Citrix Workspace™ app

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

Contents

Citrix Workspace™ app 3

What's new 7

App Protection 30

System requirements and compatibility 35

App Protection features 38

Features in Technical Preview 60

Configure App Protection 60

Configure Anti-keylogging and Anti-screen capture 75

Configure Anti-DLL Injection 83

Configure Policy Tampering Detection 89

Configure App Protection Posture Check 92

Block DoubleHop Launch 100

Configure Screen Capture Allow List 101

Configure Process exclusion list 106

Configure USB Filter Driver Exclusion List 109

Configure allow list for the apps which use LD_PRELOAD functionalities 116

Disable App Protection 121

Disable Screen Capture Notifications 124

Troubleshoot 125

Generic troubleshooting 131

Troubleshoot Policy Tampering Detection 136

Troubleshooting App Protection Posture Check 139

Log collection 141

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

Advanced Troubleshooting on Windows 143

App Protection Health Checker 146

Contextual App Protection for Workspace 148

Prerequisites 149

Scenario 1 149

Scenario 2 153

Scenario 3 161

Scenario 4 163

Contextual App Protection for StoreFront 165

Prerequisites 167

Scenario 1 167

Scenario 2 171

Scenario 3 173

Scenario 4 174

Scenario 5 177

App Protection support for hybrid launch through Workspace 177

App Protection support for hybrid launch through StoreFront 181

Blocking of Screen Capture from AI-Powered tools 189

App Protection events to Director and Monitor 190

Citrix Workspace app release timelines 195

Citrix Workspace app feature matrix 197

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

Citrix Workspace™ app

August 27, 2026

About Citrix Workspace app

Citrix Workspace app provides instant, secure, and seamless access to all the resources that your end users need to stay productive. Citrix Workspace app includes access to virtual desktops, virtual apps, web and SaaS apps, and features such as embedded browsing, and single sign-on (from anywhere and from any device).

Citrix Workspace app is a client application that can be deployed across devices on both cloud and on-premises environments. It builds on the capabilities of what was previously known as Citrix Receiver™, and includes Citrix client technologies such as - HDX, the Citrix Gateway plug-ins, and Secure private access.

The client app is optimized to run on all client OS like Windows, macOS, Linux, iOS, and Android. It can also be accessed via a browser. For more details on the supported browsers, see Workspace Browser Compatibility.

Citrix Workspace app, powered by Citrix protocol and HDX™ (high-definition experience), delivers high-performance virtual app and desktop sessions. It is enhanced to deliver a secure login and internet browsing experience, easy management of your apps and desktops, advanced search capabilities, and more.

> **Note:**
>
> The app UI might vary based on the deployment of resources, that is, on cloud (leveraging workspace platform) or on-premises (leveraging StoreFront platform).

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

For information about the differences between LTSR and Current Releases, see Lifecycle Milestones for Citrix Workspace app.

Citrix Workspace app is available for the following operating systems:

- Citrix Workspace app for Android
- Citrix Workspace app for ChromeOS
- Citrix Workspace app for HTML5
- Citrix Workspace app for iOS

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

- Citrix Workspace app for Linux
- Citrix Workspace app for Mac
- Citrix Workspace app for Windows
- Citrix Workspace app for Windows (Store)

> **Important**
>
> **Data collected for Citrix Workspace app updates:**
>
> With respect to devices connected to the Internet, Citrix Workspace app might without additional notice, check for updates that are available for download and installation to the device and let the user know of their availability. Only non-personal identifiable information is transmitted when this happens, except to the extent that IP addresses may be considered personally identifiable in some jurisdictions.

Configure Citrix Workspace app using Global App Configuration service

Global App Configuration service provides a centralized interface to configure the Citrix Workspace app settings for end users. You can configure settings for both cloud and on-premises stores from a single interface. These settings are applicable to both managed and unmanaged devices (BYOD). For more information, see Global App Configuration service.

Language support

Citrix Workspace apps are adapted for use in languages other than English. This section lists the supported languages in the latest release of Citrix Workspace apps.

The following table lists the languages supported for Citrix Workspace app on various operating systems or platforms. A ☑ indicates that the app is available in that particular language.

Language	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows Store
English	☑	☑	☑	☑	☑	☑	☑	☑
Danish	☑			☑				
Dutch	☑	☑	☑	☑	☑	☑	☑	☑
French	☑	☑	☑	☑	☑	☑	☑	☑
German	☑	☑	☑	☑	☑	☑	☑	☑
Italian	☑	☑	☑	☑	☑	☑	☑	☑

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

Language	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows Store
Japanese	☑	☑	☑	☑	☑	☑	☑	☑
Korean	☑	☑	☑	☑	☑		☑	☑
Portuguese (Brazil)	☑	☑	☑	☑	☑	☑	☑	☑
Russian		☑	☑		☑		☑	☑
Simplified Chinese	☑	☑	☑	☑	☑	☑	☑	☑
Spanish	☑	☑	☑	☑	☑	☑	☑	☑
Swedish	☑			☑				
Traditional Chinese		☑	☑				☑	☑

Feature flag

This article discusses feature flag management and the various Citrix Workspace apps that support feature flags.

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. Through this improvement, Citrix aims to deliver an optimal user experience by efficiently managing feature flags and minimizing disruptions. To ensure optimal functioning of features which are under feature flags, you need to enable traffic to the URL `features.netscalergateway.net`.

If any issues arise, the feature can be quickly disabled without impacting the overall product experience, ensuring a seamless and reliable experience for our customers.

No configurations are needed to enable traffic for feature management, except when a firewall or proxy is blocking outbound traffic. In such cases, you need to enable traffic using specific URLs or IP addresses, depending on your policy requirements.

> **Note:**
>
> If using NetScaler Gateway with split tunneling OFF and split DNS OFF, ensure that NetScaler can resolve and connect to `features.netscalergateway.net` on port 443.

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

The following table calls out the various apps that support feature flags and the release versions in which feature flags were introduced in these apps.

App	Feature flag support	Version	Documentation
Citrix Workspace app for Android	Yes	2409	Feature flag management for Citrix Workspace app for Android
Citrix Workspace app for ChromeOS	Yes	2409	Feature flag management for Citrix Workspace app for ChromeOS
Citrix Workspace app for HTML5	Yes	2409	Feature flag management for Citrix Workspace app for HTML5
Citrix Workspace app for iOS	Yes	24.10.0	Feature flag management for Citrix Workspace app for iOS
Citrix Workspace app for Linux	No	-	-
Citrix Workspace app for Mac	Yes	2409	Feature flag management for Citrix Workspace app for Mac
Citrix Workspace app for Windows	Yes	2409	Feature flag management for Citrix Workspace app for Windows

Citrix Workspace App telemetry

Citrix Workspace app collects telemetry data about user and device usage through the product for license entitlement enforcement as well as to manage, measure and improve the software and service.

All telemetry collection is performed in accordance with the terms of our EUA and Privacy Policy.

For more information, see Citrix Virtual Apps and Desktops telemetry data elements.

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

Important update about Citrix Receiver

Beginning August 2018, Citrix Workspace app replaces Citrix Receiver. While you can still download older versions of Citrix Receiver, new features and enhancements are released for Citrix Workspace app.

Citrix Workspace app is a new client from Citrix that works similar to Citrix Receiver and is fully backward-compatible with your organization's Citrix infrastructure. Citrix Workspace app provides the full capabilities of Citrix Receiver, and new capabilities based on your organization's Citrix deployment.

Citrix Workspace app is built on Citrix Receiver technology, and is fully backward compatible with all Citrix solutions.

For more information, visit the Workspace app FAQ page.

What's new

October 8, 2026

Learn about new features and enhancements for Citrix Workspace™ app on Android, ChromeOS, HTML5, iOS, Linux, Mac, and Windows, App Protection, Citrix Enterprise Browser™, Workspace UI, Global App Configuration service, and Workspace Platform.

Citrix Workspace app for Android - 26.7.0

The following is the list of features:

- Improved Session Toolbar Experience
- Support for Two-Finger Horizontal Scrolling
- Support for One UI 8 on Samsung DeX
- Improved Graphic Settings Usability and Automatic Synchronization
- Support for In-Session **FIDO2** Passkeys for Passwordless Sign-In
- Deprecation Notice

Citrix Workspace app for ChromeOS - 2603.60

This release addresses areas that improve overall performance and stability.

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

Citrix Workspace app for ChromeOS - 2603.50

The following is the list of features that are available in Citrix Workspace app 2603.50 for ChromeOS:

- Enhanced in-session reconnection experience

Citrix Workspace app for ChromeOS - 2603.10

This release addresses areas that improve overall performance and stability.

Citrix Workspace app for HTML5 - 2603.10

This release addresses areas that improve overall performance and stability.

Citrix Workspace app for ChromeOS - 2603

The following is a list of features that are available in Citrix Workspace app 2603 for ChromeOS:

- Keyboard input mode refinement
- Audio quality improvement with reliable transport protocols
- AOT log content enhancement
- Service Continuity for connectorless workloads
- Loss tolerant mode for graphics
- Enhanced EDT lossy connection support with Secure HDX
- Enhanced in-session reconnection experience [Technical Preview]

Citrix Workspace app for HTML5 - 2603

The following is a list of features that are available in Citrix Workspace app 2603 for HTML5:

- Keyboard input mode refinement
- Audio quality improvement with reliable transport protocols
- AOT log content enhancement
- Support for single-tenant Microsoft Entra ID

Citrix Workspace app for Mac - 2609

The following is a list of features that are available in Citrix Workspace app 2609 for Mac:

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

- Support for macOS 27 Golden Gate
- HDX Direct support for direct connections

Citrix Workspace app for Mac - 2607

The following is a list of features that are available in Citrix Workspace app 2607 for Mac:

- Microsoft Teams VDI Plugin —generally available and installed by default
- Version rollback support for auto update
- Faster and less disruptive automatic updates (side-by-side silent update)
- Session Pre-Launch support
- Improved Point of Presence (PoP) selection
- DNS caching for improved session resilience (Technical Preview)
- EDT MTU Rediscovery (Technical Preview)
- Streaming read and write for Client Drive Mapping (CDM) (Technical Preview)
- HDX Direct for Service Continuity for connectorless workloads (Technical Preview)
- HDX graphics super resolution (Technical Preview)
- Location redirection for virtual sessions (Technical Preview)
- Enhanced call connect times with Unified Communications SDK
- Optimized Overlay Clipping for multimedia sessions
- Resilient and secure third-party plugin execution (Technical Preview)
- OAuth redirection support for Bidirectional content redirection
- Adaptive Webcam Bitrate
- PDF printing enhancements
- Health checker tool for CAM and MDM Policy

Citrix Workspace app for Mac - 2603.11

The following is a list of features that are available in Citrix Workspace app 2603.11 for Mac:

- Support for Citrix Snipping Tool integration (Technical Preview)
- Deprecation of Datagram Transport Layer Security (DTLS) 1.0

Citrix Workspace app for Linux - 2604

The following is a list of features that are available in Citrix Workspace app 2604 for Linux:

- Enhanced Browser Content Redirection with Server-Side Certificate Validation
- Entra ID single sign-on for NetScaler Gateway stores
- Removal of Citrix Enterprise Browser

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

- Google Chrome support for FIDO2 authentication
- Enhanced Call Connect times with UCSDK Optimization
- Service continuity for connectorless workloads
- Shortcuts menu for macOS VDA
- Scanner workflow optimization
- EDT Lossy support with Secure HDX 2.0
- Removal of ARM64 support
- Dual VCSDK binary sets for Linux (Technical Preview)
- Dual CWA package sets for Linux (Technical Preview)

Citrix Workspace app for Mac - 2603

The following is a list of features that are available in Citrix Workspace app 2603 for Mac:

- Gesture support for remote Mac sessions
- Bidirectional Content Redirection
- Deprecation of macOS 13.0 Ventura
- Always On Tracing (AOT) support for Citrix Workspace app for Mac
- Microphone troubleshooting
- Shield V2 service continuity
- Support for Microsoft Teams VDI Plugin installation
- Virtual channel plugin manager

Citrix Workspace app for Android - 2603

The following are the features:

- Always On Tracing (AOT)
- Smarter control of reconnection alert using Mobile Device Management (MDM) and Global App Configuration Service (GACS)
- Mobile Device Management (MDM) nested JSON configuration support
- Enhanced automatic keyboard show-hide with Windows VDA
- Improved support for EDT Lossy connections with Secure HDX
- Anti-keylogging support for Web Interface
- Real-time keyboard settings in Citrix Workspace app for Android
- IdP chained logout on inactivity timeout
- Session toolbar configuration through Global App Configuration service and Mobile Device Management
- Deprecation announcement of Android 13
- Deprecation notification of legacy features

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

Citrix Workspace app for Linux - 2601

- Seamless Integration of Endpoint Analysis (EPA)
- Entra ID single sign-on (SSO) from web browsers
- Single sign-on (SSO) through cookie sharing for on-premises stores
- Microsoft Edge support for FIDO2 and Entra ID SSO
- FIDO2 authentication timeout configuration
- Identity Provider (IDP) logout on Workspace (WSP) inactivity timeout
- Automatic Maximum Transmission Unit (MTU) adaptation
- Enhanced keyboard settings
- Transparent key pass-through on Wayland and XWayland
- Improved session reconnection experience
- Extended logging support
- Modular Browser Content Redirection
- Force Gateway route for StoreFront discovery
- Audio Quality Enhancer for reliable transport

Citrix Workspace app for ChromeOS - 2511.10

This release addresses areas that improve overall performance and stability. It contains changes to improve responsiveness of the session during high server load. This release is compatible with ChromeOS versions 144.

