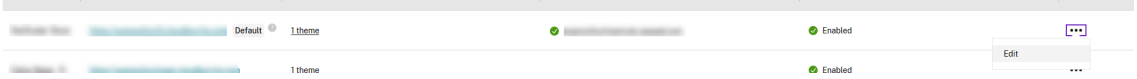
Starting with 24.2.0, Citrix Workspace app for iOS provides administrators an option to disable the user from changing the store name. With this feature, administrators can easily identify and maintain consistency in the store names.

To allow the end-users to change the store name, do the following steps:

1. Sign in to Citrix Cloud with your credentials.
2. Navigate to **Workspace Configuration > Access**. Under **Workspace URL**, you can find a list of existing store URLs.

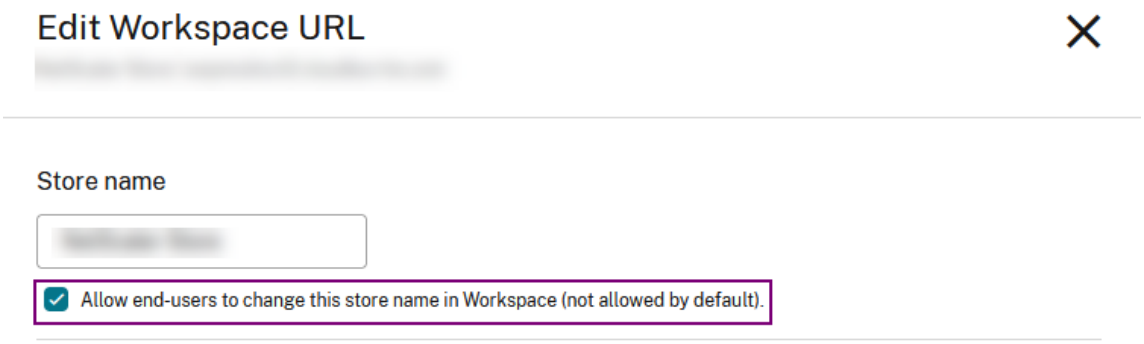


3. Click the ellipsis menu for the store that you want to allow end-users to change the store name.
4. Select **Edit**.



5. On the **Edit Workspace URL** dialog box, select **Allow end-users to change this store name in Workspace (not allowed by default)**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Click **Save**.

Auto-populate store name

Starting with the 24.2.0 version, Citrix Workspace app for iOS supports store name updates by the administrator and automatically pushes the updated store names to the user. This feature improves the user experience by eliminating the need for manual intervention when updating the store name.

> **Note:**
>
> This feature can take effect only if the administrator has disabled the user from changing the store name.

End user experience monitoring enhancement

We now support the EUEM (End user experience monitoring) client startup metrics. EUEM helps in collecting highly granular session experience monitoring data in real time. It sends the data to the Director dashboard, so that the administrator can monitor the user experience. The data is collected through the Session experience monitoring service (SEMS) present on the VDA. Client startup metrics data available for monitoring on the dashboard includes:

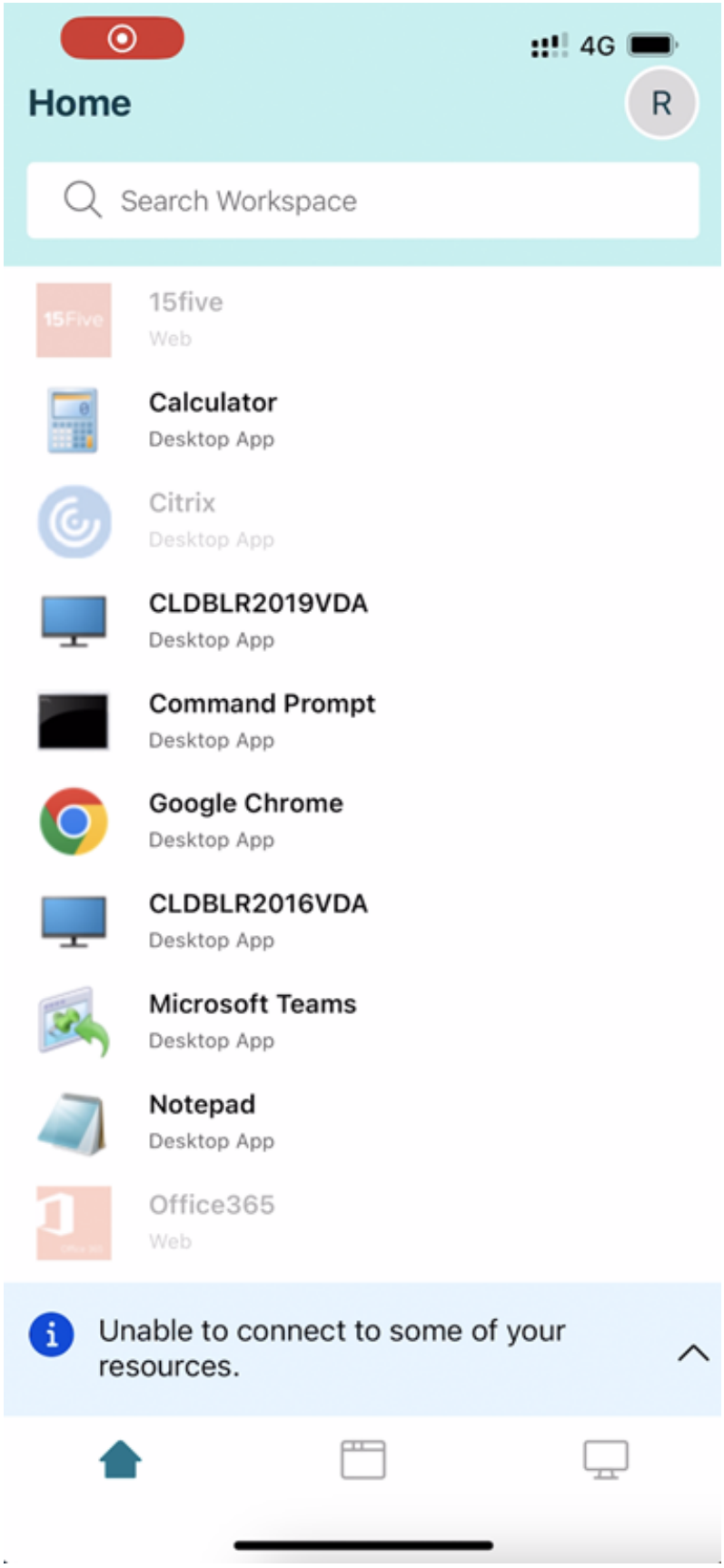
- ICA file download duration.
- Session creation client duration. Session creation client duration represents the time taken to create a session. It is calculated from the moment that an ICA file is launched till the connection is established.
- Session lookup client duration. Session lookup client duration represents the time taken to query every session for hosting the requested published application. The check is performed on the client to determine whether an existing session can handle the application launch request.
- Citrix real-time recording of the ICA round trip time, also known as ICA RTT. ICA RTT is the time that elapses from when the user presses a key until the response is displayed at the endpoint.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhanced the user interface for Service continuity offline mode

Starting with the 24.1.0 release, the Citrix Workspace app for iOS's user interface has been improved to be more informative, modern, and provide a user-friendly experience during Citrix Workspace outages. The fuzzy search feature is also included for offline mode. With this feature, you can find the results for apps or desktops with closely matching text and misspelled search terms. For more information about the Service continuity, see Service continuity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Global App Configuration service channel support

Starting with the 23.4.5 release, administrators can now use the Global App Configuration service to define settings and test them before rolling out the configuration to all end users. This process ensures that features and functionalities are well-tested before production.

> **Note:**
>
> - Citrix Workspace app for iOS supports the **Default** and **Test channel** configurations. By default, all users are on the **Default** channel.

For more information, see the Global App Configuration service documentation.

For more information on how to configure, see Global App Configuration service channel support.

Access Global App Configuration service enabled web stores

Starting with the 23.7.5 version, admins can now configure a web store (web interface) for email-based store discovery. Based on the email address entered by the end users while adding a store (on the Welcome screen), the Global App Configuration service helps identify the custom web (web interface) URL defined by the admin. The end user is then directed automatically to the web store configured by the admin. To know more about configuring web store URLs for end-users, see Allowed custom web portal.

Configure Workspace app using Unified Endpoint Management solutions

May 15, 2026

Starting with the 23.3.0 version, Citrix Workspace app for iOS supports admin configuration of the Workspace app using AppConfig-based key-value pairs using Unified Endpoint Management (UEM) solutions.

How to configure

To configure your Workspace Store URL using Unified Endpoint Management solutions, follow these steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> For demonstrative purposes, Microsoft Intune is used as the UEM solution in this example. The steps below and UI shown differs depending on your UEM provider.

1. Sign in to your Unified Endpoint Management (UEM) provider.
2. Add the Citrix Workspace app that you want to manage by your UEM provider. You can upload the app by using your UEM provider's portal to enable management by your UEM provider. Alternatively, you can link to the app in the App Store.
3. Create an app configuration policy for your app.
4. Add a key and value pair to the XML property list and fill in the following values:
    - **key**: `url`
    - **value type**: `String`
    - **value**: your store URL (for example, `prodcwa.cloud.com`)

Settings Edit

Configuration key	Value type	Configuration value
url	String	prodcwa.cloud.com

Limitations

- If a cloud store is already set up, and the administrator configures a new cloud store, your existing cloud store is deleted. It also deletes any associated data or settings of the existing cloud store. You receive a notification in Citrix Workspace. You must then sign in again so that the new cloud store is added to Citrix Workspace.
    - The above statement only applies to existing cloud stores. If an on-prem store is already configured and the admin configures a new cloud or on-prem store, then the new store is added and no deletion occurs.
- To apply new configurations, you must force-quit and restart the Citrix Workspace app.

Enhancements to Unified Endpoint Management solutions

Starting with the 23.4.5 version, Citrix Workspace app for iOS supports a couple more configurations using AppConfig-based key-value pairs to configure the Citrix Workspace app. Previously, administrators could configure Store URLs. Now, administrators can restrict end users to modify Store URLs and control how the app appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration key	Value type	Configuration value
url	String	myworkprod0.cloud.com
restrict_user_store_modification	Boolean	true
storeType	Integer	1

The following are the details:

Configuration key	Value type	Configuration value
`url`	`String`	The store URL. For example, `prodcwa.cloud.com`
`storeType`	`Integer`	• (default) If set to 1, users can view the native or the default store loading. - If set to 2, users can view the store inside a web interface.
`restrict_user_store_modification`	`Boolean`	• If set to **true**, users can't modify the store (add/delete/edit). - If set to **false**, users can modify the store. **Note:** If the flag is set to true, all the existing stores are deleted before adding a UEM -configured store.

Support for configuring device name through UEM

Starting with the 24.3.5 version, Citrix Workspace app for iOS enables administrators to assign and identify device names based on user groups through Unified Endpoint Management (UEM).

To configure the device name using UEM, do the following steps:

> **Note:**
>
> For demonstrative purposes, Microsoft Intune is used as the UEM solution in this example. The steps below and the UI shown differ depending on your UEM provider.

1. Sign in to your UEM provider.
2. Add Citrix Workspace app that you want to manage by your UEM provider. You can upload the app by using your UEM provider's portal to enable management by your UEM provider. Alternatively, you can link to the app in the App Store.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Create an app configuration policy for your app.
4. Add a key and value pair to the XML property list and fill in the following values:

    - key: deviceName
    - value type: String
    - value: Name of the device (for example, MY_IPHONE_Device)



Support for configuring Citrix Workspace app settings through UEM

Previously, you can only configure the store URL in the Citrix Workspace app using the Unified Endpoint Management (UEM).

Starting with the 24.7.0 version, you can also configure the Citrix Workspace app settings on the managed devices using any UEM solution that is deployed in your infrastructure.

> **Note:**
>
> As an administrator, if you have an option of configuring the Citrix Workspace app settings using UEM and Global App Configuration service (GACS), UEM settings take precedence over GACS.

The following is a sample json file to configure the Citrix Workspace app settings:

```
<dict>
    <key>stores</key>
    <array>
        <dict>
            <key>url</key>
            <string>https://teststore.cloud.com</string>
            <key>storeType</key>
            <integer>1</integer>
            <key>displayName</key>
            <string>Cloud Store 1</string>
            <key>appSettings</key>
            <array>
                <dict>
                    <key>category</key>
                    <string>audio</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
                        <dict>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                                <key>name</key>
                                <string>settings_audio_stream</string>
                                <key>value</key>
                                <true/>
                            </dict>
                        </array>
                    </dict>
                    <dict>
                        <key>category</key>
                        <string>authentication</string>
                        <key>userOverride</key>
                        <false/>
                        <key>settings</key>
                        <array>
                            <dict>
                                <key>name</key>
                                <string>settings_auth_web_browser</string>
                                <key>value</key>
                                <string>embedded</string>
                            </dict>
                        </array>
                    </dict>
                </array>
            </dict>
            <dict>
                <key>url</key>
                <string>https://teststore.cloud.com</string>
                <key>storeType</key>
                <integer>1</integer>
                <key>displayName</key>
                <string>StoreFront1</string>
                <key>appSettings</key>
                <array>
                    <dict>
                        <key>category</key>
                        <string>audio</string>
                        <key>userOverride</key>
                        <false/>
                        <key>settings</key>
                        <array>
                            <dict>
                                <key>name</key>
                                <string>settings_audio_stream</string>
                                <key>value</key>
                                <false/>
                            </dict>
                        </array>
                    </dict>
                    <dict>
                        <key>category</key>
                        <string>authentication</string>
                        <key>userOverride</key>
                        <false/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                    <key>settings</key>
                    <array>
                        <dict>
                            <key>name</key>
                            <string>settings_auth_web_browser</string>
                            <key>value</key>
                            <string>system</string>
                        </dict>
                    </array>
                </dict>
            </array>
        </dict>
    </array>
    <key>storesToDelete</key>
    <array>
        <string>test.cldblr.com</string>
        <string>test.cloud.com</string>
    </array>
    <key>restrict_user_store_modification</key>
    <false/>
</dict>
```

> **Note:**
>
> The `userOverride` flag allows the user to modify the Citrix Workspace app settings. If the `userOverride` flag is set to true, the user can change the settings. If the `userOverride` flag is set to false for any settings, then the user can't modify it in the Citrix Workspace app settings.

Key-Value pair table for Workspace app settings

The following table provides the key-value pair information:

> **Note:**
>
> You must add settings that are specific to a category in one block under that category.

Category	Setting	Description	Key	Value	Value Type	Default value
authentication	Skip use of biometrics prompt	Enables or disables biometric authentication.	settings_skip_touch_id_for_biometric_protected_password_saving_value	true/false	Boolean	FALSE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Setting	Description	Key	Value	Value Type	Default value
audio	Audio	Provides access to users to turn the audio on or off from the virtual app or desktop.	settings_audio_stereo	true/false	Boolean	TRUE
keyboard	Use Unicode Keyboard	Allows users to use a standard Unicode keyboard.	settings_use_unicode_keyboard	true/false	Boolean	TRUE
keyboard	Automatic keyboard	Enables or disables the in-session keyboard.	settings_automatic_keyboard	true/false	Boolean	TRUE
keyboard	Keyboard Layout Sync	Allows users to switch to a preferred keyboard layout on the device.	settings_keyboard_layout_sync	true/false	Boolean	FALSE
keyboard	Use Custom Keyboards	Allows users to use third-party keyboards that are down-loaded in the virtual session.	settings_allow_keyboard_extensions	true/false	Boolean	FALSE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Setting	Description	Key	Value	Value Type	Default value
display	Session Resolution	Allows users to select the screen resolution.	settings_resolution	0-9	Integer	5 (iPad) 3 (iPhone)
display	Presentation Mode	Allows you to use your iOS device as a trackpad to control your session while using an external display.	settings_presentation_mode	true/false	Boolean	FALSE
display	External Display	Connects an external display to the device.	settings_external_display	true/false	Boolean	TRUE
advanced	Strict Certificate Validation	Enforces stricter control on server certificate validation.	settings_strictCertValidation	True/false	Boolean	FALSE
advanced	TLS Versions	Allows users to change their TLS settings for trou-bleshooting purposes.	settings_tlsVersion	0-3	Integer	0

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Setting	Description	Key	Value	Value Type	Default value
advanced	Use Native Combo Box	Enables the use of the iOS native selection feature.	settings_native_combobox	true/false	Boolean	TRUE
advanced	Touch Enable (iPAD only)	Enables touch for all apps and desktops, including those that do not have the touch option enabled natively.	settings_multitouch	true/false	Boolean	true (iPad) false (iPhone)
advanced	Fullscreen View	Allows you to view your apps and desktops in full screen.	settings_mobile_view_fullscreen	true/false	Boolean	true (iPad) false (iPhone)
advanced	Reconnect upon Login	Allows a session to automatically reconnect when a new account is added or during sign-in.	settings_reconnect_login	true/false	Boolean	FALSE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Setting	Description	Key	Value	Value Type	Default value
advanced	Reconnect upon Refresh	Automatically reconnects to a session launched from another device upon refresh of the apps or desktops on the second device.	settings_reconnect_refresh	true/false	Boolean	FALSE
advanced	Enable HTTP Proxy	Allows you to use the HTTP proxy for a session.	settings_use_local_proxy	true/false	Boolean	TRUE
advanced	Use derived credentials	Allows to use derived credentials.	setting_useDerivedCredentials	true/false	Boolean	FALSE
advanced	Smart Card in session	Allows the use of a smart card device within a session. This setting doesn't allow users to authenticate to the session.	settings_usesmartcardInsideSession	true/false	Boolean	FALSE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Setting	Description	Key	Value	Value Type	Default value
advanced	Allow EDT	Enables adaptive transport support.	settings_allowedt	true/false	Boolean	TRUE
advanced	Auto Tablet Mode	Enables to launch the virtual session in tablet mode, when there is no external keyboard or mouse detected.	settings_enableTabletMode	true/false	Boolean	TRUE
advanced	Keep the Display On	Keep the screen on.	settings_stay_awake	true/false	Boolean	FALSE
advanced	Use iPAD storage	Allows you to access local drives on your device.	settings_clientdrive	true/false	Boolean	false
X1 Mouse	Allow X1 Mouse	Allows you to switch access to your Citrix X1 Mouse.	settings_allowtrackpad	true/false	Boolean	FALSE
X1 Mouse	Citrix® X1 Mouse speed	Allows users to control the speed of the mouse cursor within the virtual session.	settings_x1MouseSpeed	1-2	Integer	200 (iPadPro) 100 (All other devices)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Setting	Description	Key	Value	Value Type	Default value
X1 Mouse	Use remote cursor image forCitrix X1 Mouse	Makes the cursor match the app or desktop within a session. For example, if the cursor is over a text box, it changes to match the text box.	settings_X1_mouse_use_server_side_cursor	true/false	Boolean	TRUE
authentication	Web Browser for Authentica-tion	Allows you to identify usage of SafariView-Controller instead of WKWeb on the device.	settings_auth_system_browser	true/false	String	Embedded
thirdPartyServices	LaunchDarkly	Enables the Launch-Darkly flag on the Citrix Workspace app features.	enableLaunchDarkly	true/false	Boolean	true (non-EU regions)

Key-Value pair table for new toolbar menu options

The following table provides the key-value pair information for new toolbar:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Setting	Description	Key	Value	Value Type	Default value
toolbar	New Toolbar	The Key which enables the new toolbar.	enableNewToolbar	true/false	Boolean	TRUE
toolbar	Disconnect	Provides options to logout from or disconnect the session or cancel the action.	enableCloseToolbarOption	true/false	Boolean	TRUE
toolbar	Keyboard	Enables or disables the in-session keyboard.	enableKeyboardToolbarOption	True/false	Boolean	TRUE
toolbar	Pointer	Enables or disables the pointer in a session.	enablePointerToolbarOption	True/false	Boolean	TRUE
toolbar	Magnifier	Magnifies the selected portion of the session.	enableMagnifierToolbarOption	True/false	Boolean	TRUE
toolbar	Switch apps	Enables switching between apps opened.	enableSwitchAppsToolbarOption	True/false	Boolean	TRUE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Setting	Description	Key	Value	Value Type	Default value
toolbar	Connection Strength	Displays the Network connection strength of the session.	enableConnectionStrengthToolbarOption	true/false	Boolean	TRUE
toolbar	Ctrl+Alt+Del	Provides options to close, lock or logout the session.	enableCtrlAltDelToolbarOption	true/false	Boolean	TRUE
toolbar	Devices	Enables connection to external devices	enableDevicesToolbarOption	true/false	Boolean	TRUE
toolbar	Devices-Pair	Enables pairing option with external peripherals.	enablePairToolbarOption	true/false	Boolean	TRUE
toolbar	Virtual Mouse	Enables virtual mouse in the session.	enableSoftMouseToolbarOption	true/false	Boolean	TRUE
toolbar	Arrow Keys	Enables the four arrow keys using which user can navigate within the session.	enableArrowKeysToolbarOption	true/false	Boolean	TRUE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Setting	Description	Key	Value	Value Type	Default value
toolbar	Display	Takes the user to the display settings of the CWA app	enableDisplaySettingsToolbarOption	true/false	Boolean	TRUE
toolbar	Casting	Enables or disables the casting functionality	enableCastingToolbarOption	true/false	Boolean	TRUE
toolbar	Camera	Enables users to activate the front, rear or external camera.	enableCameraToolbarOption	true/false	Boolean	TRUE
toolbar	Scan document	Enables users to scan a document from within the Desktop session.	enableScanDocumentToolbarOption	true/false	Boolean	TRUE
toolbar	Help	Activates the Help menu useful for the first time user to navigate the toolbar menu.	enableHelpToolbarOption	true/false	Boolean	TRUE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Key-Value pair table for Session Reconnect settings

The following table provides the key-value pair information for new toolbar:

Category	Setting	Description	Key	Value	Value Type	Default value
Advanced	Session reconnect	Enables session reconnect	settings_manual_reconnect	true/false	Boolean	TRUE

Peripheral devices

August 26, 2026

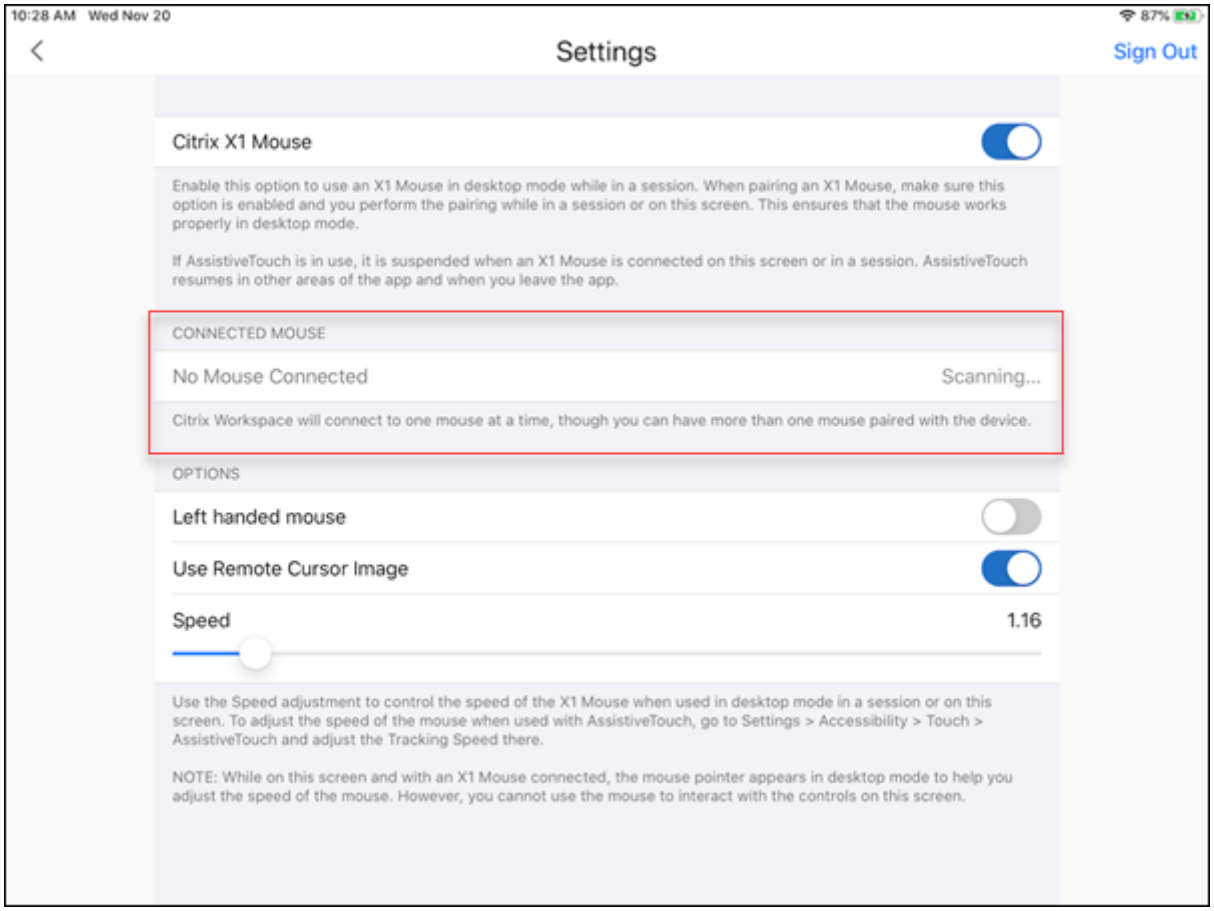
Citrix® X1 Mouse

Citrix X1 Mouse pairing and connection status

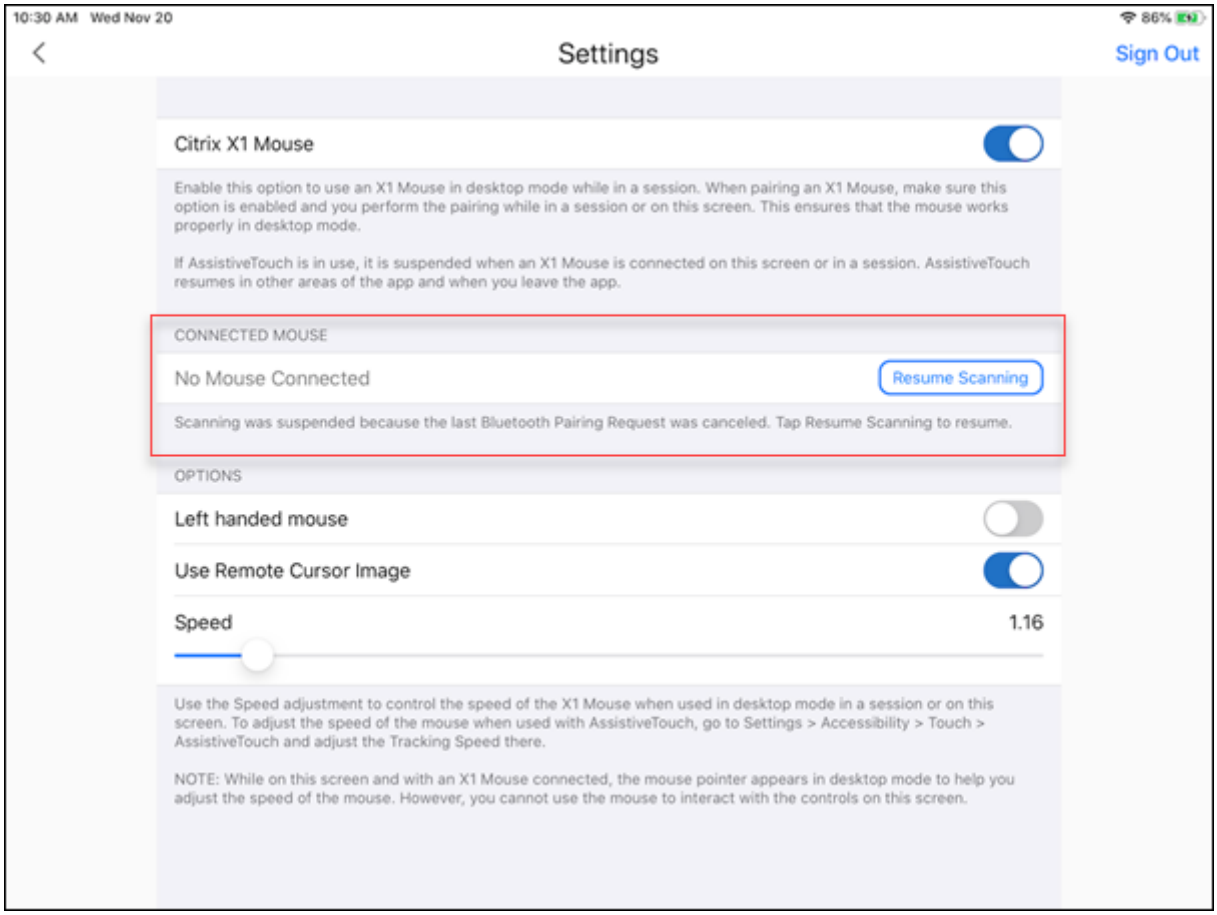
This feature lets you have more control over the Citrix X1 Mouse pairing process. On the **Settings** screen, you can:

- Pair the Citrix X1 Mouse. You can also pair an X1 Mouse when you are in a session.
- View the connection status.

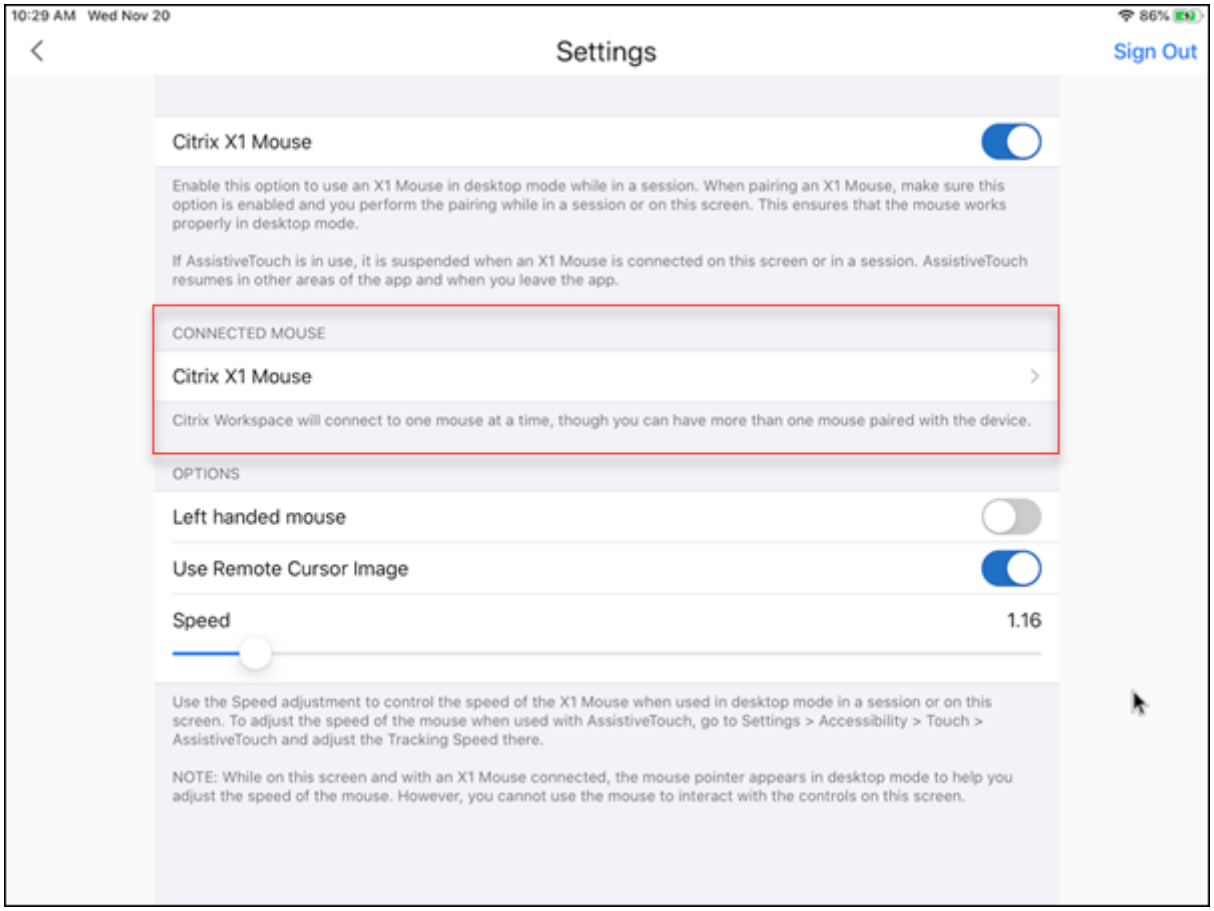
© 1997–2026 Citrix Systems, Inc. All rights reserved.



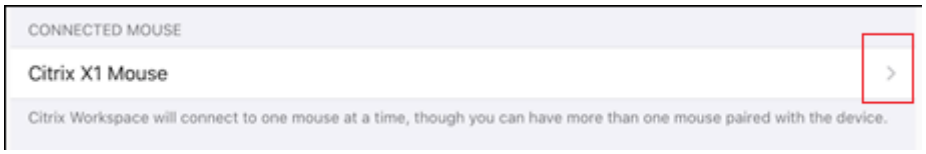
© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



- View the Citrix X1 Mouse properties such as **Name**, **UUID**, **Firmware Revision**, and **Battery Level**. To do so, tap the Citrix X1 Mouse entry under **CONNECTED MOUSE**.



Connected mouse properties:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



AssistiveTouch With the AssistiveTouch feature enabled on iOS 13 or later, you can see the AssistiveTouch cursor if you switch between desktop mouse mode and AssistiveTouch mode.

> **Note:**
>
> In desktop mouse mode, the pointer cursor appears. In AssistiveTouch mode, the round cursor appears.

The AssistiveTouch cursor appears in the following cases:

- Leave a session
- Go to the iOS App Switcher screen
- Go to the iOS home screen or another app

Desktop mode resumes when you navigate back to Citrix Workspace app and when you are in a session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

External monitor and toolbar support

You can use the Citrix X1 Mouse to operate the toolbar on an external monitor. You can move the toolbar notch horizontally, while the toolbar is closed. When you connect your iOS device to the external monitor, Citrix Workspace app automatically detects the screen resolution of the external monitor. You can use the **Display** button on the toolbar to select a particular screen resolution. You can access the **Display** option without having to add an account or sign in first.

Generic Mouse

Generic mouse and trackpad support

You can use a generic mouse or trackpad to right-click, scroll, and hover in HDX™ sessions. The actions are similar to the Citrix X1 Mouse. The style of the local mouse cursor changes to match that of the remote cursor.

> **Notes:**
>
> - This feature is available on iPadOS 13.4 and later.
> - This feature isn't supported on iPhones.

Limitation If you have an external monitor connected while in a session, the generic mouse cursor remains on the native device due to an iOS limitation.

Generic mouse support on external monitors

You can use a generic mouse on external monitors connected to an iPad. Generic mouse is supported on devices running iOS 13.4 or later.

> **Important:**
>
> To use a generic mouse with external monitors, ensure that **Presentation** mode is turned off in your Citrix Workspace app by navigating to **Settings** > **Display options**.

The toolbar on the external monitor is hidden when you use a generic mouse. Also, the mouse pointer is mirrored on the external monitor and appears on both your iPad screen and on the external monitor simultaneously.

Extended multi-monitor support with Generic Mouse for iPad

You can extend the desktop session onto an external monitor when you connect your iPad with a Generic Mouse. This feature supports iPadOS version 14.0 and later.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - This feature can be partially available in earlier versions. To use the complete feature, upgrade to version 22.1.0.
> - Disable AssistiveTouch in iOS **Settings** > **Accessibility** > **Touch** > **AssistiveTouch** for the Citrix Workspace app to receive primary mouse clicks.

Configure Extend mode To enable the **Extend** mode:

1. Connect the external monitor to the iPad using the HDMI cable and the required adapters.

   > **Note:**
   >
   > The setup works best with an Apple's USB-C to Digital AV Multiport Adapter or Lightning Digital AV Adapter.

2. Navigate to the application **Settings** > **Display options** and toggle **ON** the **External display**. Different display modes appear. Mirror and Presentation modes also use Generic Mouse, if the iPadOS version is 14.0 and later.
3. Select the **Extend** option.

   You can select one of the following display modes:

   - Mirror: Allows you to mirror the display on the external monitor connected to the iPad.
   - Presentation: Allows you to change your external monitor to trackpad.
   - Extend: Allows you to display different views or screens on each display.

> **Note:**
>
> - Set the **Extend** mode before you launch and extend the desktop session.
> - The **Extend** mode isn't supported on the iPhone until announced.

Configure display arrangement To configure the display arrangement:

1. Select the **Extend** mode, the **Display arrangement** option appears.
2. Reposition the **External display** tile left, top, right, or bottom to the iPad display.

> **Note:**
>
> You can adjust the display arrangement when you're in a session using the in-session toolbar > **Display** setting icon.

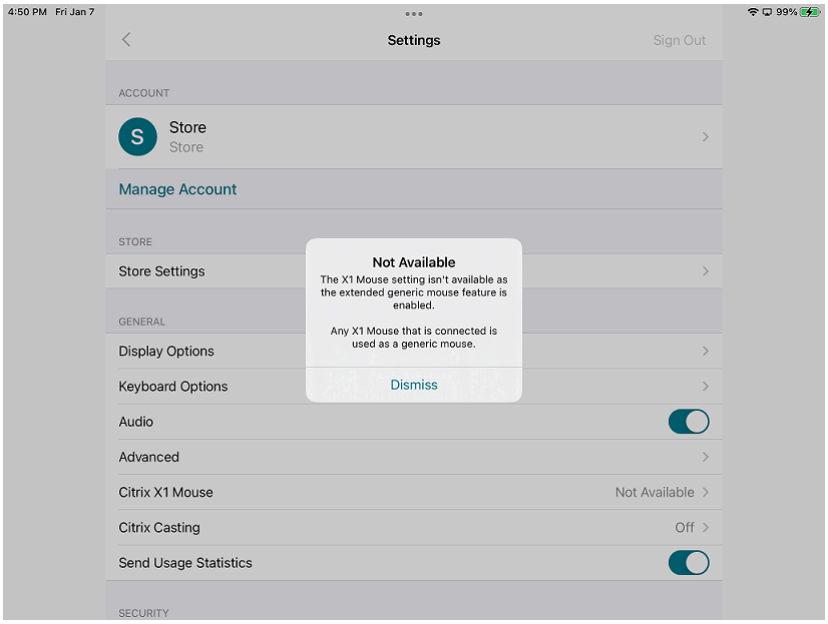
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The external display resolution depends on:
>
> - adapters
> - iPad
> - other hardware used

Generic Mouse mode versus Citrix X1 Mouse mode

The Generic Mouse mode automatically takes precedence over the Citrix X1 Mouse mode. If you have an X1 Mouse connected, it's used as a Generic Mouse instead. So, the X1 Mouse settings page isn't accessible when the Generic Mouse feature flag is enabled.

> **Note:**
>
> For iPadOS version 14.0 and later, any X1 Mouse that is connected to the iPad behaves as a blue-tooth mouse.