Citrix Workspace app for Android - 25.11.0

- Seamless single sign-on for Entra ID joined VDAs
- Loss tolerant mode for audio
- Seamless integration of deviceTRUST® with Citrix Workspace™ app for Android
- Persistent client names for Android devices
- Enhanced on-screen keyboard experience
- Enhanced USB diagnostic tool for VDA
- Synchronized audio volume control with audio device auto sync
- Improved reconnection experience for mobile VDI users

Citrix Workspace app for Mac - 2511.1

- Bidirectional Content Redirection support on Mac endpoints
- Modular Browser Content Redirection
- Support for Global App Configuration service in hybrid launches

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

- uberAgent add-on support for managed devices
- Citrix Enterprise Browser
- Improved session failure reporting
- Enhanced USB diagnostic tool for VDA
- Endpoint Analysis Plugin updates

Citrix Workspace app for ChromeOS - 2511

- Integration of deviceTRUST with Citrix Workspace app for ChromeOS
- Always On Tracing (AOT)
- Default audio device selection
- Entra ID single sign-on support for VDA with Azure AD credentials
- Global App Configuration service v2 authenticated user group support

Citrix Workspace app for iOS - 25.9.0

- Enhanced troubleshooting with Citrix Troubleshoot Connection
- Support for landscape mode on iPhone
- Enhanced desktop launch experience
- Improved Caps Lock synchronization for external keyboards
- Audio device and volume sync improvements
- Deprecation notifications of legacy features

Citrix Workspace app for HTML5 - 2511

- Default audio device selection
- Entra ID single sign-on support for VDA with Azure AD credentials
- Always on tracing (AOT)

Citrix Workspace app for Android - 2509

- Visibility in to real-time progress during resource launches
- Multimonitor experience improvements
- Enhanced troubleshooting with Citrix Troubleshoot Connection
- Deprecation announcement of Android 13
- Deprecation notification of legacy features

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

Citrix Workspace app for Linux - 2508.10

- Entra ID SSO support for cloud

Citrix Workspace app for Windows - 2508.10

- ARM64 support for USB redirection

Citrix Workspace app for Linux - 2508

- Mandate end users to authenticate and access apps and desktops through native app
- Addition of DisableClientAppManagement flag
- SSO to Citrix Workspace™ app through cookie sharing using Credential Insertion SDK
- Ubuntu 24.04+ webkit2gtk dependency resolution
- Hardware acceleration in Browser Content Redirection
- Keyboard settings change take effect without reconnect
- Audio Quality Enhancer to improve audio performance
- Enhanced Connection Strength Indicator
- Background blur for webcam redirection using UI
- Support for H.264 hardware decoding for seamless apps
- Support for H.264 hardware decoding
- Browser Profile Sharing in Browser Content Redirection (Tech Preview)
- Support for EDT timeout configuration
- NFC support for FIDO2 Authentication
- GACS supports Citrix Workspace app for Linux
- Enhanced file transfer capabilities for Linux clients
- PDF Universal Printing
- Smart card authentication support for Boot-to-VDI- Technical Preview
- Audio Quality Enhancer for EDT loss tolerant mode

Citrix Workspace app for Mac - 2508

- Support for macOS 26 Tahoe
- Support for regional GACS discovery endpoints for US Government customers
- Support for Virtual Channel plug-in Manager for Microsoft Teams on Mac
- Enhanced self-service troubleshooting and user experience
- MDM policy for blocking Global AppConfig Service (GACS) requests
- Enhanced keyboard settings configuration
- Enlightened Data Transport (EDT) connection timeout configuration

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

- Enhanced session toolbar notch size
- Seamless mode API enhancement for Virtual Channel Software Development Kit (VCSDK)
- Audio Quality Enhancer for EDT loss tolerant mode

Citrix Workspace app for Windows - 2508

- Extends long term support to Windows 11 IoT enterprise LTSC
- Automated Endpoint Analysis client installation
- Service continuity enabled without self-service mode
- Citrix Troubleshoot Connection
- Enhanced storebrowse session handling
- Support for GACS claimed URLs for the US Gov region
- Automated sign-out on session disconnect
- ADMX file import support for Intune
- Modular Browser Content Redirection
- Microsoft Teams plugin automatic installation
- Zoom 64-bit plug-in management support
- uberAgent® add-on support for managed devices in Citrix Workspace app
- Enhanced background blur persistence for webcam
- Enhanced keyboard layout settings notification
- License telemetry upload using Citrix Workspace app
- Enable noise suppression
- Browser Profile Sharing in Browser Content Redirection - Technical Preview
- Version upgrade for Chromium Embedded Framework
- HDX™ graphics superresolution upscaling (Preview)
- Citrix Enterprise Browser™
- App Protection support for ARM64 on Windows
- App Protection Health Checker

Citrix Workspace app for HTML5 - 2509

- High DPI support for multiple monitors
- Enhanced Alt+ key shortcuts support in double-hop RDP scenarios
- Generic Client IME enhancement for Citrix Workspace app for HTML5 on Chromebook with multi monitors
- Configuration for blocking Global App Configuration service (GACS) requests
- Configuration for blocking feature flag requests
- Enhanced session toolbar notch size

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

Citrix Workspace app for ChromeOS - 2509

- High DPI support for multiple monitors
- Loss tolerant mode for audio
- Enhanced Alt+ key shortcuts support in double-hop RDP scenarios
- Google Admin Policy for blocking Global App Configuration service (GACS)
- Google Admin Policy for blocking feature flag requests
- Enhanced session toolbar notch size

Citrix Workspace app for ChromeOS - 2507

- Adaptive transport (EDT)

Citrix Workspace app for iOS - 25.7.2

- Support for iOS 26
- Enhanced Connection Strength Indicator
- Auto-launch desktops and apps
- Support iPad and iPhone in Lockdown mode

Citrix Workspace app for Windows - 2507 LTSR

- Citrix Troubleshoot Connection
- Extends long-term support to Windows 11 IoT enterprise LTSC
- Automated Endpoint Analysis client installation
- Service continuity enabled without self-service mode
- Enhanced session timeout enforcement on citrix Gateway
- Enhanced storebrowse session handling
- Support for GACS claimed URLs for the US Gov region
- Automated sign-out on session disconnect
- ADMX file import support for Intune
- Modular Browser Content Redirection
- Zoom 64-bit plug-in management support
- Simplified distribution of uberAgent on endpoints through Citrix Workspace app
- Enhanced background blur persistence for webcam
- Enhanced keyboard layout settings notification
- License telemetry upload using Citrix Workspace app
- Enable noise suppression
- Version upgrade for Chromium Embedded Framework

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

Citrix Workspace app for Windows - 2503.10

- Audio Quality Enhancer to improve audio performance
- Enhancement to auto-update

Citrix Workspace app for HTML5 - 2505

- Enhanced multi-monitor support with auto-detection and custom display selector
- Disable downloading of Citrix Workspace app logs in error dialogs

Citrix Workspace app for ChromeOS - 2505

- Enhanced multi-monitor support with auto-detection and custom display selector
- Improved video rendering in optimized Zoom sessions
- Persistent auto USB redirection

Citrix Workspace app for Mac - 2505

- Citrix Workspace app for Mac on macOS Tahoe Beta2
- Simplified authentication into on-premises store
- Support for voice dictation
- Troubleshoot launch failure self service
- Prevent launching of ICA files from disk
- Monitoring Zoom plug-in metrics on Director
- Auto-Update enhancements for active users in Citrix Workspace app for Mac
- Keyboard accessibility support for the toolbar on the Virtual Desktop
- Enhancement to Connection Strength Indicator on Citrix Viewer toolbar
- Support for macOS window tiling in Citrix Workspace app for Mac
- Platform-specific toolbar update: Ctrl+Alt+Del button hidden for macOS VDA sessions
- Enhanced user interface and experience
- Default audio device selection

Citrix Workspace app for Linux - 2505

- Supporting Linux distributions
- App Protection support for eLux 7
- Improved proxy handling with FQDN support
- Enhancement to Fullscreen or Extend button behavior
- New storebrowse commands to create an autostart entry for boot-to-virtual-desktop

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

Citrix Workspace app for Windows - 2503

- Client-side graphics optimizations
- Persistent session in Citrix Workspace app
- Enhanced Desktop Viewer toolbar
- Enhancement to connection strength indicator on Desktop Viewer toolbar
- Multi-monitor layout selection
- Enhancements on Desktop Lock or Boot to VDI feature
- Simplified SSON
- Seamless integration of deviceTRUST with Citrix Workspace app
- Enhancement to auto-update
- Enable auto-update for active users only
- Enhanced installation process for Citrix Workspace app with App Protection
- Improved installation process for Citrix Workspace app
- Auto-sync backend resource changes for Start menu and Desktop shortcuts
- Install Zoom and Webex plug-in managers during Citrix Workspace app installation
- Log collection support for non-admin users
- Enhanced security and compatibility with AppLocker
- Version upgrade for Chromium Embedded Framework
- Improved audio performance in Microsoft Teams
- Monitor third-party UC app optimization status using Citrix Director
- Hybrid launch support using GACS for on-premises stores

Citrix Workspace app for iOS - 25.3.0

- Enhanced session resolution
- Enhanced audio quality with real-time Echo Cancellation
- New In-Session toolbar

Citrix Workspace app for Linux - 2503

- Boot to Virtual Desktop
- Seamless Integration of deviceTRUST
- Integration with eLux 7
- New command for storebrowse
- Connection strength indicator on Desktop Viewer toolbar
- Enable Audio Quality Enhancer to improve audio performance
- On-screen keyboard enhancement for multi-touch
- Enhanced multi-monitor custom layout

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

- Enhanced battery status indicator
- Default audio device selection
- Bidirectional content redirection supports OAuth redirection
- Improved audio performance in Microsoft Teams
- Support for H.264 hardware decoding for seamless apps (Technical Preview)

Citrix Workspace app for Mac - 2503

- Support for automatic installation of deviceTRUST plug-in with Citrix Workspace app
- Quit background processes with Quick Access menu
- Managing display of app shortcuts on Mac Launchpad
- Enhanced desktop launch experience
- Enhanced structure for Help menu
- Improved session timeout experience (Technical Preview)
- Enhanced keyboard settings for VDA OS and session type
- Optimized graphics performance for Selective Thinwire
- UCSDK deviceID enhancement
- Clipboard support for copying files and folders
- Enhanced Multi-Monitor Management for desktop sessions
- Loss tolerant mode for graphics
- USB Redirection of mass storage devices
- HDX direct support
- Enable Audio Quality Enhancer to improve audio performance
- Hybrid launch support using GACS for on-premises stores
- Enhancing hybrid mode support with GACS for cloud stores (Technical Preview)
- Deprecation announcement of macOS Monterey 12

Citrix Workspace app for HTML5 - 2502

- Enhancements to the improved in-session toolbar
- Connection strength indicator
- Service continuity [Technical Preview]
- Support for horizontal scrolling on trackpad
- Session launch diagnostics
- Enhanced seamless app launch and resizing experience
- Support for Unified Communications (UC) SDK

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

Citrix Workspace app for ChromeOS - 2502

- Enhancements to the improved in-session toolbar
- Connection strength indicator
- Adaptive transport (EDT)
- Support for horizontal scrolling on trackpad
- Session launch diagnostics
- Enhanced seamless app launch and resizing experience
- Support for Unified Communications (UC) SDK
- Zoom optimization - lock screen support
- Asset ID character limit increase

Citrix Workspace app for iOS - 25.1.4

- 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

Workspace UI - 25.04

- Pinned links support

Citrix Workspace app for Android - 24.9.0

- Support for DPI Matching on Samsung DeX in multi-display mode
- Connection strength indicator

Citrix Workspace app for ChromeOS - 2411.1

- Scanner redirection support
- Enhanced session reliability
- Enhanced desktop launch experience
- Enhanced virtual desktop screen resizing experience
- Support for HTTP Proxy
- Improved in-session toolbar
- Sustainability initiative from Citrix Workspace app - Customize the sustainability message

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

- Enhanced troubleshooting with endpoint telemetry in Citrix Director
- Citrix VDA for macOS - clipboard and keyboard shortcuts
- Enhanced log collection
- Enhanced keyboard and IME diagnostics tool
- Enhanced display control with multi-monitor selector

Citrix Workspace app for Linux - 2411

- Supporting Linux distributions
- NFC support for FIDO2 authentication (Technical Preview)
- Echo cancellation
- Noise suppression
- Connection Strength Indicator on Desktop Viewer toolbar (Technical Preview)
- Enhanced desktop launch and screen resizing experience
- Multi-monitor layout selection (Technical Preview)
- Audio Quality Enhancer for Adaptive Audio (Technical Preview)
- Sustainability initiative from Citrix Workspace app
- Bidirectional content redirection
- HDX direct
- Customization of Desktop Viewer toolbar
- Support for WebHID API in UCSDK

Citrix Workspace app for Mac - 2411

- Enhancing Citrix security with pre-populated user name
- Version control using MDM and GACS
- Auto updates support scheduling
- Auto-update enhancement for active users
- UCSDK HID Implementation
- HDX Direct
- Support for plug and play webcam redirection
- Auto-update support for user groups
- Support for log collection when session launch fails
- Support for browser content redirection (Technical Preview)
- Enhanced display control with Multi-Monitor selector (Technical Preview)
- USB Redirection of mass storage devices (Technical Preview)
- HDX Direct V2 for non-shield scenario (Technical Preview)
- Enable Audio Quality Enhancer to improve audio performance (Technical Preview)

  Enforcing Citrix access using Citrix Workspace app

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

Citrix Workspace app for HTML5 - 24.11.0

- Enhanced desktop launch experience
- Enhanced virtual desktop screen resizing experience
- Enhanced session reliability
- Improved in-session toolbar
- Sustainability initiative from Citrix Workspace app
- Enhanced log collection
- Enhanced troubleshooting with endpoint telemetry in Citrix Director
- Progressive Web App version of Citrix Workspace app for HTML5 for StoreFront
- Citrix VDA for macOS - clipboard and keyboard shortcuts
- Enhanced keyboard and IME diagnostics tool

Citrix Workspace app for iOS - 24.12.0

- 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

Citrix Workspace app for ChromeOS - 2411

- Scanner redirection support
- Improved in-session toolbar
- Sustainability initiative from Citrix Workspace app - Customize the sustainability message
- Improved support for HTTP proxy
- Enhanced troubleshooting with endpoint telemetry in Citrix Director
- Support for macOS VDA - clipboard and keyboard shortcuts
- Enhanced desktop launch experience
- Enhanced virtual desktop screen resizing experience
- Enhanced log collection
- Enhanced keyboard and IME diagnostics tool
- Enhanced session reliability
- Enhanced display control with multi-monitor selector (Technical Preview)

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

Citrix Workspace app for Windows - 2409

- Support for Windows 11 24H2
- Feature flag management
- Single sign-on support for Edge WebView when using Microsoft Entra ID
- Enhanced virtual desktop screen resizing experience
- Enhanced desktop launch experience
- Enhancement to sustainability initiative
- Streamlined beacon checks
- .NET requirements
- SOCKS5 proxy support for EDT
- Customization of Desktop Viewer toolbar
- Remember USB connections
- Disabling the "Exiting Full Screen Mode"tip prompt
- Support for WebHID API in UCSDK
- Support for TLS protocol version 1.3
- Disabling TLS 1.0 or 1.1 communication protocols
- Default audio device selection
- Connection Strength Indicator on Desktop Viewer toolbar
- Enable Audio Quality Enhancer to improve audio performance (Technical Preview)
- Virtual Channel Plugin Manager
- Deprecation of HDX RealTime Optimization Pack for Skype for Business

Citrix Workspace app for iOS - 24.10.0

- Feature V2 for feature flag management.

Citrix Workspace app for HTML5 - 2409

- What's new

Citrix Workspace app for Android - 24.9.0

- Supports GACS authenticated microservices (Cloud)
- Enhanced EDT congestion control
- Support for more than one session on Samsung DeX with Samsung Knox

For more information on latest features, technical preview features, known issues, fixed issues, see What's new.

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

Citrix Workspace app for Linux - 2408

- Support for RHEL 9.4 x86-64, Ubuntu 2204 x86-64, Raspberry Pi OS Bullseye-arm64, Debian 11.9 x86-64
- Enhanced virtual desktop screen resizing experience
- Enhanced Desktop Viewer toolbar
- Customize toolbar
- Accessibility support for enhanced Desktop Viewer toolbar
- Performance optimization for graphics
- Endpoint Analysis support for multi-factor (nFactor) authentication
- Enhancement to Storebrowse commands
- Multiple webcam resolutions support
- Fast smart card
- Improved loading experience for shared user mode
- Support for Optimized Microsoft Teams on ARM64 devices
- Version upgrade for Chromium Embedded Framework
- App protection
- Manage settings for user groups using configuration profile [Technical Preview]
- NFC support for FIDO2 Authentication [Technical Preview]
- Enhanced Unified Communications SDK API [Technical Preview]
- Support for WebHID API in UCSDK [Technical Preview]
- Support integrated windows authentication for browser content redirection [Technical Preview]
- Support for H.264 and H.265 hardware decoding [Technical Preview]
- Clipboard Support for HTML-formatted text [Technical Preview]

Citrix Workspace app for ChromeOS - 24.9.0

- Adaptive transport (Technical Preview)

For more information on features, known issues, fixed issues, see What's new.

Citrix Workspace app for iOS - 24.9.0

- Support for iOS 18
- Support for Rapid Scan
- Support for sustainability initiative
- Enhanced multi app window management
- Skip the Enable Biometrics Prompt
- Fetching GACS Endpoints via Email/Domain-Based Discovery API

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

- Support for GACS Authenticated Microservices (Cloud)
- Support for App Protection

Citrix Workspace app for Mac - 2409

- Client App Management
- Support for restricting users to modify the update channel
- Support for Rapid Scan
- Enhanced virtual desktop screen resizing experience
- Enhanced desktop launch experience
- Enhanced clipboard support for HTML text, files and folders
- Support for managing composite USB device redirection using DDC policies
- Enhancements to the smart card reader authentication
- Enhanced Desktop Viewer toolbar
- Connection Strength Indicator
- HDX Direct (Technical Preview)
- Support for multiple webcam resolutions (Technical Preview)
- Support for Plug and play webcam redirection (Technical Preview)

Workspace UI - 24.37

- Enhanced UI centralized layout

For more information on features, technical preview features, known issues, fixed issues, see What's new.

Citrix Workspace app for HTML5 - 2408

- HDX adaptive throughput
- Technical Preview
  - Secure HDX
  - Improved in-session toolbar

Citrix Workspace app for ChromeOS - 2408

- HDX adaptive throughput
- Enhancements to service continuity
- Enhancements to Chrome HDX SDK APIs

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

- Technical Preview
    - Support to share app window during screen sharing.
    - Scanner redirection support
    - Secure HDX

For more information on latest features, technical preview features, known issues, fixed issues, see What's new.

Citrix Workspace app for Android - 24.7.0

- Support for adaptive audio
- Add many stores using UEM
- Jailbroken devices
- Enhancement to support desktop-like experience in a single session on Samsung DeX
- Support for App Protection

For more information on latest features, technical preview features, known issues, fixed issues, see What's new.

Workspace UI - 24.30

- Manage installation prompt for Workspace Web extension

For more information on features, technical preview features, known issues, fixed issues, see What's new.

Citrix Workspace app for iOS - 24.7.0

- Support for DTLS 1.2
- Detect and display keyboard language change in the virtual session
- Support for adaptive audio
- Support for configuring Citrix Workspace app settings through UEM
- Technical Preview
    - Support for authentication using FIDO2 when connecting to an on-premises store
    - Support for multiple audio devices
    - Support for App Protection

For more information on latest features, known issues and fixed issues, see What's new.

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

Citrix Workspace app for Windows - 2405

- Compatibility with the higher versions of .NET
- Single sign-on support for ARM64-based devices
- New Add-ons and packaging
- Configure store names for your store URL
- Improved Beacon checker tool
- Option to prevent endpoint from going to sleep when a session is active
- Enhancement to relative mouse
- Share system audio
- Upgraded version of WebRTC for the optimized Microsoft Teams
- Support for MJPEG webcams
- Version upgrade for Chromium Embedded Framework
- Enhanced System Logs for browser content redirection
- App Protection support for double-hop scenario
- Citrix Enterprise Browser
    - Modify the user-agent of Citrix Enterprise Browser
    - Additional security restrictions for the Citrix Enterprise Browser

For more information on features, technical preview features, known issues, fixed issues, see What's new.

Citrix Workspace app for iOS - 24.5.0

- Support for authentication using FIDO2 when connecting to a cloud store
- Support for document scanner

For more information on latest features, technical preview features, known issues, fixed issues, see What's new.

Citrix Workspace app for Linux - 2405

- Support for RHEL9 x64, Ubuntu 2204 x86-64, RaspiOS-bullseye-arm64, Debian 11x86-64
- Enhanced system logs for browser content redirection
- Improved loading experience for shared user mode

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

- UI option to manage monitor plug and play feature
- Composite USB device redirection using DDC policies
- Enhanced the user interface for seamless login experience
- Support for multiple passkeys in HDX session
- Version upgrade for Chromium Embedded Framework
- Deprecation announcement of PNAgent support
- Deprecation announcement of SUSE
- Deprecation notice

For more information on latest features, technical preview features, known issues, fixed issues, see What's new.

Citrix Workspace app for ChromeOS - 2402.1

- Service continuity
- Config utility tool
- Virtual Channel SDK
- HTTP proxy setting on Chromebook
- Short name for store URL

For more information on latest features, technical preview features, known issues, fixed issues, see What's new.

Citrix Workspace app for Android - 24.5.0

- Support for authentication using FIDO2 when connecting to a cloud store
- Document scanner
- Deprecation announcement
- Technical Preview
  - Audio redirection with external microphones
  - Single sign-on for Microsoft Entra ID enabled VM

For more information on latest features, technical preview features, known issues and fixed issues, see What's new.

Workspace UI - 24.20

- Enhanced search experience
- Performance improvement

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

For more information on features, technical preview features, known issues, fixed issues, see What's new.

Global App Configuration service - 2406

- Clone settings across stores, channels, and configuration profiles

For more information on features, technical preview features, known issues, fixed issues, see What's new.

Citrix Workspace app for HTML5 - 2312

- Support for secondary ringer
- Simulcast implementation for optimized Microsoft Teams video conference calls

For more information on latest features, technical preview features, known issues, fixed issues, see What's new.

Citrix Workspace app for Mac - 2405

- Support for unified build for both Apple silicon and Intel-based Mac devices
- Support for Mac with M3 chips
- Support for Activity Manager on the quick access menu for cloud stores
- Support for resetting Citrix Workspace app
- Support for device touch ID for FIDO2 password-less authentication
- Enhanced virtual apps and desktops launch experience for on-premises stores and custom web portals
- Support for automatic installation of the End-Point Analysis (EPA) plug-in with Citrix Workspace app
- Support for optionally installing Citrix Enterprise Browser
- Support for Citrix Workspace widgets
- Provision to manage multiple proxy servers using PAC files
- Upgraded version of WebRTC for the optimized Microsoft Teams
- Support for printing PDF documents with selected orientation
- Enable Packet Loss Concealment to improve audio performance
- Modernized Citrix Virtual Channel SDK for Citrix Workspace app for Mac
- Enhancement to the keyboard Settings
- Support for extending the desktop session to external monitors automatically

For more information on latest features, technical preview features, known issues, fixed issues, see What's new.

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

Citrix Workspace app for Windows - 2403

- Sustainability initiative for cloud hybrid launch
- Enhanced domain pass-through for single sign-on (Enhanced SSO)
- Support for advanced NetScaler policies for Storebrowse on Windows
- Version upgrade for Chromium Embedded Framework
- Install Microsoft teams VDI plug-in for Citrix
- Hide Troubleshooting option for end users
- Deprecation of PNAgent support
- App Protection
    - Screen Capture Allow List
    - Process exclusion list
    - USB Filter Driver Exclusion List
- Citrix Endpoint Analysis
- Citrix Enterprise Browser
    - Security indicator when visiting websites
    - Citrix Enterprise Browser introduces additional settings in the Global App Configuration service

For more information on features, technical preview features, known issues, fixed issues, see What's new.

Citrix Enterprise Browser - 121.1.1.26

- Simplified single sign-on for Web and SaaS apps through the Global App Configuration service

For more information on features, technical preview features, known issues, fixed issues, see What's new.

Workspace Platform - 2402

- Create multiple Workspace URLs - General Availability (GA)

For more information on features, technical preview features, known issues, fixed issues, see What's new.

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

App Protection

May 18, 2026

App Protection is a feature for the Citrix Workspace app that provides enhanced security when using virtual desktops, virtual apps, web and SaaS apps. App Protection is supported for on-premises Citrix Virtual Apps and Desktops deployments, and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) with StoreFront and Workspace. It means that App Protection is supported on all cloud environments, on-premises environments, and hybrid environments. App Protection is also supported when you are connecting to StoreFront or Workspace via ADC Gateway.

For more information on App Protection features, see Features and Configure sections.

After buying this feature, make sure you enable the App Protection license.

> **Disclaimer:**
>
> App Protection policies work by filtering access to required functions of the underlying operating system (specific API calls required to capture screens or keyboard presses). Doing so means that App Protection policies can provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys might emerge. While we continue to identify and address them, we can't guarantee full protection in specific configurations and deployments.
>
> Citrix App Protection policies work effectively with underlying operating system components, including ICA files. Citrix might not provide support if intentional tampering or modification of the underlying components is detected, to provide the integrity of policies applied.

App Protection behavior on different environments

The behavior of App Protection depends on how you access the resources that are configured with App Protection policies. These resources include Virtual Apps and Desktops, internal web apps, and SaaS apps. You can access these resources using a supported native Citrix Workspace app client or a web browser. App Protection performs varyingly on different environments:

- **Unsupported Citrix Receivers or Citrix Workspace apps** - The resources that are configured with App Protection policies are not available.
- **Supported Citrix Workspace app versions** - The resources that are configured with App Protection policies are available and launches properly.
- **Hybrid launch using Workspace store URL** - The resources that are configured with App Protection policies are always available. To successfully launch the resources on a web browser using the Workspace store URL, see App Protection for hybrid launch for Workspace.

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

- **Hybrid launch using StoreFront store URL** - The resources that are configured with App Protection policies are not available if the StoreFront customization is not deployed. To successfully launch the resources on a web browser using the StoreFront store URL, see App Protection for hybrid launch for StoreFront.

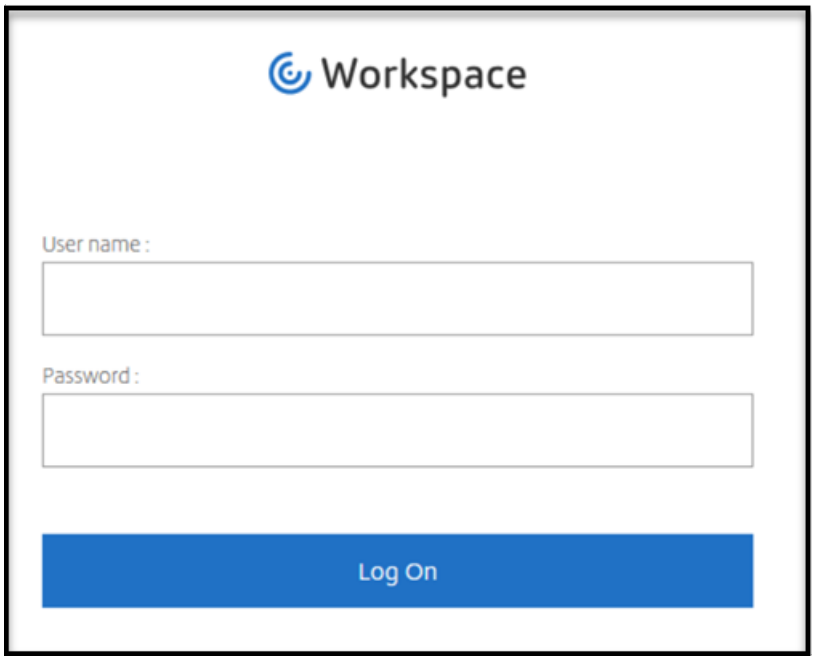
Protection is applied under the following conditions:

- **Anti-screen capture** –For Citrix Workspace app for Windows and Citrix Workspace app for Mac, it is enabled if any protected window is visible on the screen. To disable protection, minimize all protected windows. For Citrix Workspace app for Linux, it is enabled if any protected window is active. To disable protection, close all protected windows.
- **Anti-keylogging** –Enabled if a protected window is in focus. To disable protection, change focus to another window.

What does App Protection protect?

App Protection protects the following Citrix windows:

- Citrix® sign in windows

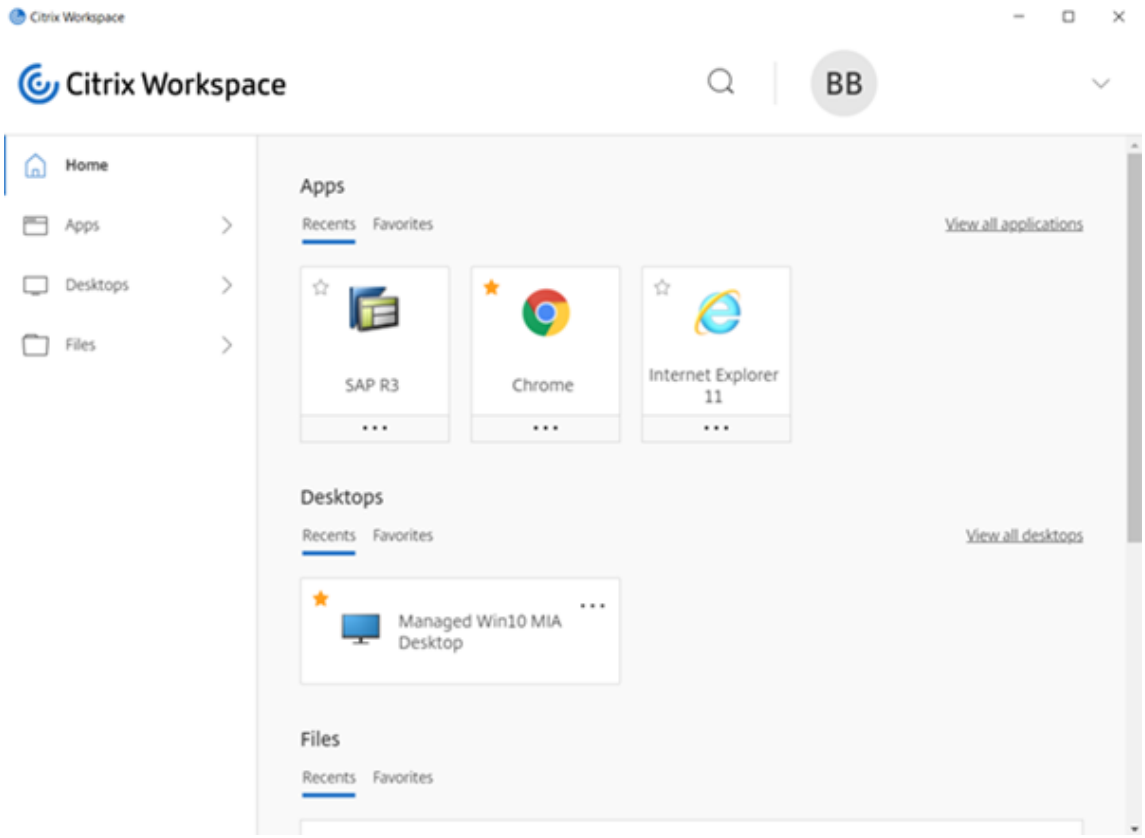


- Citrix Workspace app HDX session windows (For example, managed desktop)

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



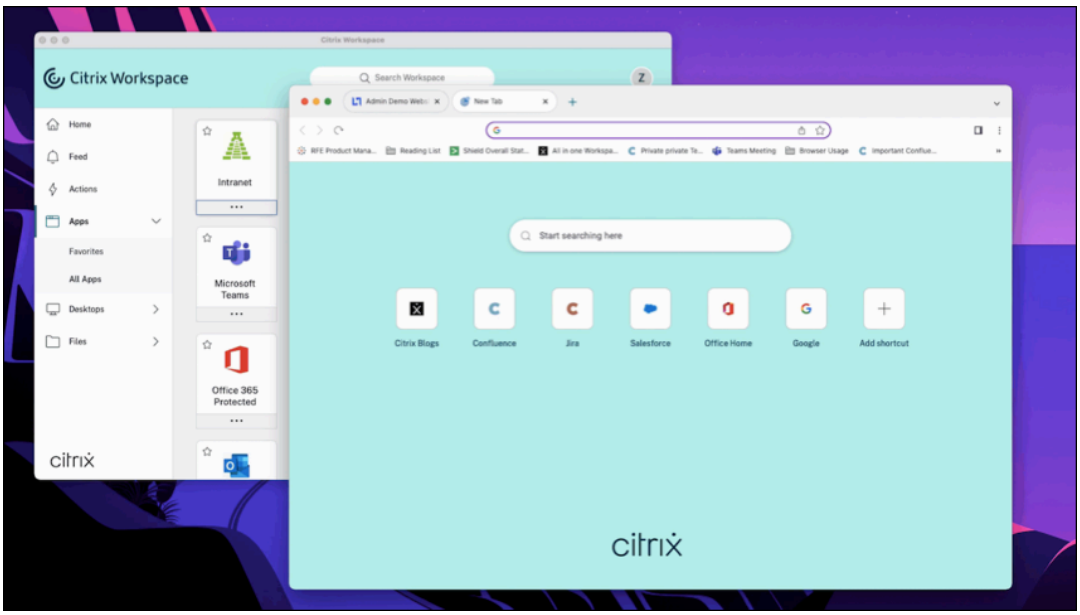
- Self-Service (Store) windows



- Web and SaaS apps
  - Citrix Workspace app for Windows and Citrix Workspace app for Mac - Web and SaaS apps open in the Citrix Enterprise Browser. If the apps are configured to have the App Protection

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

policies through the Citrix Secure Private Access, then App Protection is applied on a per tab basis.