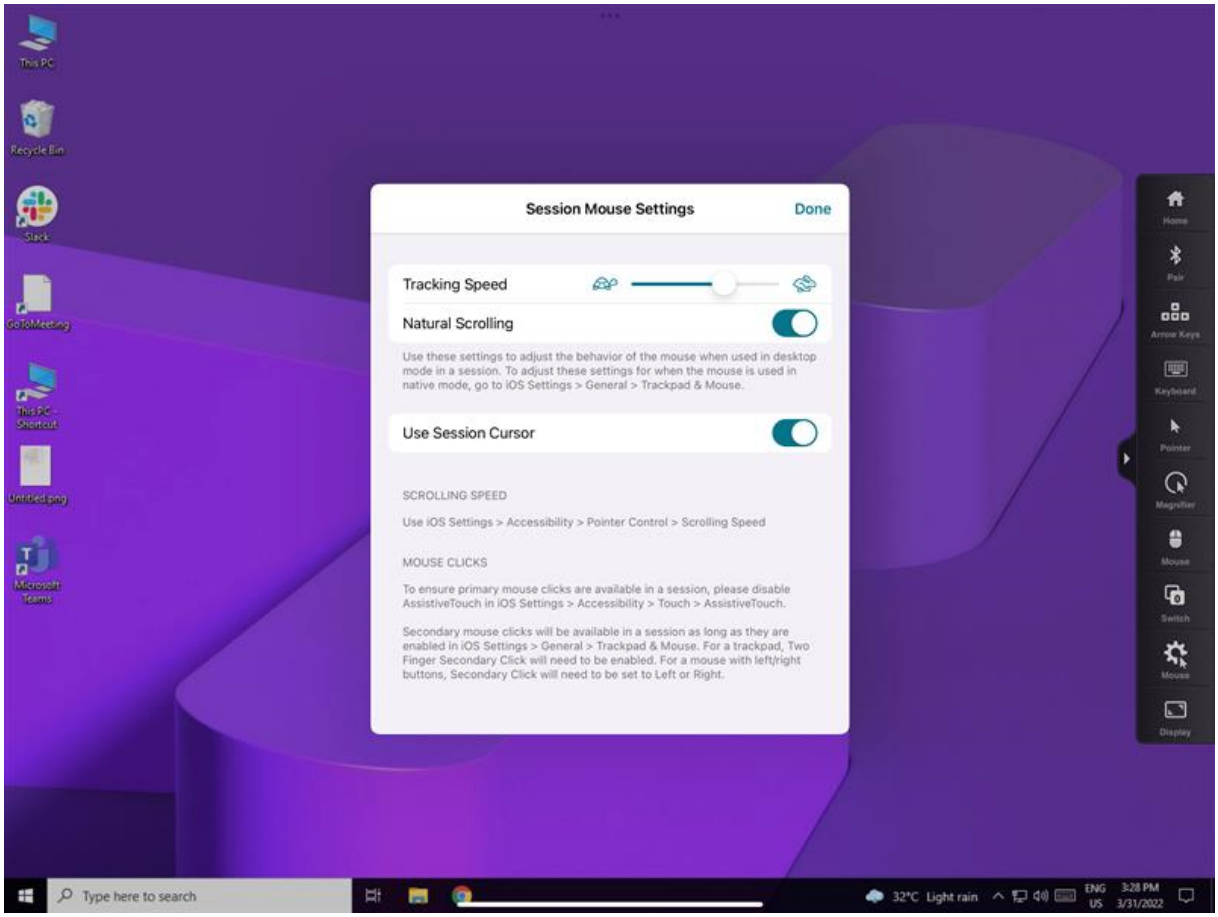


Generic Mouse icon

The **Mouse** settings icon is added on the in-session toolbar next to the **Display** settings icon. Use the **Mouse** settings to adjust the tracking speed of the Generic Mouse when you are in a session. You can also toggle using the remote cursor image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> You can adjust the tracking speed of the native mouse from the iOS settings.



Feature limitations

- To ensure that the Citrix Workspace app receives primary mouse clicks, disable AssistiveTouch in iOS **Settings** > **Accessibility** > **Touch** > **AssistiveTouch**.
- Tracking Speed and Natural Scrolling options from iOS settings doesn't affect the generic mouse inside the session. However, scrolling speed can be controlled from the iOS **Settings**.
  You can access Tracking speed and Natural scrolling options from the **Mouse Settings** screen inside the session toolbar.
- When an iPad is used in the split mode and the monitor is connected, the generic mouse works only in the mirror mode inside a desktop session.
- If the native cursor is over the multi-tasking menu before the app obtains the pointer lock, that is, before the session launch, the mouse events aren't received.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

As a workaround, pull down the Notification Center and move the native pointer to a different location and dismiss the Notification Center.

- Audio redirection fails when you connect an iPad to an external monitor. The audio plays through the iPad speakers. [HDX-39159]

Known issues in the feature

- While the session is active, the desktop image that appears on an iPad or an external monitor gets disturbed when you change the:
  - Display arrangement
  - Resolution
  - Orientation or
  - Display modes

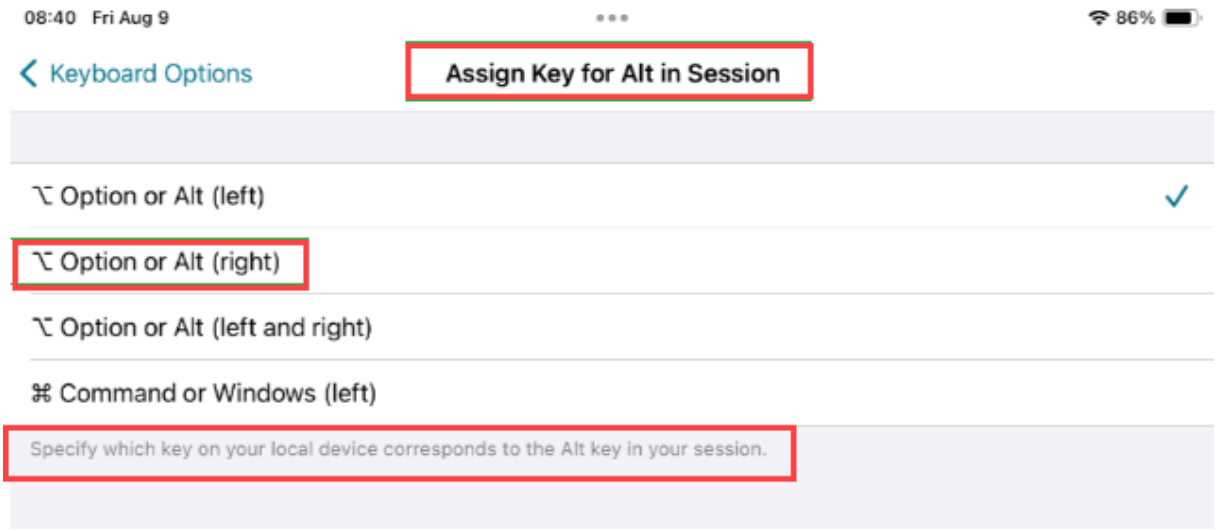
  As a workaround, disconnect and reconnect the monitor. If the issue persists, disconnect, and relaunch the session. [HDX-37038] [HDX-36979] [HDX-36925] [HDX-36924].
- On rare occasions, you can observe a few seconds lag in the audio when the video is played on the external monitor. [HDX-39159]
- On rare occasions, the VDA display is truncated on an iPad and on the external monitor. As a workaround, disconnect, and reconnect the monitor. If the issue persists, disconnect and relaunch the session. [HDX-37100]
- When you maximize the video to full-screen on the external monitor, you might observe video quality issues. [HDX-39159]
- On rare occasions, inside a desktop session, an attempt to move the apps from an iPad to the external monitor fails. As a workaround, disconnect and reconnect the monitor. If the issue persists, disconnect, and relaunch the session. [HDX-36981]
- On rare occasions, when you connect an iPad to an external monitor using third-party adapters, the Display Modes aren't visible under the Display Options. [HDX-39713]
- Sometimes, a line is observed under the mouse pointer inside the VDA session. [RFIOS-9569]

Keyboard support

Right option key mapping for Alt key

Starting with version 24.12.0, Citrix Workspace app for iOS introduces an enhancement allowing users to map the right Option key to **Alt** key in the session. This new option complements the existing mappings - left Option key, **Command or Windows** key, and both Option keys - offering users greater flexibility in keyboard configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Keyboard layout synchronization

Keyboard layout synchronization enables users to switch preferred keyboard layouts on the client device. This feature is disabled by default.

To enable keyboard layout synchronization, go to **Settings** > **Keyboard Options** and enable the **Keyboard Layout Sync** option.

> **Note:**
>
> Using the local keyboard layout option activates the client IME (Input Method Editor). If you are working in Japanese, Chinese, or Korean language and prefer to use the server IME, disable the local keyboard layout option by clearing the option in **Preferences** > **Keyboard.**

Prerequisites

- For Linux VDA, enable Client keyboard layout sync and IME improvement policy.
- For Windows VDA, enable Unicode Keyboard Layout Mapping, Client Keyboard Layout Sync, and IME Improvement policies.
- The VDA must be version 7.16 or later.

Keyboard layout support for Windows VDA & Linux VDA

Keyboard layout on iOS	Keyboard Language	Keyboard Layout on Windows	Keyboard Layout on Linux
Belarusian(Belarus)	Belarusian(Belarus)	Belarusian(Belarus) Keyboard	by

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Keyboard layout on iOS	Keyboard Language	Keyboard Layout on Windows	Keyboard Layout on Linux
Bulgarian	Bulgarian	Bulgarian (Typewriter) keyboard	bg
Chinese (Simplified)	Chinese (Simplified, China)	Citrix IME - Chinese (Simplified, China)	zh
Chinese (Traditional)	Chinese (Traditional, Taiwan)	Citrix IME - Chinese (Traditional, Taiwan)	tw
Croatian	Croatian (Croatia)	Croatian keyboard	hr
Czech	Czech	Czech keyboard	cz
Danish	Danish	Danish keyboard	df
Dutch	Dutch (Netherlands)	United States-International keyboard	us
Dutch(Belgium)	Dutch	Belgian (Period) Keyboard	be
English (Australia)	English (Australia)	US keyboard	us
English (Canada)	English (Canada)	US keyboard	us
English (UK)	English (United Kingdom)	United Kingdom keyboard	gb
English(US)	English (United States)	US keyboard	us
Estonian	Estonian	Estonian keyboard	ee
Finnish	Finnish	Finnish keyboard	fi
French (Canada)	French (Canada)	French Keyboard	fr
French (Switzerland)	French (France)	Swiss French Keyboard	ch
French(French)	French (France)	French Keyboard	fr
German (Austria)	German (Austria)	German keyboard	at
German (Switzerland)	German (Switzerland)	Swiss German keyboard	ch
German(Germany)	German (Germany)	German keyboard	at
Greek	Greek	Greek keyboard	gr
Hungarian	Hungarian	Hungarian keyboard	hu
Icelandic	Icelandic	Icelandic keyboard	is
Irish	Irish		ie

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Keyboard layout on iOS	Keyboard Language	Keyboard Layout on Windows	Keyboard Layout on Linux
Italian	Italian (Italy)	Italian keyboard	it
Japanese	Japanese	Citrix IME - Japanese	jp
Korean	Korean	Citrix IME - Korean	kr
Latvian	Latvian	Latvian keyboard	lv
Norwegian	Norwegian (Bokmål)	Norwegian keyboard	no
Polish	Polish	Polish (Programmers) keyboard	pl
Portuguese (Brazil)	Portuguese (Brazil)	Portuguese (Brazil ABNT) keyboard	br
Portuguese (Portugal)	Portuguese (Portugal)	Portuguese keyboard	pt
Romanian	Romanian (Romania)	Romanian (legacy) keyboard	ro
Russian(Russia)	Russian	Russian keyboard	ru
Slovak	Slovak	Slovak keyboard	sk
Slovenian	Slovenian	Slovenian keyboard	si
Spanish (Mexico)	Spanish (Mexico)	Latin American keyboard	latam
Spanish (Spain)	Spanish (Spain)	Spanish keyboard	es
Swedish(Sweden)	Swedish (Sweden)	Swedish keyboard	se
Turkish	Turkish	Turkish F keyboard	tr
Ukrainian	Ukrainian	Ukrainian keyboard	ua

Special key support

Support for the following single keys on an external keyboard of iOS 13.4 and later:

- PageUp
- PageDown
- Home
- End
- F1
- F2
- F3

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11
- F12

Special key combinations support

This release adds support for the following key combinations on iOS external keyboards:

- Windows + R
- Windows + D
- Windows + E
- Windows + L
- Windows + M
- Windows + S
- Windows + CTRL+ S
- Windows + T
- Windows + U
- Windows + Number
- Windows + UP
- Windows + Down
- Windows + Left
- Windows + Right
- Windows + X
- Windows + K
- CTRL + ESC

Extended keyboard enhancements

Starting with the 23.5.0 version, extended keyboard functionality is enhanced to provide a better user experience. The following are the enhancements:

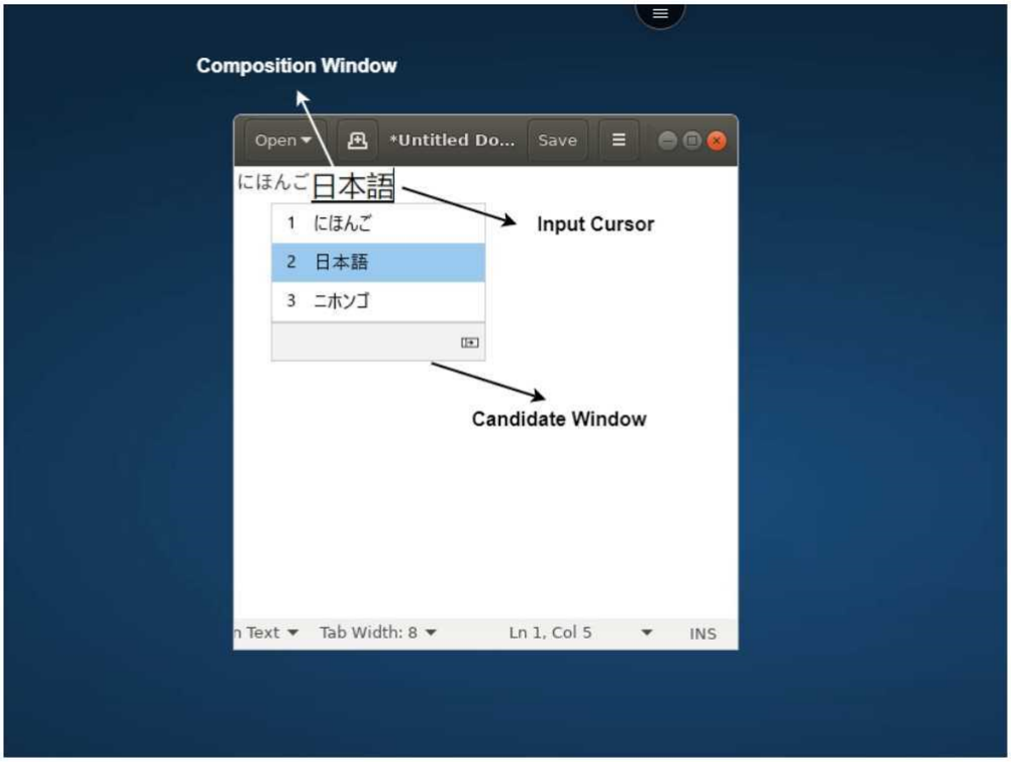
- Pin or unpin the extended toolbar UI.
- Rotate the extended toolbar in sync with screen rotation.
- Support Windows icon key and 3-key combination shortcuts.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Improve experience in multiple monitor use case scenarios.
- Auto open or collapse the extended toolbar UI.
- Improve the experience for Stage Manager mode (on iPad with M1 chip).

IME user interface

Generally, IME provides UI components such as candidate window and composition window. The composition window contains the composition characters and composition UI elements, for example, underline and background color. The candidate window displays the candidate list.



The composition window enables you to distinguish between the confirmed characters and the composing characters. The composition window and the candidate window move with the input cursor.

As a result, the feature provides:

- An enhanced input of characters at the cursor location in the composition window.
- An enhanced display in the composition and the candidate window.

Currently, you can use this feature on the sessions hosted on Windows VDAs and supports both soft keyboards and external physical keyboards.

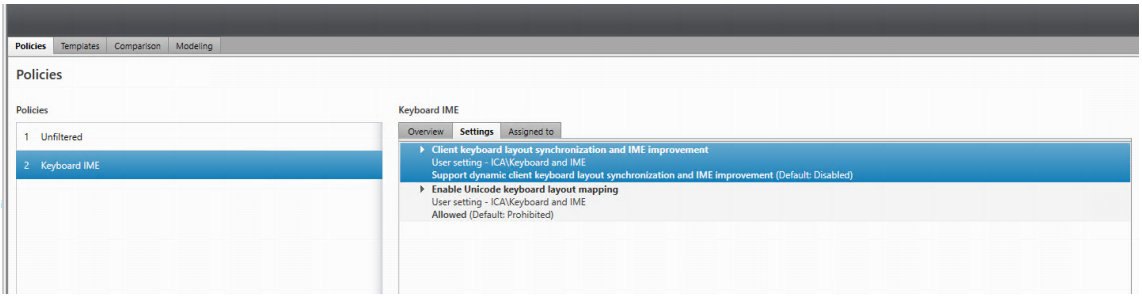
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Generic Client IME for East Asian languages

Generic Client Input Method Editor (IME) feature enhances input and display experience with Chinese, Japanese, and Korean (CJK) language characters on iOS devices. This feature allows you to compose CJK characters at the cursor position when you are in a session with your client IMEs. The feature is available for the Windows VDA environments. You are recommended to use the client IME instead of the VDA-side IME for a better user experience.

Prerequisites

- Enable the Client keyboard layout synchronization and IME improvement and Enable Unicode keyboard layout mapping on your Windows VDA through the group policy.



For more information see, Knowledge Center article CTX312404.

You can also enable the options using the following registries on your Windows VDA:

```
- HKLM\Software\Citrix\ICA\IcaIme\DisableKeyboardSync value = DWORD 0
- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\EnableKlMap value =
  DWORD 1
- HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\DisableWindowHook value
  = DWORD 1
```

- Enable the **Settings** > **Keyboard Options** > **Keyboard Layout Sync** option from Citrix Workspace app.

Support for scancode input mode

Starting with the 24.1.0 release, you can select **Scancode** as the keyboard input mode while using an external physical keyboard. This feature is helpful when you use iOS devices with an external Windows PC's standard keyboard. With **Scancode**, you can use the keyboard layout of the VDA instead of the iOS's keyboard. In this way, you can completely follow the input style of the external Windows keyboard instead of iOS. It is beneficial when typing in East-Asian languages, as it significantly improves the overall user experience. The end user might find themselves using the keyboard layout of the server instead of the client. For more understanding, see the Use Case section in this article.

To use the **Scancode** feature, do the following steps:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open Citrix Workspace app for iOS and navigate to **Settings > Keyboard Options**.
2. Tap **Input mode for external keyboards**.
3. Select one of the following options:

   - **Scancode:** Sends the key position from the client-side keyboard to VDA and VDA generates the corresponding character. Applies server-side keyboard layout.
   - **Unicode:** Sends the key from the client-side keyboard to VDA and VDA generates the same character in VDA. Applies client-side keyboard layout.

   By default, **Unicode** is selected as the input mode for both software or touch keyboard and external keyboard.
4. Tap **Scancode**.

   When you are in a session, you can switch the remote, server, or VDA keyboard layout and input with the remote, server, or VDA keyboard layout.

Use case For example, consider a scenario where you're using a US international keyboard layout that is connected to your iOS device.
When you choose **Scancode** and type the key next to the CapsLock on your external keyboard, the **scancode 1E** is sent to the VDA. The VDA then uses **1E** to display the character **a**.
If you choose **Unicode** and type the key next to CapsLock on your external keyboard, the character **a** is sent to the VDA. So, even if the VDA uses another keyboard layout that has a different character in the same position, the character **a** appears on the screen.

> **Note:**
>
> **Unicode** is the preferred mode for typing when you use a touch keyboard on your mobile devices. Because the keys on a touch keyboard generally don't generate a scancode.

Enhancements to external keyboard shortcut support

Starting with the 24.1.0 version, Citrix Workspace app for iOS now enables you to use more shortcuts from external keyboards when in a remote desktop or app session. The following are important improvements made to external keyboard shortcuts:

- Support for Windows keyboard specific keys such as **Insert**, **Delete**, and number pad.
- When you keep a key pressed down and don't release it, the remote desktop/app responds correctly.
- Support shortcuts with more than three keys.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In addition, you can now configure the specific key for **Alt** by using the following options via **Settings > Keyboard Options > Assign Specific Key for Alt**:

- **Option or Alt (left)**: Sends **Alt** using **Option (left) or Alt (left)**.
- **Command or Windows (left)**: Sends **Alt** using **Command (left) or Windows (left)** keys.
- **Option or Alt (left and right)**: Sends **Alt** using the **Option or Alt (left and right)** key.

Assigning specific key for Alt option helps to avoid conflict between the macOS **Option** key and the Windows **Alt** key.

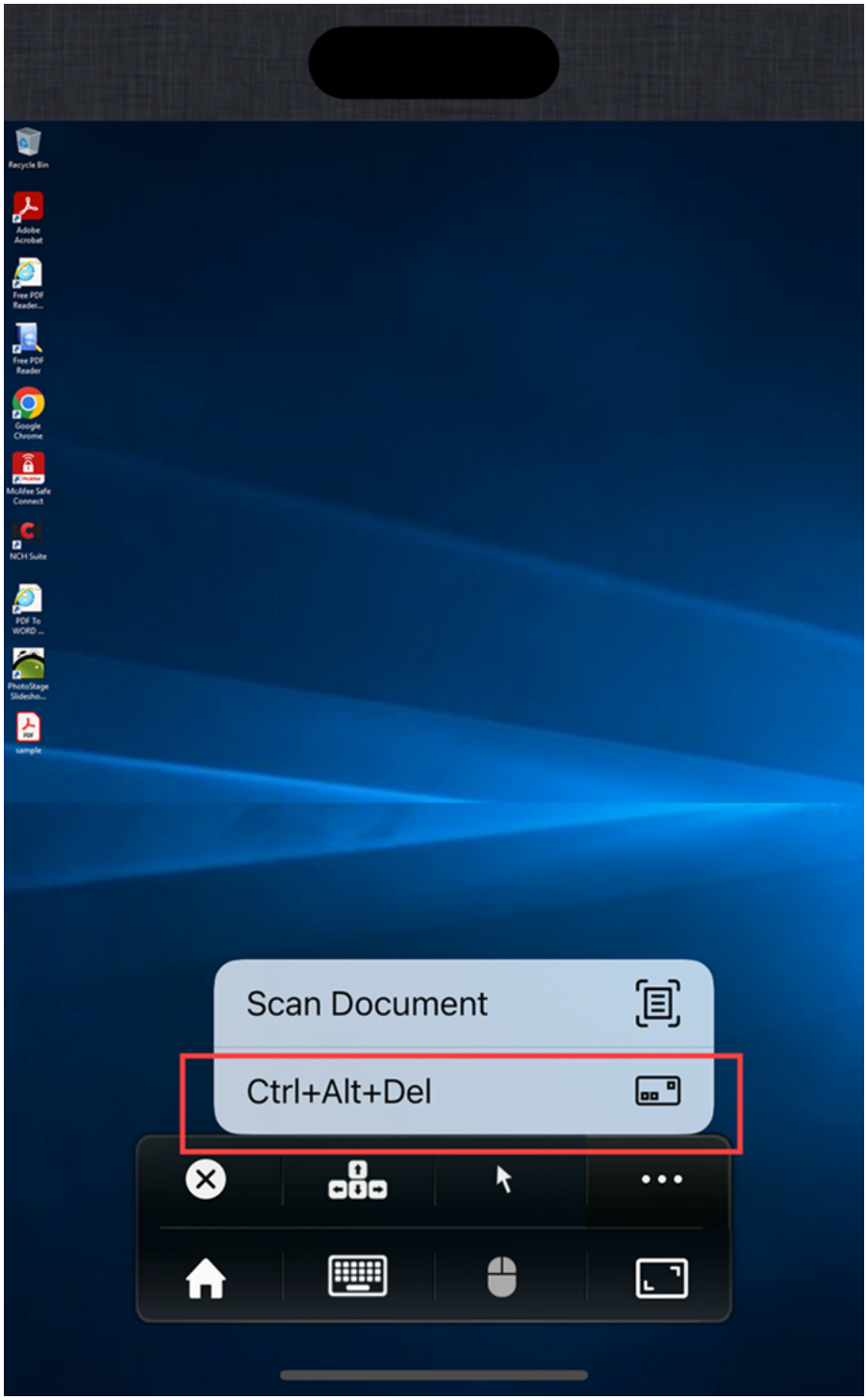
Limitations The following iOS system shortcuts are currently not supported:

- **Command (Windows)-H**: Go to the Home screen.
- **Command (Windows)-Space bar**: Show or hide the Search field.
- **Command (Windows)-Tab**: Switch to the next most recently used app among your open apps.
- **Command (Windows)-Shift-3**: Take a screenshot.
- **Command (Windows)-Shift-4**: Take a screenshot and immediately open Markup to view or edit it.
- **Command (Windows)-Option (Alt)-D**: Show or hide the Dock.
- **Command (Windows)-Ctrl-Q**: Lock the device.
- **AltGr** in the Europe keyboard is not supported. If you want to enter special characters with **AltGr**, use the following shortcuts instead:
  - macOS **Option+*** shortcut or
  - Windows OS **Alt + number pad shortcut**.

Addition of Ctrl+Alt+Del shortcut to Session Toolbar

Starting with the version, the session toolbar now has an option to perform the **Ctrl+Alt+Del** function with the tap of a button. This option facilitates users to sign out, switch users, lock the system, or access the Task Manager.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

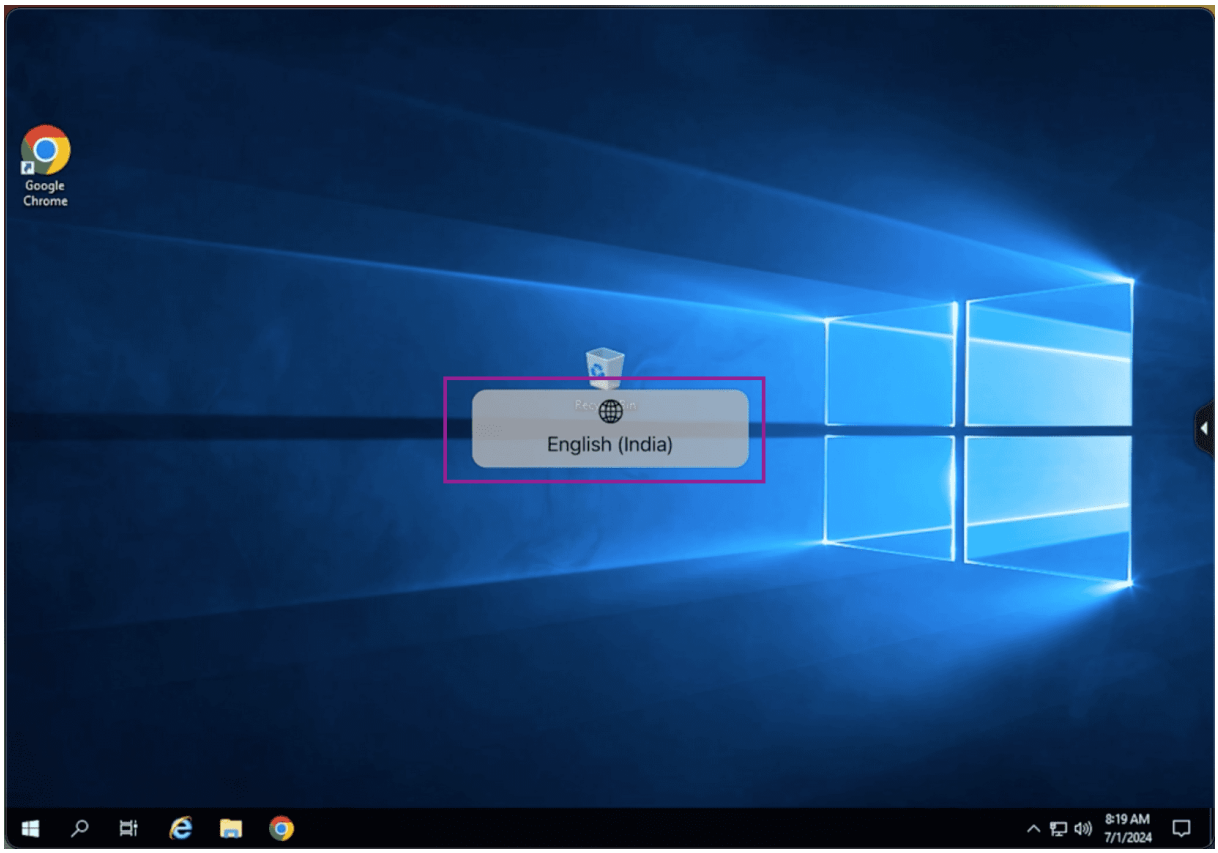


Detect and display keyboard language change in the virtual session

Starting with the 24.7.0 version, Citrix Workspace app for iOS now automatically detects and displays a message within the virtual session when user switches the keyboard language. When you switch keyboard languages using the globe key in the device keyboard or external keyboard, a message ap-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

pears on the screen notifying about the current keyboard language. This feature ensures that you're aware of the current keyboard language within the virtual session.



Microphone and camera access

You can now access your microphone and camera for audio-video conferencing through a VDA session. Citrix Workspace app requires your permission to access microphone or camera which can be provided by navigating to **Settings** on your device and enabling the camera or microphone.

Also, microphone and camera access per store as a part of the client-selective trust security feature has been included to allow Citrix Workspace app to trust access from a VDA session.

Citrix Workspace app requires the user's permission to access the microphone or camera.

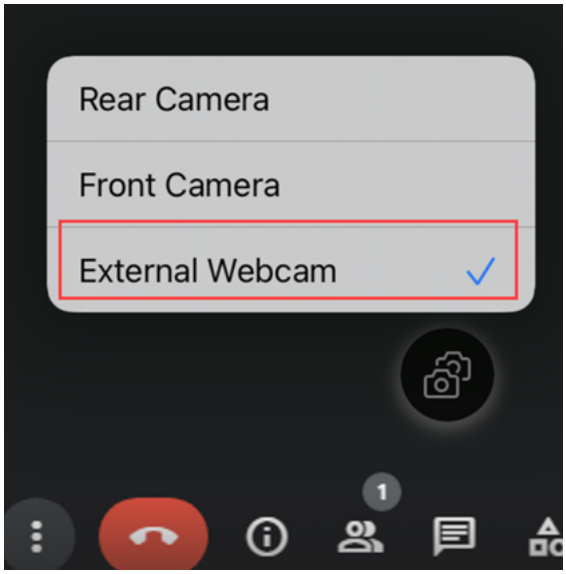
You can configure the access levels by navigating to **Settings > Store Settings**. In the **Store Settings** menu, click a store to enable the required microphone or camera access. The selected setting for microphone or camera access is applied on a per store basis.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

External Webcam support

Citrix Workspace app for iOS now supports externally connected webcams within your DaaS sessions. Connect a webcam via USB and use it for video conferencing by clicking the Camera icon, then selecting the **External Webcam** option. It enhances the session experience by using the resources available to end users.

> **Note:**
>
> - The External Webcam is only supported on iPads running iOS 17 or later with a USB-C connector.
> - The External Webcam option appears only after an external camera is detected.
> - The client app settings have no effect on the camera within an HDX session. You must use the camera floating button that is enabled by Citrix to switch the camera position.



The next time you use a video conferencing app, the system remembers your preference and uses the camera preference accordingly. For example, if you concluded the last video call with **External Webcam** preference, next time the External Webcam is selected by default.

You can change your camera preference by tapping the camera icon on your screen. You can also change the camera preference during your calls.

This feature is available for customers on both cloud and on-premises stores.

Support for Accessibility and VoiceOver

Starting with the 24.9.0 version, Citrix Workspace app for iOS supports the Accessibility and VoiceOver feature. This feature helps end users who have difficulty seeing the screen. The narrator reads the screen elements aloud when using the Citrix Workspace and the virtual sessions UI.

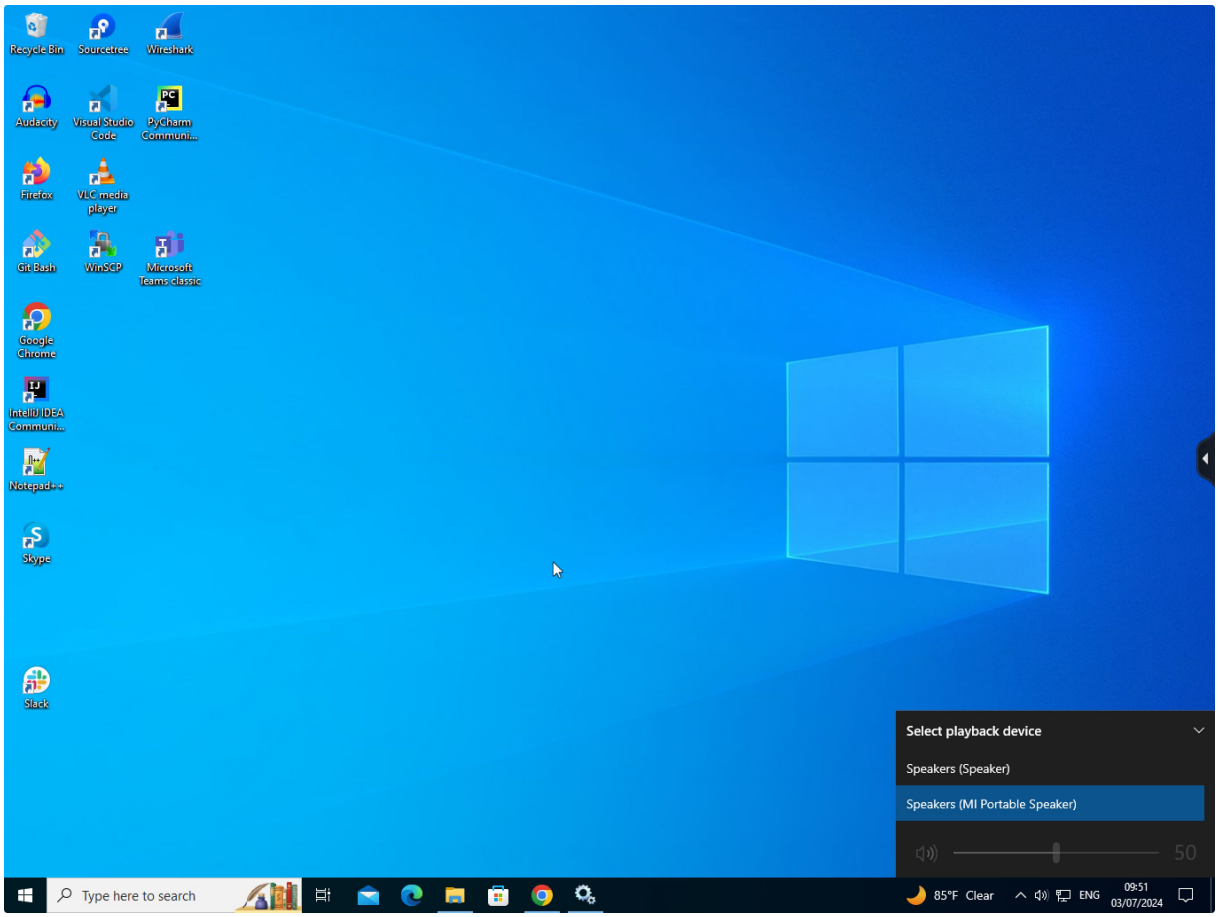
© 1997–2026 Citrix Systems, Inc. All rights reserved.

To enable the VoiceOver feature, navigate to iOS **Settings > Accessibility > VoiceOver** and turn it on.

You must use the accessibility standard gestures provided by iOS to interact with the Citrix Workspace app. For example, you can swipe left and right on the screen to navigate between the menus as the voiceover for each item plays. For more information, see Get started with accessibility features on iPhone and Get started with accessibility features on iPad in the Apple support documentation.

Support for multiple audio devices

Starting with the 24.7.0 version, Citrix Workspace app for iOS supports displaying all available audio devices that are connected locally in the virtual desktop session. With this feature, you can switch audio devices within the virtual desktop session. If you switch audio devices in the device settings locally, the changes are applied to the virtual desktop session automatically. This feature is also supported for plug-and-play devices.



Limitation

- Devices that are speaker-only and microphone-only are not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Apple's AirPlay devices are not supported.
- This feature supports either a bluetooth device or a wired headset device at a time in the virtual session.

Support for adaptive audio

Starting with the 24.5.0, Citrix Workspace app for iOS supports HDX adaptive audio. This feature improves the user experience by providing improved audio quality and low latency.

For more information, see the Audio policy setting article in the Citrix Virtual Apps and Desktops documentation.

Rear camera support

Starting with the 23.2.0 version, Citrix Workspace app for iOS now supports switching the camera position from front to rear and the other way around within an HDX session.

When you invoke the camera in the virtual session, a camera floating button appears on the screen to allow the switching of the camera position. You can also move the floating button freely around the screen and place it anywhere.

To switch the camera position between the front and rear positions in the virtual sessions, do the following steps:

1. Open a client app that captures video.
2. Start the video recording.
3. Tap the camera floating button that appears on the screen to switch between front and rear camera.

> **Note:**
>
> The client app settings have no effect on the camera within an HDX session. You must use the camera floating button that is enabled by Citrix to switch the camera position.

Known issues The floating button is partially or fully obstructed when the Casting feature or the Document Scan feature is enabled.

Graphics and Display

Improved graphics performance

Starting with the 24.1.0 version, Citrix Workspace app for iOS supports hardware accelerated H.264 video encoding or decoding. The multimedia engine of Citrix HDX now uses Apple's Video Toolbox

© 1997–2026 Citrix Systems, Inc. All rights reserved.

framework for encoding and decoding. This framework compresses and decompresses video faster and in real time. This enhancement reduces the load on the CPU during multimedia usage.

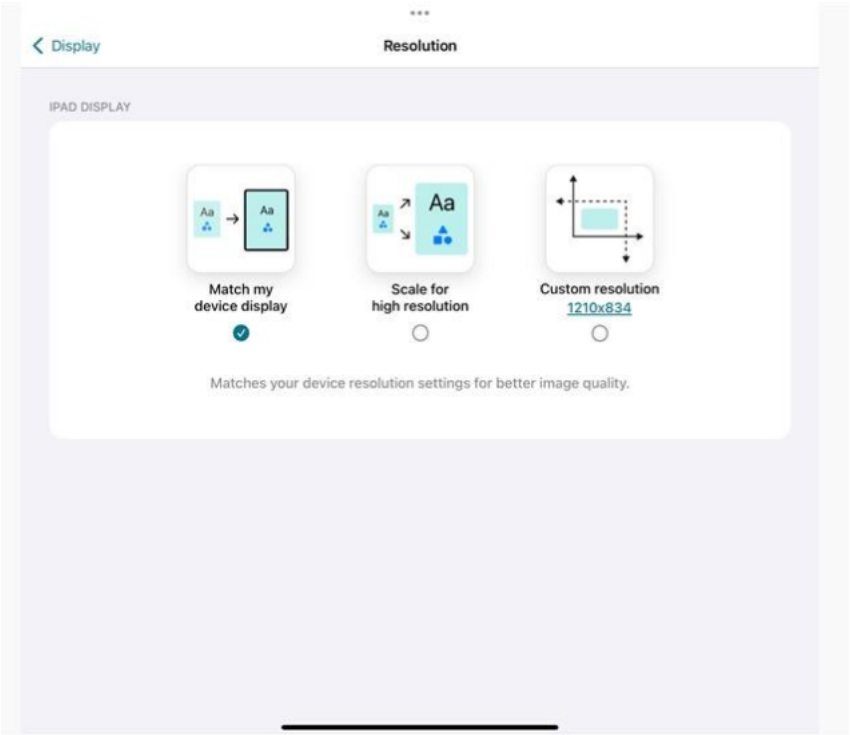
Graphic settings auto-synchronization with native iOS settings

The newly added **Match my device display** option automatically reads the DPI scale from iOS settings, so you do not need to configure resolution manually. For external displays, the app replaces the resolution list with five consolidated options. This update reduces configuration complexity and provides a more native display experience.