- Citrix Workspace app for Linux - Citrix Enterprise Browser is not supported.

> **Note:**
>
> To offer the App Protection solution, few Citrix signed DLLs such as `ctxapclient32.dll` and `ctxapclient64.dll` are injected into all processes. Until Citrix Workspace app for Windows versions 2405.12 and 2402 CU3, an additional DLL, `FeatureFlagHelper32.dll` and `FeatureFlagHelper64.dll` was being injected. These DLLs are harmless and it is safe to have the traces of these DLLs in the log files of other processes.

What doesn't App Protection protect?

- The following items under the Citrix Workspace apps icon in the navigation bar:
  - Connections Center
  - All links under Advanced Preferences
  - Personalize
  - Check for Updates
  - Sign Out
- If you choose to protect a virtual desktop with anti-screen-capturing, users can still screen share from apps within the virtual desktop. However, for the apps outside of the virtual desktop, you can't take screenshots, or record the virtual desktop.

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

Limitations

The following limitations exist by design:

- App Protection enabled virtual apps and desktops are blocked from launching when accessed within RDP sessions.
- Within the RDP session, App Protection isn't supported on the Web and SaaS apps opened using the Citrix Enterprise Browser.
- App Protection is not supported if you're on an unsupported version of the Citrix Workspace app or Citrix Receiver. In that case, resources are hidden.
- When the App Protection features are applied to virtual apps and desktops, outgoing screen sharing might be affected if optimization is used.
- Citrix Workspace app with App Protection might not be compatible with some other security solutions or apps using similar underlying technology.
- App Protection is not supported when you launch resources from within the Citrix Secure Browser, or with Remote Browser Isolation.
- In Citrix Workspace app for Linux, you're unable to use snap applications when App Protection is installed.
- Anti-Screen capture enabled resources appear grey when using DisplayLink to connect to external monitors on Mac. This is because DisplayLink on Mac uses Screen Recording technology to cast the screen and will be blocked by App Protection. As an alternative, end users can use cable based connectors (for example, USB Type C) to connect to external monitors.

Contextual App Protection

Contextual App Protection provides the granular flexibility to apply the App Protection policies conditionally for a subset of users - based on users, their device, and the network posture. For more information, see the following articles:

- Contextual App Protection for StoreFront
- Contextual App Protection for Workspace

App Protection for hybrid launch

Hybrid launch of Citrix Virtual Apps and Desktops is when you log in to Citrix Workspace app through the browser (Citrix Workspace for Web), and use the applications through the native Citrix Workspace app. The term hybrid is the result of users applying the combination Citrix Workspace app for Web and the native Citrix Workspace app to connect and use the resources. App Protection supports hybrid launch in Workspace and StoreFront. For more information, see the following articles:

- App Protection for hybrid launch for Workspace

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

- App Protection for hybrid launch for StoreFront

System requirements and compatibility

June 3, 2026

System requirements

As a prerequisite, make sure that you have installed the Citrix Workspace app using administrator rights.

Minimum versions of Citrix® components

- Citrix Workspace app 24.9.0 for iOS
- Citrix Workspace app 2108 for Linux
- Citrix Workspace app 2203.1 LTSR for Windows
- Citrix Workspace app 2002 for Windows
- Citrix Workspace app 2305.1 for Windows (Store)
- Citrix Workspace app 2001 for Mac
- Citrix Workspace app 25.7.0 for Android
- StoreFront 1912 LTSR
- Delivery Controller™ 1912
- Valid Citrix licenses. For more information, contact your Citrix Sales Representative or Citrix Partner.

> **Note:**
>
> If the users are on devices or Workspace app versions that don't support App Protection, then they can't access the protected resources. The protected resources include Virtual Apps and Desktops and Web and SaaS apps.

Licenses

The following section explains the different types of licenses available for App Protection based on the products, platforms, and use cases.

IT-managed VDI For all editions of IT-managed VDI, App Protection is available as an add-on. For more information, see IT-managed VDI.

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

Citrix DaaS™ for Hyperscalers

- Azure
- Google
- AWS

Citrix DaaS In the Feature Matrix for Citrix DaaS article, navigate to **DaaS cloud Services > Security and Monitoring > App Protection**.

Citrix Secure Private Access App Protection is available as a standalone attachment for Citrix Secure Private Access. For more information, navigate to **Citrix cloud services > Citrix Secure Private Access** in the Service descriptions for Citrix Services article.

Citrix Universal™ subscription App Protection is included with the following services:

- Citrix Universal Premium
- Citrix Universal Premium Plus

It is available as an add-on with the following editions:

- Citrix Universal Advanced
- Citrix Universal Advanced Plus

For more information, see this article.

Operating system platforms

App Protection policies runtime is installed on the endpoint that you are connecting *from* and not on the VDA you are connecting *to*. So, only the operating system version of the endpoint is significant. (App Protection can connect to VDAs hosted on any supported operating systems described in Citrix Virtual Apps and Desktops System requirements.)

The App Protection feature is supported on endpoints running the following operating systems:

- **Windows:**
  - Windows 11 (64-bit Edition and ARM64 Editions)
  - Windows 10 (32-bit and 64-bit Editions)

    > **Note:**

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

> Starting with Citrix Workspace app for Windows version 25.7.0, App Protection is supported on the devices with Arm64 edition of the Windows operating system.

- **macOS:**
  - High Sierra (10.13) or higher
- **Linux:**
  - 64-bit Ubuntu 22.04
  - 64-bit Ubuntu 24.04
  - 64-bit RHEL 9
  - ARM64 Raspberry Pi OS (Debian 11 Bullseye, Debian 12 Bookworm)

> **Note:**
>
> App Protection is supported from eLux 7 onwards.
>
> For App Protection, Citrix Workspace app for Linux requires a Gnome Display Manager along with the supported operating systems. Supported GNOME versions is till GNOME 42.5 and GNOME 46 or later.
>
> App Protection supports Ubuntu 24.04 and Raspberry Pi OS (Debian 12 Bookworm) starting with Citrix Workspace app Linux 2411 or higher.

- **iOS**
  - iOS 18
  - iOS 17
  - iOS 16
- **Android**
  - Android 12
  - Android 13
  - Android 14

> **Note:**
>
> Currently, anti-screen capture is supported on Android, but anti-keylogging is not. Therefore, if you try to launch a resource which has anti-keylogging enabled, launch will fail.

Compatibility matrix

Compatibility matrix for Citrix Cloud based products

App Protection features compatible with Citrix Cloud based products are as follows:

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

Feature	Citrix Cloud™	Citrix Cloud Japan
Anti-keylogging and Anti-screen capture for virtual apps and desktops	Yes	Yes
Anti-keylogging and Anti-screen capture for web or SaaS apps	Yes	No
Anti-DLL for Windows	Yes	Yes through Group Policy Object (GPO)
Anti-DLL Allow Listing	Yes	Yes through GPO
Global App Configuration service (GACS)	Yes	No
Authentication or Self-Service plug-in screen protection for Linux	Yes	Yes through AuthManConfig.xml
Authentication or Self-Service plug-in screen protection for Mac	Yes through GACS	Yes through GACS
Authentication or Self-Service plug-in screen protection for Windows	Yes	Yes through GPO
CAS App Protection ScreenShot events	Yes	No
Contextual App Protection	Yes	Yes based on the user
Policy Tampering Detection	Yes	Yes
App Protection Posture Check	Yes	Yes
Local App Allowlisting or Filter - Windows	Yes	Yes through GPO
Local App Protection - Windows	Yes	Yes through GPO

App Protection features

September 28, 2026

This article highlights the App Protection features supported by Citrix Workspace app for Windows,

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

Citrix Workspace app for Linux, and Citrix Workspace app for Mac.

Anti-keylogging

For Citrix Workspace™ app for Windows, Linux, and Mac

With encryption, App Protection's anti-keylogging capabilities scramble the text the user is typing for both physical and on-screen keyboards. The anti-keylogging feature encrypts the text before any keylogging tool can access it from the kernel or OS level. A keylogger installed on the client endpoint reading the data from the OS or driver captures the hashed text instead of the keystrokes that the user is typing. App Protection policies are active not only for published applications and desktops, but for Citrix Workspace authentication dialogs as well. Your Citrix Workspace is protected from the moment when your users open the first authentication dialog. App Protection scrambles keystrokes, returning indecipherable text to key loggers.

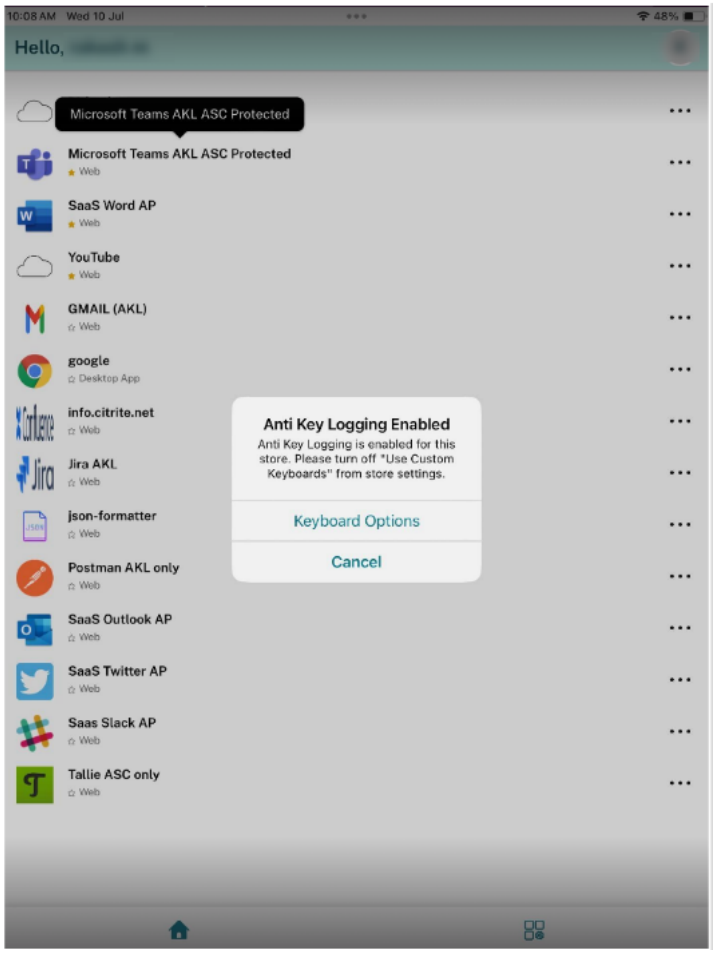
The admins can choose to enable anti-keylogging for the following types resources:

- Virtual Apps and Desktops
- Internal web and SaaS apps
- Authentication screens
- Self-Service plug-in (SSP) screens

For Citrix Workspace app for iOS

This feature protects against keylogging attempts at the application level, ensuring that sensitive information entered into protected applications remains secure. This feature allows you to use only the Apple provided default keyboards ensuring that keystrokes entered into protected applications cannot be captured. App Protection prevents the usage of custom keyboards as part of the anti-keylogging feature. If you have enabled custom keyboards, you can disable them and then continue using the resources that are enabled using App Protection's anti-keylogging feature.

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



The admins can choose to enable anti-keylogging for the following:

- Virtual Apps and Desktops
- Web and SaaS apps opened through WebView
- Authentication screens

For more information about configuring the App Protection feature, see Configure App Protection.

Citrix Workspace app for Android

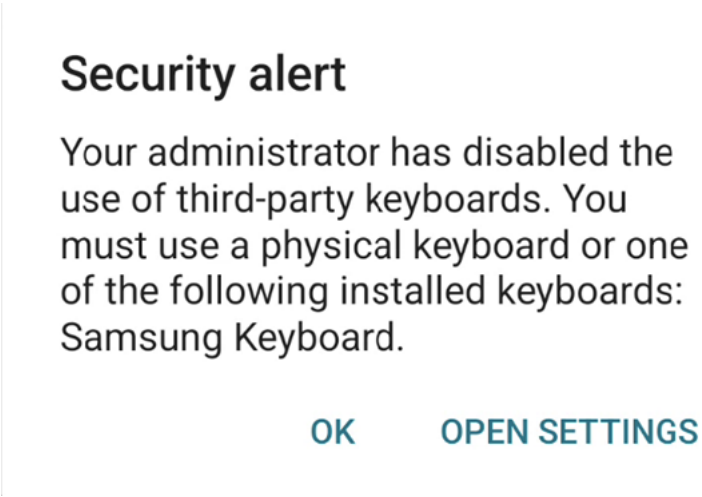
Starting from the 25.7.0 version, Citrix Workspace app for Android supports the App Protection Anti-Keylogging feature.

After anti-keylogging is enabled, the following restrictions apply:

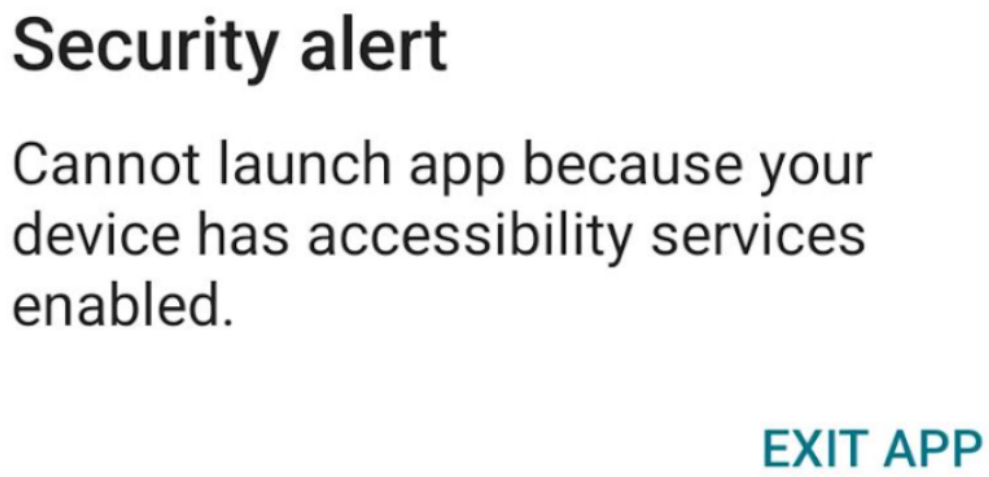
- A user can't use a non-OEM keyboard on anti-keylogging enabled resources. For example, a user has to use the Samsung Keyboard on a Samsung device.
  If a user is using a non-OEM software keyboard, then during launch of the resource, the keyboard

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

gets blocked. The user can then continue with the launch and use a physical keyboard or must go to the settings and change the keyboard to the OEM keyboard.

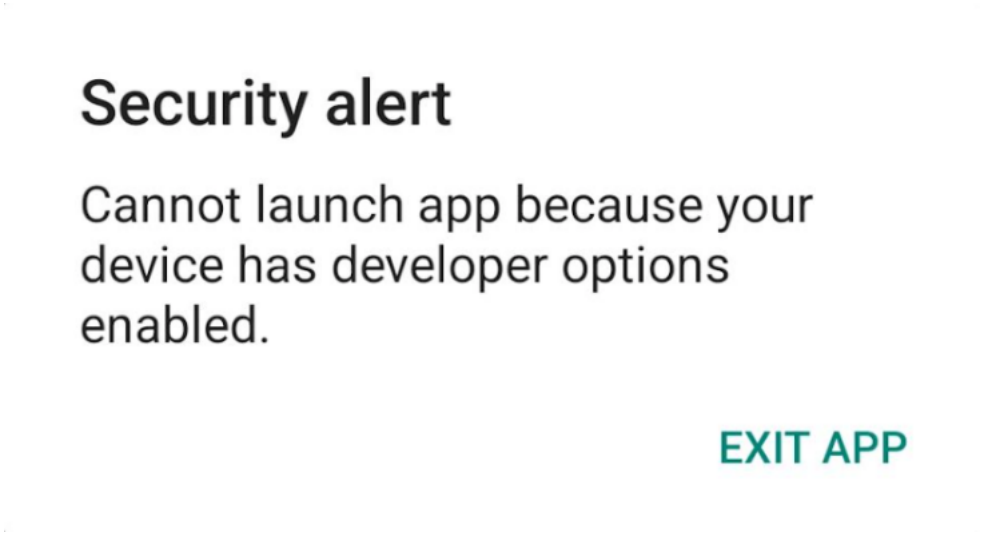


- Accessibility service has to be disabled.
  In case accessibility service enabled, resource launch is blocked with the following error:



- Developer mode has to be disabled.
  In case developer mode is enabled, launch is blocked with the following error:

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



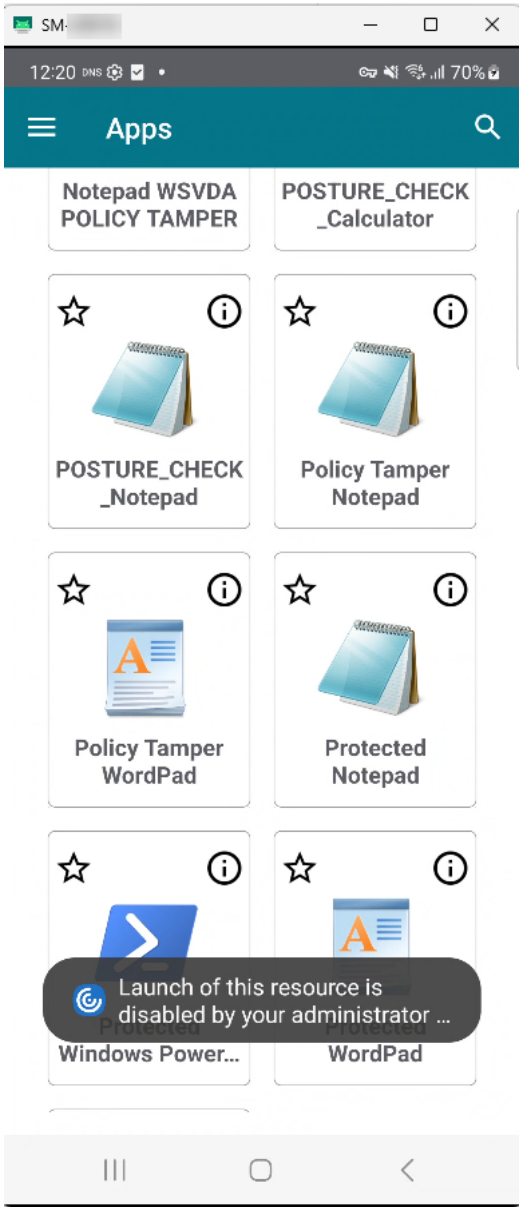
Recommendations Turn on Root detection. A rooted device significantly reduces the security posture of the end user. We recommend you to turn on the Root Detection feature. Click here for instructions.

Feature limitations We do not support anti-keylogging on **Custom Chrome** Tab and **Custom Portal**.
If you install the Citrix Workspace app on a managed device, the administrative app primarily governs its security. In this setup, the admin app retains comprehensive control over the device and might capture keystrokes even when Anti-Keylogging is enabled.

Earlier versions (prior to 25.7.0) For Citrix Workspace app for Android versions prior to 25.7.0, the anti-keylogging feature is not supported. When you attempt to open an app with anti-keylogging enabled, the app fails to launch and displays the following error message:

"**Launch of this resource is disabled by your administrator for security reasons**"

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



Anti-screen capture

For Citrix Workspace app for Windows, Linux, and Mac

Anti-screen capture prevents an app from trying to take a screenshot or recording the screen within a virtual app or desktop session. The screen capture software can't detect content within the capture region. The area selected by the app grays out, or the app captures nothing instead of the screen section that it expects to copy. The anti-screen capture feature applies to snip and sketch, Snipping Tool, and **Shift+Ctrl+Print Screen** on Windows.

Another use case for anti-screen capture is preventing sharing of sensitive data in a virtual meeting or

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

web conferencing applications like GoToMeeting, Microsoft Teams, or Zoom. App Protection prevents unintended sharing by returning a blank screen in web conferences when apps are protected. This feature makes sure that the sensitive data isn't accidentally leaked from the organization. This feature can help with compliance in regulated industries, as the intention is not considered when disclosing a data breach.

The admins can choose to enable anti-screen capture for the following types resources:

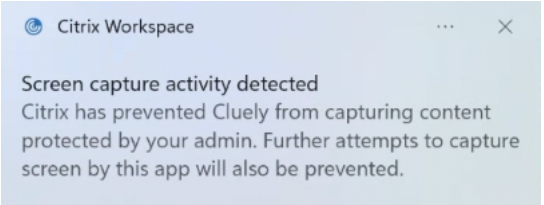
- Virtual Apps and Desktops
- Internal web and SaaS apps
- Authentication screens
- Self-Service plug-in (SSP) screens

> **Note:**
>
> If you have launched two virtual desktops where one virtual desktop is enabled with the Anti-screen capture feature and the other virtual desktop isn't enabled with the Anti-screen capture feature, then the Anti-screen capture feature is applicable for both the virtual desktops. You can't take the screenshot of either virtual desktops.
>
> In case if you have minimized the virtual desktop that is enabled with Anti-screen capture, the Anti-screen capture feature is still applicable for the virtual desktop without the Anti-screen capture feature.

Screen capture detection and notification For Citrix Workspace app for Windows, you can view a notification when a possible attempt of screen capture is made on any protected resources. For information on the resources protected by App Protection, see What does App Protection protect?

The notification appears when there is an:

- attempt to take a screenshot or record video through a screen-capturing tool.
- attempt to take a screenshot through the Print Screen key.



For steps to disable screen capture notifications, refer to the documentation Disable screen capture notifications.

> **Note:**
>
> The notification appears only once per running instance of the screen capture tool. The notifica-

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

> tion appears again if you relaunch the tool and try to capture the screen.

For Citrix Workspace app for iOS

Starting with the 24.9.0 version, Citrix Workspace app for iOS supports the anti-screen capture feature. 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.

The anti-screen capture is supported on both single and multi-monitor scenarios. To enable the feature, perform the configuration steps mentioned at the Configuration section.

The admins can choose to enable anti-screen capture for the following:

- Virtual Apps and Desktops
- Web and SaaS apps opened through WebView
- Authentication screens

Anti-screen capture support This feature prevents unauthorized screen captures, recordings, QuickTime screen mirroring, screen sharing, and app switching. Anti-screen capture feature is available for authentication screen, web or SaaS apps, and Citrix Virtual Apps and Desktops. When you capture a screen, a custom message **Screen Capture is disabled by your administrator for security reasons** is shown in the capture media instead of the actual content displayed on the screen. Anti-screen capture protects against various forms of unauthorized screen access such as:

- **Screenshot:** Prevents screenshots from being taken.
- **Screen recording:** Blocks screen recording software.
- **Screen mirroring:** Disables mirroring of the screen to other devices.
- **Screen share:** Restricts screen sharing functionality.
- **App switcher:** Prevents sensitive information from being visible in app switcher previews.

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



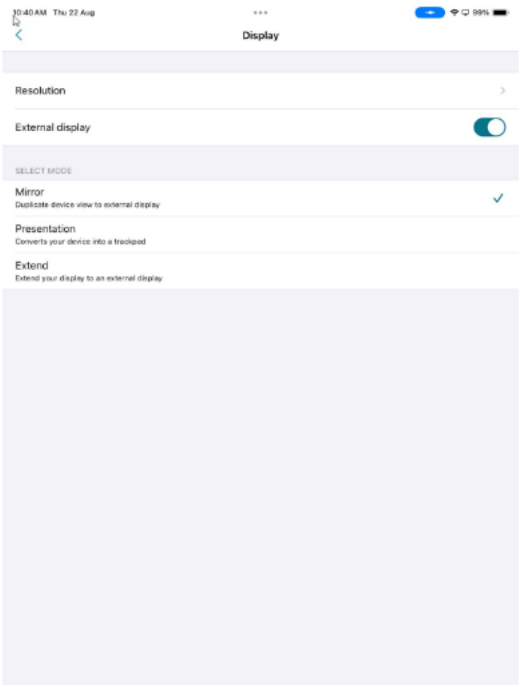
Behavior of Resources with Anti-Screen Capture Enabled in Multi-Monitor Setups Multi-monitor mode refers to the configuration in which an iOS or iPadOS device is connected to an external display, allowing the device to use multiple screens simultaneously.

There are three modes supported:

- **Mirror:** Duplicates the iPad display on the connected external monitor.
- **Presentation:** Projects the desktop interface to the external monitor while the iPad screen functions as a trackpad.
- **Extend:** Enables different content to be shown on each display, allowing for independent views across the iPad and the external monitor.

Virtual Apps and Desktops:
The user sees the virtual app or desktop on the external monitor, depending on the selected display mode. When the user attempts to take a screenshot, the content on all screens is protected.

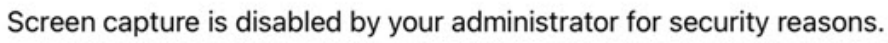
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Authentication Screens, web or SaaS apps:

On the external monitor, the user sees the following screen instead of the actual authentication screen, web or SaaS apps.

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



In all scenarios, when the user tries to capture a screenshot of an anti-screen capture enabled resource will be blocked.

For Citrix Workspace app for Android

This feature restricts the ability of clients to be compromised by screen capturing malware. Also, prevents unauthorized screen captures, recordings, mirroring, screen sharing, and app switching.

Anti-screen capture feature is available for authentication processes, web or SaaS apps, and Citrix Virtual Apps and Desktops. Citrix Workspace app for Android doesn't allow you to take screenshots. When you try to capture a screen, you get a prompt that you are not allowed to take screenshots.

The admins can choose to enable anti-screen capture for the following:

- Virtual Apps and Desktops
- Web and SaaS apps
- Authentication screens

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

Starting with the Citrix Workspace app for Android 24.7.0 version, the anti-screen capture feature is available by default. However, to enable the feature, perform the configuration steps mentioned at the Configuration section.

Limitations:

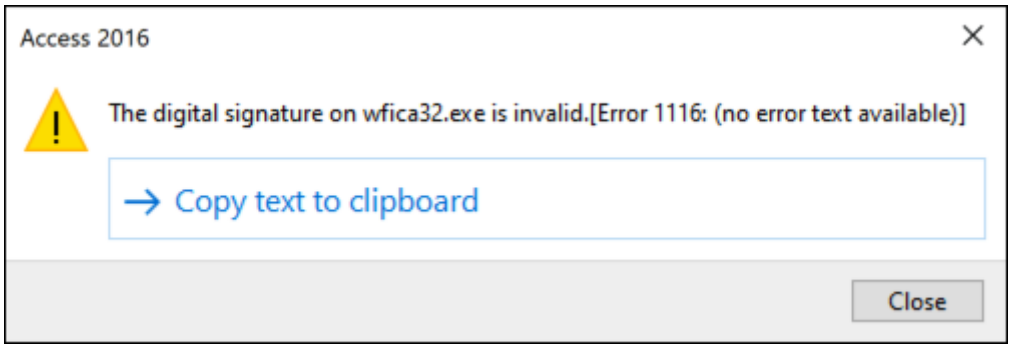
- The App Protection policies are downloaded for each store. If a store has the policies downloaded and you are moving to another store for which the policies aren't downloaded, the anti-screen capture feature isn't protected in the new store.
- The anti-screen capture feature is not supported on the authentication screens when **ChromeCustomTab** is used. However, this feature is supported when using native authentication or WebView. The **ChromeCustomTab** is enabled by default on the Cloud stores and you can change it to WebView by changing the AndroidWebViewType to webview using the PowerShell module. For more information, see Set-WorkspaceCustomConfigurations.

Anti-DLL Injection

The Anti-DLL Injection security enhancement helps protect the Citrix Workspace app from certain unauthorized dynamic-link libraries (DLL) or untrusted modules. If such untrusted modules are injected, the Citrix Workspace app detects these interventions and stops the modules from loading. Also, if any untrusted or malicious DLL is detected before the session launch, App Protection blocks the session launch and displays an error message. Closing the error message exits the virtual app and desktop session.

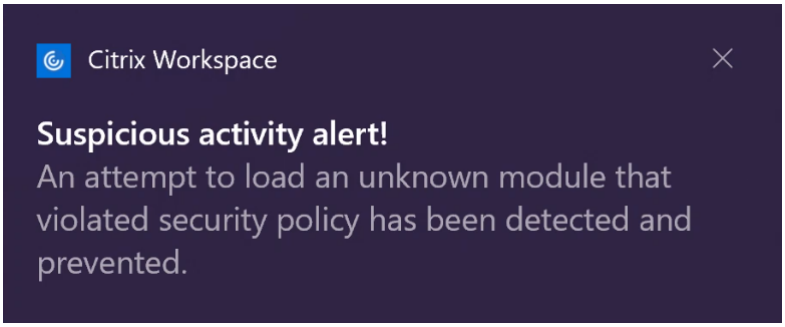
This feature is applicable for all protected virtual apps and desktops and the Citrix Workspace app authentication window (on-premises deployment/StoreFront).

This enhancement exits the session immediately when certain untrusted or malicious DLLs exist on the protected component.



The enhancement displays a notification when an untrusted or malicious DLL is blocked. Closing the message exits the virtual app and desktop session.

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



Disclaimer: This capability works by filtering access to required functions of the underlying operating system (specific API calls required to load DLLs). Doing so means that it can provide protection even against certain custom and purpose-built hacker tools. However, as operating systems evolve, new ways of loading DLLs can emerge. While we continue to identify and address them, we cannot guarantee full protection in specific configurations and deployments.

This feature support Citrix Workspace app for Windows version 2206 and later.

Compatibility with HDX™ optimization for Microsoft Teams

Optimized Microsoft Teams supports screen sharing when Citrix Workspace app is enabled with App Protection in the Desktop Viewer mode only. When you click **Share content** in Microsoft Teams, the screen picker provides the following options:

- **Window** option to share any open app - This option is displayed only if the VDA version is 2109 or later.
- **Desktop** option to share the contents on your VDA desktop - This option is displayed only for the following versions of Citrix Workspace app:
  - Citrix Workspace app for Linux version 2311 or later
  - Citrix Workspace app for Mac version 2308 or later
  - Citrix Workspace app for Windows version 2309 or later

> **Note:**
>
> For Citrix Workspace app for Linux, the Desktop share option is disabled by default. To enable it, add the `UseGbufferScreenSharing` parameter in your *config.json* file as follows:

```
mkdir -p /var/.config/citrix/hdx_rtc_engine
vim /var/.config/citrix/hdx_rtc_engine/config.json
{

      "UseGbufferScreenSharing":1
 }
```

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

Optimized Microsoft Teams enabled with App Protection also supports the Citrix virtual monitor layout which allows you to share each virtual monitor individually.