To use this feature, go to **Settings** > **Display options** > **Resolution**.

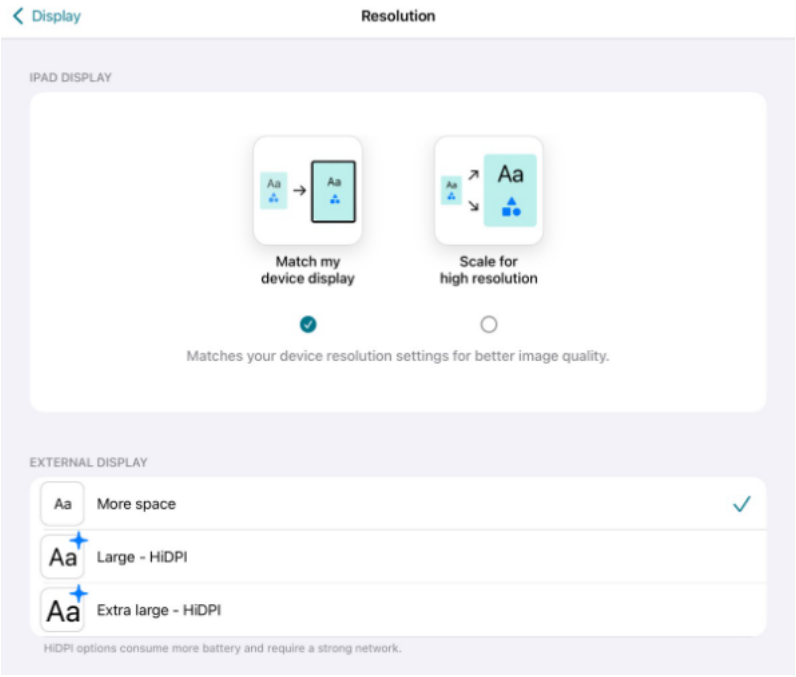
The following screenshots show the display options on iPhone and iPad:

- Main display resolution options.



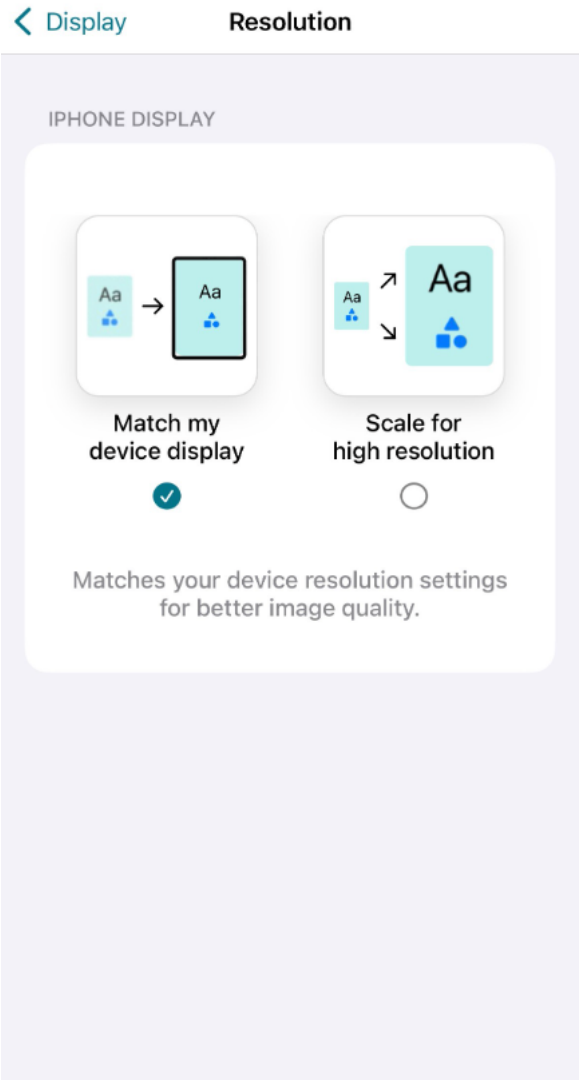
- External display resolution options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



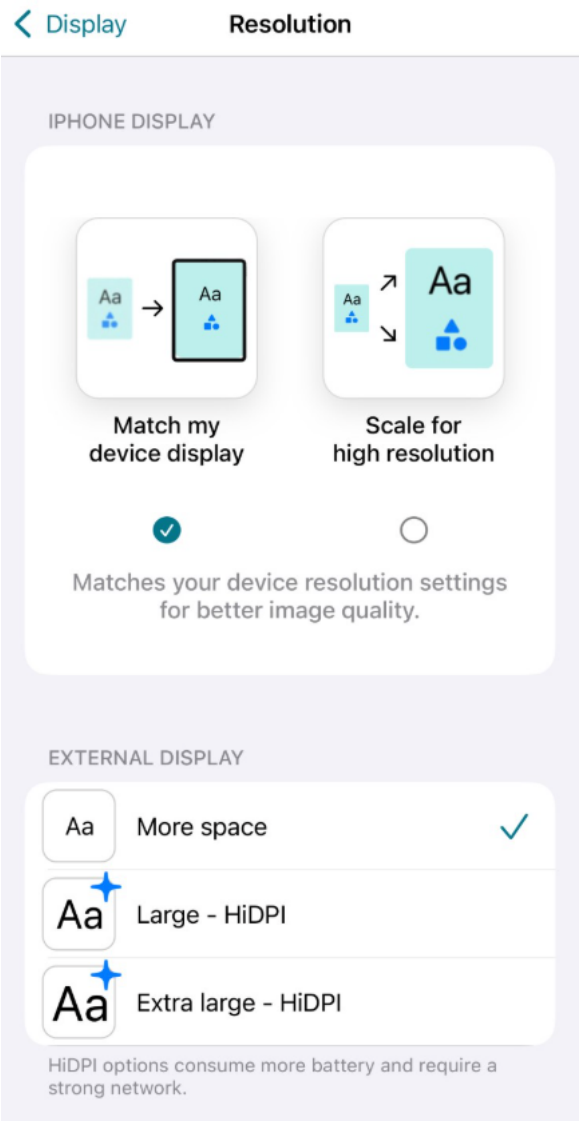
- Main display resolution options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- External display resolution options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Client Drive Mapping (CDM)

You can select a specific device storage access for every configured store. Device storage access has the following options.

- No access
- Read-only access
- Read and write access
- Ask me every time

If you select **Ask me every time**, a prompt appears, asking you to select the type of device storage access at every launch. By default the **No access** option is selected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> This feature applies only on direct ICA® launches and Citrix Gateway configured stores. Stores without end-to-end SSL setup aren't supported.

The **Device Storage** settings are available under a new section in the settings called **Store Settings**. To view **Device Storage**, navigate to **Settings** > **Store Settings**.

Citrix Ready® workspace hub

The Citrix Ready workspace hub combines digital and physical environments to deliver apps and data within a secure smart space. The complete system connects devices (or things), like mobile apps and sensors, to create an intelligent and responsive environment.

Citrix Ready workspace hub is built on the Raspberry Pi 3 platform. The device running Citrix Workspace app connects to the Citrix Ready workspace hub and casts the apps or desktops on a larger display.

For more information about the Citrix Ready workspace hub, see the Citrix Ready workspace hub documentation.

Citrix Ready workspace hub supports a Secure Sockets Layer (SSL) connection between mobile devices and the hub for security purposes. Set a Fully Qualified Domain Name (FQDN) either manually or automatically to uniquely identify each device. For more information, see the Security connection in the Citrix Ready workspace hub documentation.

Citrix Ready workspace hub is enabled on Citrix Workspace app when all the following system requirements are met:

- Citrix Workspace app 1810.1 for iOS or later
- Bluetooth enabled
- Mobile device and workspace hub using the same Wi-Fi network

Configure Citrix Ready workspace hub

To turn on Citrix Ready workspace hub features, go to **Settings** and tap **Citrix Casting** to enable the feature on your device. For more information, see the help documentation for the iOS devices.

Citrix Workspace app integrates a new procedure to add or to remove a workspace hub from the trusted list on iOS devices. For more information, see Security Connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for document scanner

Starting with the 24.5.0 version, Citrix Workspace app for iOS supports the document scanner feature. With this feature, you can now scan and save multiple documents, all within the desktop session. This feature is enabled by default.

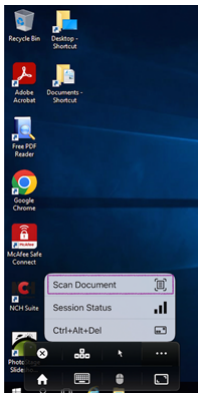
Prerequisites

- Client drive mapping (CDM) must be enabled for the store.
- The document scanner feature requires read and write access on your device. To enable access, follow these steps:

    1. From your profile, tap **Application Settings > Store Settings**.
    2. Tap your current store.
    3. Tap **Device Storage** and then select **Full Access**.

To scan documents using the document scanner, do the following steps:

1. From the in-session toolbar, tap the ellipsis menu and select **Scan Document**. The camera app opens.

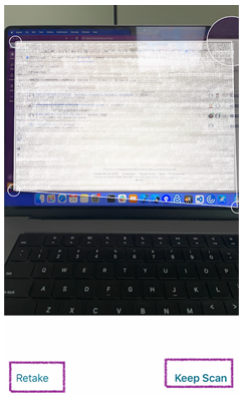


2. Tap the shutter button to capture the photo. If you choose to capture again, tap **Retake**.

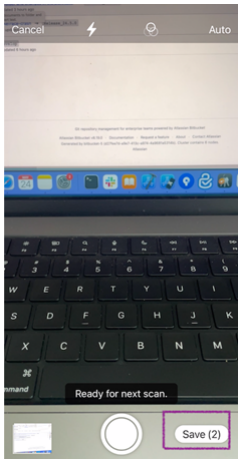


© 1997–2026 Citrix Systems, Inc. All rights reserved.

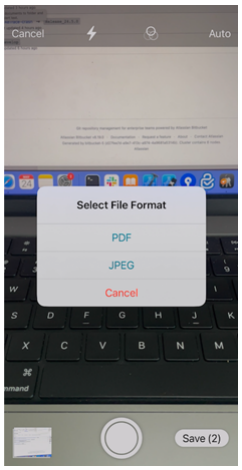
3. Optional: Crop the scanned document. After cropping to the required size, tap **Keep Scan**. The camera app opens again to allow you to capture more images.



4. After capturing the required images, tap **Save**.

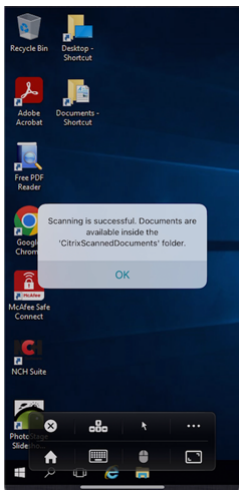


5. Select the file format option to save the scanned document in the required format.

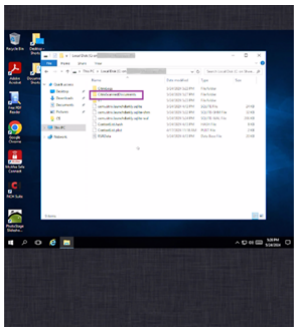


6. Tap **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



All scanned documents are accessible inside the **CitrixScannedDocuments** folder on the device's local storage.You can also access the **CitrixScannedDocuments** in the session file manager.



Support for AirPrint enabled printers

Starting with the 23.9.0 version, end users can now print documents from their active sessions on iOS devices with AirPrint technology enabled printers. It eliminates the need to have printers connected via cable or network. The AirPrint enabled printers are listed along with the other available printers once users initiate a print command.

To print using an AirPrint enabled printer, users must ensure the following.

- The required printer must be AirPrint compatible and AirPrint enabled.
- The user's device must be connected to the same Wi-Fi network as the AirPrint enabled printer.

This functionality is available for iOS platforms on both cloud and on-premises environments.

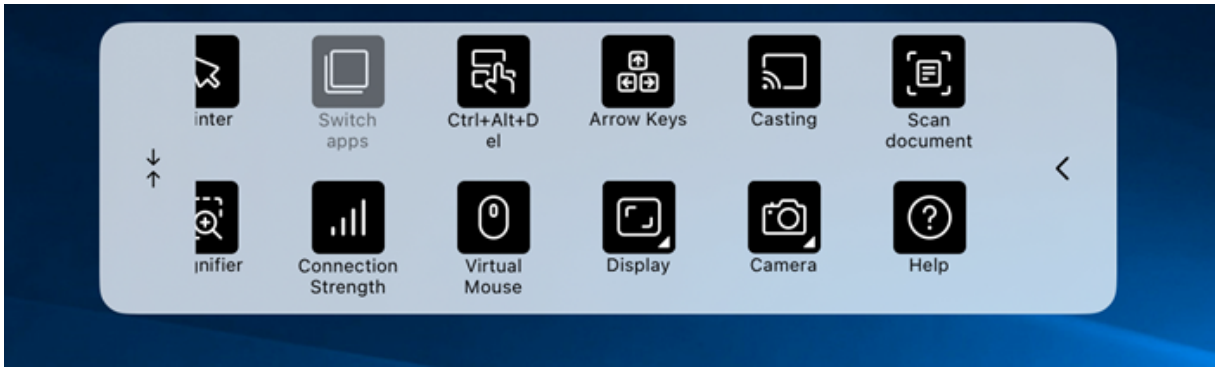
User Experience

May 15, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

New In-Session toolbar

Starting with version 25.3.0, the new toolbar is enabled by default when no admin setting configured through Global App Configuration service (GACS) and Mobile Device Management (MDM).



Enhance cross-multi screen experience

Starting with version 25.1.0, Citrix Workspace app for iOS improves the user experience for iPads connected to external monitors or docks. These updates include the ability to distribute applications across multiple screens for improved multitasking. This feature is enabled by default.

Users can select from a range of available resolutions for both external monitors and the iPad's native screen, catering to diverse preferences. Multiple screen configurations are preserved even when switching between local apps and sessions, ensuring continuity and productivity. This feature also resolves mouse lock issues caused by Stage Manager.

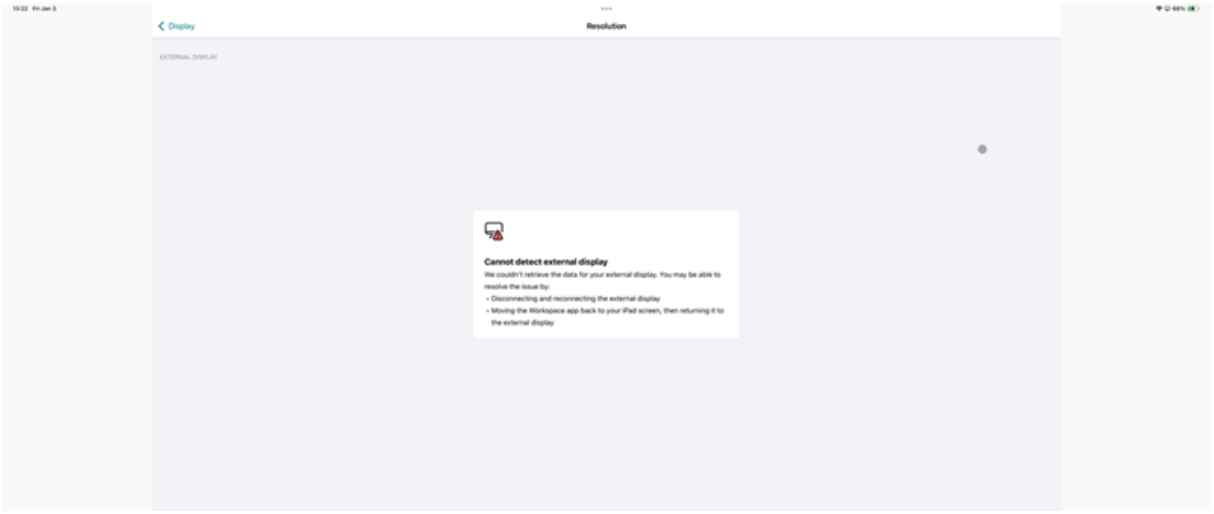
Prerequisites:

Stage Manager must be enabled on the iPad.

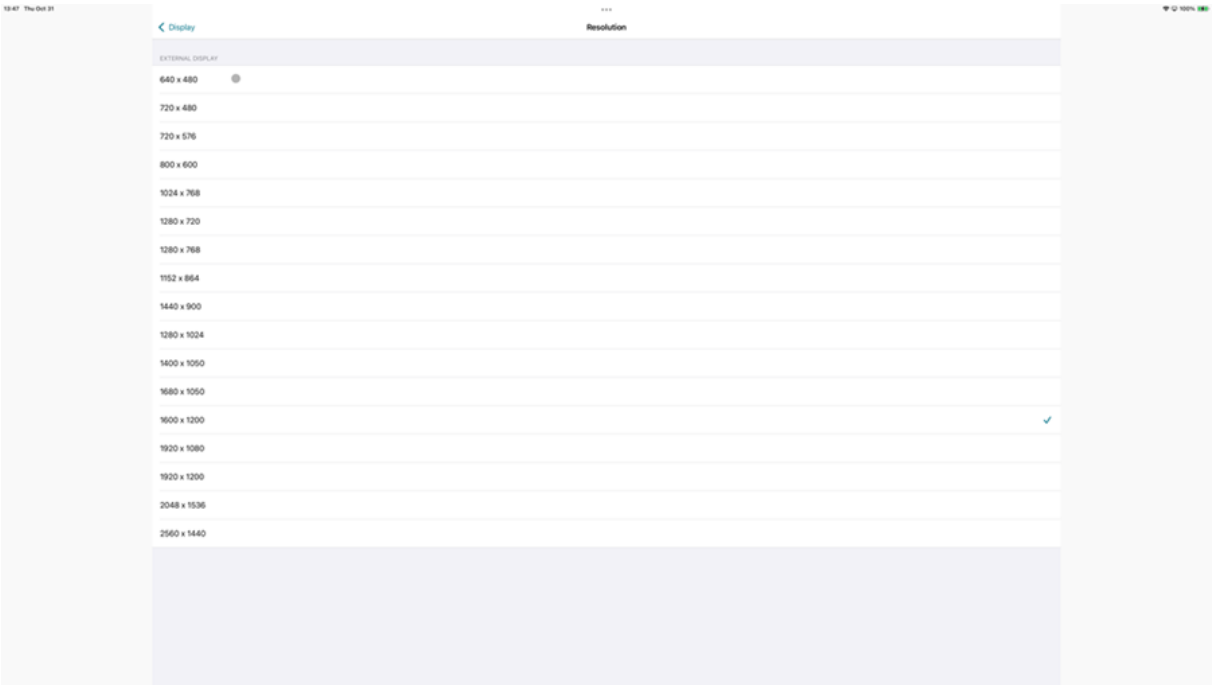
Limitations:

If the user launches the Citrix Workspace™ app directly on an external display, the resolution list appears empty when switching to fullscreen mode. This occurs due to an iOS system defect, and Citrix Workspace app displays a **Cannot detect external display** warning, as shown in the screenshot.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A list of supported external display resolutions for fullscreen mode:



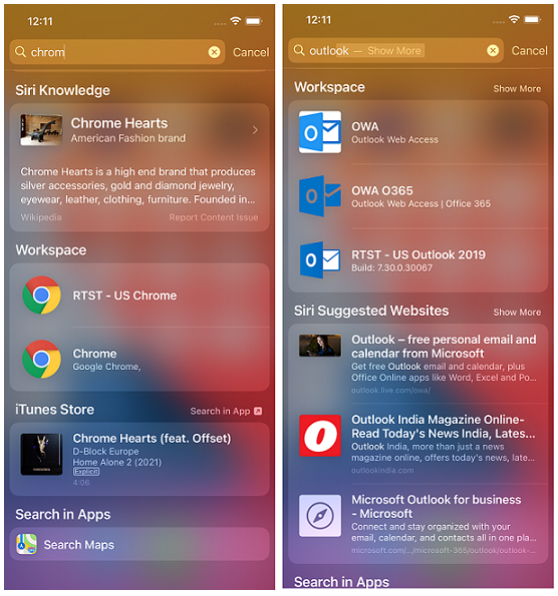
When the session enters fullscreen mode on an external display, a toast message appears, prompting users to move the Citrix Workspace app window back to the iPad screen if they want to use multi-monitor features as shown in the following image.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Spotlight search enhancement

The app icon matches the corresponding app search. Previously, the Citrix Workspace app icon was displayed for all the searches.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Accessing recent apps by 3D-Touch gesture

You can access a list of recently launched apps for quick access when you use the 3D-Touch (long-press) gesture on the **Citrix Workspace app** icon.

Battery status indicator

The battery status of the device now appears in the notification area within the virtual desktop session.

This feature is supported only on VDA versions 7.18 and later.

> **Note:**
>
> In sessions running on Microsoft Windows 10 VDAs, the battery status indicator might take about 1 to 2 minutes to appear.

Long press functionality to access resource

You can now long-press the Citrix Workspace app icon and access your most recently launched resource. You can now quit the Citrix Workspace app and access your most recently launched resource.

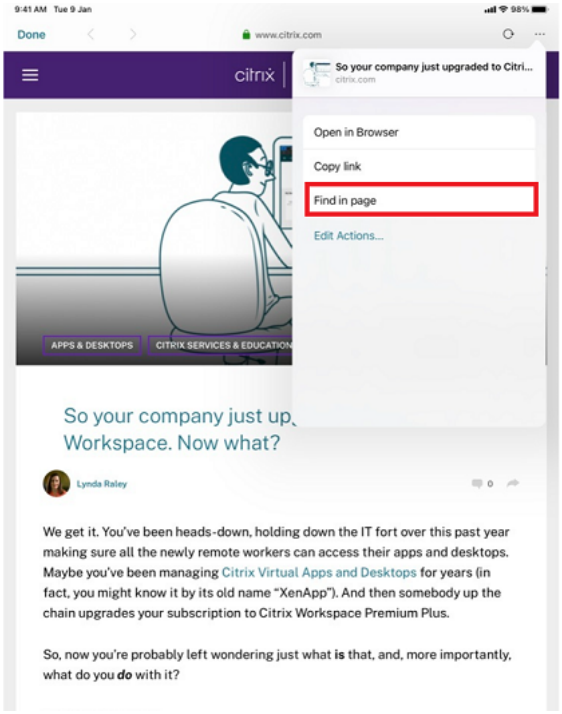
Find in page enhancement

The Find in page enhancement lets you search for words or phrases. This usability enhancement is applicable within your Web and Software-as-a-Service (SaaS) apps.

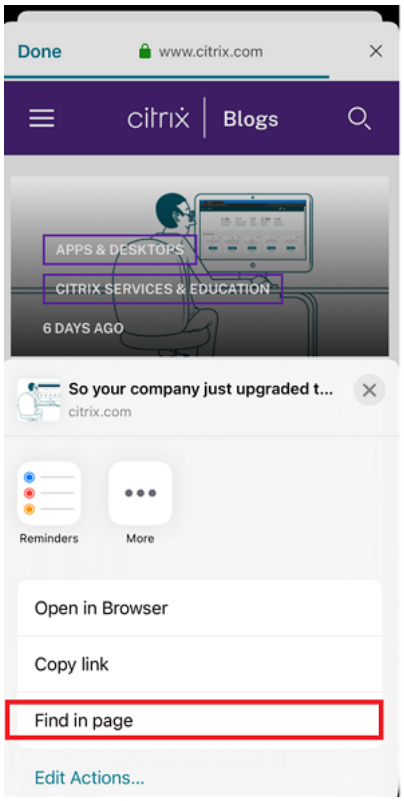
To search:

1. On your iPad, tap the ellipsis (…) button on the upper-right corner and then select **Find in page.**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

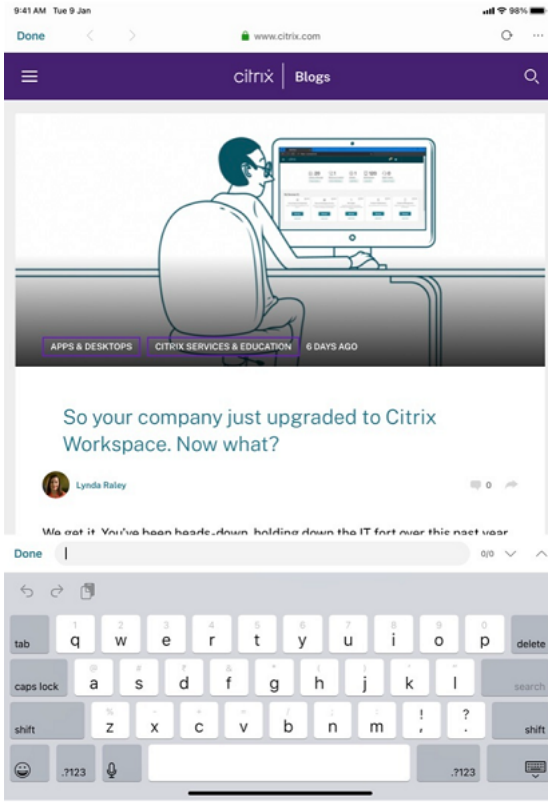


On your iPhone, tap the ellipsis (…) button on the lower-right corner and then select **Find in page.**



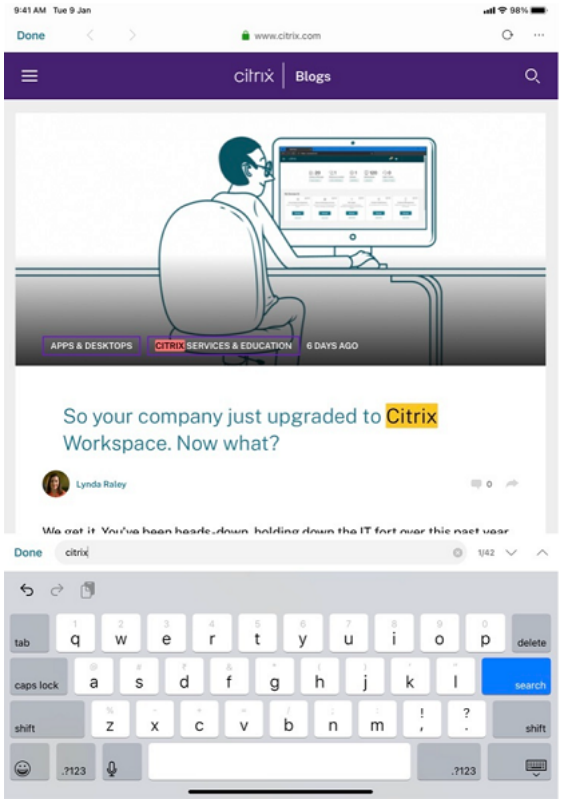
The on-screen keyboard appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Type the text that you want to search for in the text box (for example, type the word “Citrix®”). The search results appear.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Reposition the in-session toolbar

You can reposition the in-session toolbar either on the top or on the right of the screen. When you drag the toolbar notch away from the toolbar edge, the rectangle drag indicator and the drop target appear. Drop the drag indicator over the drop target to reposition the toolbar.

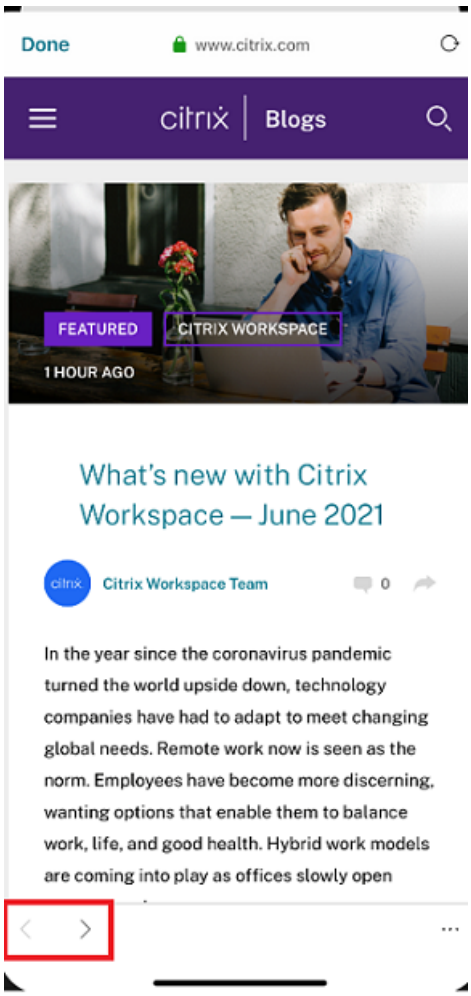
> **Notes:**
>
> - The feature is applicable for iPad users only.
> - The feature functions with touch or mouse.
> - The feature functions with an iPad or on an external display.
> - The last toolbar position persists for the next session or the application launch.

Switch between SaaS and web apps

The usability enhancement lets you navigate back and forth within web and Software-as-a-Service (SaaS) apps.

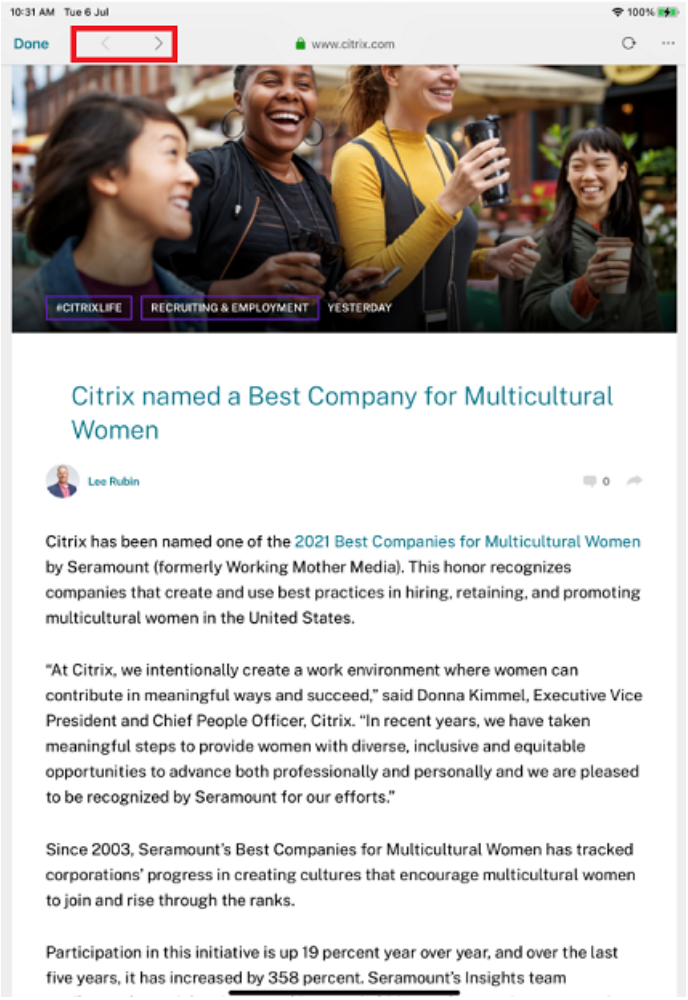
The navigation buttons appear at the bottom left of your Workspace web and SaaS app sessions of your iPhone.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The navigation buttons appear at the top left of your Workspace web and SaaS app sessions of your iPad.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Migration from on-premises to cloud account

Administrators can seamlessly migrate the end users from an on-premises StoreFront store URL to a Workspace URL. Administrators can do the migration with minimum end-user interaction using the Global App Configuration Service.

To configure:

1. Navigate to the Global App Configuration Store Settings API URL and enter the cloud store URL. For example, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Navigate to **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** > click **POST**.
3. Click **INVOKE API**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Enter and upload the payload details. Enter the StoreFront store expiry date in the epoch timestamp in milliseconds format.

   For example,

```
"migrationUrl": [
{


"url": "<cloud store url>"
"StoreFrontValidUntil": "<epoch timestamp in milliseconds>",
 }

]   ,
```

5. Click **EXECUTE** to push the service.

End-user Experience

As an end user, if you're using the Citrix Workspace app for the first time, after successful authentication, the **Introducing the new Citrix Workspace** migration screen appears (if eligible). After you tap the **Try new Citrix Workspace now** option, migration begins. Upon successful migration, you can access the Workspace store (cloud store).

> **Note:**
>
> You can skip the migration for three attempts. Later, the migration is forced without an option to skip.



After you migrate to the Workspace (cloud) store, you can view both the StoreFront and the Workspace store under **Settings**. When you switch from a cloud store to the on-premises StoreFront store, a feedback screen appears to gather your response.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The StoreFront store has an expiry date. Post the expiry date, the store gets deleted.

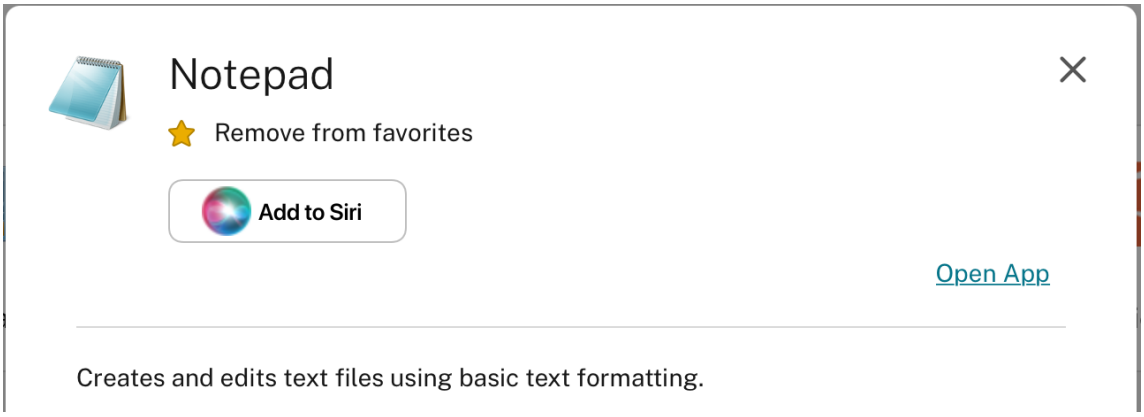
Siri integration

You can interact with Siri to launch resources like apps and desktops without launching Citrix Workspace app each time.

To configure

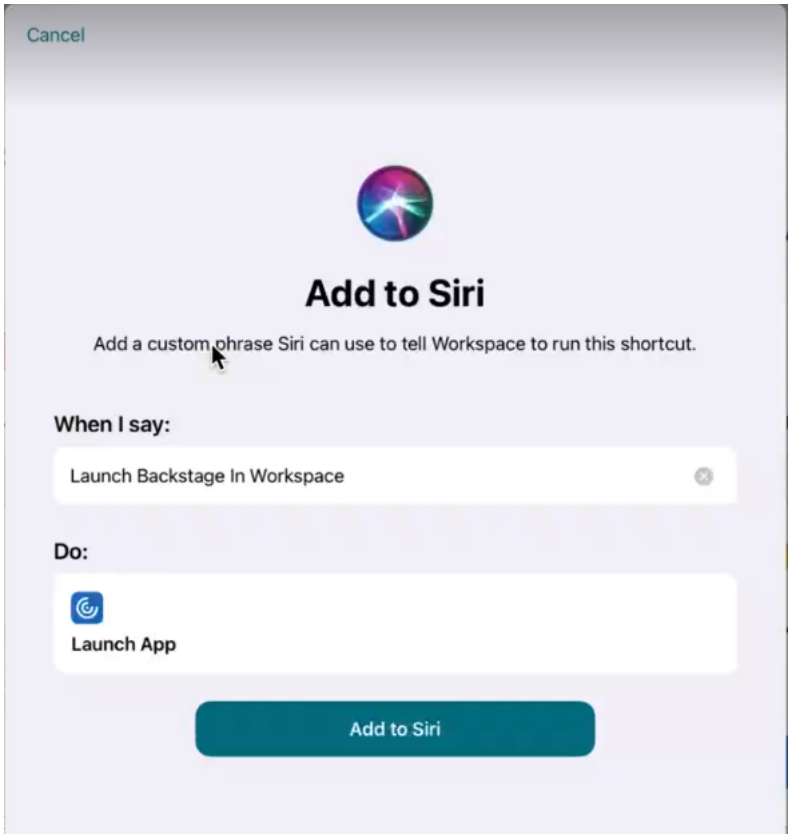
1. Launch Citrix Workspace app and tap **Apps** or **Desktops**. Select the resource that you want to add to the Siri shortcut.
2. Tap ellipsis (…). A dialog box appears.

   > **Note:**
   >
   > If you're an iPhone or an iPad Desktop user, tap **ellipsis** (…) > **App Details** screen > **View Details**. A dialog box appears. Continue with step 3.

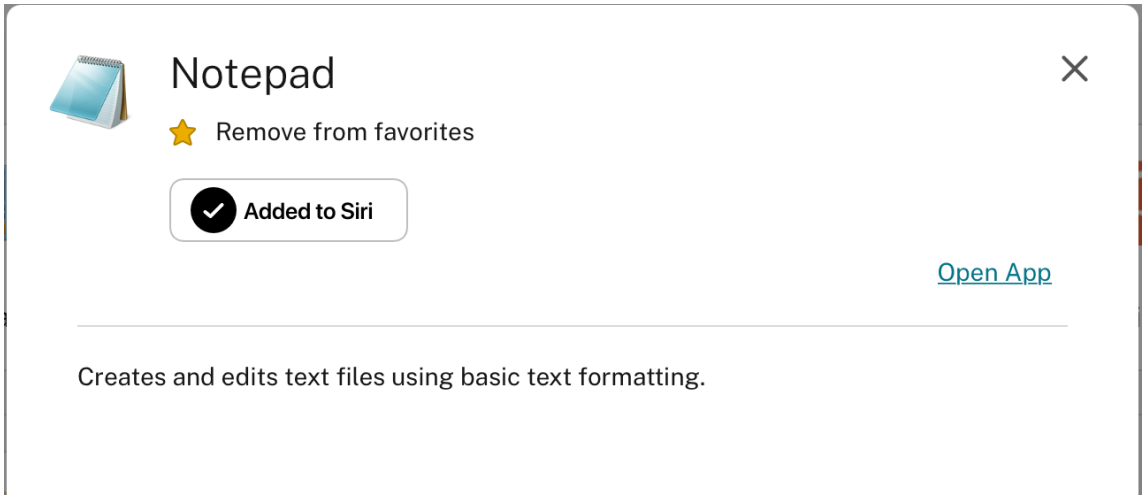
3. Tap **Add to Siri**. The **Add to Siri** dialog box appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. (Optional) Edit the custom phrase for invoking Siri. Tap **Add to Siri**. The resource is now added to the Siri shortcut. Close the dialog box.

> **Note:**
>
> A few devices support recording the custom phrase for invoking Siri.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Application Settings

Launch Citrix Workspace app and tap on your profile icon > **Application Settings** > **Siri Configuration**. To enable the feature, tap **Add to Siri**.

You can now use your voice to launch the resource.

To edit or delete the shortcut

1. Select the resource.
2. Tap ellipsis (…). A dialog box appears.
3. Tap **Added to Siri**. The **Edit Shortcut** dialog box appears.

Support for separate session window from Citrix Workspace app

Starting with the 24.1.0 version, Citrix Workspace app for iOS introduces a separate session window that makes multitasking more efficient and user-friendly. With this feature, you can have a desktop-like experience. When the Separate Session Window feature is enabled, you may simply drag & drop sessions onto the connected external monitors. As a result, the iPad's main monitor can be used to multitask with other apps.