> **Limitation:**
>
> - Optimized Microsoft Teams enabled with App Protection doesn't support screen sharing on Published Desktops enabled with Local App Access (LAA).
> - Client-rendered content such as Browser content using BCR cannot be captured or shared. If you try to screen capture, it is displayed as a black screen.
>
> **Note:**
>
> For Citrix Workspace app for Linux, this feature is in Technical Preview.

Local App Protection (Preview)

App Protection offers enhanced security to defend customers against keyloggers, and accidental and malicious screen capture at endpoints. Currently App Protection capabilities are only offered for Workspace resources. With this feature, App Protection capabilities are extended to local apps on endpoints. Starting with Citrix Workspace app 2210 for Windows, App Protection can be applied to local apps on Windows devices.

Register for the Preview of this feature using the Podio form.

Policy Tampering Detection

Policy Tampering Detection feature prevents the user from accessing the virtual app or desktop session if the App Protection anti-screen capture and anti-keylogging policies are tampered. If policy tampering is detected, then the virtual app or desktop session is terminated.

> **Note:**
>
> The policy Tampering Detection feature will be enabled by default from Citrix Virtual Apps and Desktops (CVAD) version 2511 onwards.
>
> From CVAD 2511, session launches will fail if you are enabling App Protection using the `Default.ica` file. Instead, enable the policies on the delivery group from the Desktop Delivery Controller (DDC) using Web Studio or PowerShell. For more information, see Configure anti-keylogging and anti-screen capture.

To configure Policy Tampering Detection, see Configure Policy tampering detection.

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

Posture Check

To detect and block launching virtual apps and desktops that are enabled with App Protection policies from Citrix Workspace app versions that do not support the Policy Tampering Detection feature, enable App Protection Posture Check.

> **Note:**
>
> If Posture Check is enabled and you are using the Citrix Workspace app version that does not support Posture Check, then the sessions enabled with App Protection policies are terminated.
>
> When the Posture Check policy is configured on the VDA and an administrator or user attempts to connect to the VDA machine using RDP, the session disconnects because the RDP client is not capable of supporting App Protection policies.

To configure Posture Check, see Configure Posture Check.

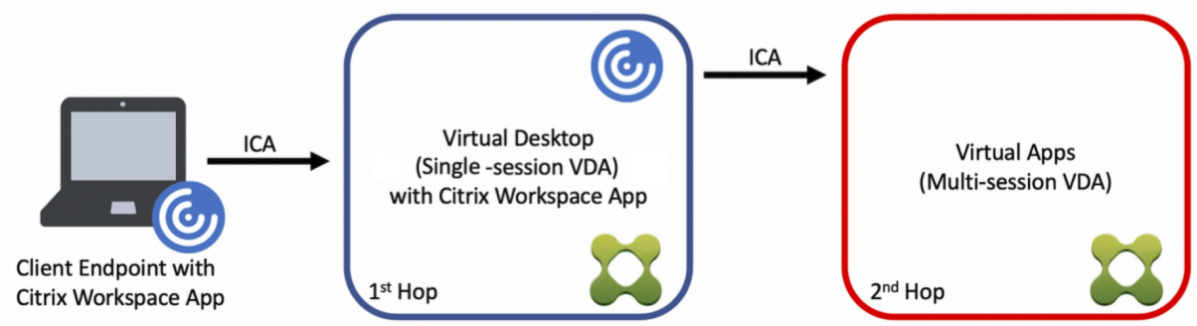
> **Limitation:**
>
> Posture Check stops working intermittently when you are using Windows Workstation VDAs hosted on Microsoft Azure with VDA 2308. This limitation is resolved in VDA version 2311 and later.

App Protection support for double-hop scenario

Starting with the Citrix Workspace app for Windows 2405 version, App Protection is supported for the double-hop scenario when installed on a workstation VDA (such as Windows 10 or Windows 11) for a single-session VDA.

Double-hop indicates a scenario where a Citrix Virtual App or Virtual Desktop session is running within a Citrix Virtual Desktop session. For more information, see Double-hop in Citrix Virtual Apps and Desktops.

The following image describes the double-hop scenario:



App Protection with double-hop means that the App Protection policies are enabled on the virtual apps and desktops that are opened from the first hop.

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

The first hop where the App Protection feature is enabled and from where you are opening the protected virtual apps or desktops can only be single-session OS VDA.

The following are the expected behaviors for App Protection with double-hop in multi-session OS VDA and single-session VDA:

App Protection in multi-session OS VDA

App Protection isn't supported in a multi-session OS VDA (such as Windows Server 2k19 or Windows Server 2k22). Hence, App Protection won't be installed in such machines.

You can install Citrix Workspace app without App Protection on a multi-session OS. However, resources that are enabled with App Protection policies don't enumerate and cannot be opened in a multi-session OS VDA.

App Protection in Single Session OS VDA

With the Citrix Workspace app for Windows 2405 version, the App Protection features are supported when installed on a workstation VDA (such as Windows 10 or Windows 11).

The following features are currently supported:

- Anti-keylogging
- Anti-screen capture

> **Limitations:**
>
> 1. **App Protection in Single Session Pooled VDA**
>
>   - Since App Protection has drivers, the Admin must perform operations such as Citrix Workspace app Upgrade and Uninstall that need a reboot on the base image.
>   - If the operations are carried out by the end user with admin privileges within the pooled session, it is not persisted to the base image and the machine might go into an inconsistent state.
>
> 2. Launching AntiScreencapture enabled resources in Double Hop is not supported when Display Capture is configured to use DDAPI (Display Device API).

What scenario is supported?

When the second hop virtual app or desktop enabled with anti-screen capture and anti-keylogging is opened within the first hop virtual desktop session, it is protected from screen capture and keylogging tools that are running within the first hop virtual desktop session.

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

What scenario is not supported?

- If the first hop virtual desktop doesn't have App Protection policies enabled, it is possible for screen capture and keylogging tools installed on the client endpoint to capture screens or keystrokes even when the second hop has App Protection policies enabled.
- If the end user is accessing the first hop machine using an RDP session, App Protection for the second hop isn't supported.

This feature is enabled by default. Therefore needs no separate configuration. The admin needs to configure the App Protection policies for the resources.

Recommendation for end-to-end protection

To have end-to-end protection, it is recommended to enable App Protection policies on each hop (both first and second). This way, keylogging, and screen capture tools running either on the client or the first hop isn't able to capture the sensitive content of the second hop session.

Block double-hop launch

App Protection features aren't supported in a double-hop scenario when using the Citrix Workspace app for Windows versions older than 2405. You are allowed to open virtual apps, desktops, web apps, or SaaS apps that are enabled with App Protection policies in a double-hop scenario. However, the App Protection features are not applied.

You can block the opening of virtual apps, desktops, web apps, or SaaS apps enabled with the App Protection feature in a double-hop scenario.

For more information about enabling the Block Double-hop Launch setting, see Enable Block Double-Hop Launch setting.

Citrix Analytics Service for App Protection

When you use Citrix Virtual Apps and Desktops, user events corresponding to their activities and actions are generated. Citrix Analytics for Security has a feature named **Self-service search** that records those user events and provides you the insights about them. **Self-service search** enables you to find, filter, and explore those user events so that you can understand what user event is done and act depending on the severity of the event. For more information about **Self-service search**, see Self-service search.

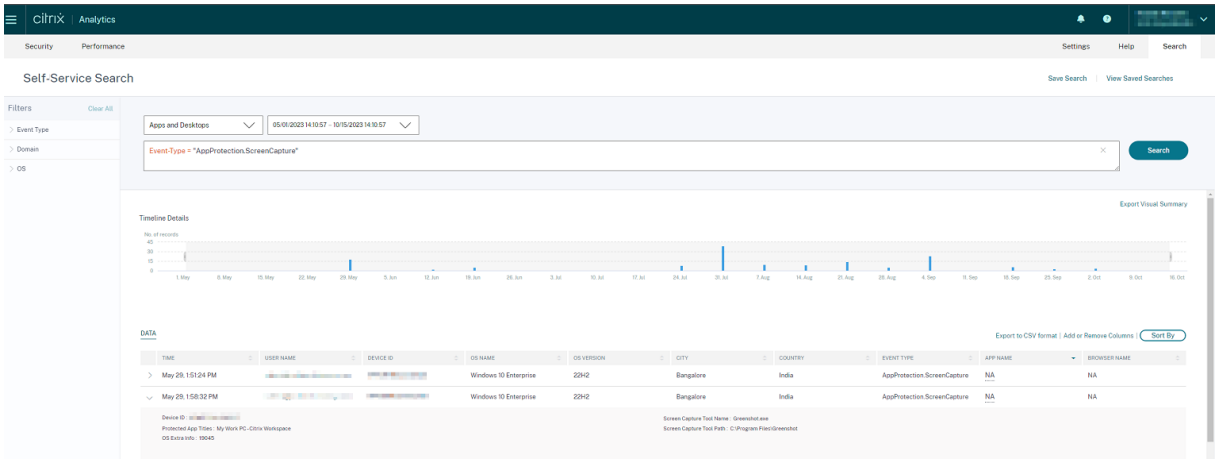
Self-service search for Apps and Desktops has an event type `AppProtection.ScreenCapture` that allows you to determine if any attempts are made to take screenshots of the virtual apps or

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

desktops that are enabled with App Protection policies. For more information about how to search for a user event, see Specify search query to filter events.

This service provides the following information:

- Device ID
- Protected App Titles
- OS Extra Info
- Screen Capture Tool Name
- Screen Capture Tool Path



Screen Capture Allow List

If Citrix Workspace app, virtual apps and desktops, or SaaS apps are enabled with the App Protection Anti-screen capture policy, then you can't capture their screens using any screen-capturing tool.

However, starting from the Citrix Workspace app for Windows 2402 release, the Screen Capture Allow List feature enables you to add an app to the screen capture allow list. This feature enables you to use the allow listed app and capture the screen of the resource enabled with the App Protection Anti-screen capture policy. To add an app to the screen capture allow list, see Configure the Screen Capture Allow List.

> **Important:**
>
> It isn't recommended to run an allow-listed app on your device for a longer period because it decreases the security posture. You can use the allow-listed apps for sharing your screen temporarily during scenarios such as troubleshooting. It is recommended to adhere to the following conditions:
>
> - Run the allow-listed app for a short period along with the resource enabled with the App Protection Anti-screen capture feature.

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

- Terminate the allow-listed app immediately after the required task is completed.
- Add a watermark when sharing the screen while using the resource enabled with the App Protection Anti-screen capture feature for more security.

Screen capture allow list needs to be configured in GACS. The feature is compatible with both on-premises and Cloud environments, provided GACS is configured.

Process exclusion list

When you launch any process or application on your device, App Protection DLLs are injected into each process if the App Protection is enabled. Sometimes, this might cause the process or application not to work due to compatibility issues with the DLL.

Starting from the Citrix Workspace app for Windows 2402 release, you can add any process to the Process exclusion list to avoid the injection of the App Protection DLL into that particular process and recover from any compatibility issues caused by the presence of App Protection DLLs. To configure the Process exclusion list, see Configure Process exclusion list.

Important:

It's not recommended to exclude processes as it decreases the security posture. You can use this to temporarily unblock the usage of the application and raise a support ticket for further investigation.

Process exclusion list needs to be configured in GACS. The feature is compatible with both on-premises and Cloud environments, provided GACS is configured.

USB Filter Driver Exclusion List

Important:

USB filter driver exclusion list needs to be configured in GACS. The feature is compatible with both on-premises and Cloud environments, provided GACS is configured.

Sometimes, when you're using specialized external keyboards such as gaming keyboards with the Citrix Workspace app, the App Protection USB Filter Driver might cause compatibility issues and block you from using the keyboard.

Starting from the Citrix Workspace app for Windows 2402 release, the USB Filter Driver Exclusion List feature allows you to exclude any USB device that has compatibility issues with the Citrix Workspace app using the device Vendor ID and Product ID. To add any device to the USB Filter Driver Exclusion List, see Configure USB Filter Driver Exclusion List.

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

> **Note:**
>
> It isn't recommended to exclude devices permanently. Use this feature to temporarily unblock the user from using the device and raise a support ticket to investigate the compatibility issue further.

Allow list for the apps which use LD_PRELOAD functionalities for Citrix Workspace app for Linux

App protection blocks the launch of a protected session if other apps using LD_PRELOAD are running. To allow legitimate apps, you can configure the allow list feature with admin approval. This feature is only for Citrix Workspace app for Linux.

To enable the feature, perform the configuration steps mentioned at the Configure allowlist LD_PRELOAD section.

The matrix provides a one-view summary of App protection features across different platforms

Platform Feature Matrix

Feature	Windows	Mac	Linux	iOS	Android	HTML5	ChromeOS
Anti-Keylogging (Virtual Apps & Desktops)	✓	✓	✓	✓	✓	☒	☒
Anti-Screen Capture (Virtual Apps & Desktop)	✓	✓	✓	✓	✓	☒	☒
Anti-Keylogging (Web & SaaS - CEP)	✓	✓	☒	-	-	☒	☒

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

Feature	Windows	Mac	Linux	iOS	Android	HTML5	ChromeOS
Auth/Self-Service Screen Protection	✓	✓	✓	-	-	☒	☒
Screen capture allows list support	✓	☒	☒	☒	☒	☒	☒
Anti-DLL Injection	✓	☒	☒	☒	☒	☒	☒
Anti-DLL Allow Listing	✓	☒	☒	☒	☒	☒	☒
Contextual App Protection	✓	✓	✓	✓	✓	☒	☒
Dynamically enable or disable Anti-Keylogging for CVAD sessions based on device context	✓	☒	☒	☒	☒	☒	☒
Policy Tampering Detection	✓	✓	✓	✓	✓	☒	☒
App Protection Posture Check	✓	✓	✓	✓	✓	☒	☒

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

Legend

✓ Supported	⊠ Not Supported	• Not Applicable / Not Documented

Key Platform Notes

- **Linux:** App Protection activates only when the protected window is active (not just visible), unlike Windows/Mac. Enterprise Browser (Web/Saas protection) is not supported. Requires GNOME Display Manager (version up to 42.5 and 46+).
- **Mac:** DisplayLink external monitors render protected content as grey because DisplayLink uses screen recording technology that conflicts with anti-screen capture.
- **Windows ARM64:** Supported from Citrix Workspace app version 25.7.0 onwards.
- **iOS:** Supported from Citrix Workspace app version 24.9.0 minimum.
- **HTML5 / ChromeOS:** App Protection is entirely unsupported on these platforms. No features are available.
- **RDP Sessions:** Launching App Protection-enabled resources from within any RDP session is blocked by design across ALL platforms. App Protection hooks OS-level APIs on the endpoint, but the RDP protocol remotes the framebuffer before those protections can act, bypassing anti-screenshot controls.

Custom Web Store

Custom web stores allow users to have a browser-like experience in the Citrix Workspace app. Admins can configure the feature using Global App Configuration service: Getting started with Global App Configuration service REST APIs.

Prerequisites

- **Citrix Workspace app for Windows**: Version 2203 or later
- **Citrix Workspace app for Mac**: Version 2204 or later
  (For details, see About this release, Citrix Workspace app for Mac)
- **Citrix Workspace app for iOS**: Version 2511 or later
- **Citrix Workspace app for Android**: Version 2603 or later (to be added in the future)

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

Features in Technical Preview

November 26, 2025

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.

Configure App Protection

October 16, 2026

App Protection provides enhanced security when you use the Citrix Workspace app. The feature restricts the ability of clients to be compromised with keylogging and screen-capturing malware. App Protection prevents exfiltration of confidential information, such as user credentials and sensitive information displayed on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

This article explains how to configure App Protection on Citrix Workspace app on different platforms.