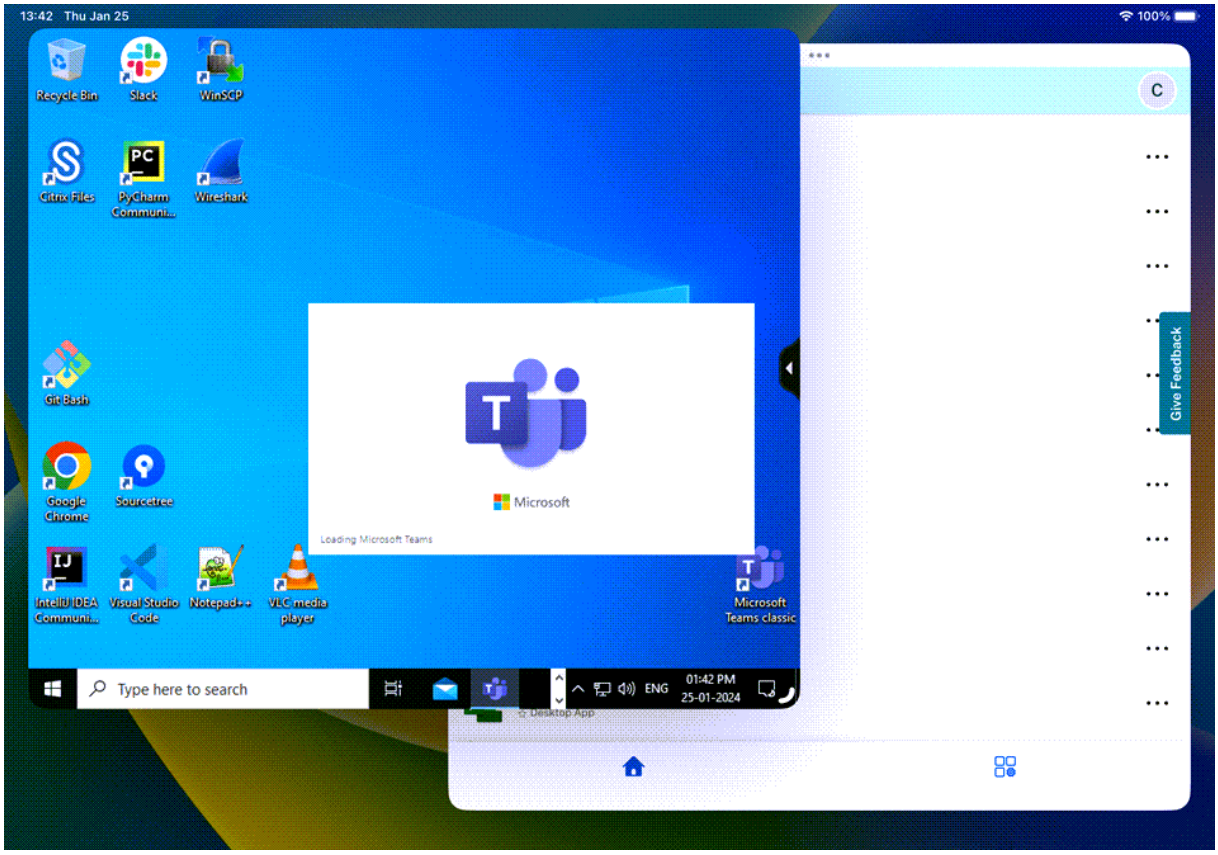
The following improvements are included with this feature:

- When you click the **Home** button on the session menu bar, the Citrix Workspace UI window opens instead of closing the HDX™ session window. This enhancement allows you to use the Citrix Workspace UI and the HDX session at the same time. If you start a new session from the Citrix Workspace UI, the existing one is automatically disconnected.
- When you click the **Display Options** button on the session menu bar, a setting window appears on top of the HDX session. This window allows you to adjust the session resolution instead of the Citrix Workspace UI settings.

> **Note:**
>
> This feature is supported only on devices that support the Stage Manager feature. All iPhone devices and some iPad devices do not support this feature. For more information about the Stage Manager feature, see Turn Stage Manager on or off on your iPad in the Apple support documentation.

To configure the separate session window feature, navigate to **Settings -> Advanced -> Multitasking** and select **Separate Session Window**.

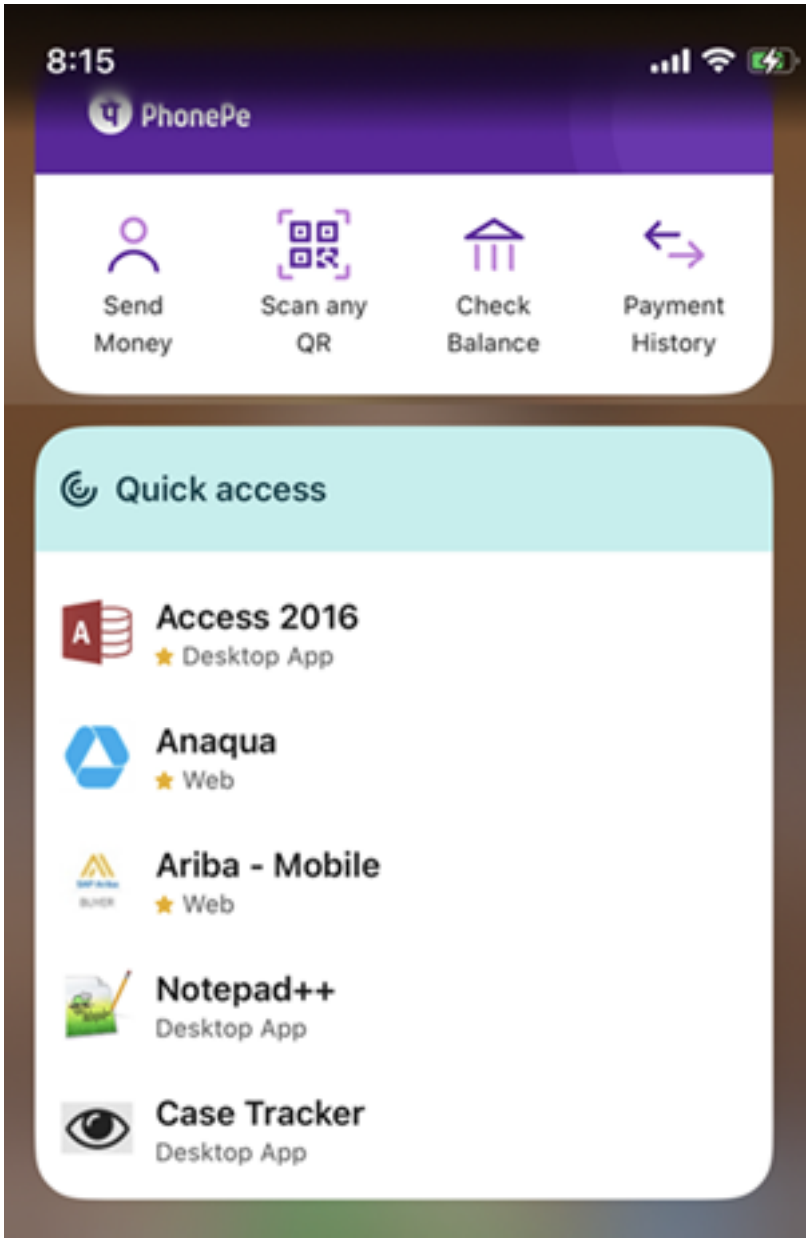
© 1997–2026 Citrix Systems, Inc. All rights reserved.



View apps and desktops as widgets

Starting with the 23.11.0 version, end users can now launch their virtual apps and desktops directly from their iPhones and iPads. They do not need to open the Citrix Workspace app to start an app or desktop session. A user can have a maximum of five virtual apps and desktops as widgets.

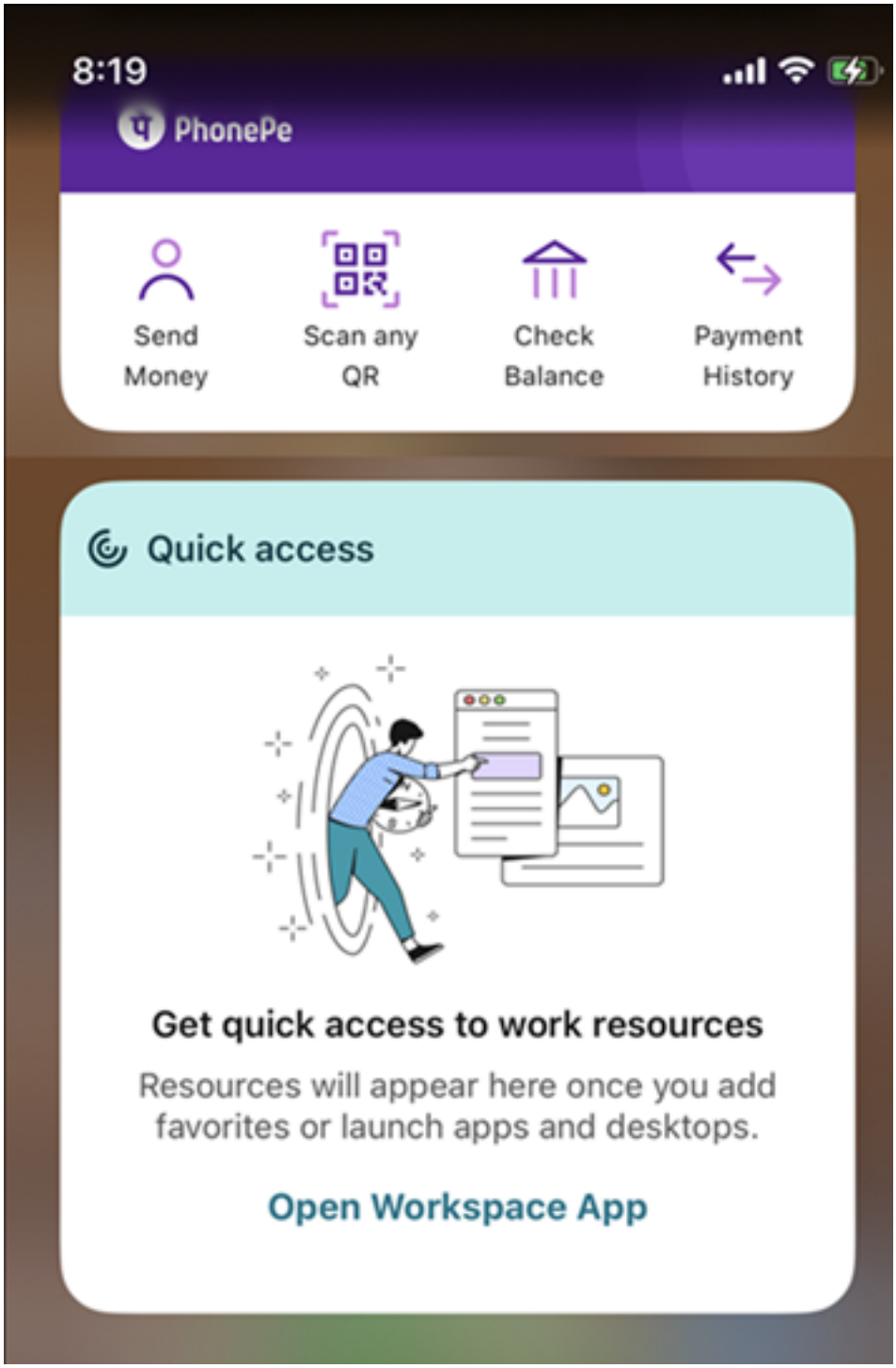
© 1997–2026 Citrix Systems, Inc. All rights reserved.



The widgets are created automatically as per the following criteria:

- Three Favorite and two recently opened apps or desktops are displayed as widgets
- If there are no Favorite apps or desktops, up to five recently opened apps and desktops are displayed as widgets
- If there are no recently opened apps or desktops, up to five Favorite apps or desktops are displayed as widgets
- If no apps or desktops have been added as Favorite yet and no apps or desktops were opened recently, users are prompted to open the Citrix Workspace app for iOS. They can then mark certain apps or desktops as Favorites.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Webview for Web and SaaS apps

September 7, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Webpage

External sharing of webpages

You can share the webpages you open from Citrix Workspace app with others. You can:

- copy a link from within a webview
- directly open a webpage in Safari
- send links directly to people or apps

To do share, tap the ... icon on the top right of the webview or long tap any link within the webview and tap the option you need.

Webview

Enhanced webview with native controls for SaaS apps

You can have an enhanced webview with native controls for SaaS apps. This enhancement allows you to:

- View the URL of your apps.
- View the security information of your apps.
- Share your apps.

Also, you can now swipe your apps left and right to move forward and backward, respectively.

Citrix Workspace mobile app web viewer

The web viewer is an in-app browsing solution running within the Citrix Workspace app. It enables users to open web or SaaS apps from the Citrix Workspace app in a secure manner. The web viewer ensures a consistent user interface while accessing various web or SaaS apps. It improves productivity and gives a better performance in rendering the apps.

With a continued focus on enriching the user-experience, the new web viewer brings you an enhanced and a more native browser-like experience, complete with the following features:

- VPN-less access to internal webpages
- SSO for web and SaaS with Adaptive access policies
- File downloading with preview
- Seamless navigation between pages and sites
- Ability to share URLs
- Find in page

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- consistent view when accessing links through the activity feed

Administrators can enable Secure Private Access (SPA) including download, clipboard, navigation restrictions, file upload, and watermarking in varying combinations on a per URL basis.

Password management

September 7, 2025

Save passwords

Using the Citrix Web Interface Management console, you can configure the authentication method to allow users to save their passwords. When you configure the user account, the encrypted password is saved until the first time the user connects. Consider the following:

- If you enable password saving, Citrix Workspace app for iOS stores the password on the device for future logons and does not prompt for passwords when users connect to applications.

  > **Note:**
  >
  > The password is stored only if users enter a password when creating an account. If no password is entered for the account, no password is saved, regardless of the server setting.

- If you disable password saving (default setting), Citrix Workspace app for iOS prompts users to enter passwords every time they connect.

> **Note:**
>
> For StoreFront direct connections, password saving isn't available.

To override password saving

If you configure the server to save passwords, users who prefer to require passwords at logon can override password saving:

- When creating the account, leave the password field blank.
- When editing an account, delete the password and save the account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to use

Citrix Workspace app has a feature that streamlines the connection process by allowing you to save your password, which eliminates the extra step of having to authenticate a session every time you open Citrix Workspace app.

> **Note:**
>
> The **Save password** functionality currently supports the PNA protocol. It does not support StoreFront *native* mode. However, this functionality works when StoreFront enables PNA *legacy* mode.

Configure StoreFront to save password

To configure StoreFront to enable the **Save password** functionality:

1. If you are configuring an existing Store, go to step 3.
2. To configure a new StoreFront deployment, follow the best practices described in Install, set up, upgrade, and uninstall.
3. Open the Citrix StoreFront management console. Ensure the base URL uses HTTPS and is the same as the common name specified when generating your SSL certificate.
4. Select the Store that you want to configure.
5. Click **Configure XenApp® Service Support**.
6. Enable **XenApp Service support**, select the **Default store** (optional), and Click **OK**.
7. Navigate to the template configuration file at c:\inetpub\wwwroot\Citrix\<store name>\Views\PnaConfig\.
8. Make a backup of Config.aspx.
9. Open the original Config.aspx file.
10. Edit the line <EnableSavePassword>**false**</EnableSavePassword> to change the **false** value to **true**.
11. Save the edited Config.aspx file.
12. On the StoreFront server, run PowerShell with administrative rights.
13. In the PowerShell console:

    a. `cd "c:\\Program Files\\Citrix\\Receiver StoreFront\\Scripts"`

    b. Type "Set-ExecutionPolicy RemoteSigned"

    c. Type ".\ImportModules.ps1"

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Type "Set-DSServiceMonitorFeature –ServiceUrl" `https://localhost:443/StoreFrontMonito`

14. If you have a StoreFront group, run the same commands on all the members in the group.

Configure Citrix Gateway to save passwords

> **Note:**
>
> This configuration uses Citrix Gateway load balance servers.

To configure Citrix Gateway to support the saved password functionality:

1. Log in to the Citrix Gateway management console.
2. Follow the Citrix best practices to create a certificate for your load balance virtual servers.
3. On the configuration tab, navigate to **Traffic Management** > **Load Balancing** > **Servers** and click **Add**.
4. Enter the server name and IP address of the StoreFront server.
5. Click **Create**. If you have a StoreFront group, repeat step 5 for all the servers in the group.
6. On the configuration tab, navigate to **Traffic Management** > **Load Balancing** > **Monitor** and click **Add**.
7. Enter a name for the monitor. Select **StoreFront** as the Type. At the bottom of the page, select **Secure** (required since the StoreFront server is using HTTPS).
8. Click the **Special Parameters** Tab. Enter the StoreFront name configured earlier, and select the **Check Backed Services** and click **Create**.
9. On the **Configuration** tab navigate to **Traffic Management** > **Load Balancing** > **Service Group**s and click **Add**.
10. Enter a name for your Service Group and set the protocol to **SSL** and click **Ok**.
11. On the right hand of the screen under Advanced Settings, select **Settings**.
12. Enable Client IP and enter the following for the Header value: **X-Forwarded-For** and click **OK**.
13. On the right-hand of the screen under Advanced Settings, select **Monitors**. Click the arrow to add new monitors.
14. Click the **Add** button and then select the **Select Monitor** drop-down menu. A list of monitors (configured on Citrix Gateway) appears.
15. Click the radio button beside the monitor that you created earlier and click **Select**, then click **Bind**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

16. On the right hand of the screen (under Advanced Settings), select **Members**. Click the arrow to add new service group members.
17. Click the **Add** button and then select the **Select Member** drop-down menu.
18. Select the **Server Based** radio button. A list of server members (configured on Citrix Gateway) appears. Click the radio button beside the StoreFront server that you created earlier.
19. Enter 443 for the port number and specify a unique number for the Hash ID, then click **Create**, then click **Done**. If everything has been configured properly, **Effective State** should show a green light, indicating that monitoring is functioning properly.
20. Navigate to **Traffic Management -> Load Balancing -\ > Virtual Servers** and click **Add**. Enter a name for the server and select **SSL** as the protocol.
21. Enter the IP address for the StoreFront load-balanced server and click **OK**.
22. Select the **Load Balancing Virtual Server Service Group** binding, click the arrow, and add the Service Group created previously. Click **OK** twice.
23. Assign the SSL certificate created for the Load Balance virtual server. Select **No Server Certificate**.
24. Select the Load Balance server certificate from the list and click **Bind**.
25. Add the domain certificate to the Load Balance Server. Click **No CA certificate**.
26. Select the domain certificate and click **Bind**.
27. On the right side of the screen, select **Persistence**.
28. Change the Persistence to **SOURCEIP** and set the time-out to **20**. Click **Save,** then click **Done**.
29. On your domain DNS server, add the load balance server (if not already created).
30. Launch Citrix Workspace app for iOS on your iOS device and enter the full XenApp URL.

GACS & MDM Support for Session Toolbar Configuration

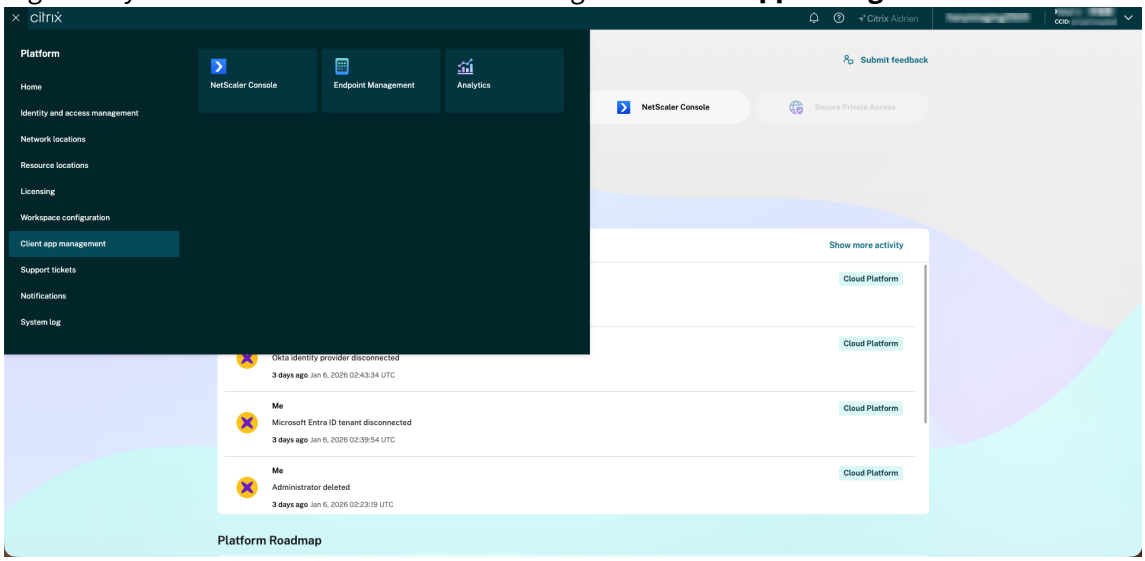
January 14, 2026

You can configure this feature using the Global App Configuration Service (GACS) and Mobile Device Management (MDM).

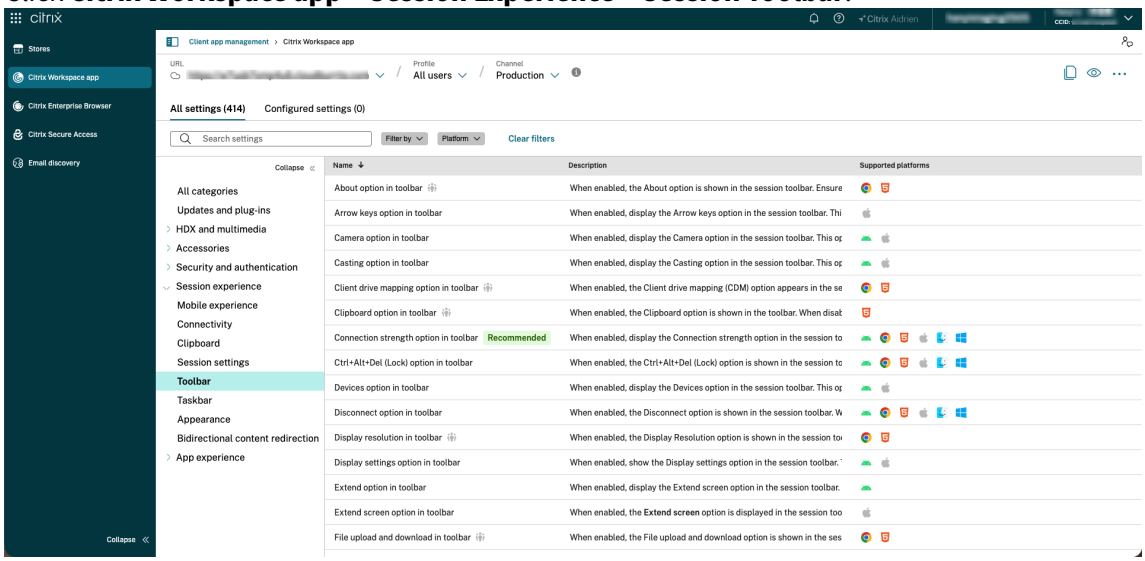
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Using GACS

1. Sign in to your **Citrix Cloud™** account and navigate to **Client App Management**.

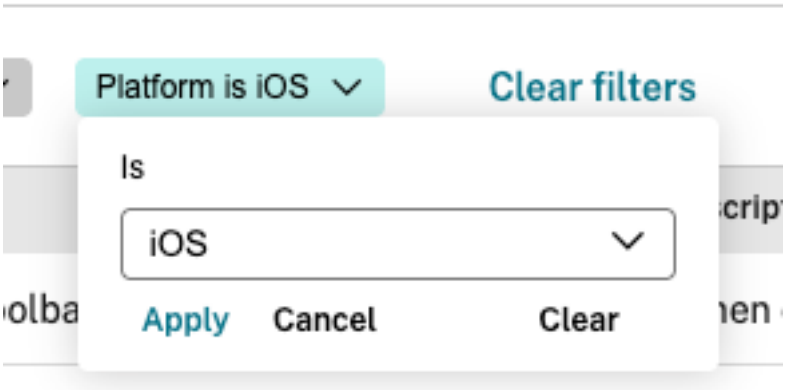


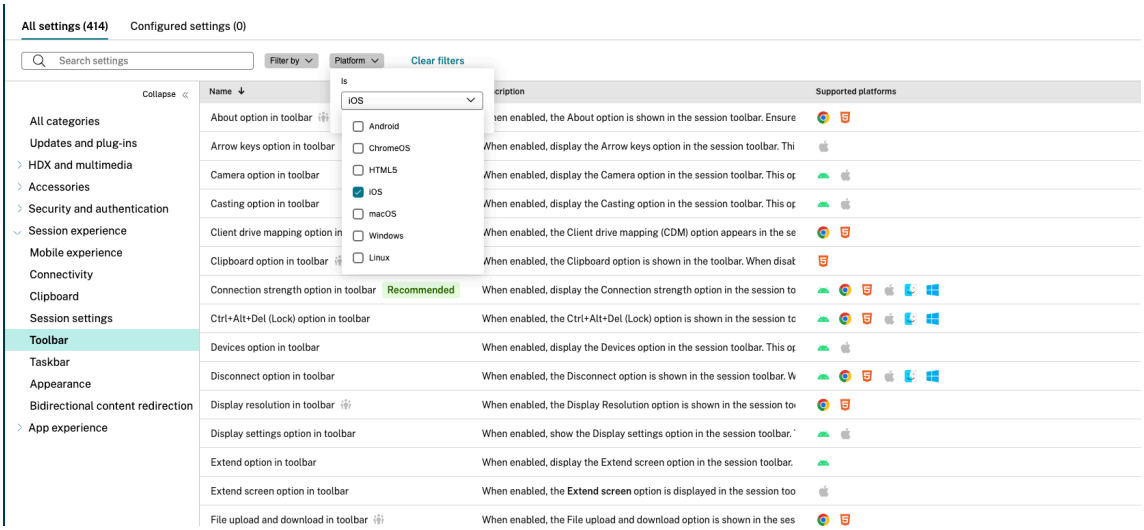
2. Click **Citrix Workspace app > Session Experience > Session Toolbar**.



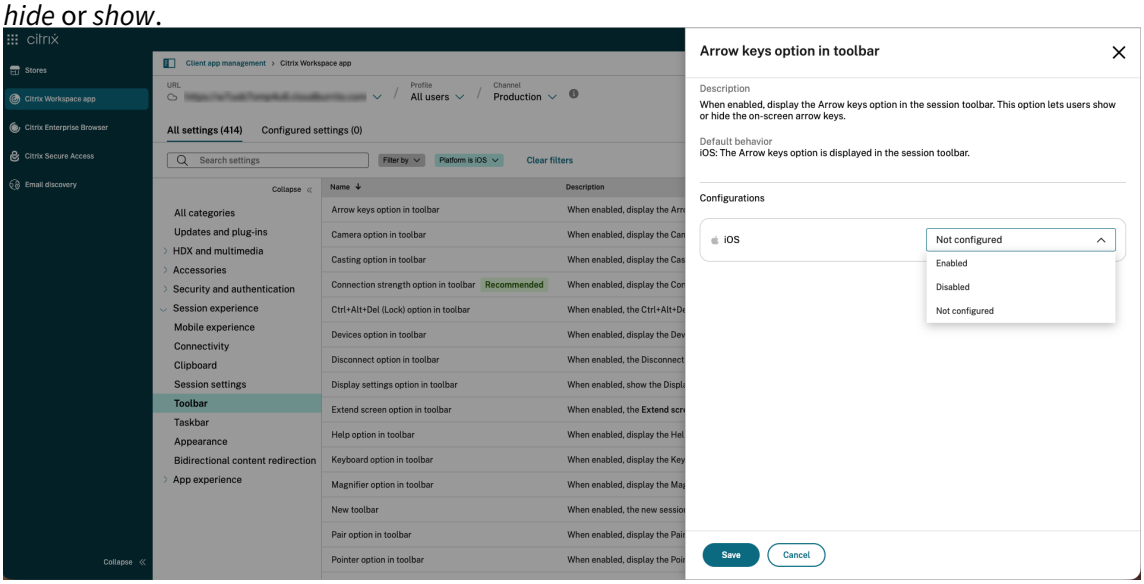
3. Under the **Toolbar** section. Navigate to the required option in the toolbar and click the column you want to edit. You can also filter by platform (such as iOS or any other platform), then click **Apply**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



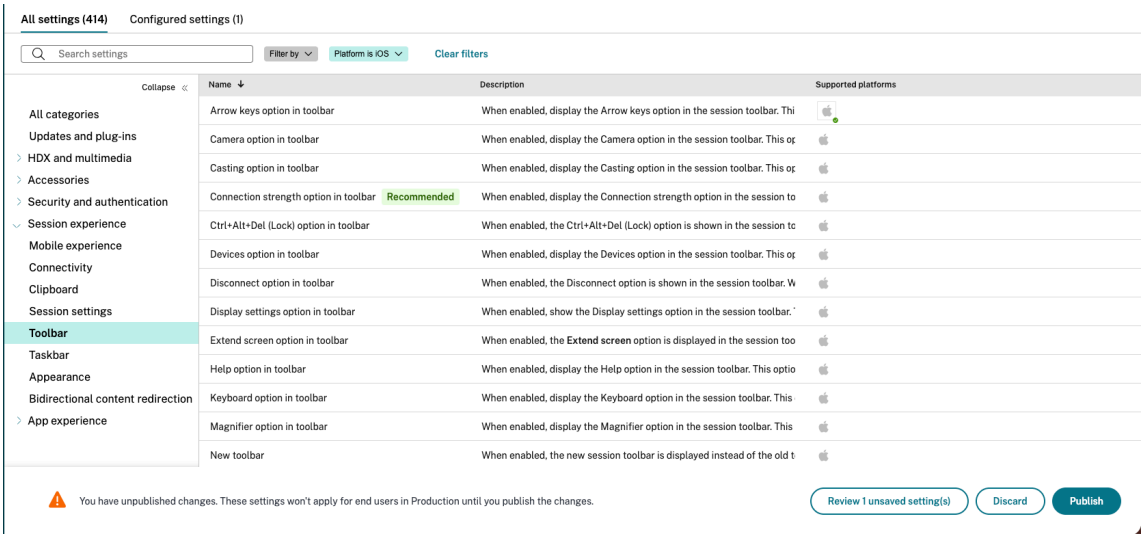


4. Select the configuration checkbox and then click. You can now customize the toolbar option to *hide* or *show*.



5. Click **Save** after changing the configuration.
6. Click **Publish** to save the settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> Changes may take up to 6 hours to take effect due to Citrix Cloud caching.

Using MDM

This configuration is deployed through your MDM solution as a **Managed App Configuration** for the Citrix Workspace app bundle ID. MDM configurations are given priority over GACS settings. Settings are stored in `XML`/`plist` format as part of Apple's Managed App Configuration.

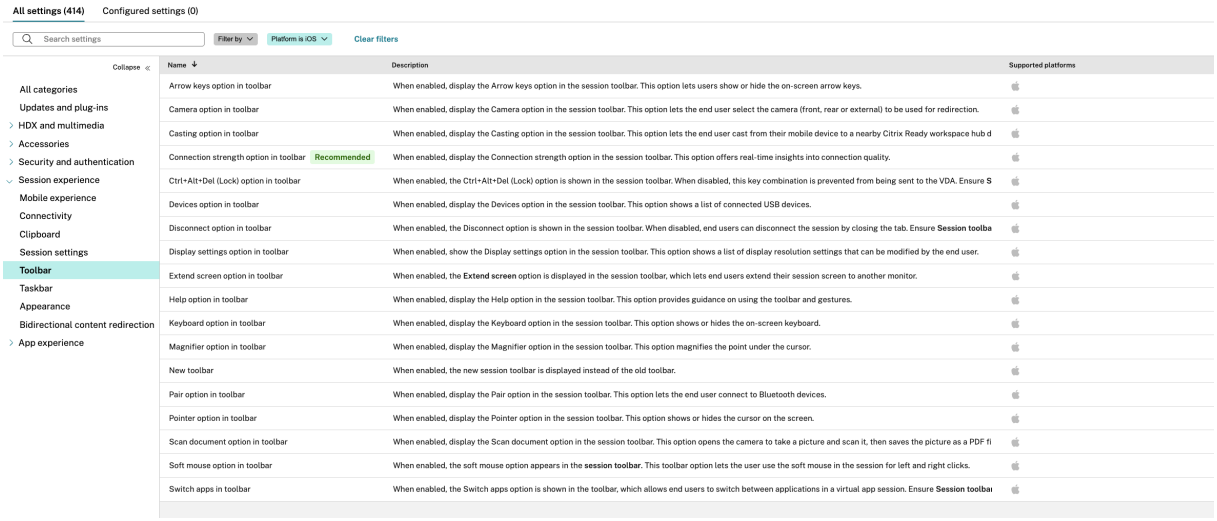
Example MDM Configuration for Toolbar

```
<dict>
    <key>category</key>
    <string>toolbar</string>
    <key>userOverride</key>
    <false/>
    <key>settings</key>
    <array>
        <dict>
            <key>name</key>
            <string>enableKeyboardToolbarOption</string>
            <key>value</key>
            <true/>
        </dict>
        <dict>
            <key>name</key>
            <string>enableCloseToolbarOption</string>
            <key>value</key>
            <false/>
        </dict>
        <dict>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
21                 <key>name</key>
22                 <string>enableCameraToolbarOption</string>
23                 <key>value</key>
24                 <true/>
25             </dict>
26         </array>
27 </dict>
```

iOS Toolbar Icons Configuration



Name	Description	MDM Setting Key
Arrow keys option in toolbar	When enabled, display the Arrow keys option in the session toolbar. This option lets users show or hide the on-screen arrow keys.	`enableArrowKeysToolbarOption`
Camera option in toolbar	When enabled, display the Camera option in the session toolbar. This option lets the end user select the camera (front, rear or external) to be used for redirection.	`enableCameraToolbarOption`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Description	MDM Setting Key
Casting option in toolbar	When enabled, display the Casting option in the session toolbar. This option lets the end user cast from their mobile device to a nearby Citrix Ready workspace hub device.	`enableCastingToolbarOption`
Connection strength option in toolbar	When enabled, display the Connection strength option in the session toolbar. This option offers real-time insights into connection quality.	`enableConnectionStrengthToolbar`
Ctrl+Alt+Del (Lock) option in toolbar	When enabled, the Ctrl+Alt+Del (Lock) option is shown in the session toolbar. When disabled, this key combination is prevented from being sent to the VDA. Ensure Session toolbar is enabled for this setting to take effect.	`enableCtrlAltDelToolbarOption`
Devices option in toolbar	When enabled, display the Devices option in the session toolbar. This option shows a list of connected USB devices.	`enableDevicesToolbarOption`
Disconnect option in toolbar	When enabled, the Disconnect option is shown in the session toolbar. When disabled, end users can disconnect the session by closing the tab. Ensure Session toolbar is enabled for this setting to take effect.	`enableCloseToolbarOption`
Display settings option in toolbar	When enabled, show the Display settings option in the session toolbar. This option shows a list of display resolution settings that can be modified by the end user.	`enableDisplaySettingsToolbarOpt`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Description	MDM Setting Key
Help option in toolbar	When enabled, display the Help option in the session toolbar. This option provides guidance on using the toolbar and gestures.	enableHelpToolbarOption
Keyboard option in toolbar	When enabled, display the Keyboard option in the session toolbar. This option shows or hides the on-screen keyboard.	enableKeyboardToolbarOption
Magnifier option in toolbar	When enabled, display the Magnifier option in the session toolbar. This option magnifies the point under the cursor.	enableMagnifierToolbarOption
New toolbar	When enabled, the new session toolbar is displayed instead of the old toolbar.	enableNewToolbar
Pair option in toolbar	When enabled, display the Pair option in the session toolbar. This option lets the end user connect to Bluetooth devices.	enablePairToolbarOption
Pointer option in toolbar	When enabled, display the Pointer option in the session toolbar. This option shows or hides the cursor on the screen.	enablePointerToolbarOption
Scan document option in toolbar	When enabled, display the Scan document option in the session toolbar. This option opens the camera to take a picture and scan it, then saves the picture as a PDF file.	enableScanDocumentToolbarOption
Soft mouse option in toolbar	When enabled, the soft mouse option appears in the session toolbar. This toolbar option lets the user use the soft mouse in the session for left and right clicks.	enableSoftMouseToolbarOption

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Description	MDM Setting Key
Switch apps in toolbar	When enabled, the Switch apps option is shown in the toolbar, which allows end users to switch between applications in a virtual app session. Ensure Session toolbar is enabled for this setting to take effect.	`enableSwitchAppsToolbarOption`

Store configuration

September 7, 2025

Enhanced new customizable toolbar

Starting with version 24.12.0, Citrix Workspace app for iOS introduces a new customizable toolbar. The revamped desktop viewer toolbar enhances user experience and support by offering greater flexibility. Admins can now tailor the in-session toolbar to meet their organization's needs.

Feature	Description
Admin Control	Admins can customize the toolbar, choosing what options are shown to the end user.
UI & Skinning	The **Desktop Viewer** toolbar has been revamped with a new user interface and skinning options.
Switchable Layout	The toolbar can switch between a single and double-column layout.
Customizable Toolbar	Admins can choose to push either the old or new toolbar to users.
Drag Functionality	In landscape mode, the toolbar notch can only be moved along the top edge of the screen. In portrait mode, the notch can be dragged horizontally from left to right or right to left, as well as vertically along the screen's edge.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Feature	Description
Quick Access Icons	New icons are introduced for quick access to frequently used features.
Gesture Guide	Provides guidance on single click, right click, drag, zoom, toggle pointer, and keyboard usage.
Toolbar Guide	Includes options for devices, keyboard, pointer, magnifier, soft mouse, display, camera, switch, scroll and more.

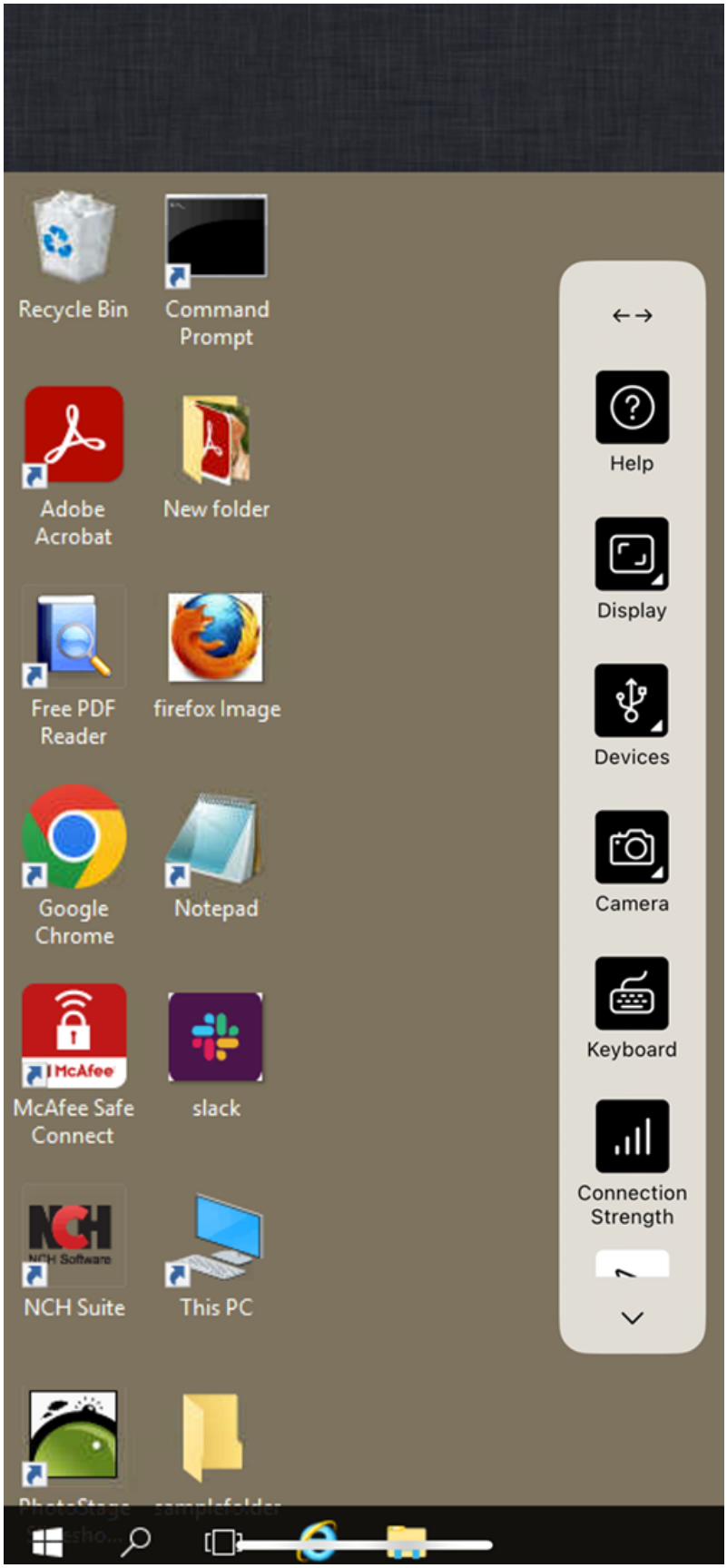
Standard menu options:

Menu Option	Description
Arrow Keys	Displays a navigation arrow keypad for session navigation.
Keyboard	Displays the iOS system soft keyboard along with an extended keyboard accessory with control keys.
Pointer	Displays a Windows-like mouse pointer inside the session window.
Magnifier	Displays a window like mouse pointer along with a magnifying lens.
Virtual Mouse	This option displays a soft-mouse on screen.
Switch	Switch-apps is used to switch between multiple virtual apps that are opened at a time in single Virtual Desktop Agent
Display	Displays full-screen display settings modal view.
Ctrl+Alt+Del	Sends the Ctrl+Alt+Del key combination to the Virtual Desktop Agent.
Pair	Allows pairing with Secondary iPhone or iPad device to act as a track pad.
Disconnect	If sustainability feature is enabled it gives an option to choose between signout and disconnect, else it disconnects the session.
External Mouse settings	Displays session mouse settings modal view.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Menu Option	Description
Camera	You can select the type of camera to use: front, rear, or external. Opens the camera to scan documents into a PDF and upload them to the Virtual Desktop Agent.
Help Guide	Provides guidance on using toolbar features, gestures, and menu options for navigating and interacting with the session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Variable menu options:

Menu Option	Description
Scan	Displays a full-screen camera to scan documents.
Cast	Displays options for casting the screen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

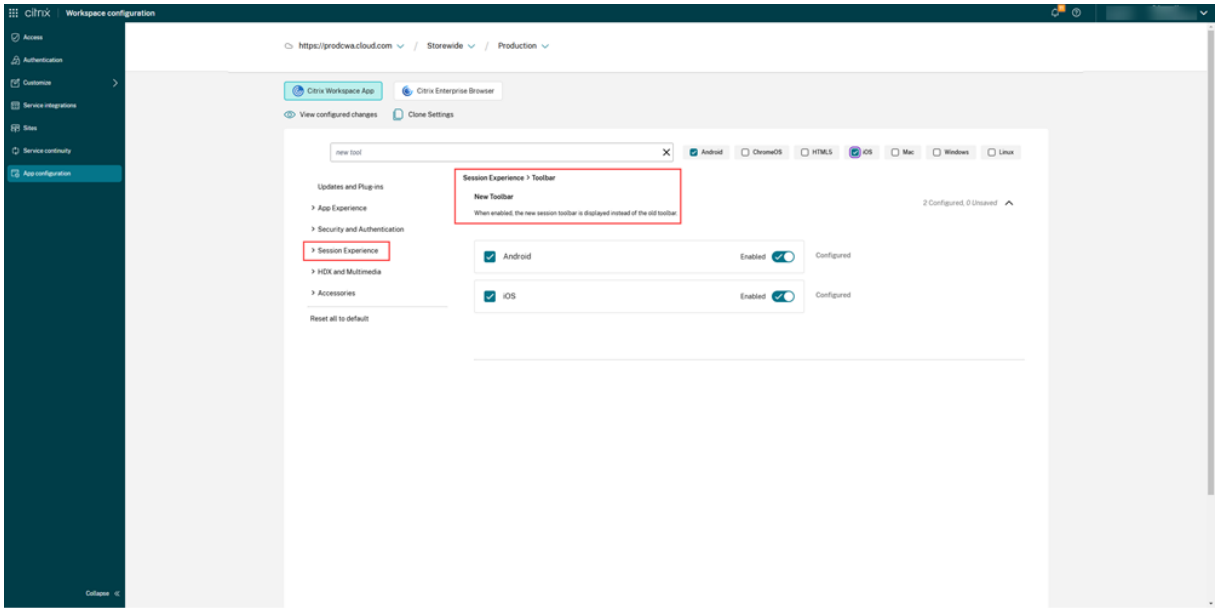


You can enable the feature through Global App Configuration service (GACS) and ensure the feature flag is turned on.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To enable this feature through GACS, admins should follow these steps:

1. Navigate to **Workspace Configuration** > **App Configuration** > **Configure** in Citrix Cloud.
2. Under **Citrix Workspace™ app**, select **Session Experience**.
3. Click **Toolbar** and enable the required option.



Authenticate

December 8, 2025

Enhanced Citrix® security with pre-populated user name

Starting with version 25.1.0, you can use Unified Endpoint Management (UEM) to push the user name in a specific format to manage devices. On iOS, Citrix Workspace app reads this configuration, retrieves the user name, and pre-populates it within the authentication prompt, making it read-only. This ensures that only the registered device owner can authenticate and access the app on that specific device.

Administrators gain the ability to manage user authentication efficiently across multiple iOS devices from a central location, while ensuring only authorized users can sign in.

This feature also simplifies the login process by eliminating the need for users to manually enter their credentials, reducing the risk of errors and enhancing the overall user experience. By combining robust access control with a seamless login flow, Citrix Workspace™ app for iOS supports both enhanced security and improved usability.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

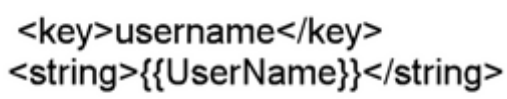
You can configure this feature through UEM using the following settings:

> **Note:**
>
> This example uses Microsoft Intune as the UEM solution for demonstration. The steps and UI may vary depending on your UEM provider.

1. Sign in to your UEM provider.
2. Add the Citrix Workspace app to your UEM provider for management. Upload it through the UEM portal or link it to the App Store.
3. Create an app configuration policy for your app.
4. Add a key and value pair to the XML property list and fill in the following values:

    - **key:** `username`
    - **value type:** `String`
    - **value:** Payload variable which is documented in Microsoft Intune portal.

Microsoft Intune:



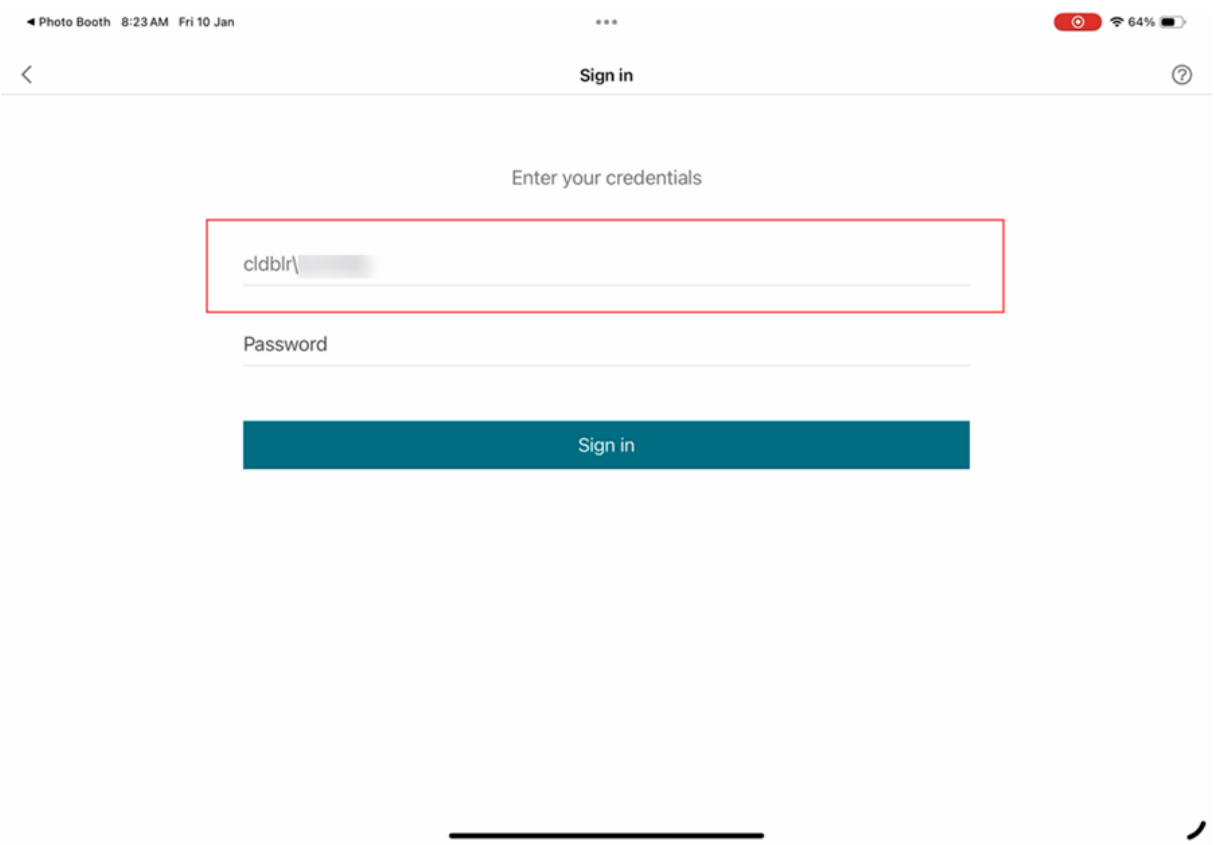
For more information, see - iOS and iPadOS device settings to use common iOS/iPadOS features in Intune.

Jamf:

```
<key>username</key>
    <string>$USERNAME</string>
```

For more information, see - Payload Variables for Configuration Profiles.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Limitation:

The system supports only the Native Login page. For web-based login, pre-filling the user name is not supported.

Fast smart card

Starting with version 24.12.0, Citrix Workspace app for iOS introduces smart card enhancements for improved authentication performance and usability. This update brings significant improvements to smart card support, making the user experience smoother and more efficient. With the integration of concurrent protocol support and fast smart card protocol, users can expect faster authentication and seamless use of smart card readers. The fast smart card is compatible with CNG (Crypto Next Generation) API on the Windows desktop.

> **Note:**
>
> Contact Citrix Help Desk to activate this feature.

Limitations:

- Concurrency is not fully supported in Citrix Workspace app iOS.
- Plug and Play is not supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enforcing Citrix access using Citrix Workspace app

Starting with version 24.12.0, admins can mandate users on iOS devices to access Citrix Workspace exclusively through the native app. When this feature is enabled, users attempting to access the store URL and third-party browsers are automatically redirected to the Citrix Workspace app. This ensures they can take advantage of all the native app's capabilities and enjoy a seamless user experience. Additionally, this feature gives admins greater control over the user environment and enhances security by keeping the authentication process within the native app, eliminating the need to download ICA files.

Admins can enable this feature using their Citrix Cloud account. This feature is currently supported for Cloud stores only. For more information, see Mandate end users to authenticate and access apps and desktops through native app.

Skip enable biometrics prompt

Previously, end users were prompted to choose whether to use biometrics Touch ID or Face ID for authentication in the Citrix Workspace app. Starting with version 24.9.0, administrators can now skip this prompt, streamlining the login process for users.

When biometrics are enabled, user passwords are securely stored in the keychain and protected by biometric authentication. Upon expiration of the authentication token, users are automatically prompted for biometric verification. If biometrics are not configured on the device, users need to manually enter their credentials when the token expires.

This feature is currently supported only for on-premise stores using Lightweight Directory Access Protocol (LDAP) authentication.

Configuration

The following methods can be used to enable the biometric authentication:

- Mobile Device Management (MDM)
- Global App Configuration service (GACS)

To enable biometric authentication through MDM, admins must use the following setting:

- Key: `settings_skip_consent_for_biometric_protected_password_saving`
- Value: **`true`** / **`false`**
- Default value: **`false`**

  –If set to **`true`**, biometric re-login feature is automatically applied for end users, without providing them an option to select or decline it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

–If set to `false`, biometric re-login feature is optional, and users can choose to accept or decline it.

To enable biometric authentication through GACS, admins must use the following steps:

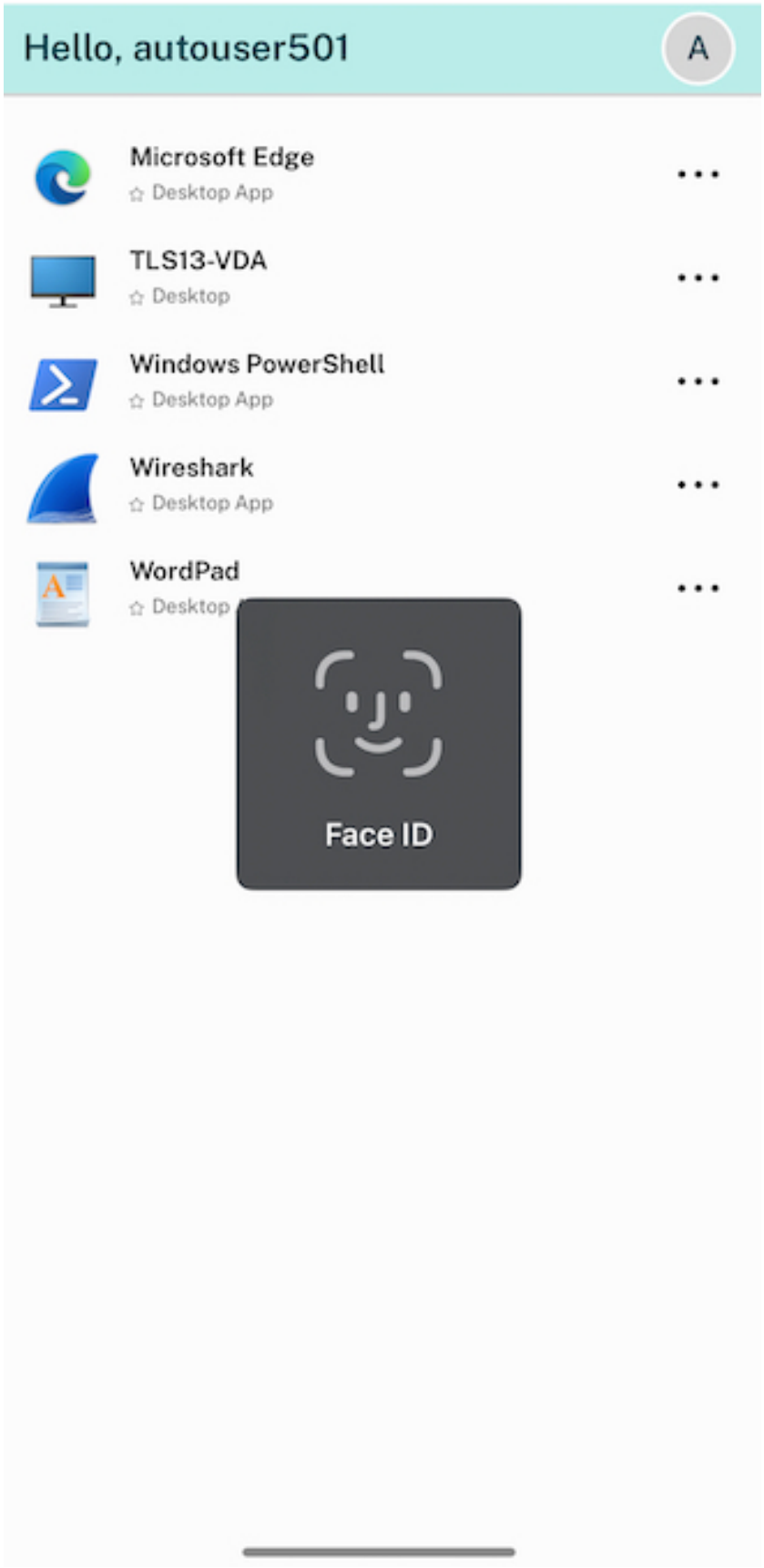
1. Navigate to **Workspace Configuration** > **App Configuration** > **Configure** in Citrix Cloud.
2. Under **Citrix Workspace app**, select **Security and Authentication**.
3. Under **Authentication**, enable **Skip use biometrics prompt**.

For more information, see Support for configuring Citrix Workspace app settings through UEM.

Support for enforcing biometric authentication to access Citrix Workspace app

Administrators can now enforce a device's biometric authentication to access Citrix Workspace app for their users. With this feature, when you open Citrix Workspace app after dismissing it or bring it to the forefront after minimizing it, a prompt for Face ID or Touch ID verification appears to unlock and sign in. If the device does not support biometric authentication, the password or passcode authentication method is used to access the app. If the passcode is not enabled on the device, the account is signed out, requiring the user to sign in again to access the Citrix Workspace application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Administrators can configure this feature using the unified endpoint management solution with the following key value pairs:

- **key**: verify_biometric_on_app_foreground_transition
- **value type**: Boolean
- **value**: true or false
    - If set to **true**, biometric authentication is required for end users to access Citrix Workspace app.
    - If set to **false**, biometric authentication is not enforced to access Citrix Workspace app. Users have the option to disable biometric authentication.

Support for authentication using FIDO2 when connecting to an on-premises store

Starting with the 24.7.0 version, users can authenticate to Citrix Workspace app for iOS using FIDO2-based password-less authentication when connecting to an on-premises store. FIDO2 offers a seamless authentication method, allowing enterprise employees to access Citrix Workspace app for iOS without the need to enter user name or password. This feature supports both roaming (USB only) and platform authenticators (PIN code, Touch ID, and Face ID only).

You can configure this feature using the Global App Configuration Service and unified endpoint management.

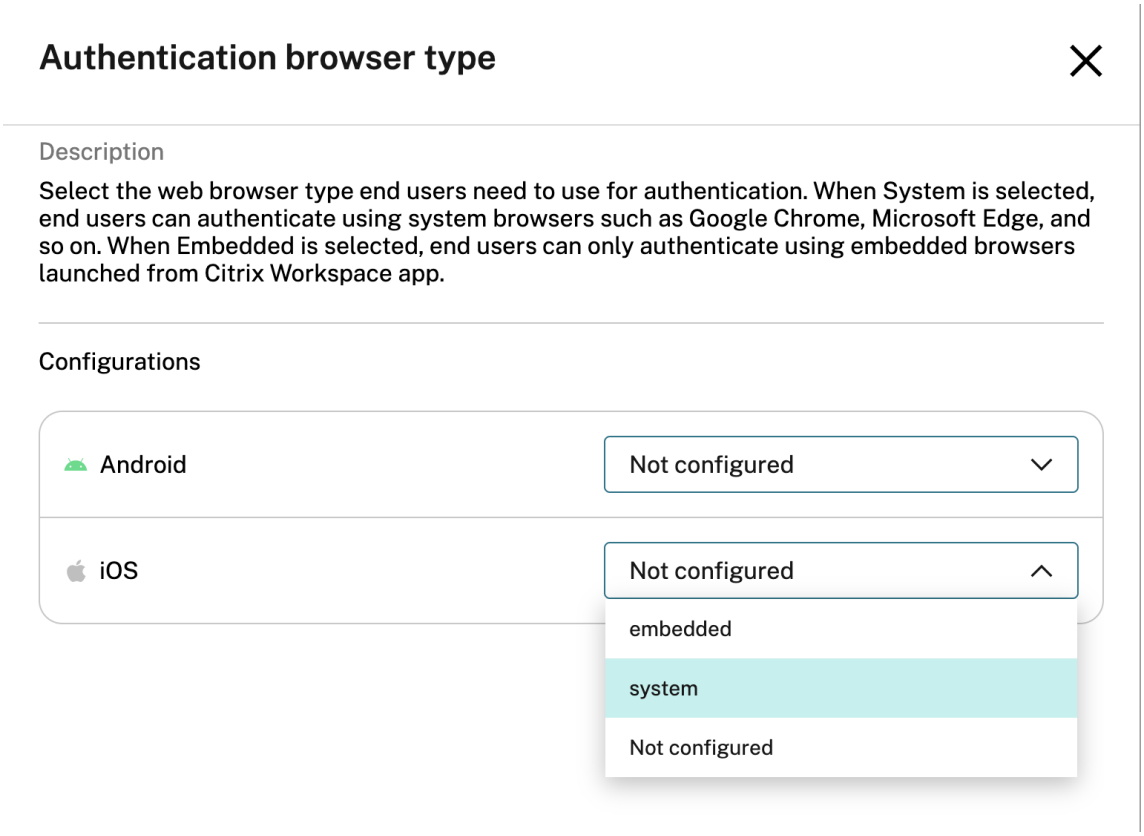
> **Note:**
>
> This feature is supported only on the system browser.

Using Global App Configuration Service

To configure using Global App Configuration service, do the following steps:

1. Sign in to Citrix Cloud with your credentials.
2. Navigate to **Workspace Configuration** > **App configuration**.
3. On the **App configuration** page, select the store and then tap **Configure**.
4. On the **Workspace URL** page, navigate to **Security and Authentication** > **Authentication**.
5. Under **Authentication browser type**, select **iOS** and then select **system** from the drop-down menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Tap **Publish Drafts** to publish the settings for the selected store.

For more information about Global App Configuration service, see Configure settings for on-premises stores in the Global App Configuration service documentation.

Using the unified endpoint management solutions

To configure using unified endpoint management, do the following steps:

1. Sign in to your Unified Endpoint Management (UEM) provider.
2. Add the Citrix Workspace app that you want to manage by your UEM provider. You can upload the app by using your UEM provider's portal to enable management by your UEM provider. Alternatively, you can link to the app in the App Store.
3. Create an app configuration policy for your app.
4. Add the key and value pair to the XML property list and fill in the following values:

```
<dict>
                    <key>category</key>
                    <string>authentication</string>
                    <key>userOverride</key>
                    <false/>
                    <key>settings</key>
                    <array>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
8                           <dict>
9                               <key>name</key>
10                              <string>settings_auth_web_browser</string>
11                              <key>value</key>
12                              <string>system</string>
13                          </dict>
14                      </array>
15      </dict>
```

For more information, see Configure Workspace app using Unified Endpoint Management solutions.

Client certificate authentication

> **Important:**
>
> - When using StoreFront, Citrix Workspace app supports:
>   - Citrix Access Gateway Enterprise Edition Version 9.3
>   - NetScaler Gateway Version 10.x through Version 11.0
>   - Citrix Gateway Version 11.1 and later
> - Citrix Workspace app for iOS supports client certificate authentication.
> - Only Access Gateway Enterprise Edition 9.x and 10.x (and later releases) support client certificate authentication.
> - Double-source authentication types must be CERT and LDAP.
> - Citrix Workspace app also supports optional client certificate authentication.
> - Only P12 formatted certificates are supported.

Users signing in to a Citrix Gateway virtual server can also be authenticated based on the attributes of the client certificate that is presented to the virtual server. Client certificate authentication can also be used with another authentication type, LDAP, to provide double-source authentication.

Administrators can authenticate end users based on the client-side certificate attributes as follows:

- the client authentication is enabled on the virtual server.
- the virtual server requests for a client certificate.
- to bind a root certificate to the virtual server on Citrix Gateway.

When users sign in to the Citrix Gateway virtual server, after authentication, users can extract the user name and domain information from the **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** field in the certificate. It is in the format `username@domain`.

The authentication is completed when the user extracts the user name and domain, and provides the required information (such as password). If the user does not provide a valid certificate and credentials, or if the username/domain extraction fails, authentication fails.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can authenticate users based on the client certificate by setting the default authentication type to use the client certificate. You can also create a certificate action that defines what is to be done during the authentication based on a client SSL certificate.

To configure the XenApp® farm

Create a XenApp farm for mobile devices in the Citrix Virtual Apps™ console or Web Interface console. The console depends on the version of Citrix Virtual Apps that you've installed.

Citrix Workspace app uses a XenApp farm to get information about the applications a user has rights to. The same information is shared to the apps that are running on the device. This method is similar to the way that you use the Web Interface for traditional SSL-based Citrix Virtual Apps connections, where you can configure the Citrix Gateway.

Configure the XenApp farm for Citrix Workspace app for mobile devices to support connections from the Citrix Gateway as follows:

1. In the XenApp farm, select **Manage secure client access** > **Edit secure client access** settings.
2. Change the Access Method to Gateway Direct.
3. Enter the FQDN of the Citrix Gateway appliance.
4. Enter the Secure Ticket Authority (STA) information.

To configure the Citrix Gateway appliance

For client certificate authentication, configure Citrix Gateway with two-factor authentication using the Cert and LDAP authentication policies. To configure the Citrix Gateway appliance:

1. Create a session policy on Citrix Gateway to allow incoming Citrix Virtual Apps connections from Citrix Workspace app. Specify the location of your newly created XenApp farm.

    - Create a session policy to identify that the connection is from Citrix Workspace app. As you create the session policy, configure the following expression and choose Match All Expressions as the operator for the expression:

      ```
      REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace
      ```

    - In the associated profile configuration for the session policy, on the **Security** tab, set **Default Authorization** to **Allow**.

      On the **Published Applications** tab, if the setting isn't a global setting (you selected the Override Global checkbox), verify if the **ICA® Proxy** field is set to **ON**.

      In the Web Interface **Address** field, enter the URL including the config.xml for the XenApp farm that the device users use, for example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- /XenAppServerName/Citrix/PNAgent/config.xml
  or
- /XenAppServerName/CustomPath/config.xml.

- Bind the session policy to a virtual server.
- Create authentication policies for Cert and LDAP.
- Bind the authentication policies to the virtual server.
- Configure the virtual server to request client certificates in the TLS handshake. To do so, navigate to the **Certificate** > **open SSL Parameters** > **Client Authentication** > set **Client Certificate** to **Mandatory**.

> **Important:**
>
> - If the server certificate that is used on the Citrix Gateway is a part of a certificate chain. For example, if it is an intermediate certificate, then install the certificates on the Citrix Gateway. For information about installing certificates, see the Citrix Gateway documentation.
> - The user needs to manually import the certificate if the client certificate is set to mandatory before authentication can be done.

To configure the mobile device

If client certificate authentication is enabled on Citrix Gateway, users are authenticated based on certain attributes of the client certificate. After authentication, you can extract the user name and domain from the certificate. You can apply specific policies for each user.

1. From Citrix Workspace app, open the **Account**, and in the Server field, type the matching FQDN of your Citrix Gateway server. For example, GatewayClientCertificateServer.organization.com. Citrix Workspace app automatically detects that the client certificate is required.
2. Users can either install a new certificate or choose one from the already installed certificate list. For iOS client certificate authentication, download and install the certificate from Citrix Workspace app only.
3. After you select a valid certificate, the user name and domain fields on the sign-in screen is prepopulated using the user name from the certificate. An end user can type other details, including the password.
4. If client certificate authentication is set to optional, users can skip the certificate selection by pressing Back on the certificates page. In this case, Citrix Workspace app proceeds with the connection and provides the user with the logon screen.
5. After users complete the initial sign-in, they can start applications without providing the certificate again. Citrix Workspace app stores the certificate for the account and uses it automatically for future logon requests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support to switch web browser for authentication

Starting with the 23.2.0, administrators can now switch the browser being used for the authentication process from embedded browser to system browser on iOS or iPad devices, when an advanced authentication policy is configured on the on-premises Citrix Gateway and StoreFront Deployment.

Configure Rewrite policy for authentication process Administrators can switch the browser being used for the authentication process from embedded browser to system browser. It is only possible when an advanced authentication policy is configured on the on-premises Citrix Gateway and StoreFront Deployment. To configure an advanced authentication policy, configure the NetScaler Rewrite policy by using the NetScaler command line:

1. `enable ns feature REWRITE`
2. `add rewrite action insert_auth_browser_type_hdr_act insert_http_header X-Auth-WebBrowser "\"System\""`
3. `add rewrite policy insert_auth_browser_type_hdr_pol "HTTP.REQ.URL.EQ(\"/cgi/authenticate\")"insert_auth_browser_type_hdr_act`
4. `bind vpn vserver <VPN-vserver-Name> -policy insert_auth_browser_type_hdr_p -priority 10 -gotoPriorityExpression END -type AAA_RESPONSE`

Moving to the system browser provides more capabilities such as:

- Better experience with certificate-based authentication.
- Ability to use an existing user certificate from the device keystore during the authentication process.
- Support for few third-party authenticators like SITHS eID.

Embedded browser is used as the default browser for authentication if the administrator hasn't configured the above Rewrite policy.

This table lists the browsers that are used for authentication based on the configuration on the NetScaler® Gateway and Global App Config Service:

NetScaler Gateway	Global App Configuration Service	Browser used for authentication
System	System	System
System	Embedded	System
Embedded	System	System
Embedded	Embedded	Embedded
No Configuration	System	System

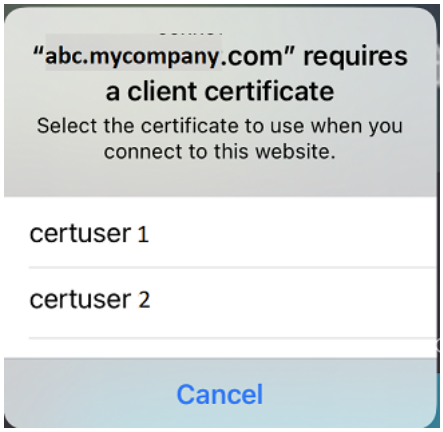
© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway	Global App Configuration Service	Browser used for authentication
No Configuration	Embedded	Embedded

Support certificate-based authentication for on-premises stores

End users can now handle certificate-based authentication where, the certificates are saved onto the device keychain. While signing in, Citrix Workspace app detects the list of certificates on your device, and you can choose a certificate for authentication.

> **Important:**
>
> After you choose the certificate, the selection persists for the next Citrix Workspace app launch. To choose another certificate, you can "Reset Safari"from iOS device settings or reinstall Citrix Workspace app.



> **Note:**
>
> This feature supports on-premises deployments.

To configure:

1. Navigate to the Global App Configuration Store Settings API URL and enter the cloud store URL. For example, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Navigate to **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** > click **POST**.
3. Click **INVOKE API**.
4. Enter and upload the payload details. Select one of the following values:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- “Embedded”: you can use WKWebView. This option is set by default.
- “system”: you can use the Safari view controller.

For example,

```
"category": "Authentication",
"userOverride": false,
"settings": [
{
  "name": "Web Browser to use for Authentication", "value": "*
     Embedded*/*System*"  }
 ,
```

On iOS or iPad devices, administrators can switch the browser being used for the authentication process. You can switch from embedded browser to system browser, when an advanced authentication policy is configured on the on-premises Citrix Gateway and StoreFront Deployment. For more information, see Configure Rewrite policy for authentication process.

5. Click **EXECUTE** to push the service.

Smart cards

Citrix Workspace app supports SITHS smart cards for in-session connections only.

If you're using FIPS Citrix Gateway devices, configure your systems to deny SSL renegotiations. For details, see Knowledge Center article CTX123680.

The following products and configurations are supported:

- Supported readers:
  - Precise Biometrics Tactivo for iPad Mini Firmware version 3.8.0
  - Precise Biometrics Tactivo for iPad (fourth generation) and Tactivo for iPad (third generation) and iPad 2 Firmware version 3.8.0
  - BaiMobile® 301MP and 301MP-L Smart Card Readers
  - Thursby PKard USB reader
  - Feitian iR301 USB reader
  - Type-C CCID-compliant readers
  - Twocanoes smart card utility reader
- Supported VDA Smart Card Middleware
  - ActiveIdentity
- Supported smartcards:
  - PIV cards
  - Common Access Card (CAC)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Supported configurations:
  - Smart card authentication to Citrix Gateway with StoreFront 2.x and XenDesktop 7.x or later or XenApp 6.5 or later

To configure Citrix Workspace app to access apps

1. If you want to configure Citrix Workspace app automatically to access apps when you create an account, in the Address field, type the matching URL of your store. For example:
   - StoreFront.organization.com
   - netscalervserver.organization.com
2. Select the **Use Smartcard** option when you're using a smart card to authenticate.

> **Note:**
>
> Logons to the store are valid for about one hour. After that time, users must log on again to refresh or launch other applications.

Support for Type C-based Generic Readers

Starting with the 23.12.0 version, Citrix Workspace app for iOS now supports Type-C CCID compliant readers for Smart Card authentication. Previously, only lightning port-based readers were supported. The inclusion of Type-C smart card readers within the Citrix Workspace app offers dual advantages: users can authenticate through Citrix Workspace app and seamlessly use the smart card within their virtual desktop sessions.

Support for the Twocanoes smart card utility reader

Starting with the 24.3.5 version, Citrix Workspace app for iOS supports the Twocanoes smartcard utility readers. For more information about supported smart card readers, see Smart Cards.

> **Note:**
>
> The Twocanoes smart card utility USB-C reader is supported for both Citrix Workspace app login and virtual session login. However, the Twocanoes smart card utility Bluetooth reader is supported only for Citrix Workspace app login and not for virtual session login.

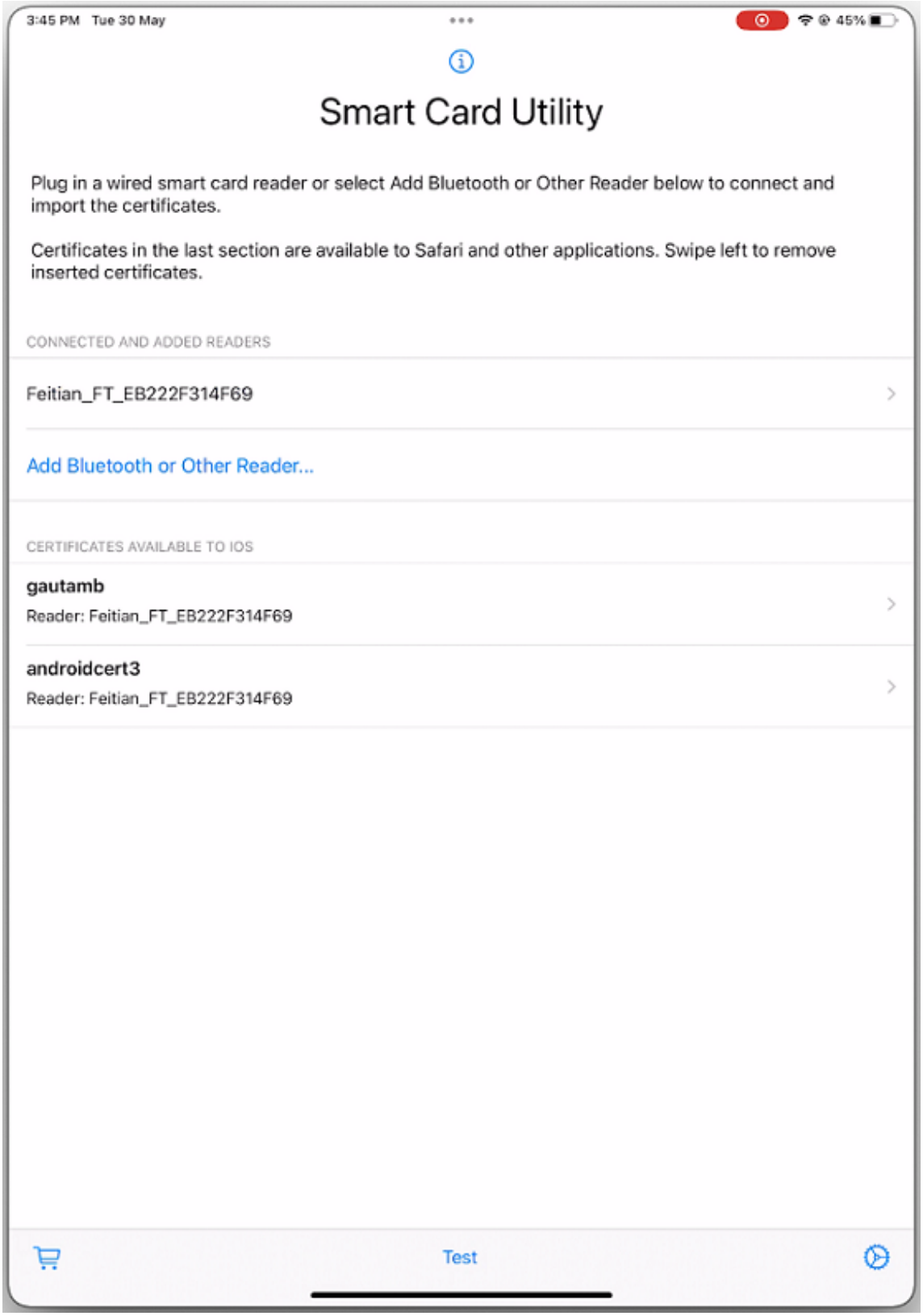
To configure the Twocanoes smart card utility Bluetooth reader, do the following steps:

1. Download and install the Smart Card Utility app from the App store. For more information, see Smart Card Utility Bluetooth Reader Quick Start in the Twocanoes knowledge base.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Make sure that the Bluetooth on your device is turned on and the smart card is inserted into the reader.
3. Open the Smart Card Utility app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



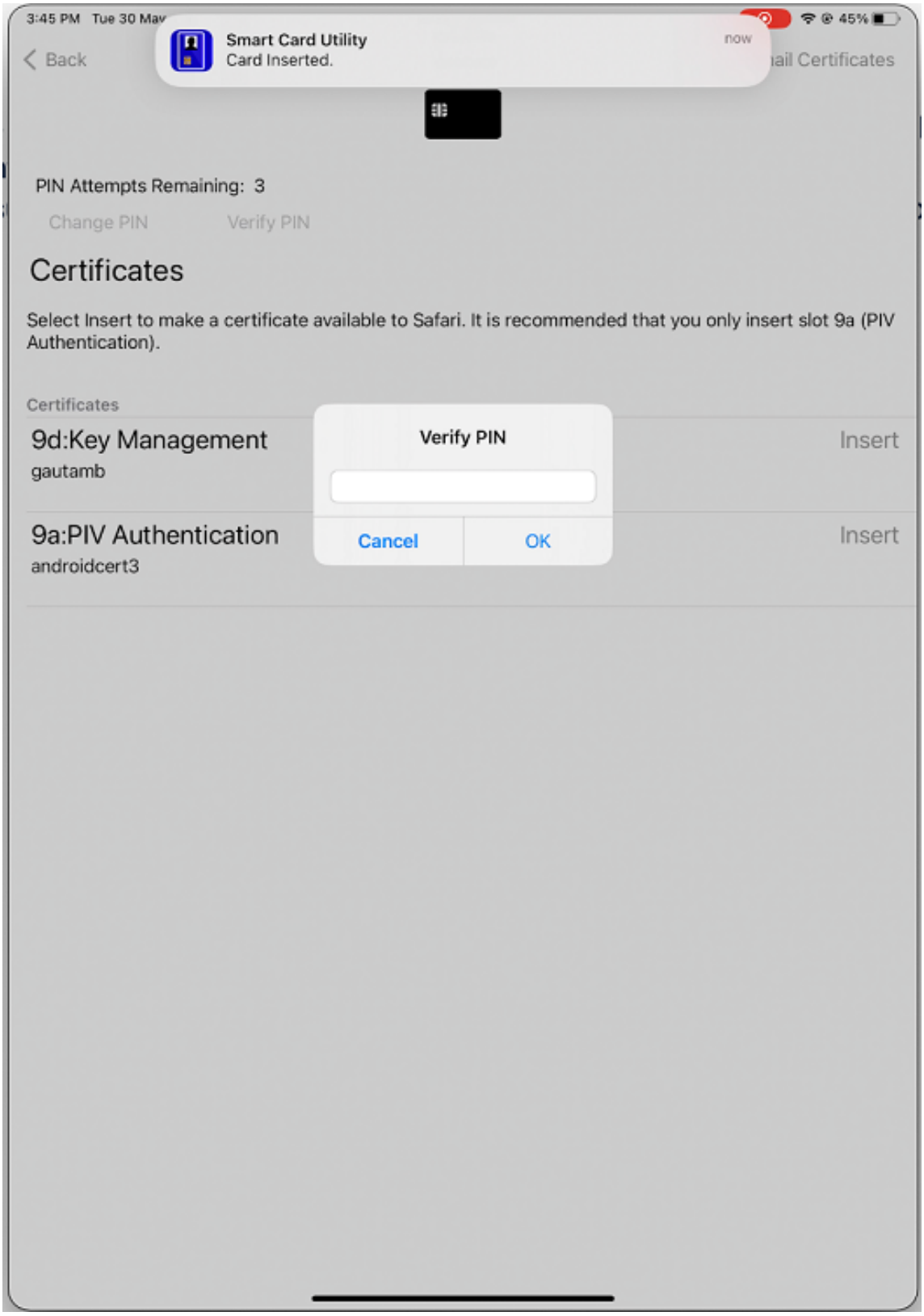
4. If you are using the Bluetooth reader, then tap **Add Bluetooth or Other Reader...** and select

© 1997–2026 Citrix Systems, Inc. All rights reserved.

your reader to connect.

> **Note:**
>
> If the reader is enabled with pin pairing, then you must enter the **PIN** when prompted. The **PIN** is available on the backside of the reader.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

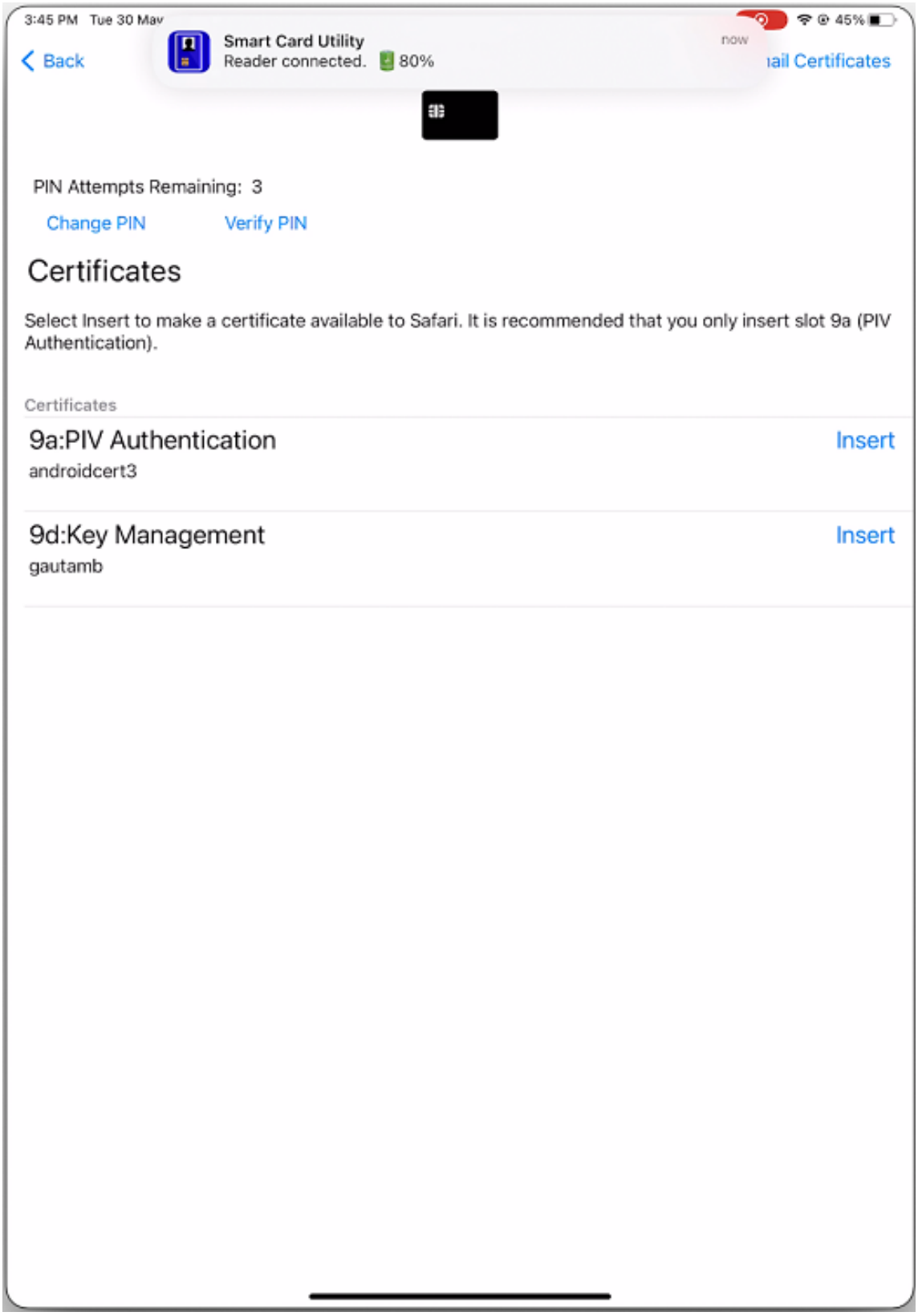


5. Tap **Insert** on the required certificate to copy it to the keychain interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> The Smart Card Utility app has implemented a cryptokit extension provided by Apple to write certificates to the keychain interface in the form of tokens. For more information, see Configure Smart Card Authentication in the Apple developer documentation.

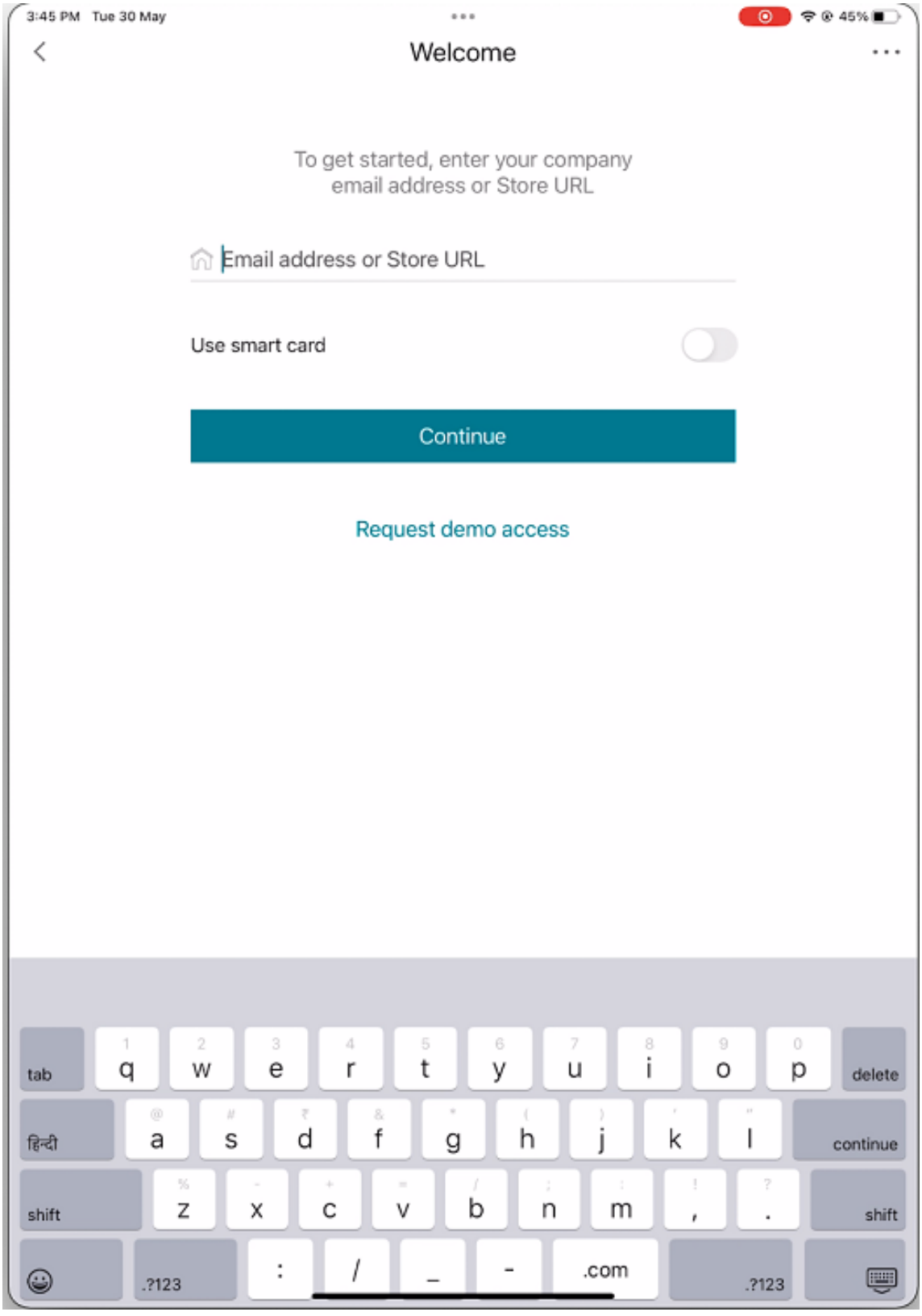
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Make sure that the reader remains connected to the device.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

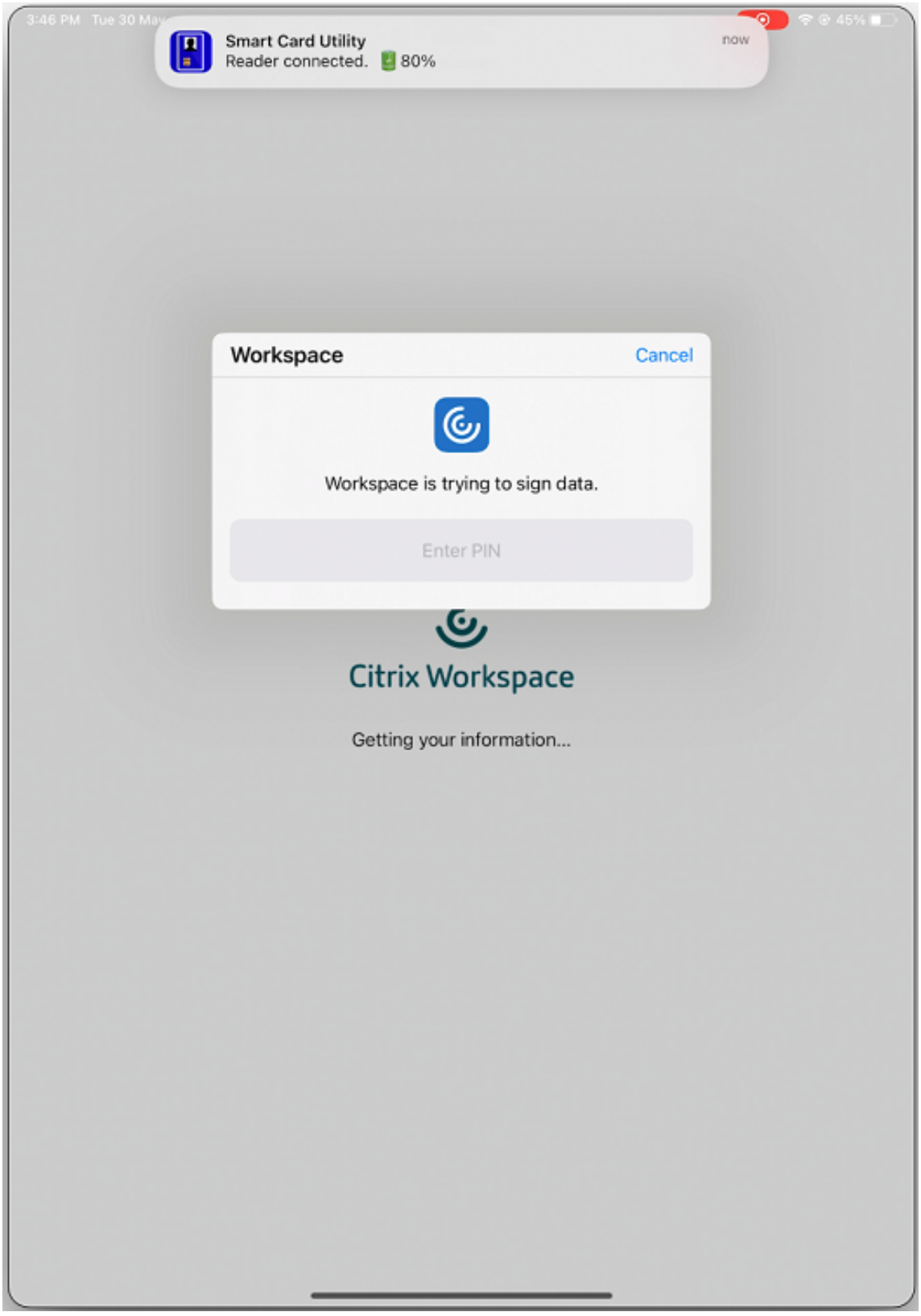
7. Open Citrix Workspace app and enter the store URL that is configured with smart card authentication.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

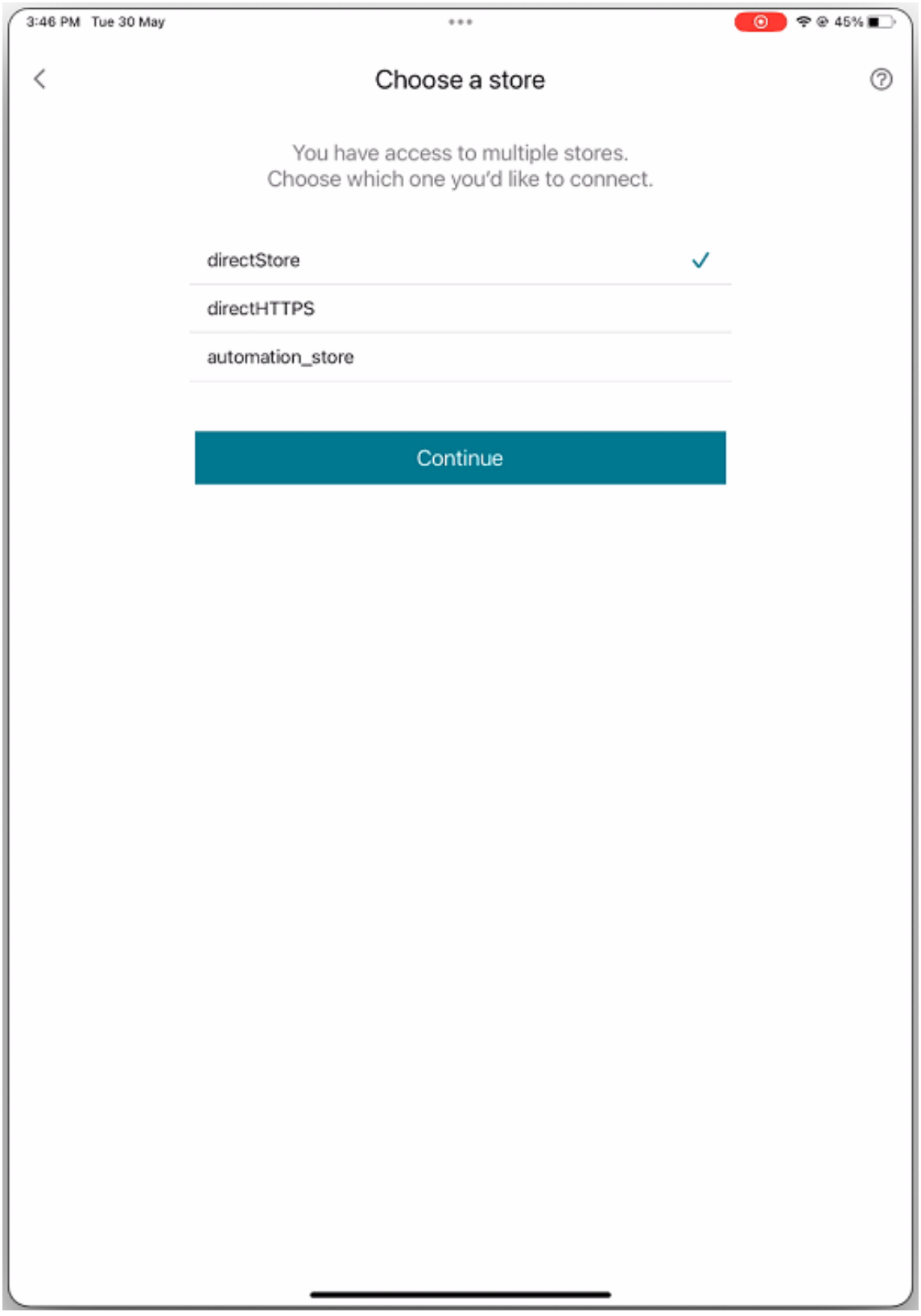
8. On the Certificates screen, select the required certificate and enter the smart card PIN provided by your IT administrator to sign in.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. If you have access to multiple stores, then select the required store and tap **Continue**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. After successful authentication, you are signed in to the Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

YubiKey support for smart card authentication

Starting with the 23.12.0 version, you can now perform smart card authentication using YubiKey. This feature provides a single-device authentication experience for Citrix Workspace app and for the virtual sessions and published apps in the VDA session. It eliminates the need to connect smart card readers or other external authenticators. It simplifies the end-user experience as YubiKey supports a wide variety of protocols, such as OTP, FIDO and so on.

To sign in to Citrix Workspace app, end users need to insert the YubiKey into their iPhone or iPad, turn on the Smart card toggle, and provide their Store URL.

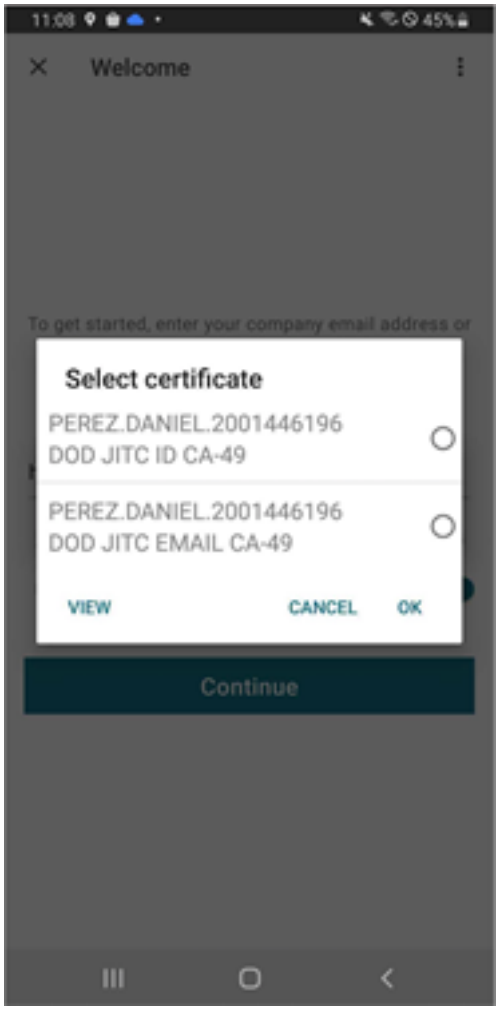
> **Note:**
>
> This feature supports only direct connection to Citrix Workspace app on StoreFront deployments and not through Citrix Gateway. The YubiKey support for smart card authentication through Citrix Gateway will be available on the future release.
> Citrix Workspace app for iOS supports only the YubiKey 5 series. For more information on YubiKey, see YubiKey 5 series.

Support for multiple certificates in smart card authentication

Previously, Citrix Workspace app for iOS displayed the certificate available on the first slot of the connected smart card.

Starting with the 24.1.0 version, Citrix Workspace app for iOS displays all the certificates available on the smart card. This feature allows you to select the required certificate while authenticating through smart card authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



View all certificates available on smart card

Starting with the 23.7.5 version, Citrix Workspace app for iOS now displays multiple certificates available on the smart card and allows you to select the certificate for smart card-based authentication. The required certificate can be selected from the **Select certificate** page once the smart card toggle has been enabled.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

RSA SecurID authentication

Citrix Workspace app supports RSA SecurID authentication for Secure Web Gateway configurations. The configurations are through the Web Interface and for all Citrix Gateway configurations.

URL scheme required for the software token on Citrix Workspace app for iOS: The RSA SecurID software token used by Citrix Workspace app registers the URL scheme com.citrix.securid only.

If end users have installed both the Citrix Workspace app and the RSA SecurID app on their iOS device, users must select the URL scheme **com.citrix.securid** to import the RSA SecurID Software Authenticator (software token) to Citrix Workspace app on their devices.

To import an RSA SecurID soft token

To use an RSA Soft Token with the Citrix Workspace app, as an administrator, ensure that the end users follow:

- the policy for PIN length
- the type of PIN (numeric only and alphanumeric)
- the limits on PIN reuse

After the end user is successfully authenticated to the RSA server, the end user needs to set up the PIN only once. After the PIN verification, they're also authenticated with the StoreFront server. After all the verification, the Workspace app displays available published applications and desktops.

To use an RSA soft token

1. Import the RSA soft token provided to you by your organization.
2. From the email with your SecurID file attached, select **Open in Workspace** as the import destination. After the soft token is imported, Citrix Workspace app opens automatically.
3. If your organization provided a password to complete the import, enter the password provided to you by your organization and click **OK**. After clicking **OK**, you'll see a message that the token was successfully imported.
4. Close the import message, and in Citrix Workspace app, tap **Add Account**.
5. Enter the URL for the Store provided by your organization and click **Next**.
6. On the Log On screen, enter your credentials: user name, password, and domain. For the Pin field, enter **0000**, unless your organization has provided you with a different default PIN. The PIN 0000 is an RSA default, but your organization might have changed it to follow with their security policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. At the top left, click **Log On**. A message appears to create a PIN.
8. Enter a PIN that is 4 to 8 digits long and click **OK**. A message appears to verify your new PIN.
9. Enter your PIN again and click **OK**. You can now access your apps and desktops.

Next Token Code

Citrix Workspace app supports the next token code feature when you configure Citrix Gateway with RSA SecurID authentication. If you enter three incorrect passwords, an error message appears on the Citrix Gateway plug-in. To sign in, wait for the next token. The RSA server can be configured to disable a user's account if a user logs on too many times with an incorrect password.

Derived credentials

Support for Purebred derived credentials within Citrix Workspace app is available. When connecting to a Store that allows derived credentials, users can log on to Citrix Workspace app using a virtual smart card. This feature is supported only on on-premises deployments.

> **Note:**
>
> Citrix Virtual Apps and Desktops™ 7 1808 or later are required to use this feature.

To enable derived credentials in Citrix Workspace app:

1. Go to **Settings** > **Advanced** > **Derived Credentials**.
2. Tap **Use Derived Credentials**.

To create a virtual smart card to use with derived credentials:

1. In **Settings** > **Advanced** > **Derived Credentials**, tap **Add New Virtual Smart Card**.
2. Edit the name of the virtual smart card.
3. Enter an 8-digit numeric-only PIN and confirm.
4. Tap **Next**.
5. Under Authentication Certificate, tap **Import Certificate…**
6. The document picker displays. Tap **Browse**.
7. Under Locations, select **Purebred Key Chain**.
8. Select the suitable authentication certificate from the list.
9. Tap **Import Key**.
10. Repeat steps 5–9 for the Digital Signature Certificate and the Encryption Certificate, if wished.
11. Tap **Save**.

You can import three or less certificates for your virtual smart card. The authentication certificate is required for the virtual smart card to work properly. The encryption certificate and digital signature certificate can be added for use in a VDA session.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> When connecting to an HDX™ session, the created virtual smart card is redirected into the session.

Known limitations

- Users can only have one active card at a time.
- Once a virtual smart card is created, it can't be edited. Delete and create the card.
- A PIN can be invalid up to ten times. If it is invalid after ten tries then the virtual smart card gets deleted.
- When you select derived credentials, the virtual smart card overrides a physical smart card.

User-Agent

Citrix Workspace app sends a User-Agent string in network requests that can be used to configure authentication policies including redirection of authentication to other Identity Providers (IdPs).

> **Note**
>
> The version numbers mentioned as part of the User-Agent in the following table are examples and it is automatically updated based on the versions that you are using.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scenario	iOS (WkWebView)	iOS (Safari View Controller)	iPadOS (WkWebView)	iPadOS (Safari View Controller)
Cloud store	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/24.7.0 iOS/18.0 X1Class CWACapable 302Redirection-Capable CFNetwork Darwin CWA-iPhone AuthManager/24.7.0.1	Default Safari User-Agent string.	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/24.7.0 iOS/18.0 X1Class CWACapable 302Redirection-Capable CFNetwork Darwin CWA-iPad AuthManager/24.7.0.1.	Default Safari User-Agent string.
Cloud store - SaaS and Web app	Default WKWebview User-Agent string.	Default Safari User-Agent string.	If isFeatureUseSafariUserAgentForSaasWebviewEnabled is enabled, then following User-Agent is sent Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15) AppleWebKit/605.1.15 (KHTML, like Gecko) / Version/13.4 If Safari/605.1.15 shouldTunnelWebViewTraffic is set to True, then following User-Agent is sent Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15) AppleWebKit/605.1.15	Default Safari User-Agent string.
On-premises store	Default WKWebview User-Agent string.	Default Safari User-Agent string.		Default Safari User-Agent string.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Scenario	iOS (WkWebView)	iOS (Safari View Controller)	iPadOS (WkWebView)	iPadOS (Safari View Controller)
On-premises store with NetScaler Gateway	Default WKWebview User-Agent string.	Default Safari User-Agent string.	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/24.7.0 iOS/18.0 X1Class CWACapable 302Redirection-Capable CFNetwork Darwin CWA-iPad AuthManager/24.7.0.1	Default Safari User-Agent string.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

On-premises store with NetScaler Gateway and nFactor authentication	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/24.7.0 iOS/18.0 X1Class CWACapable 302Redirection-Capable CFNetwork Darwin CWA-iPhone AuthManager/24.7.0.1	Default Safari User-Agent string.	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/24.7.0 iOS/18.0 X1Class CWACapable 302Redirection-Capable CFNetwork Darwin CWA-iPad AuthManager/24.7.0.1	Default Safari User-Agent string.

User-agent string for WKWebView

Starting with the 23.3.5 version, the user-agent string used during some of the network requests initiated through WKWebView now includes the Citrix Workspace app identifier by default.

Therefore, it has been changed from:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X)AppleWebKit
/605.1.15 (KHTML, like Gecko)Mobile/15E148 AuthManager/3.2.4.0
```

To one of the following:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X)AppleWebKit
/605.1.15 (KHTML, like Gecko)Mobile/15E148 CWA/23.3.0 iOS/15.0
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone
```

(iPhone example)

Or

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X)AppleWebKit
/605.1.15 (KHTML, like Gecko)Mobile/15E148 CWA/23.3.0 iOS/15.0
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad
```

(iPad example)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nFactor authentication

Support for multi-factor (nFactor) authentication

Multifactor authentication enhances the security of an application by requiring users to provide multiple proofs of identification to gain access. Multifactor authentication makes authentication steps and the associated credential collection forms configurable by the administrator.

Native Citrix Workspace app can support this protocol by building on the Forms logon support already implemented for StoreFront. The web logon page for Citrix Gateway and Traffic Manager virtual servers also consumes this protocol.

For more information, see SAML authentication, and Multi-Factor (nFactor) authentication.

Limitations:

- With nFactor support enabled, you can't use biometric authentication such as Touch ID and Face ID.

nFactor Advanced authentication policy support

We now support certificate-based authentication on Citrix Workspace app when configured through nFactor Advanced authentication policies on Citrix Gateway. nFactor authentication helps configure flexible and agile multi-factor schemas.

User-agent string:

While performing advanced (nFactor) authentication for Citrix Workspace app an iPhone or iPad, the authentication process is redirected to an embedded WebView. The resultant user agent string might vary slightly based on the OS version, the CWA build version, the device model, and the AuthManager version. For example, consider the following user agent strings for iPhone and iPad.

For iPhone:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 16_2 like Mac OS X)AppleWebKit
/605.1.15 (KHTML, like Gecko)Mobile/15E148 CWA/23.5.0 iOS/16.2
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone
AuthManager/3.3.0.0
```

For iPad:

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6)AppleWebKit/605.1.15 (
KHTML, like Gecko)Mobile/15E148 CWA/23.5.0 iOS/15.0 X1Class CWACapable
 302RedirectionCapable CFNetwork Darwin CWA-iPad AuthManager/3.3.0.0
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - The version or device model information might vary based on the environment.
> - To apply Citrix Workspace app for iOS-specific user agent-based policies during authentication, use the following keywords:
>   - iOS
>   - CWA
>   - CWACapable

Support for FIDO2-based authentication when connecting to HDX session

Starting with the 23.9.0 version, Citrix Workspace app for iOS now supports password-less authentication within a Citrix Virtual Apps and Desktops session using FIDO2-based authentication methods. This feature allows users to sign in to a WebAuthn-supported website in browsers such as Google Chrome or Microsoft Edge using FIDO2-supported Yubico security keys. Simply opening a WebAuthn-supported website triggers password-less authentication.
Only lightning port-based devices are supported (devices with USB-C or USB 4 ports aren't supported). Signing in to the Citrix Workspace app or desktop session using password-less authentication isn't supported.

For more information about the prerequisites, see Local authorization and virtual authentication using FIDO2 in the Citrix Virtual Apps and Desktops documentation.

Support for authentication using FIDO2 when connecting to a cloud store

Starting with the 24.5.0 version, users can authenticate to Citrix Workspace app using FIDO2-based password-less authentication when connecting to a cloud store. FIDO2 offers a seamless authentication method, allowing enterprise employees to access apps and desktops within virtual sessions without the need to enter user name or password. This feature supports both roaming (USB only) and platform authenticators (PIN code, Touch ID, and Face ID only). This feature is enabled by default.

> **Note:**
>
> FIdO2 authentication is supported with the Chrome custom tabs by default. If you are interested in using FIDO2 authentication with WebView, register your interest using this Podio form.

Support for configuring storage of authentication tokens on the on-premises deployment

Citrix Workspace app for iOS now provides an option to configure the storage of authentication tokens on the local disk for on-premises stores. With this feature, you can disable the storage of the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

authentication token for the enhanced security. After disabling, when the system or session restarts, you need to authenticate again to access the session.

To disable the storage of authentication tokens on the on-premises deployment using the administration config file, do the following:

1. Use a text editor to open the web.config file, which is typically at `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Locate the user account element in the file (store is the account name of your deployment). For example: `<account id=... name="Store">`
3. Before the `</account>` tag, navigate to the properties of that user account and add the following:

```
<properties>
    <property name="TokenPersistence" value="false" />
</properties>
```

The following is an example of the web.config file:

```
<account id="########################################" name="Store
    Service"
    description="" published="true" updaterType="None"
       remoteAccessType="StoresOnly">
    <annotatedServices>
        <clear />
        <annotatedServiceRecord serviceRef="1__Citrix_Store">
            <metadata>
                <plugins>
                    <clear />
                </plugins>
                <trustSettings>
                    <clear />
                </trustSettings>
                <properties>
                    <clear />
                    <property name="TokenPersistence" value="false"
                        />
                 </properties>
            </metadata>
        </annotatedServiceRecord>
    </annotatedServices>
    <metadata>
    <plugins>
      <clear />
    </plugins>
    <trustSettings>
      <clear />
    </trustSettings>
    <properties>
    </properties>
 </metadata>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
30      </account>
```

Reauthentication after session timeout

Starting with the 23.3.0 version, you are now prompted to reauthenticate to the Citrix Workspace app if your session has expired since your last sign-in. You are prompted for two-factor authentication or a username and password when connecting to the Citrix Workspace app from the web or a native client.

Secure

September 7, 2025

To secure the communication between your server farm and Citrix Workspace app, integrate your connections to the server farm with a range of security technologies, including Citrix Gateway.

> **Note:**
>
> Citrix recommends using Citrix Gateway to secure communications between StoreFront servers and users' devices.

- A SOCKS proxy server or secure proxy server (also known as security proxy server, HTTPS proxy server).

  You can use proxy servers to limit access to and from your network and to handle connections between Citrix Workspace app and servers. Citrix Workspace app supports SOCKS and secure proxy protocols.

- Secure Web Gateway.

  You can use Secure Web Gateway with Web Interface to provide a single, secure, and encrypted point of access through the Internet to servers on internal corporate networks.

  You can use Secure Web Gateway with Web Interface to provide single, secure, and encrypted data. The servers on internal corporate networks can access the secured data through the Internet.

- SSL Relay solutions with Transport Layer Security (TLS) protocols.

- A firewall.

  Network firewalls can allow or block packets based on the destination address and port.

  If you're using Citrix Workspace app through a network firewall that maps the server's internal network IP address to an external Internet address (that is, network address translation, or NAT), configure the external address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for multi-site store failover based on geo-location

Starting with version 24.12.0, the multi-store failover handling feature improves multi-store failover handling by running store address checks asynchronously and removing outdated store entries when a new failover store address is detected. When a failover occurs due to an outage, the Global Server Load Balancer (GSLB) redirects the client to a new site. This feature ensures that, when launching a previously added store, the Gateway detector checks if the store address has changed based on the user's geo-location. If a new address is found, the client automatically removes the old store entry and adds the new one. This process runs in the background, allowing for a seamless transition to the new store without manual intervention.
Note that this feature applies only to on-premises stores.

Prerequisite:

The user must log in to the store.

Limitation:

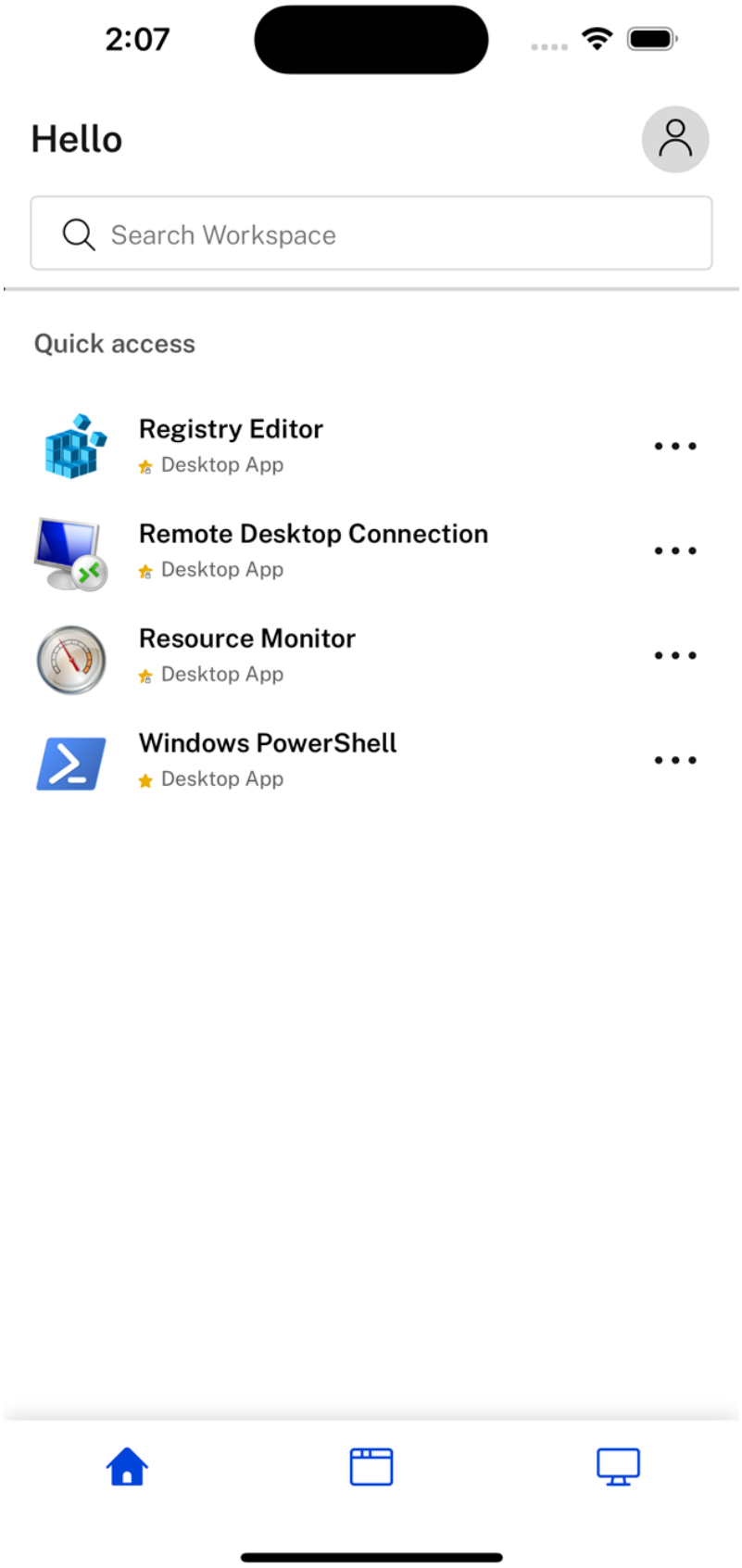
If the log-in session cookie expires, the multi-store failover does not happen automatically because the API for fetching the URL fails. In this case, the login page is prompted.

Support for WSUI on-premises using gateway

Starting with version 24.12.0, Citrix Workspace app for iOS supports Web UI for the on-premises store which is behind the gateway as well. The administrator must configure this feature, as it is not enabled by default. For more information on configuration, see New UI for on-premises stores (Technical Preview).

The following image show the current UI:

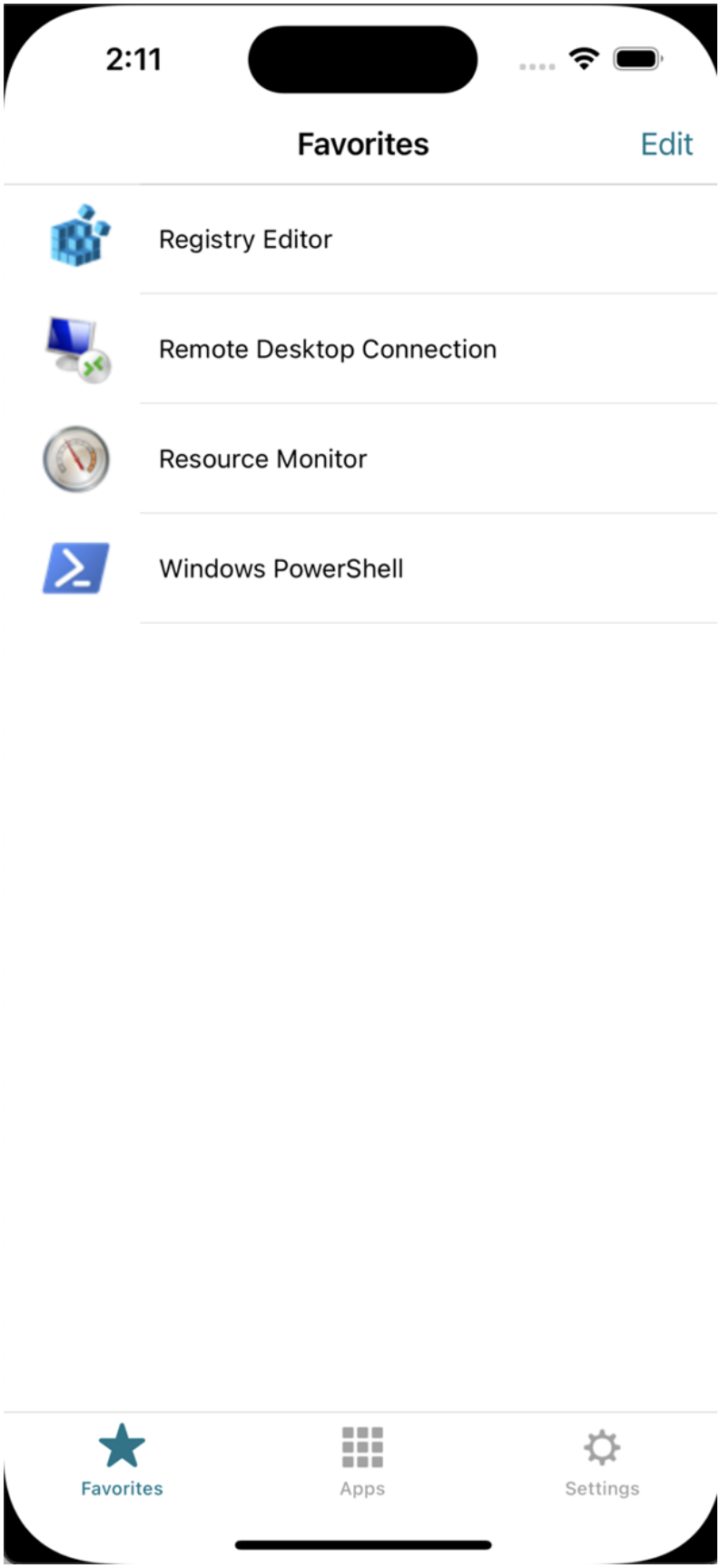
© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following image show the new UI:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gateway

To enable remote users to connect to your Citrix Endpoint Management deployment through Citrix Gateway, you can configure certificates to work with StoreFront. The method for enabling access depends on the edition of Citrix Endpoint Management in your deployment.

If you deploy Citrix Endpoint Management in your network, allow connections from internal or remote users to StoreFront through Citrix Gateway by integrating Citrix Gateway with StoreFront. This deployment allows users to connect to StoreFront to access published applications from XenApp and virtual desktops from XenDesktop. Users connect through Citrix Workspace app.

Secure Web Gateway

This topic applies only to deployments using the Web Interface.

You can use the Secure Web Gateway in either Normal mode or Relay mode to provide a secure channel for communication between Citrix Workspace app and the server. If you're using the Secure Web Gateway in **Normal** mode, Citrix Workspace app doesn't require any configuration. Verify that end users are connecting through the Web Interface.

Citrix Workspace app uses settings that are configured remotely on the Web Interface server to connect to servers running the Secure Web Gateway.

If the Secure Web Gateway Proxy is installed on a server in the secure network, you can use the Secure Web Gateway Proxy in Relay mode. If you're using Relay mode, the Secure Web Gateway server functions as a proxy and you must configure Citrix Workspace app to use:

- The fully qualified domain name (FQDN) of the Secure Web Gateway server.
- The port number of the Secure Web Gateway server.

> **Note:**
>
> Secure Web Gateway Version 2.0 doesn't support Relay mode.

The FQDN must list, in sequence, the following three components:

- Host name
- Intermediate domain
- Top-level domain

For example, `my_computer.example.com` is an FQDN, because it lists, in sequence, a host name (`my_computer`), an intermediate domain (example), and a top-level domain (`com`). The combination of intermediate and top-level domain (`example. com`) is referred to as the domain name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Proxy server

Proxy servers are used to limit access to and from your network, and to handle connections between Citrix Workspace app and servers. Citrix Workspace app supports both SOCKS and secure proxy protocols.

Citrix Workspace app uses proxy server settings to communicate with the Citrix Virtual Apps and Desktops server. The proxy server settings are remotely configured on the Web Interface server.

When Citrix Workspace app communicates with the Web server, the app uses the proxy server settings. Configure the proxy server settings for the default web browser on the user device accordingly.

Firewall

Network firewalls can allow or block packets based on the destination address and port. If you're using a firewall in your deployment, Citrix Workspace app must be able to communicate through the firewall with both the web server and Citrix server. The firewall must permit HTTP traffic for user device to Web server communication. Usually, the HTTP traffic is over the standard HTTP port 80 or 443 if a secure Web server is in use. For Citrix server communication, the firewall must permit inbound ICA traffic on ports 1494 and 2598.

If the firewall is configured for Network Address Translation (NAT), you can use the Web Interface to define mappings from internal addresses to external addresses and ports. For example, if your Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) server isn't configured with an alternate address, you can configure Web Interface to provide an alternate address to Citrix Workspace app for iOS. Citrix Workspace app for iOS then connects to the server using the external address and port number.

TLS

Citrix Workspace app supports TLS 1.2 and 1.3 with the following cipher suites for TLS connections to XenApp and XenDesktop:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Citrix Workspace app running on iOS 9 and later or version 21.2.0 does not support the following TLS cipher suites:
>
> - TLS_RSA_WITH_RC4_128_SHA
> - TLS_RSA_WITH_RC4_128_MD5

Transport Layer Security (TLS) is the latest, standardized version of the TLS protocol. The Internet Engineering Taskforce (IETF) renamed it TLS when it took over responsibility for the development of TLS as an open standard.

TLS secures data communications by providing server authentication, encryption of the data stream, and message integrity checks. Some organizations, including U.S. government organizations, require the use of TLS to secure data communications. These organizations might also require the use of validated cryptography, such as Federal Information Processing Standard (FIPS) 140. FIPS 140 is a standard for cryptography.

Citrix Workspace app supports RSA keys of 1024, 2048, and 3072-bit lengths. Root certificates with RSA keys of 4096-bit length are also supported.

> **Note:**
>
> - Citrix Workspace app uses iOS platform crypto for connections between Citrix Workspace app and StoreFront.

Configure and enable TLS

There are two main steps involved in setting up TLS:

1. Set up SSL Relay on your Citrix Virtual Apps and Desktops™ server and your Web Interface server and obtain and install the necessary server certificate.
2. Install the equivalent root certificate on the user device.

Install root certificates on user devices To secure communications between TLS-enabled Citrix Workspace app and Citrix Virtual Apps and Desktops, you need a root certificate on the user device. The certificate can verify the signature of the Certificate Authority on the server certificate.

iOS comes with about 100 s of commercial root certificates that are preinstalled. If you want to use a different certificate, you can receive one from the Certificate Authority and install it on each user device.

Depending on your organization's policies and procedures, you can install the root certificate on each user device instead of directing users to install it. The easiest and safest way is to add root certificates to the iOS keychain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To add a root certificate to the keychain

1. Send yourself an email with the certificate file.
2. Open the certificate file on the device. This action automatically starts the Keychain Access application.
3. Follow the prompts to add the certificate.
4. Starting with iOS 10, verify that the certificate is trusted by going to iOS **Settings** > **About** > **Certificate Trust Setting**.

   Under Certificate Trust Settings, see the section "ENABLE FULL TRUST FOR ROOT CERTIFICATES."Make sure that your certificate has been selected for full trust.

The root certificate is installed. The TLS-enabled clients and other applications can use the root certificate using TLS.

Support for Transport Layer Security 1.3 Starting with the 23.9.0, Citrix Workspace app for iOS now supports Transport Layer Security (TLS) 1.3 that boosts performance and efficiency. TLS 1.3 provides robust security with its strong cipher suites and one-time session keys.

End users can enable it on Citrix Workspace app for iOS as follows.

1. Go to **Advanced settings** > **TLS Versions**.
2. Select **TLS 1.3 version**.

Support for DTLS 1.2

Starting with version 24.7.0, Citrix Workspace app for iOS supports DTLS protocol version 1.2. DTLS 1.2 provides enhancements and improvements over the previous version, which includes robust encryption algorithms, better handshake protocols, and protection against various attacks. This protocol improves overall security.

> **Note:**
>
> If there is any issue with DTLS protocol version 1.2, Citrix Workspace app for iOS seamlessly falls back to the previous supported versions.

Support for Citrix Device Posture service

Starting with the 2402 version, Citrix Workspace™ app for iOS supports Citrix Device Posture service. Citrix Device Posture service is a cloud-based solution that helps administrators enforce certain requirements that end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix Secure Private Access™ resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For Citrix Workspace app for iOS, the device posture supports only the scan of the Citrix Workspace app version and operating system version of the iOS device.

For more information, see the Device Posture documentation.

> **Note**
>
> This feature is supported only for cloud stores.

XenApp and XenDesktop® Site

To configure the XenApp® and XenDesktop Site:

> **Important:**
>
> - Citrix Workspace app uses XenApp and XenDesktop Sites, which support Citrix Secure Gateway 3.x.
> - Citrix Workspace app uses Citrix Virtual Apps websites, which support Citrix Secure Gateway 3.x.
> - XenApp and XenDesktop Sites supports only single-factor authentication.
> - Citrix Virtual Apps™ websites support both single-factor and dual-factor authentication.
> - All the built-in browsers support Web Interface 5.4.

Before beginning this configuration, install and configure Citrix Gateway to operate with Web Interface. You can adapt these instructions to fit your specific environment.

If you're using a Citrix Secure Gateway connection, do not configure Citrix Gateway settings on Citrix Workspace app.

Citrix Workspace app uses a XenApp and XenDesktop Site to get information about the applications an end user has rights to. In the process, the information is presented to Citrix Workspace app running on your device. Similarly, you can use the Web Interface for traditional SSL-based Citrix Virtual Apps connections. For the same SSL-based connection, you can configure Citrix Gateway. XenApp and XenDesktop Sites running on the Web Interface 5.x have this configuration ability built in.

Configure the XenApp and XenDesktop Site to support connections from a Citrix Secure Gateway connection:

1. In the XenApp and XenDesktop Site, select **Manage secure client access** > **Edit secure client access** settings.
2. Change the Access Method to **Gateway Direct**.
3. Enter the FQDN of the Secure Web Gateway.
4. Enter the Secure Ticket Authority (STA) information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> For the Citrix Secure Gateway, Citrix recommends using the Citrix default path (//XenAppServerName/Citrix/PNAgent). The default path enables the end users to specify the FQDN of the Secure Web Gateway they're connecting to. Don't use the full path to the config.xml file that is on the XenApp and XenDesktop Site. For example, (//XenAppServerName/CustomPath/config.xml).

To configure the Citrix Secure Gateway

1. Use the Citrix Secure Gateway configuration wizard to configure the gateway.

   The Citrix Secure Gateway supports the server in the secure network that hosts the XenApp Service site.

   After selecting the **Indirect** option, enter the FQDN path of your Secure Web Gateway Server and continue the wizard steps.

2. Test a connection from a user device to verify that the Secure Web Gateway is configured correctly for networking and certificate allocation.

To configure the mobile device

1. When adding a Citrix Secure Gateway account, enter the matching FQDN of your Citrix Secure Gateway server in the **Address** field:

   - If you've created the XenApp and XenDesktop Site using the default path (/Citrix/PNAgent), enter the Secure Web Gateway FQDN: FQDNofSecureGateway.companyName.com
   - If you've customized the path of the XenApp and XenDesktop Site, enter the full path of the config.xml file, such as: FQDNofSecureGateway.companyName.com/CustomPath/config.xml

2. If you're manually configuring the account, then clear the Citrix Gateway option **New Account** dialog.

Session experience

March 12, 2026

EDT Lossy mode now supports SecureHDX (SecureICA 2.0) connections

Previously:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- EDT Lossy (unreliable sub-channel) works only with DTLS encryption.
- SecureHDX connections are limited to reliable transport only.
- Audio and video performance could be degraded on SecureHDX connections.

Currently:

- EDT Lossy now works with both DTLS and SecureHDX connections.
- Real-time performance for audio, video, and other latency-sensitive channels improves when using SecureICA 2.0.
- Better user experience with reduced latency on SecureHDX connections.

Technical overview

This enhancement modifies the network transport layer to allow unreliable UDP sub-channels when using SecureHDX (SecureICA 2.0) encryption. The unreliable sub-channel carries latency-sensitive data, such as audio and video frames, where occasional packet loss is acceptable. This approach prioritizes real-time delivery instead of retransmitting lost packets.

Prerequisites

- Enable SecureICA 2.0 on both the server and client. For more information, see Secure HDX™ Citrix Virtual Apps and Desktops™ 7 2511.
- Enable EDT Lossy on both the server and client. For more information, see Adaptive transport Citrix Virtual Apps and Desktops™ 7 2511

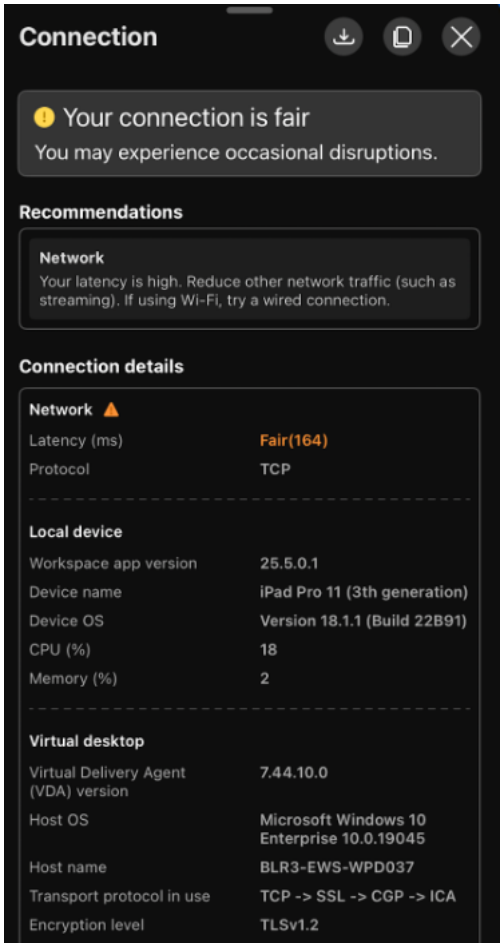
Enhanced Connection Strength Indicator

From 25.7.2, we have enhanced the connection strength indicator. This enhancement provides real-time insights into your connection quality and helps self-troubleshoot connectivity issues. This capability can be accessed from the toolbar and is enabled by default.

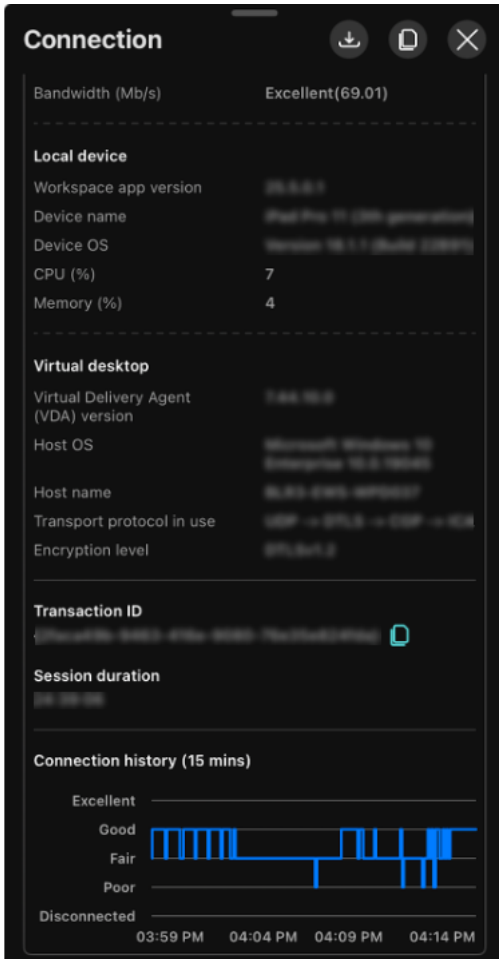
Prerequisites:

- To use this feature, enable the enhanced Desktop Viewer toolbar. Administrators must enable the new toolbarfeature through Global App Configuration service. This feature is only available in VDA 2407 or later.
- The Supportability Virtual Channel must be enabled on the client side, which is enabled by default in Citrix Workspace app iOS 24.12.0.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Benefits:

- **Immediate feedback:** The network strength icon notifies users when network issues are detected.
- **Enhanced troubleshooting:** Real-time statistics and diagnostics assist users and IT teams in identifying and resolving connectivity issues.

Connection Strength Indicator Enhancements

- **Brand-new UI:** The user interface has been redesigned for improved clarity and a better user experience.
- **Additional connection details:** The indicator now displays current device CPU and memory usage.
- **Scored metrics and recommendations:** Latency and bandwidth scores are calculated and displayed. If a score is “Fair”or “Poor,”a recommendation appears to help address the issue.
- **Connection history:** The last 15 minutes of connection scores are recorded and shown in a chart at the bottom of the layout. This composite score is based on bandwidth and latency, and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

historical data is included in logs when copied or downloaded.

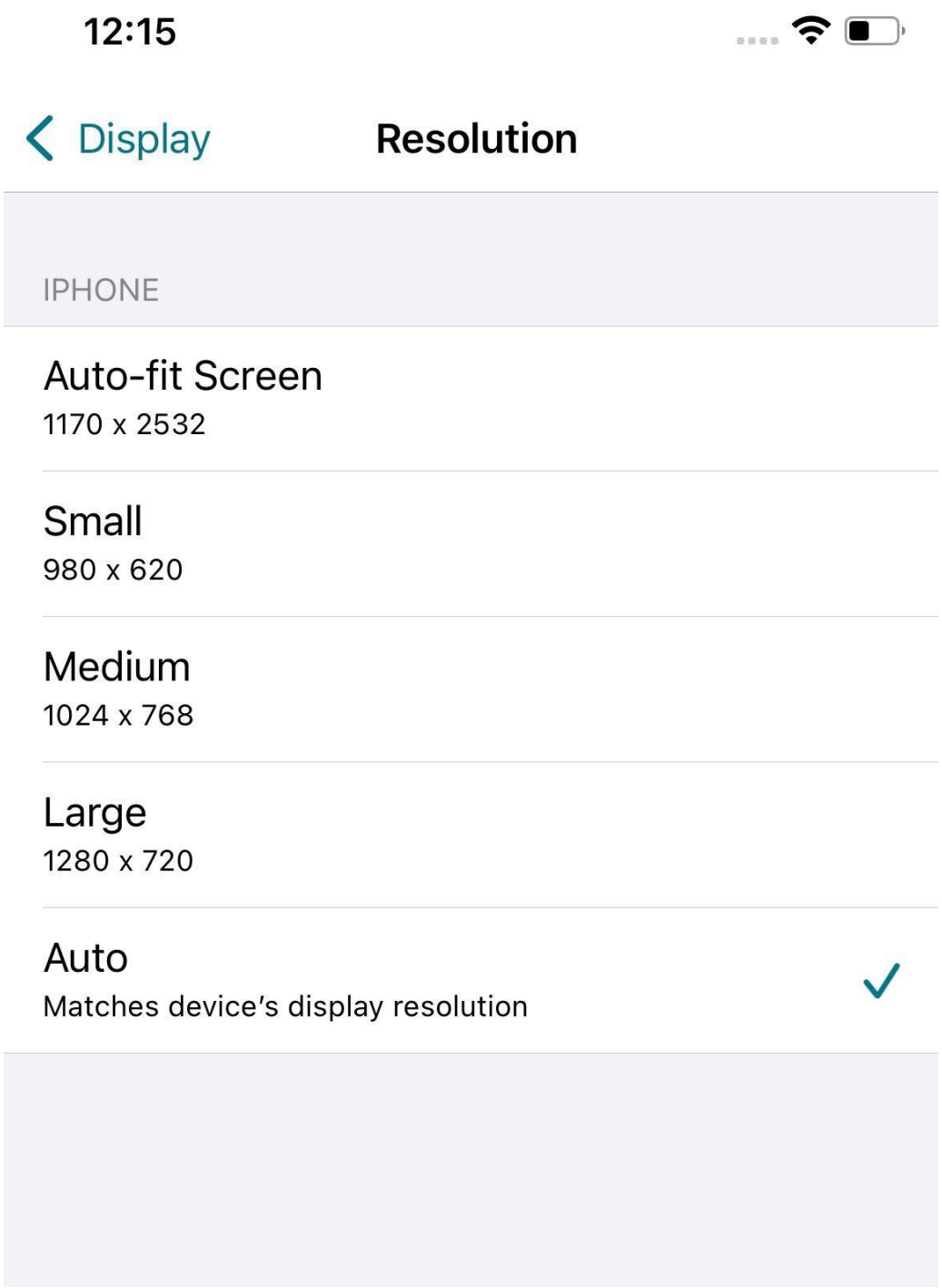
- **Download details:** All connection metrics, including latency, bandwidth, CPU, and memory usage, are recorded. Connection history for the last 15 minutes is also included in the downloadable logs.

Enhanced session resolution

Starting with version 25.3.0, Citrix Workspace app for iOS introduces enhancements to session resolution, for a more seamless user experience. Defaulting to Auto, the **DPI** settings adjust automatically whenever a user launches a session, enhancing the overall experience.

To ensure a consistent and user-friendly experience, virtual desktops now launch in landscape mode by default. This caters to widescreen applications and multitasking needs. This feature is enabled by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Default landscape orientation for virtual desktops

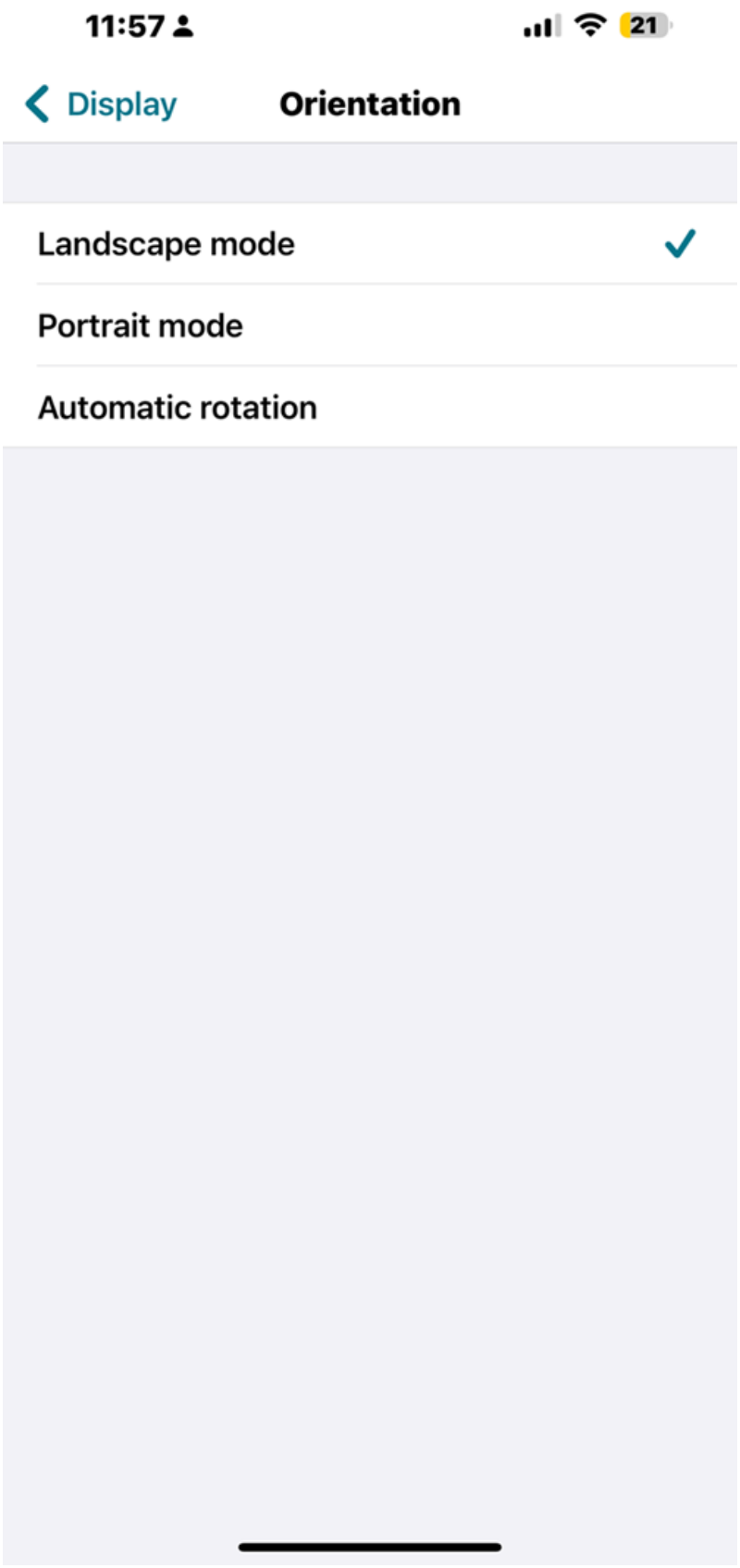
Starting with version 25.1.0, Citrix Workspace app enforces landscape orientation by default when launching a virtual desktop on iPhone devices. This ensures an optimal and consistent user experience for widescreen applications and multitasking. Users can configure orientation settings through

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the app or HDX-Toolbar to lock in landscape, lock in portrait, auto-adjust based on application metadata, or follow the device's screen orientation. This flexibility accommodates various workflows, including apps designed for portrait mode, while maintaining a seamless and user-friendly experience.

To configure the default orientation, navigate to **Settings** > **Display** > **Orientation** > **Landscape mode**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhanced secured ICA®

Starting with version 25.1.0, the new ICA encryption feature improves security by using modern encryption algorithms. This increases the security posture of our product, and subsequently gives our customers a way to enhance the security posture of their environments in a simple and reliable manner. It simplifies setup by eliminating complex certificate management and enables easy configuration through Citrix policy settings. The feature works seamlessly across all supported platforms.

Prerequisites:

- Ensure that the deployment is configured for either CVAD Service or on-premises use.
- Supported platforms include Windows, Linux, Mac, Android, iOS, HTML5, and Chrome OS.
- Administrative access to Citrix Studio is necessary.

Configuration

The feature can be activated or deactivated using a single policy or Delivery Group property. Access the Delivery Controller™ (DDC) and make the following changes:

1. Navigate to **Settings** > **Computer Setting - ICA** to configure the required policy.
2. Run the following command to update Group Policy:
   `gpupdate/force`
3. Relaunch the session to apply the changes.

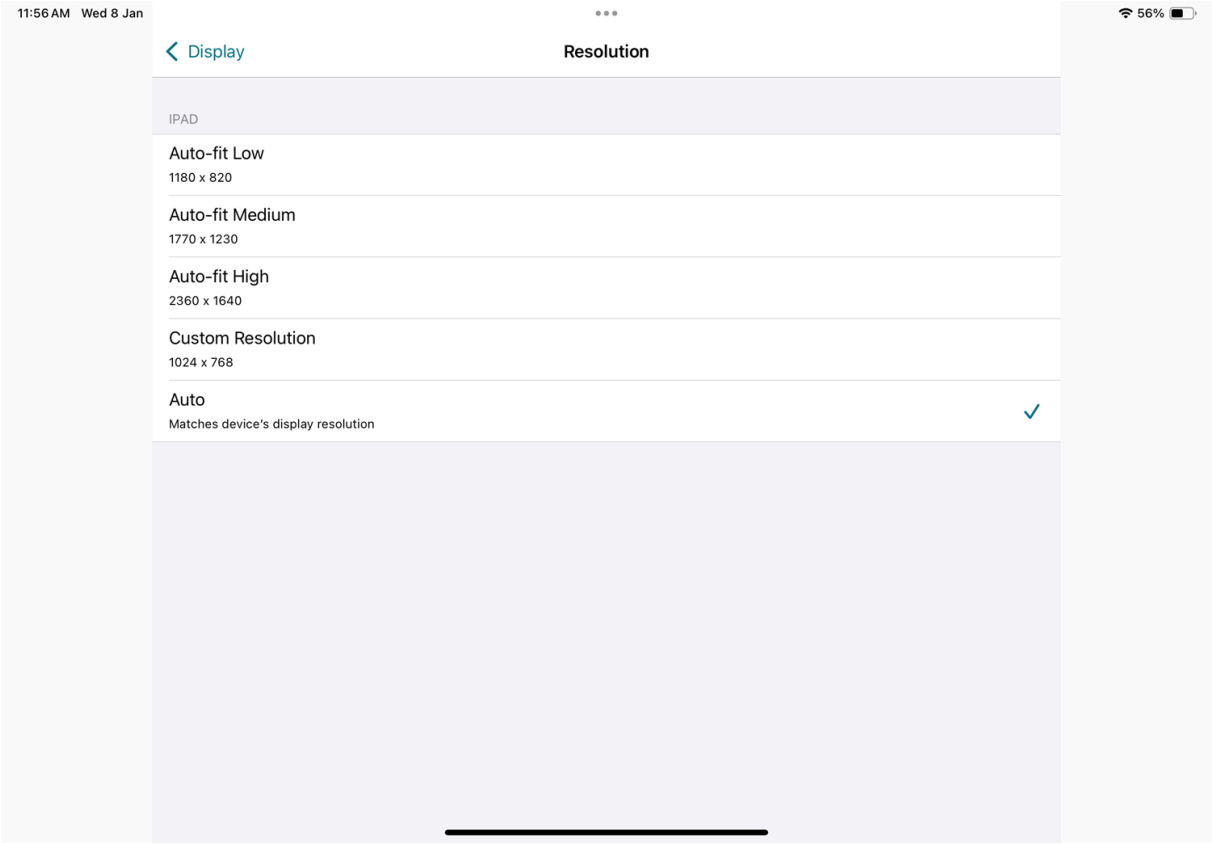
DPI matching

The DPI matching feature ensures that the virtual session is rendered according to the DPI of the device. Starting with the 25.1.0 release, a new display setting enhances DPI matching capabilities:

- Automatic Resolution Detection: The app automatically identifies the resolution of the device's screen.
- Dynamic DPI Adjustment: The DPI of the virtual desktop session dynamically adjusts to match the detected resolution of the display. This ensures optimal clarity, readability, and usability on the respective display.
- Smooth scaling UI elements, fonts, and images scale smoothly without distortion or pixelation when the DPI is adjusted.
- Supports resolutions up to 4K.

Auto (DPI Matching) option enables automatic DPI adjustment for a seamless display experience. DPI settings are accessible within the app by navigating to **Settings** > **Display** > **Resolution**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



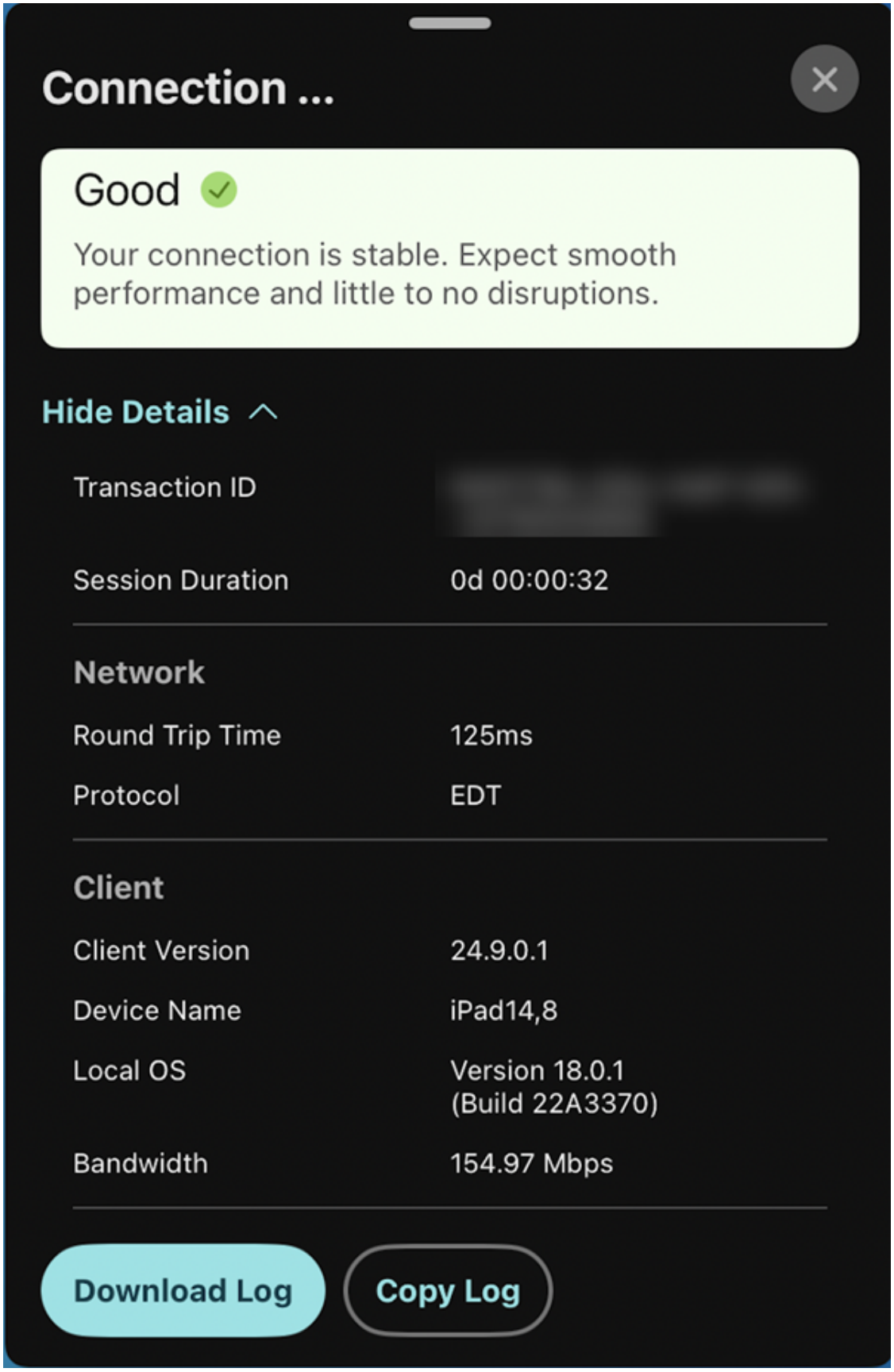
Connection Strength Indicator

Starting with version 24.12.0, Citrix Workspace app for iOS supports the Connection Strength Indicator on the **Desktop Viewer** toolbar. This feature displays a network strength icon that alerts you of network issues. By clicking the icon, you can view real-time connection statistics for the client, gateway, and VDA, and copy diagnostic information to share with IT for advanced troubleshooting.

Prerequisites:

- To use this feature, enable the enhanced Desktop Viewer toolbar. Administrators must enable the new toolbarfeature through Global App Configuration service. This feature is only available in VDA 2405 or later.
- The Supportability Virtual Channel must be enabled on the client side, which is enabled by default in Citrix Workspace app iOS 24.12.0.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Launch of In-Memory ICA solution

Starting with version 24.12.0, Citrix Workspace app for iOS enhances support for in-memory hybrid launches using the Citrix Workspace launcher. This improvement allows for a more efficient and secure user experience, eliminating the need to download ICA files.

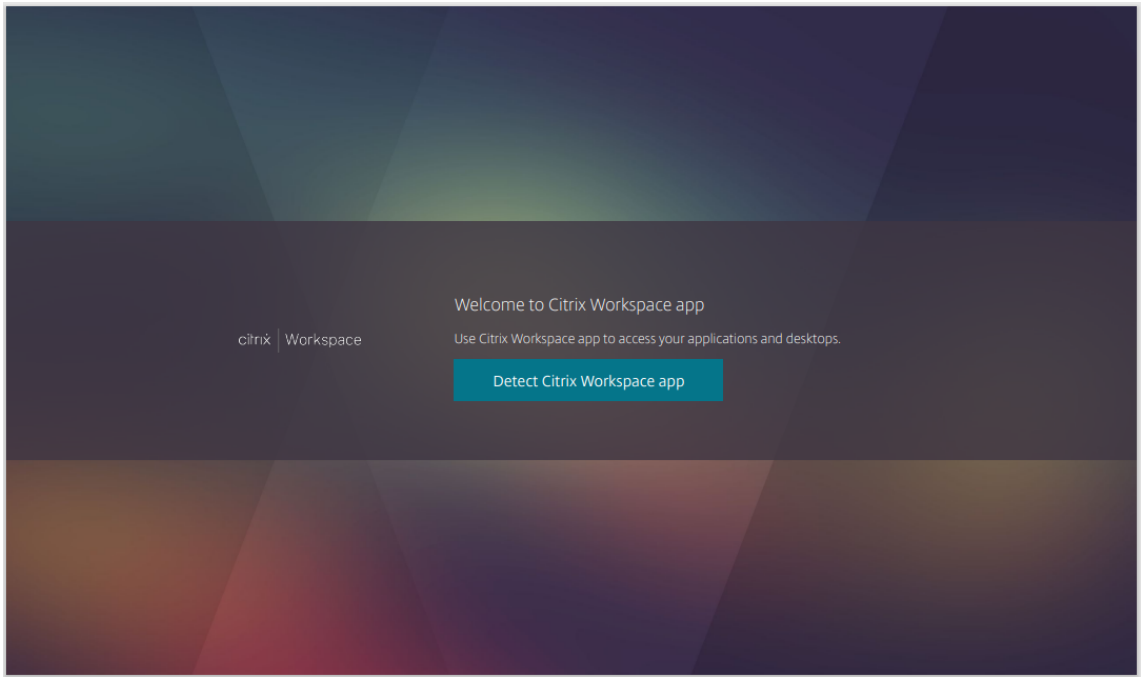
Prerequisites:

Citrix Workspace app for iOS 24.12.0 or higher.

Configuration

To launch Citrix Workspace app without downloading an ICA file, follow these steps on your iOS device:

1. Open a supported web browser (Safari, Chrome, or Firefox).
2. Go to your organization's store URL and sign in using your credentials.
3. On the welcome screen, locate and tap **Detect Citrix Workspace app**. This initiates the client detection process, which opens the Citrix Workspace app.

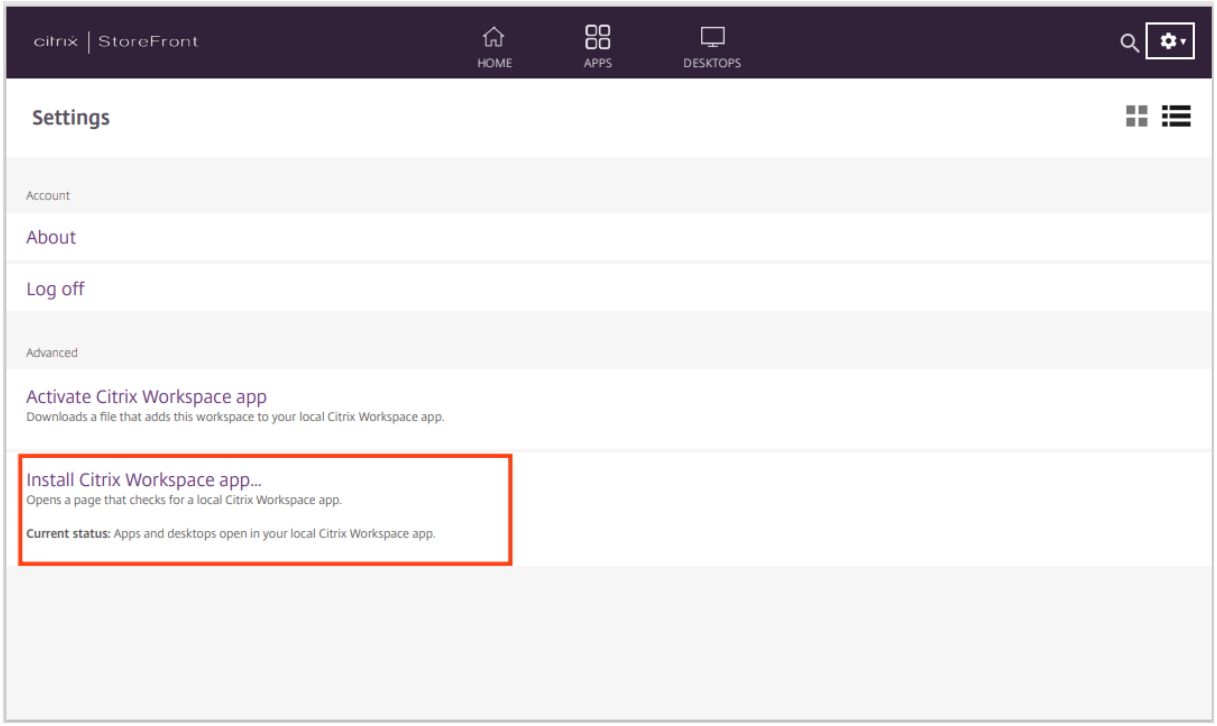


4. After detection, return to the browser. You are now on the organization store's home screen.

You can now directly access and open your apps and desktops from the organization store interface without requiring an ICA file download.

If you skip the client detection during the initial login, then you can navigate from **Settings > Install Citrix Workspace App > Client detection**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Limitation:

If client detection fails, the system automatically downloads an ICA file, and the session launches from the downloaded file.

Support for Rapid Scan

Starting with the 24.9.0 version, Citrix Workspace app for iOS supports the Rapid scan feature. You can use this feature to scan multiple documents with an iOS device, and then transfer those scanned documents to a Mac device using the Citrix Workspace app for Mac and iOS.

If you're signed into Citrix Workspace on both your Mac and iOS device, you can use Rapid Scan to scan documents with your iPhone or iPad. The scanned files are saved on your Mac, and you can also access them remotely from a virtual desktop using Client Drive Mapping. This feature works for both cloud and on-premise stores.

Prerequisites:

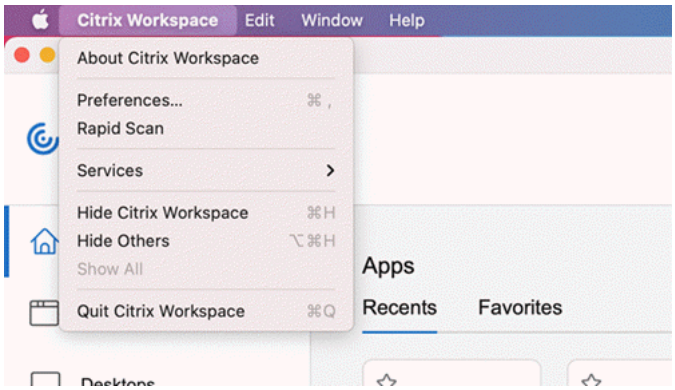
- Ensure that both devices are logged into the same Citrix Workspace account.
- Both devices must be connected to the same Wi-Fi network.
- The Citrix Workspace app for Mac must be version 24.9.0 or higher.

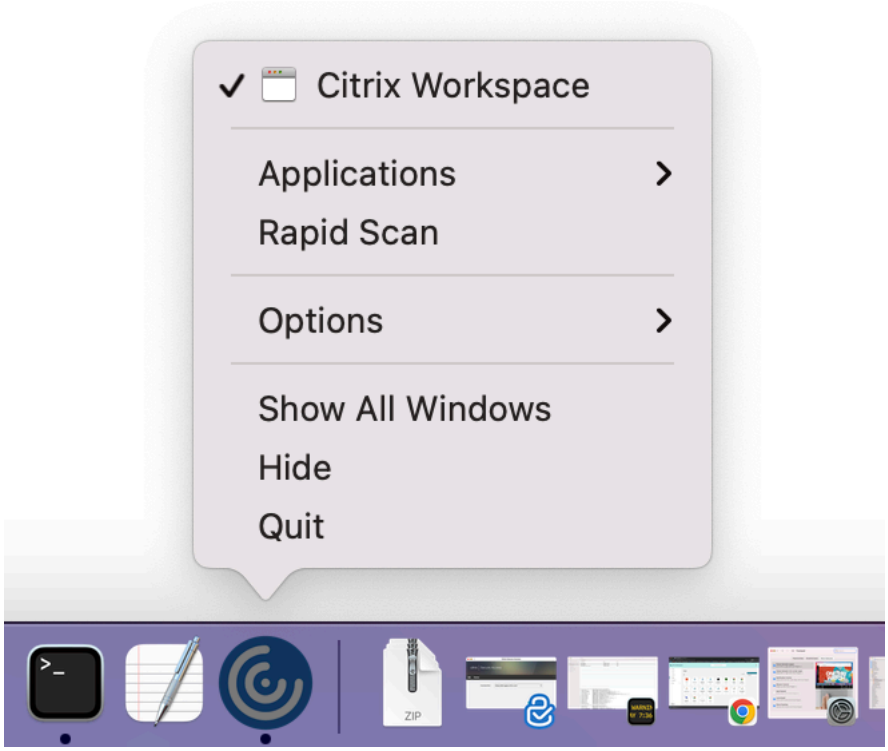
How to Use Rapid Scan:

1. Open the Citrix Workspace app on your Mac.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Long-press (or right-click) the Citrix Workspace icon in the Dock or menu bar.





3. Select **Rapid Scan** from the menu. A QR code appears on your Mac screen.
4. On your iOS device, go to **Settings** and tap **Rapid Scan**.
5. Scan the QR code displayed on your Mac using your iOS device.
6. When the confirmation window appears on your Mac, click **Yes** to establish the connection. You can now use your iOS device to scan documents.
7. Choose to save the scanned files in PDF or JPEG format.
8. By default, the scanned documents are saved to the **Downloads** folder on your Mac.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. After the download is complete, click **Open in Finder** on your Mac to locate the scanned documents.

Access scanned documents from a Virtual Desktop:

1. Client Drive Mapping (CDM) must be enabled to access your Mac's storage drives inside the Virtual Desktop. This allows you to transfer files between your Mac and the Virtual Desktop. Please contact your administrator to enable this feature.
2. Once CDM is enabled, your local drives are visible in the Virtual Desktop.
3. When prompted, allow **Read & Write** permissions to access your local disk from the Virtual Desktop.
4. Navigate to the folder where the scanned documents are stored (the **Downloads** folder by default) and copy the files to the Virtual Desktop's storage.

Support for Apple's native non-mirror mode

You can now extend the display using Apple's non-mirror mode available with iPad OS 16.2. You can multi-task by running the Citrix Workspace app, virtual apps, and virtual desktops on the external monitor and leaving the iPad screen free to run other native apps.

> **Note:**
>
> Support for Apple's non-mirror mode extend display is available on selected iPad models only. For more information, see the Apple documentation.

If you don't want to use this technical preview feature, you can always use Citrix Workspace app in full-screen mode.

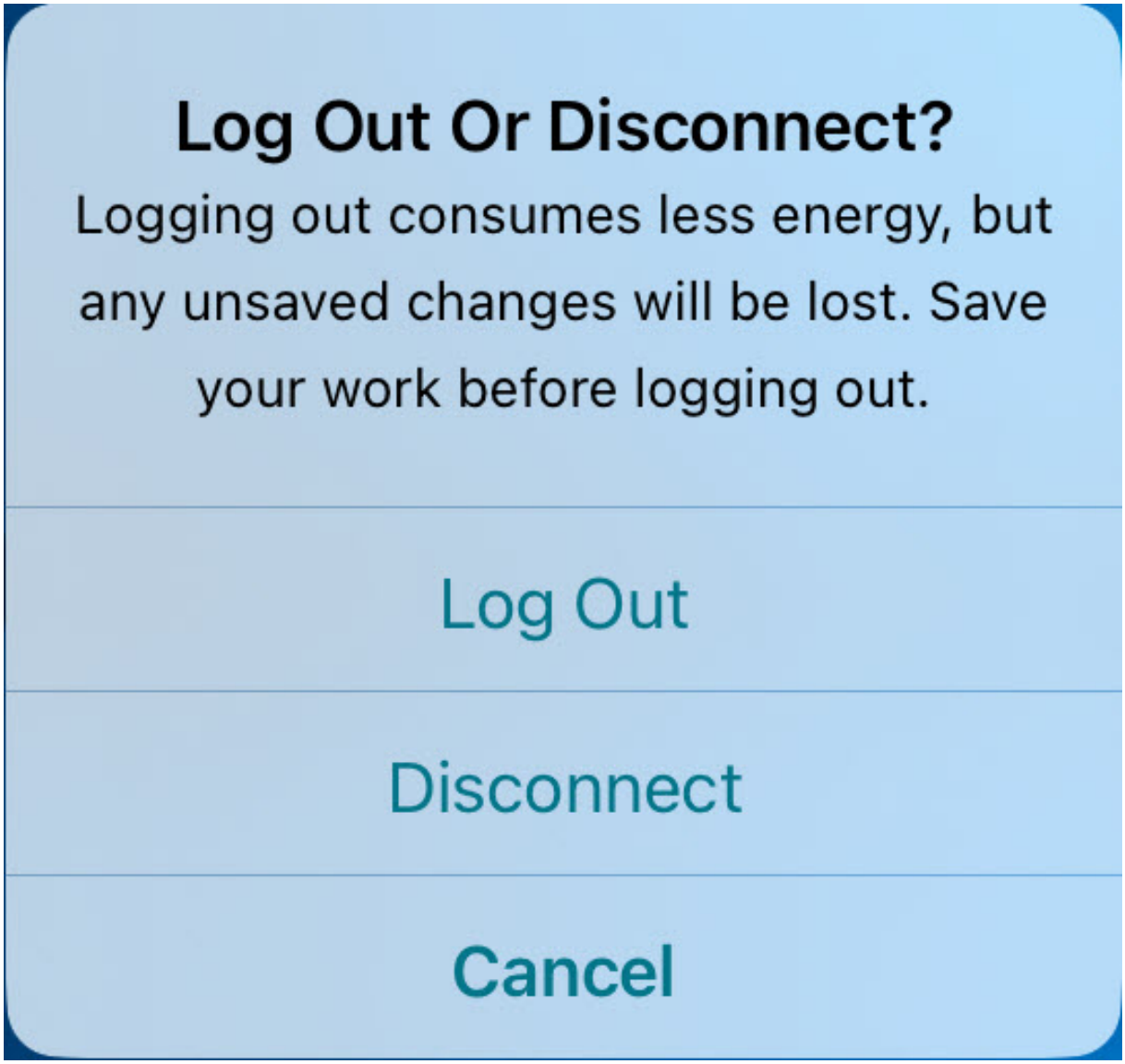
Support for sustainability initiative

Starting with version 24.9.0, users see a prompt to sign out of their desktop session upon closing a virtual desktop. This feature helps conserve energy by signing out from VMs when not needed. Previously, these sessions remained in a disconnected state, leading to unnecessary energy consumption.

When disconnecting from a session without sustainability enabled, users see a prompt with a **Disconnect and Don't ask again** option for automatic future disconnects. This default text is localized.

If users disconnect with sustainability enabled, the system prompts them to **Log out** to help conserve energy. As an administrator, you can customize the sustainability message.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Admins can choose to display the sustainability alert, which includes a leaf icon, and customize the title and prompt message. If the admin doesn't provide a title or prompt message and turns off the leaf icon while enabling the sustainability feature, a default message appears **Disconnect Desktop? Your work remains just as you left it the next time you connect to Managed %@ desktop**. The **%@** is replaced by the Virtual Desktop app name. These default messages are localized.

Note that messages configured by the admins are not localized, so admins must ensure clarity and accuracy in their text.

For more information on how to enable and customize this feature, see Sustainability initiative from Citrix Workspace app in Citrix Workspace app for Windows documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enhanced multi-app window management

Starting with version 24.9.0, Citrix Workspace app for iOS now supports seamless multi-app window management for iPads connected to external monitors. This feature enhances multitasking and productivity by allowing native multi-app experiences. It can also be enabled when the iPad device is not connected to external monitors.

With this feature, you can:

- Switch between applications and open a single app in separate windows, enhancing workflow and productivity.
- Use multiple apps in one session while connected to external monitors.

To enable the seamless multi-app, follow these steps:

1. Go to **Application Settings** > **Advanced** > **Multitasking**.
2. Enable **Separate Session Window**.
3. Enable **Multi Windows for Seamless App Session**.

Limitation:

- Stage Manager must be enabled on devices and keep it enabled during use.
- You might see a gray overlay after the launch and the HDX session window shows. This happens while the server is starting up. After a couple of seconds/minutes, the users can see the app picture and use it normally.
- This feature is only available on Stage Manager-supported devices such as Apple Silicon chip-equipped iPads.

Troubleshoot

November 17, 2025

How to check app's version

To check your Citrix Workspace app version, open your app. Tap **Settings** > **About**. The version information is displayed on your screen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to upgrade Citrix Workspace app to the latest version

You can upgrade to the latest version of Citrix Workspace app from the App Store. Search for Citrix Workspace app and tap the **Upgrade** button.

How to reset Citrix Workspace app

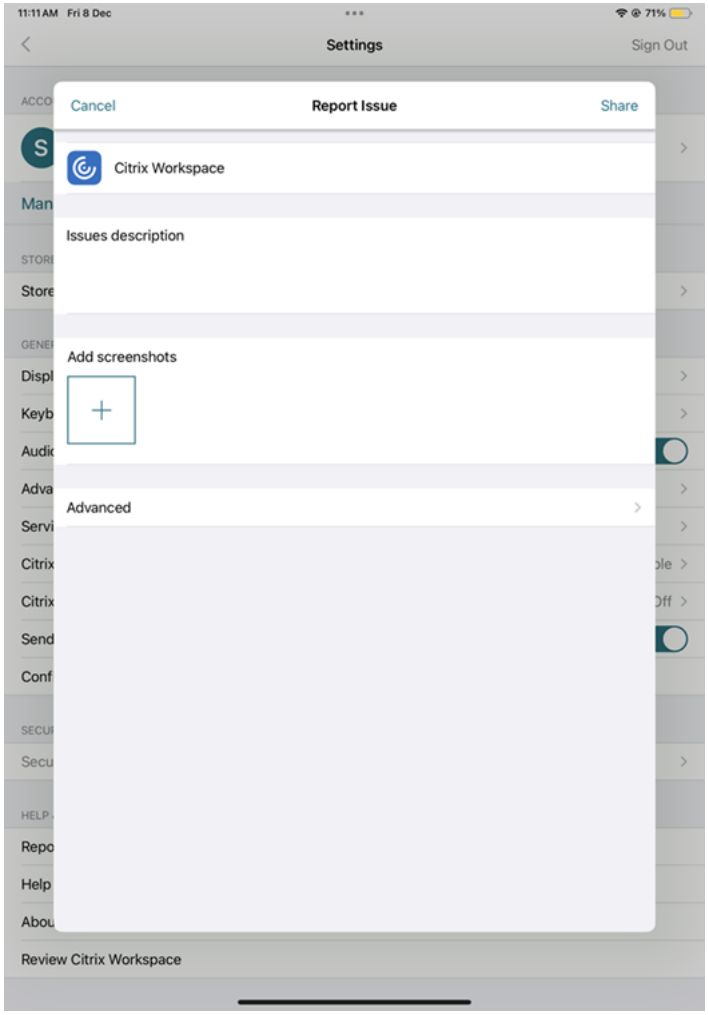
You can reset your Citrix Workspace app using one of the following methods:

- Delete any existing accounts from Citrix Workspace app
- Clear the Citrix Workspace app storage data
- Uninstall Citrix Workspace app and install the latest Citrix Workspace app for iOS that has the latest fix.

How to collect logs

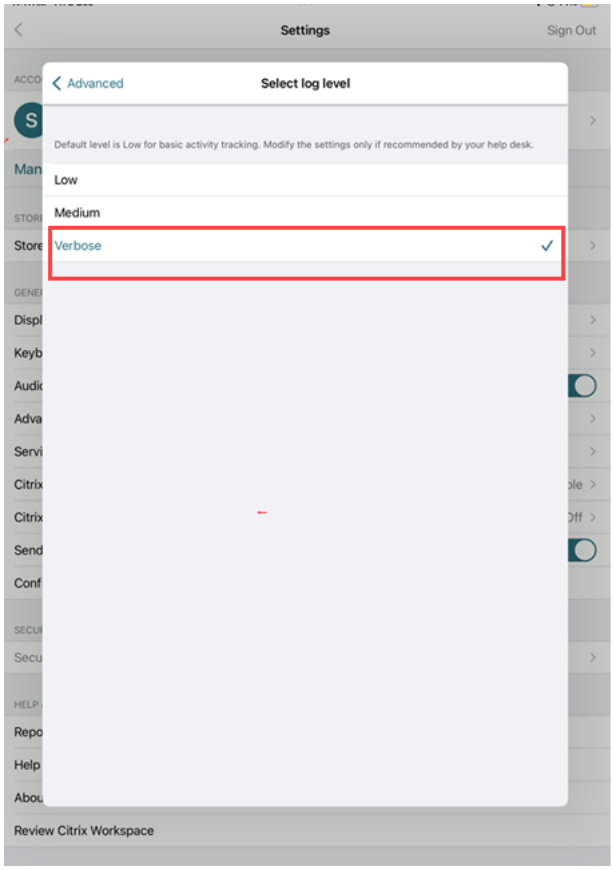
1. Open your Citrix Workspace app and navigate to **Settings**.
2. Under **Help & Support**, select **Report Issue**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



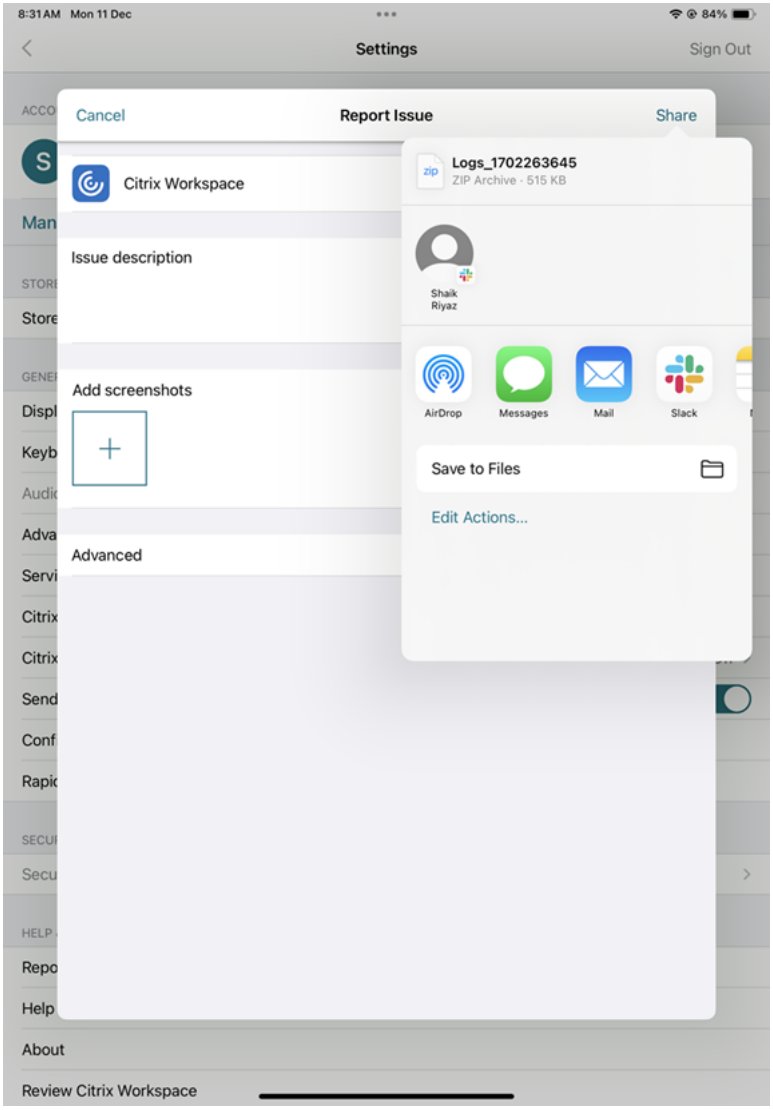
3. Reproduce your issue.
4. On the Select log level page, select **Verbose**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. On the **Select Log location** page, select **Both Console & File**.
6. Share the zip file with Citrix.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



How to request for enhancements

You can send in your requests for enhancements by email at ios_ear_support@citrix.com.

How to access technical preview features

You can request for Technical Preview features by email at ios_ear_support@citrix.com that is unique to each feature. You can find this form attached with the Technical preview announcement in the Product Documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How to provide feedback on EAR

You can provide EAR feedback by email at ios_ear_support@citrix.com.

Common issues and troubleshooting tips

Disconnected sessions

Users can disconnect (but not log off) from a Citrix Workspace app for iOS session in the following ways:

- While viewing a published app or desktop in session:
  - tap the arrow at the top of the screen to view the in-session drop-down menu.
  - tap the **Home** button to return to the launch pad.
  - notice the white shadow under the icon of one of the published apps that are still in an active session; tap the icon.
  - tap disconnect.
- Close Citrix Workspace app for iOS:
  - double-tap the device's **Home** button.
  - locate Citrix Workspace app for iOS in the iOS app switcher view.
  - tap disconnect in the dialog that appears.
- Pressing the home button on their mobile device.
- Tapping Home or Switch in the app's drop-down menu.

The session stays in a disconnected state. Although the user can reconnect later, you can verify that disconnected sessions are shown inactive after a specific interval.

To display the app in inactive mode, configure a session timeout for the ICA-TCP connection in Remote Desktop Session Host Configuration (formerly known as "Terminal Services Configuration").

For more information about configuring Remote Desktop Services (formerly known as "Terminal Services"), refer to the Microsoft Windows Server product documentation.

Expired passwords

Citrix Workspace app for iOS supports the ability for users to change their expired passwords. Prompts appear for users to enter the required information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Jailbroken devices

Your users can compromise the security of your deployment by connecting with jailbroken iOS devices. Jailbroken devices are those devices whose owners have modified them, usually with the effect of bypassing certain security protections.

When Citrix Workspace app for iOS detects a jailbroken iOS device, Citrix Workspace app for iOS displays an alert to the user.

To further help to secure your environment, you can configure StoreFront or Web Interface to help to prevent detected jailbroken devices from running apps.

Requirements

- Citrix Receiver for iOS 6.1 or later
- StoreFront 3.0 or Web Interface 5.4 or later
- Access to StoreFront or Web Interface through an administrator account

> **Note:**
>
> Citrix Workspace™ app deactivates itself if it detects a jailbroken device to protect data and maintain security. This ensures that the app cannot be used on devices with unauthorized modifications.

Loss of HDX™ audio quality

From Citrix Virtual Apps and Desktops and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service), HDX audio to Citrix Workspace app for iOS might lose quality. The issue occurs when you use audio and video simultaneously.

The issue occurs when the Citrix Virtual Apps and Desktops™ and Citrix DaaS HDX policies can't handle the amount of audio data with the video data.

For suggestions about how to create policies to improve audio quality, see Knowledge Center article CTX123543.

Failed to launch desktop and app sessions for customized store experience

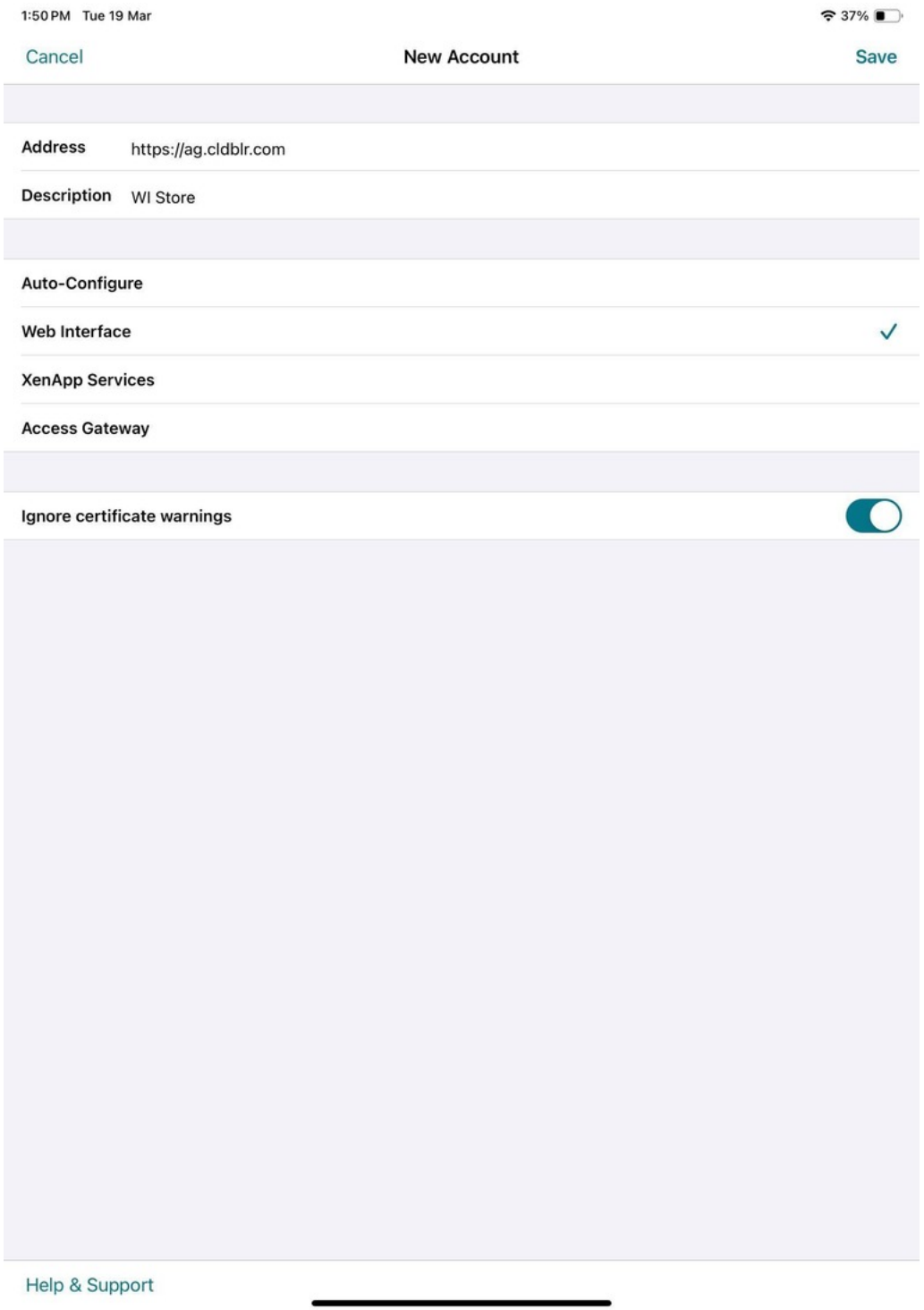
You might fail to launch desktop and app sessions from Citrix Workspace app if you have customized store experience. The auto-discovery of store type is supported only for e-mail addresses and not for store URLs. It is recommended to use email address or Web-interface login mode if you have a customized store. For more information, see Manual setupand Configuring email-based account discovery.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To configure an account manually through Web-interface login mode, do the following steps:

1. Tap the **Accounts icon > Accounts Screen > Plus Sign (+)**. The **New Account** screen appears.
2. In the lower left corner of the screen, tap the icon to the left of **Options** and tap **Manual setup**. Other fields appear on the screen.
3. In the **Address** field, type the secure URL of the site or Citrix Gateway (for example, agee.mycompany.com).
4. Select the **Web Interface** connection. This connection mode displays a Citrix Virtual Apps™ website similar to a Web browser. This UI is also known as Web View.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. For certificate security, use the setting in the **Ignore certificate warnings** field to determine whether you want to connect to the server even if it has an invalid, self-signed, or expired certificate. The default setting is OFF.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> If you do enable this option, make sure you're connecting to the correct server. Citrix strongly recommends that all servers have a valid certificate to protect user devices from online security attacks. A secure server uses an SSL certificate issued by a certificate authority. Citrix does not support self-signed certificates and does not recommend by-passing the certificate security.

6. Tap **Save**.
7. Type your user name and password (or token, if you selected two-factor authentication), and then tap Log On. The Citrix Workspace app for iOS screen appears, in which you can access your desktops and add and open your apps.

> **Note:**
>
> You must enter the user credentials for each connection, as they are not saved in the Web interface login mode.

Citrix Troubleshoot Connection

The Citrix Troubleshoot Connection feature is designed to empower end-users to effectively self-troubleshoot potential desktop or application launch failures. This enhancement aims to provide users with clear diagnostics, potential recommendations, and the ability to run fixes with a simple click.

How It Works

The feature delivers more granular and enhanced error messages to help users clearly understand the root cause of launch failures. The Troubleshoot Connection feature analyzes connection issues to the Virtual Delivery Agent (VDA) in real time during the launch process. It then presents user-friendly error messages and recommendations, enabling users to either resolve the issue directly or gather logs for a support ticket if needed.

Connection paths analyzed

The feature diagnoses potential virtual app and desktop launch issues across critical connection points, including:

- Network connectivity from the Client to the Gateway.
- Gateway to StoreFront server connection.

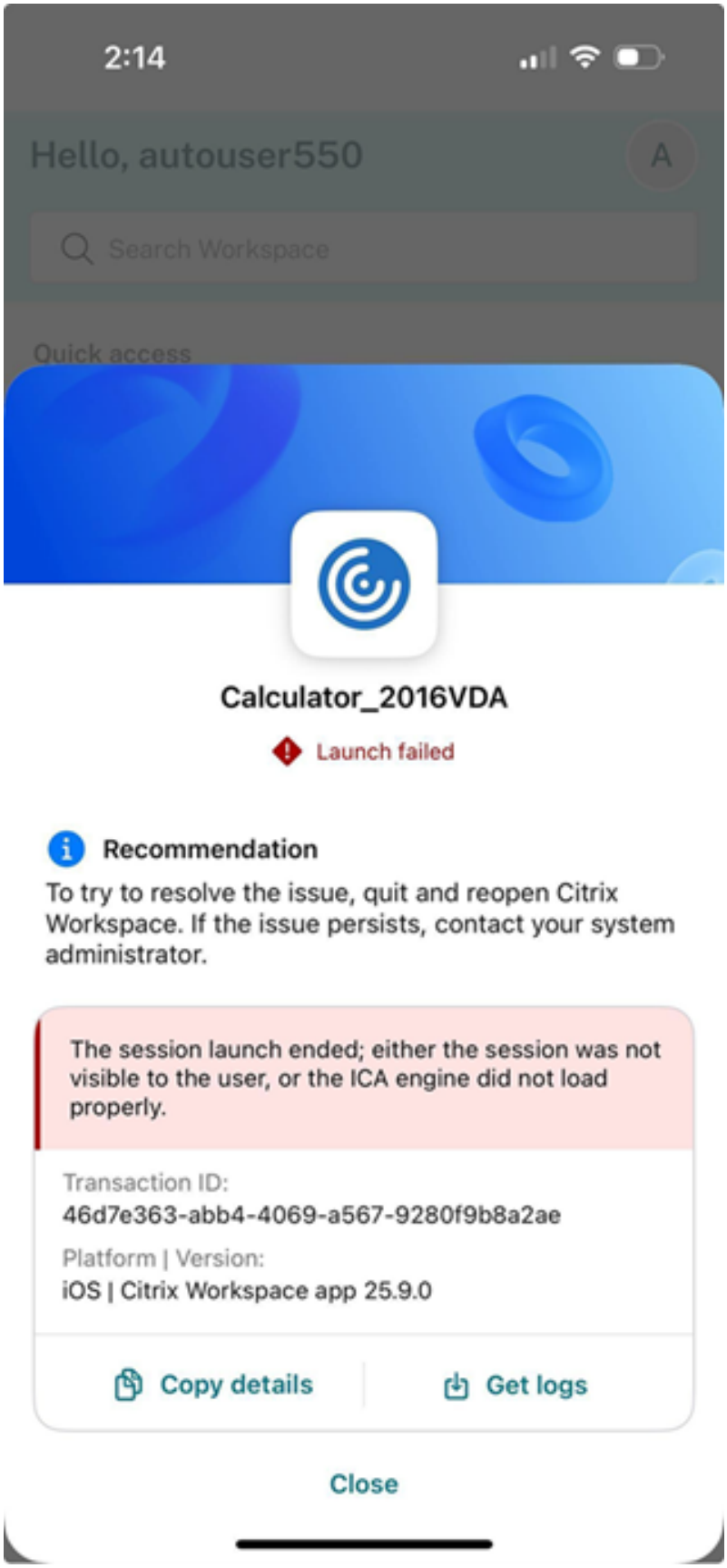
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- StoreFront server to Broker connection.
- Broker to VDA connection.

Enhanced error messages and diagnostics

In the event of launch failures, Citrix now displays clear, user-friendly error messages that pinpoint specific connection issues, such as network errors, server unavailability, or VDA failures. For administrators, detailed error codes are provided in the logs, categorized into server-side and client-side errors, serving as valuable references for deeper investigation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Self-recovery and remediation actions

The Citrix Troubleshoot Connection feature includes steps that users can take to automatically recover from common issues, thereby minimizing the need for support intervention. Following are the potential problems that can be resolved with guided remediation:

- Restart VDA
- Restart Citrix Workspace app (CWA) - Re-Login to CWA
- Refresh the resource list
- Refresh the app and try
- Reconfigure the store
- Upgrade CWA
- Reinstall CWA
- Check the network
- Wait And retry

System requirements

To use the Troubleshoot Connection feature, have the following Citrix Workspace app versions:

- **Citrix Workspace app for iOS:** Version 2509 and later

> **Note:**
>
> The error messages include server error codes as well, the details of the same for both on-premises and cloud can be obtained from the section Error codes

The Troubleshoot Connection feature is enabled by default in DaaS environments. Granular error messages and recommendations are available for both browser-launched sessions and sessions started with Citrix Workspace app. Error codes and transaction IDs are recorded in logs for administrator reference. Error codes are categorized as server-side or client-side. For certain errors, a remediation option to restart the Virtual Delivery Agent (VDA) is provided. This feature does not support sessions in hybrid mode. For example, it cannot be used when you download an ICA file in a browser, then open that file using Citrix Workspace app.

FAQs

How to improve the video performance on virtual app and virtual desktop for low-powered or mobile devices

For information on how to improve and configure virtual desktop video performance using the MaxFramesPerSecond registry value or using HDX policies, depending on your Citrix Virtual Apps and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Desktops version, see the Knowledge Center article CTX123543.

I can't see my apps or desktops after signing on to Citrix Workspace app

Contact your company's help desk or your IT Support team administrator for further assistance.

How to troubleshoot slow connections

If you face any of the following issues, follow the steps mentioned in the following **Workaround** section.

- Slow connections to the Citrix Virtual Apps and Desktops site
- Missing app icons
- Recurring Protocol Driver Error messages

Workaround Disable Citrix PV Ethernet Adapter properties for the network interface on Citrix Virtual Apps server, Citrix Secure Web Gateway™, and Web Interface server.
The Citrix PV Ethernet Adapter properties include the following properties that are enabled by default. You need to disable all of these properties.

- Large Send Offload
- Offload IP Checksum
- Offload TCP Checksum
- Offload UDP Checksum

> **Note:**
>
> Server restart isn't required. This workaround applies to the Windows Server 2003 and 2008 32-bit. This issue does not affect the Windows Server 2008 R2.

Troubleshoot issue with Numeric keys and special characters

If numeric keys or Chinese IME characters do not function as expected, you need to disable the Unicode Keyboard option.
To disable the Unicode Keyboard option:

1. Navigate to **Settings** > **Keyboard Options**.
2. Set **Use Unicode Keyboard** to **Off**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app for iOS

September 24, 2026

Citrix Workspace app for iOS is client software available for download from the App Store. It enables you to access and run virtual desktops and hosted applications delivered by Citrix Virtual Apps and Desktops.

iOS is the operating system for Apple mobile devices such as iPads and iPhones. Citrix Workspace app for iOS runs on devices using the iOS operating system, such as iPhone X, iPad mini, and iPad Pro.

Language support

Citrix Workspace app for iOS is adapted for use in languages other than English. For a list of languages supported by Citrix Workspace app for iOS, see Language support.

Deprecation

The announcement in this article gives you advanced notice of platforms, Citrix® products, and features that are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they're withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality.

Deprecated items aren't removed immediately. Citrix continues to support them in this release but they'll be removed in the future.

Item	Deprecation announced in	Removed in	Alternative
iOS operating system version 17	Citrix Workspace app for iOS version 26.9.0	Citrix Workspace app for iOS version 26.9.0	Upgrade to the latest available version of iOS
Auto-Configure, XenApp Services, and Access Gateway	Citrix Workspace app for iOS version 26.7.0	Citrix Workspace app for iOS 26.11.0	-
Allow EDT setting	Citrix Workspace app for iOS version 26.7.0	Citrix Workspace app for iOS 27.3.0	Available as Admin setting
Citrix X1 mouse	Citrix Workspace app for iOS version 25.9.0	Citrix Workspace app for iOS 26.3.0	-
Citrix Casting	Citrix Workspace app for iOS version 25.9.0	Citrix Workspace app for iOS 26.3.0	-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Item	Deprecation announced in	Removed in	Alternative
iOS operating system version 16	Citrix Workspace app for iOS version 25.7.2	Citrix Workspace app for iOS 25.7.2	Upgrade to the latest available version of iOS
iOS operating system version 15	Citrix Workspace app for iOS version 24.7.0	Citrix Workspace app for iOS 24.12.0	Upgrade to the latest available version of iOS
Support for DTLS 1.0 protocol	Citrix Workspace app for iOS version 24.5.0	-	DTLS 1.2 protocol
Support for TLS 1.0 and TLS 1.1 protocols	Citrix Workspace app for iOS version 24.4.0	Citrix Workspace app for iOS version 25.3.0	TLS 1.2 or TLS 1.3 protocol
XenApp Services (also known as PNAgent)	Citrix Workspace app for iOS version 23.7.5	-	Within Citrix workspace app, connect to stores using the store URL rather than the XenApp Services URL.
iOS operating system version 14	Citrix Workspace app for iOS version 23.10.0	Target: Citrix Workspace app for iOS 23.12.0	Upgrade to the latest available version of iOS
iOS operating system version 13.x	Citrix Workspace app for iOS version 22.9.5	Target: December 2022 and version 22.12.0	Upgrade to the latest available version of iOS
iOS operating system version 11.x and 12.x	Citrix Workspace app for iOS version 21.12.0	Target: Aug 2022 and version 22.8.0	Upgrade to the latest available version of iOS
iOS operating system version 10.x	Citrix Workspace app for iOS version 21.1.5	Release following 21.1.5	Use Citrix Workspace app for iOS version 21.1.5 or earlier

Notes:

- Existing Citrix Workspace™ app users on deprecated platform versions can't upgrade to the latest release (from the App Store) of the Citrix Workspace app.
- New Citrix Workspace app users on deprecated platform versions can only be able to download an older compatible version from the App Store.
- Users on deprecated platform versions don't get any new features or security patches that come with every newer release of the Citrix Workspace app.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.