App Protection is available on Citrix Workspace app for the following platforms:

- Citrix Workspace app for Windows
- Citrix Workspace app for Mac
- Citrix Workspace app for Linux
- Citrix Workspace app for iOS
- Citrix Workspace app for Android

> **Disclaimer**
>
> App Protection policies filter the access to required functions of the underlying operating system. Specific API calls are required to capture screen or keyboard presses. App Protection policies provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys might emerge. While we continue to identify and address them, we can't guarantee full protection in specific configurations and deployments.

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

Citrix Workspace app for Windows

Prerequisites

- Citrix Virtual Apps and Desktops™ Version 1912 LTSR or later.
- StoreFront version 1912 LTSR or Workspace.
- Citrix Workspace app version 2203.1 LTSR or later.
- A valid App Protection license
- Starting from Citrix Workspace app version 2212, the App Protection component is installed by default during the Citrix Workspace app installation.

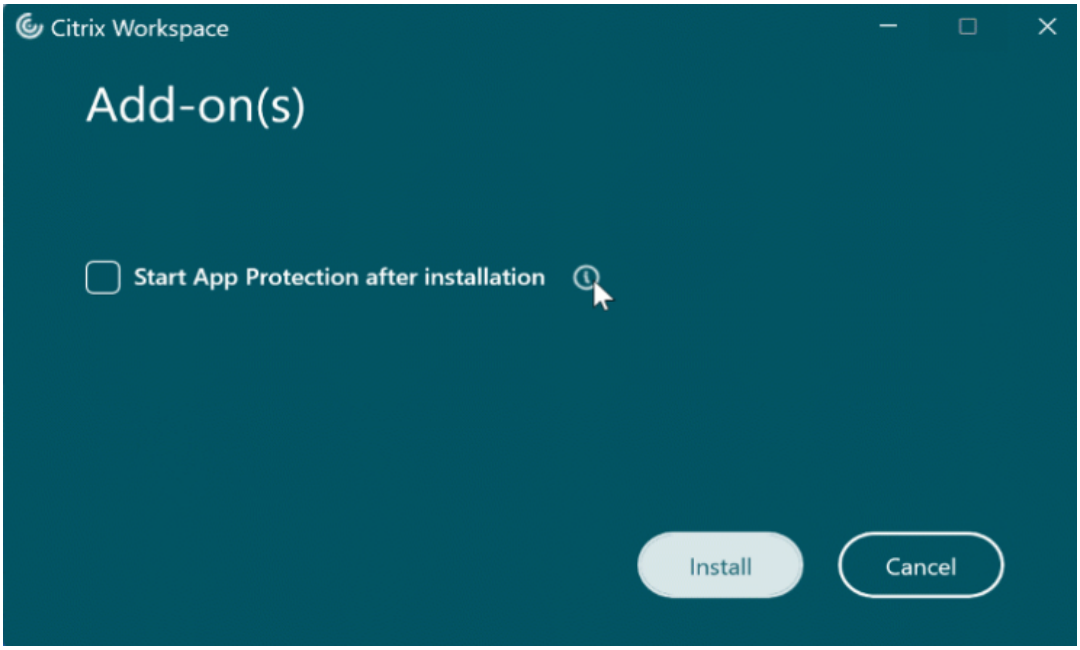
  The **Enable App Protection** checkbox that appears during the installation is replaced with **Start App Protection after installation**.

  - For Citrix Workspace app versions before 2311:



  - From Citrix Workspace app version 2311 onwards:

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



When you select this checkbox, App Protection starts immediately after the installation.

> **Note:**
>
> If you don't enable this checkbox, App Protection automatically starts upon the first start of a protected resource or component for customers who are entitled to App Protection.

Configure

Configure the following App Protection features for Citrix Workspace app for Windows:

- **Anti-keylogging and Anti-screen capture:**
  - For Virtual Apps and Desktops, see Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops.
  - For Web and SaaS Apps, see Configure Anti-keylogging and Anti-screen capture for Web and SaaS Apps.
  - For Authentication and Self-Service Plug-in:
    - Using Global App Configuration service UI, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using Global App Configuration service UI
    - Using Group Policy Object, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using Group Policy Object
    - Using API, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using GACS API
- To configure the Anti-DLL Injection feature, see Configure Anti-DLL Injection feature.

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

- To configure App Protection Policy Tampering, see Configure App Protection Policy Tampering.
- To configure App Protection Posture Check, see Configure App Protection Posture Check.
- To enable Block DoubleHop Launch setting, see Block DoubleHop Launch.

Limitations

- This feature is supported only on desktop operating systems such as Windows 11 and Windows 10.
- Starting with Version 2006.1, Citrix Workspace app isn't supported on Windows 7. So, App Protection doesn't work on Windows 7. For more information, see Deprecation.
- This feature isn't supported over Remote Desktop Protocol (RDP).

Command-line interface

You can start the App Protection component using the `/startappprotection` command line parameter. However, the previous `/includeappprotection` switch is deprecated.

The following table provides information on screens protected depending on deployment:

App Protection deployment	Screens protected	Screens not protected
Included in Citrix Workspace app	Self-service plug-in and Authentication manager / User credentials dialog	Connection Center, Devices, Citrix Workspace app error messages, Auto client reconnect, Add account
Configured on the Controller	ICA session screen (both apps and desktops)	Connection Center, Devices, Citrix Workspace app error messages, Auto client reconnect, Add account

When you're taking a screenshot, only the protected window is blacked out. You can take a screenshot of the area outside the protected window. However, if you're using the **PrtScr** key to capture a screenshot on a Windows 10 device, you must minimize the protected window.

> **Note:**
>
> This GPO policy isn't applicable for ICA and SaaS sessions. The ICA and SaaS sessions continue to be controlled using the Delivery Controller and Citrix Secure Private Access.

App Protection enhancement:

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

From Citrix Workspace app for Windows 2305 and later, anti-keylogging is enabled on the authentication and self-service plug-in screens if one of the following criteria is met:

- You have enabled App Protection using one of the following:
  - Select the **Start App Protection** checkbox during installation.
  - Start the App Protection component using the **/startappprotection** command line parameter.
- If you haven't selected the **Start App Protection** checkbox or used the **/startappprotection** command line parameter during the installation, then the anti-keylogging protection is enabled after launching the first protected resource.

> **Note:**
>
> The Global App Configuration service and Group policy objects settings override the preceding behavior. For example, if you've disabled the GACS or GPO policy for these screens, then the anti-keylogging isn't enabled on the authentication and SSP screens.

Citrix Workspace app for Linux

Starting with version 2108, the App Protection feature is now fully functional. This feature supports the Virtual Apps and Desktops, and is enabled by default. However, you must configure the App Protection feature in the `AuthManConfig.xml` file to enable it for the authentication manager and the self-service plug-in interfaces.

Installing the App Protection component

1. When you install the Citrix Workspace app using the tarball package, the following message appears: **Do you want to install the App Protection component? Warning: You can't disable this feature. To disable it, you must uninstall Citrix Workspace app. For more information, contact your system administrator. [default $INSTALLER_N]:**
2. Enter **Y** to install the App Protection component. App Protection isn't installed by default.
3. Restart your machine for the changes to reflect. App Protection works as expected only after you restart your machine.

Installing the App Protection component on RPM packages Starting with Version 2104, App Protection is supported on the RPM version of Citrix Workspace app.

To install App Protection, do the following:

1. Install Citrix Workspace app.

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

2. Install the App Protection `ctxappprotection<version>.rpm` package from the Citrix Workspace app installer.
3. Restart the system for the changes to reflect.

Installing the App Protection component on Debian packages Starting with Version 2101, App Protection is supported on the Debian version of Citrix Workspace app.

To install the App Protection component, run the following command from the terminal before installing Citrix Workspace app:

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select yes"

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

sudo apt install -f ./icaclient_<version>._amd64.deb
```

Starting with Version 2106, Citrix Workspace app introduces an option to configure the anti-keylogging and anti-screen capturing functionalities separately for both the authentication manager and self-service plug-in interfaces.

Configure

Configure the following App Protection features for Citrix Workspace app for Linux:

- To configure Anti-keylogging and Anti-screen capture for Authentication screen, see Configure using AuthManConfig.xml for authentication manager.
- To configure Anti-keylogging and Anti-screen capture for the Self-Service Plug-in screen, see Configure using AuthManConfig.xml for the Self-Service Plug-in interface.
- To configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops, see Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops.
- To configure App Protection Policy Tampering, see Configure App Protection Policy Tampering.
- To configure App Protection Posture Check, see Configure App Protection Posture Check.

Upgrade

> **Note:**
>
> App Protection service does not currently support upgrades. If it is installed alongside the Citrix Workspace app, upgrading the Citrix Workspace app might break the App Protection service and might display the following error message:

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

> *Upgrade operation is not supported while the App Protection component is installed. To upgrade, uninstall Citrix Workspace app for Linux, reboot your machine, and then install the newer version.*
>
> To prevent any issues during the upgrade, we recommend uninstalling the old version of Citrix Workspace app for Linux and restarting the machine before installing the new version. For more information, see Install, Uninstall, and Update.

Citrix Workspace app for Mac

Configure the following App Protection features for Citrix Workspace app for Mac:

- For configuring Anti-keylogging and Anti-screen capture for Authentication and Self-Service Plug-in using Global App Configuration service UI, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using Global App Configuration service UI.
- For configuring Anti-keylogging and Anti-screen capture for Authentication and Self-Service Plug-in using API, see Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using GACS API.
- To configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops, see Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops.
- To configure Anti-keylogging and Anti-screen capture for Web and SaaS Apps, see Configure Anti-keylogging and Anti-screen capture for Web and SaaS Apps.
- To configure App Protection Policy Tampering, see Configure App Protection Policy Tampering.
- To configure App Protection Posture Check, see Configure App Protection Posture Check.

Citrix Workspace app for iOS

Anti-keylogging

Prerequisites

- Citrix Virtual Apps and Desktops Version 1912 LTSR or later.
- StoreFront™ version 1912 LTSR or Workspace.
- Citrix Workspace app for iOS version 24.9.0 or later.
- A valid App Protection license.

> **Disclaimer:**
>
> App Protection policies work by filtering access to required functions of the underlying operating system (specific API calls required to capture screens or keyboard presses). This means that App Protection policies provide protection even against custom and purpose-built hacker tools. However, as operating systems evolve, new ways of capturing screens and logging keys emerge.

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

> While we continue to identify and address them, we can't guarantee full protection in specific configurations and deployments.

Configuration You can configure the **Anti-keylogging** and **Anti-screen capture** features for the following for Citrix Workspace™ app for iOS:

- **Citrix Virtual Apps and Desktops** - The **Anti-keylogging** and **Anti-screen capture** features for Citrix Virtual Apps and Desktops can be configured in DDC. The App Protection policy is applied to a delivery group in DDC. For more information, see Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops.
- **Web and SaaS apps** - The **Anti-keylogging** and **Anti-screen capture** features for Web and SaaS apps can be configured through Secure Private Access policies. For more information, see Configure Anti-keylogging and Anti-screen capture for Web and SaaS Apps.
- **Authentication screen** - The **Anti-keylogging** and **Anti-screen capture** features for the authentication screen can be configured through the Global App Configuration service and using the Unified Endpoint Management solutions.

Using Global App Configuration service You can configure the **Anti-screen capture** feature for the authentication screen using:

- Using UI
- Using API

Using UI:

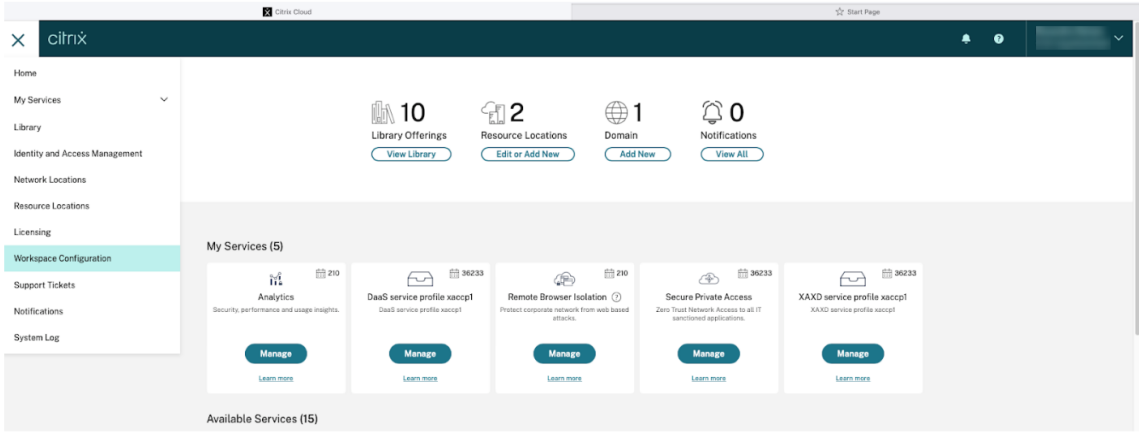
Starting with Citrix Workspace app for iOS 24.9.0 version, Citrix Workspace app allows you to configure App Protection for authentication screens using Global App Configuration service (GACS).

If you enable the anti-screen capturing functionality using the GACS, they're applicable to the authentication screen.

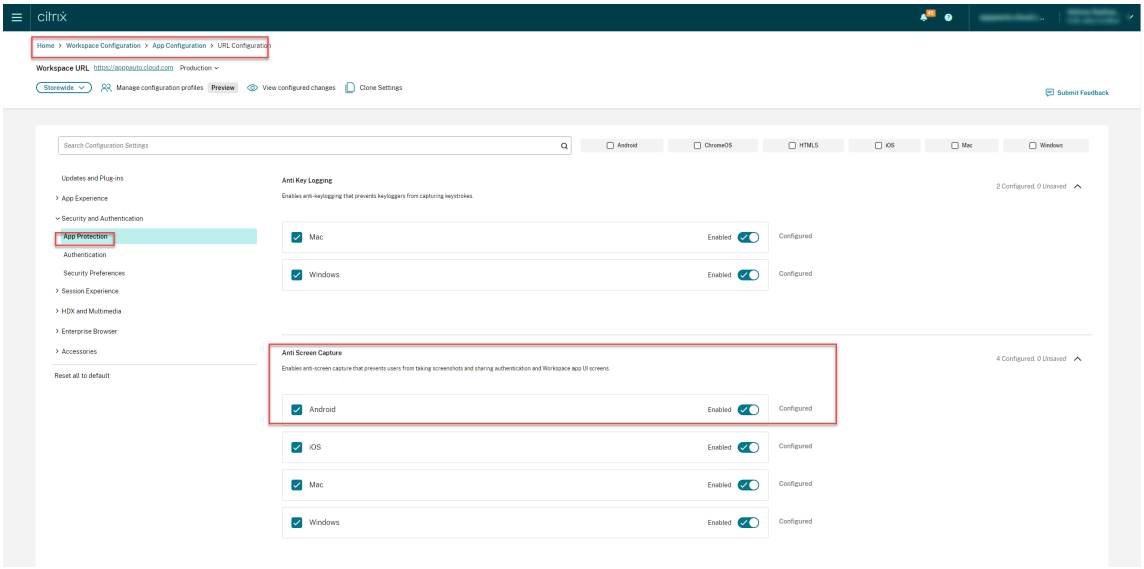
Administrators can configure App Protection using the Workspace Configuration UI:

1. Sign in to your Citrix Cloud™ account and select **Workspace Configuration**.

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

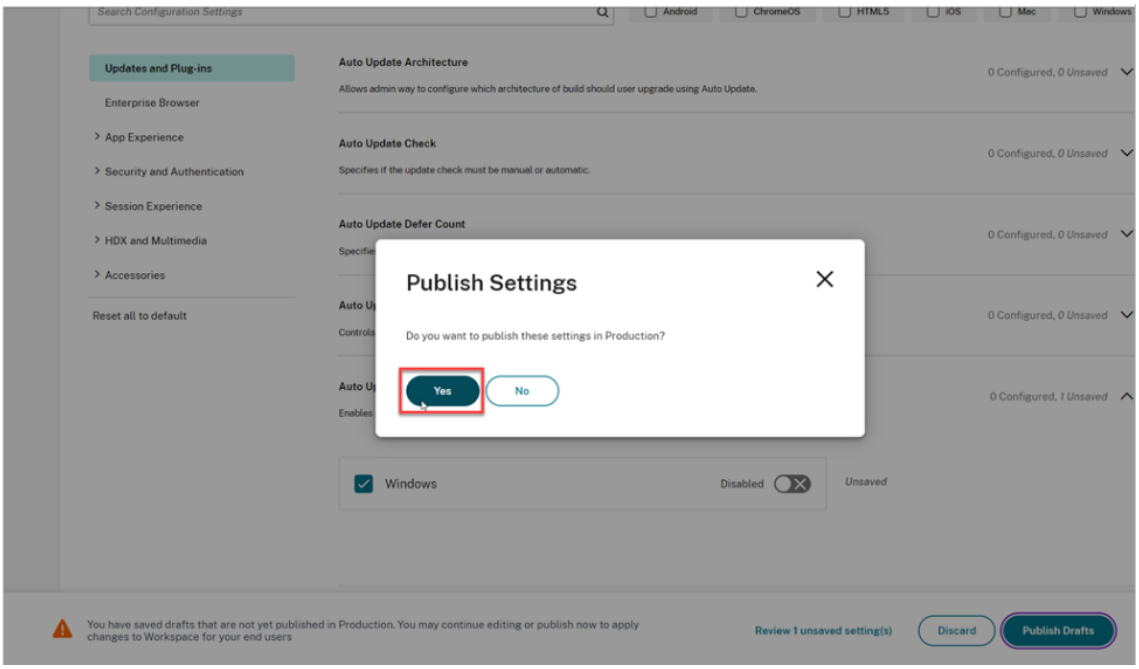


2. Select **App Configuration > Security and Authentication > App Protection**.



3. Click **Anti Key Logging** and then select the iOS Operating System.
4. Click **Anti Screen Capture** and then select the iOS Operating System.
5. Click the **Enabled** toggle button and then click **Publish Drafts**.
6. In the **Publish Settings** dialog box, click **Yes**.

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



Using API:

The administrators can use the API to configure the App Protection features. The settings are as follows for Citrix Workspace app for iOS:

Setting to enable or disable anti-screen capturing:

```
"name": "enable anti screen capture for auth" "value": "true" or "false"
```

Setting to enable or disable anti-keylogging:

```
"name": "enable anti key-logging for auth" "value": "true" or "false"
```

Example:

Following is a sample JSON file to enable anti-screen capture and anti-keylogging features for Citrix Workspace app in GACS:

```
{

          "category": "App Protection",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "settings": [{

            "name": "Enable Anti Screen Capture For Auth",
            "value": "true"
```

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

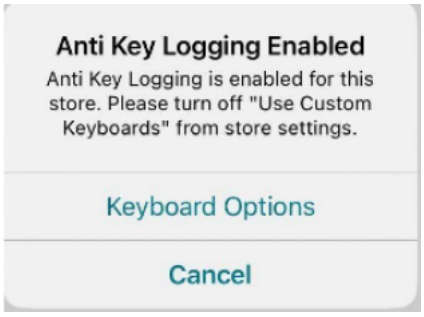
```
            }
,
           {

             "name": "Enable Anti Key Logging For Auth",
             "value": "true"
            }
]
          }
```

Using Unified Endpoint Management solutions Starting with the 24.9.0 version of Citrix Workspace app for iOS, administrators can enable App Protection feature for the authentication screen. Administrators can configure this feature using an AppConfig-based key-value pair.

- For enabling anti-screen capture:
  - Key: `enableAntiScreenCaptureForAuth`
  - value type: Boolean
  - value:
    - If set to true, the anti-screen capture feature is enabled.
    - If set to false, the anti-screen capture feature is enabled.
- For enabling anti-keylogging:
  - Key: `enableAntiKeyLoggingForAuth`
  - value type: Boolean
  - value:
    - If set to true, the anti-keylogging feature is enabled.
    - If set to false, the anti-keylogging feature is enabled.

Steps to disable custom keyboards When the anti-keylogging feature is enabled and the **Use Custom keyboards** toggle switch is turned on, you can't open virtual apps, virtual desktops, web apps, or SaaS apps and the following alert message appears:



To disable the custom keyboard, do the following:

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

1. Click **Keyboard Options** in the preceding alert dialog box.
2. Clear **Use Custom keyboards** from the store settings. The **Disable Custom Keyboards** dialog box appears.
3. Click **Exit** in the **Disable Custom Keyboards** dialog box. The **Exiting** dialog box appears.
4. Click **OK**. Citrix Workspace app exits and then restarts automatically to reflect the changes.

Limitations

- **Keylogging prevention:**

  Keylogging prevention is only effective through soft keyboards. Hardware keyboards are not protected by the anti-keylogging feature.

- **Anti-keylogging for Authentication Screen:**

  There might be conflicts due to differing policies when multiple stores are involved.

- **System browsers:**

  The anti-keylogging feature for the authentication screen is not supported when using system browsers.

- **Web interface authentication screen:**

  Anti-screen capture and anti-keylogging features aren't supported on the web interface authentication screen.

Anti-screen capture

Starting with version 24.9.0 Citrix Workspace app for iOS, the following features are enabled:

Citrix Workspace app for Android

Prerequisites

- Citrix Virtual Apps and Desktops Version 1912 LTSR or later.
- StoreFront version 1912 LTSR or Workspace.
- Citrix Workspace app for Android version 24.7.0 or later.
- A valid App Protection license

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

Configuration

You can configure the **Anti-screen capture** feature for the following:

- **Citrix Virtual Apps and Desktops** - The **Anti-screen capture** feature for Citrix Virtual Apps and Desktops can be configured in DDC. The App Protection policy is applied to a delivery group in DDC. For more information, see Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops.
- **Web and SaaS apps** - The **Anti-screen capture** feature for Web and SaaS apps can be configured through Secure Private Access policies. For more information, see Configure Anti-screen capture for Web and SaaS Apps.
- **Authentication screen** - The **Anti-screen capture** feature for the authentication screen can be configured through the Global App Configuration service and using the Unified Endpoint Management solutions.

Using Global App Configuration service You can configure the **Anti-screen capture** feature for the authentication screen using:

- Using UI
- Using API

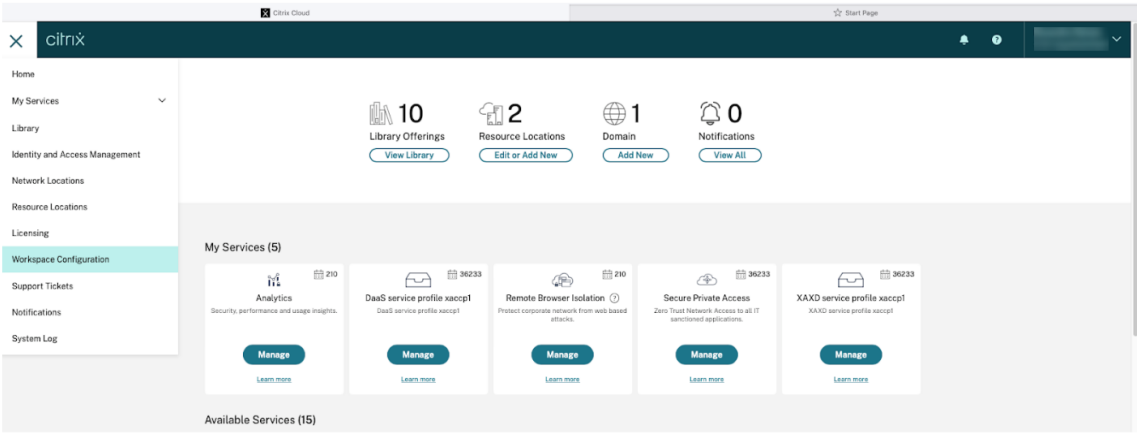
Using UI:

Citrix Workspace app allows you to configure App Protection for authentication screens using Global App Configuration service (GACS).

If you enable the anti-screen capturing functionality using the GACS, they're applicable to the authentication screen.

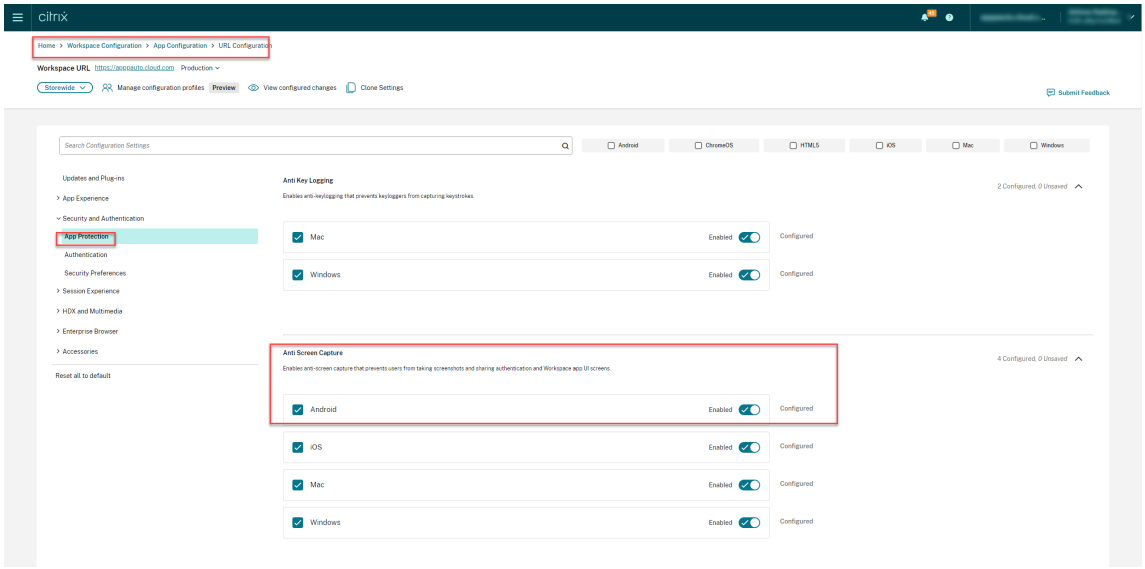
Administrators can configure App Protection using the Workspace Configuration UI:

1. Sign in to your Citrix Cloud account and select **Workspace Configuration**.

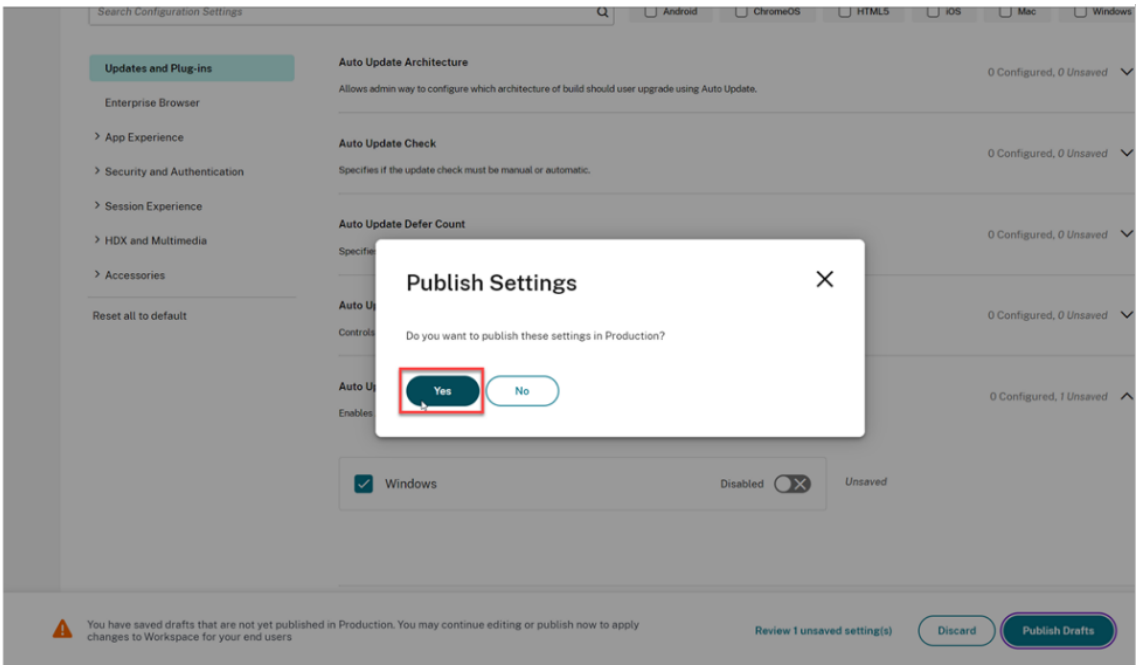


© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select **App Configuration > Security and Authentication > App Protection**.



3. Click **Anti Screen Capture** and then select the Android Operating System.
4. Click the **Enabled** toggle button and then click **Publish Drafts**.
5. In the **Publish Settings** dialog box, click **Yes**.



Using API:

The administrators can use the API to configure the App Protection feature. The setting to enable or disable anti-screen capturing for Citrix Workspace app for Android:

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

```
"name": "enable anti screen capture for auth" "value": "true"
  or "false"
```

Example: Following is a sample JSON file to enable anti-screen capture feature for Citrix Workspace app in GACS:

```
{

          "category": "App Protection",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "settings": [{

            "name": "Enable Anti Screen Capture For Auth",
            "value": "true"
           }
 ,
         ]
         }
```

Using Unified Endpoint Management solutions Starting with the 24.7.0 version of Citrix Workspace app for Android, administrators can enable the App Protection feature for the authentication screen. Administrators can configure this feature using an AppConfig-based key-value pair.

- For enabling anti-screen capture:
  - Key: `enableAntiScreenCaptureForAuth`
  - value type: Boolean
  - value:
    - If set to true, the anti-screen capture feature is enabled.
    - If set to false, the anti-screen capture feature is disabled.

Recommendation

App Protection policies are primarily focused on enhancing the security and protection of an endpoint. Review all other security recommendations and policies for your environment. You can use a **Security and Control** policy template for a recommended configuration in environments with low tolerance to risk. For more information, see Policy templates.

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

Configure Anti-keylogging and Anti-screen capture

February 26, 2026

You can configure Anti-keylogging and Anti-screen capture for the following:

- Authentication and self-service plug-in
- Virtual Apps and Desktops
- Web and SaaS apps

Configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in

You can configure Anti-keylogging and Anti-screen capture for authentication and self-service plug-in using the following methods:

Configuration method	Citrix Workspace™ app for Windows	Citrix Workspace app for Mac	Citrix Workspace app for Linux	Citrix Workspace app for iOS	Citrix Workspace app for Android
Using Group Policy Object	Yes	No	No	No	No
Using Global App Configuration service	Yes	Yes	No	Yes	Yes
Using AuthManConfig.xml	No	No	Yes	No	No

Using Group Policy Object

1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace**.
3. Depending on whether you're configuring App Protection for an authentication manager, or self-service plug-in, use one of the following steps:

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

- **Authentication manager**

  To configure anti-keylogging and anti-screen-capturing for the authentication manager, select **User authentication** > **Manage App Protection** policy.

- **Self-service plug-in interface**

  To configure anti-keylogging and anti-screen capturing for the self-service plug-in interface, select **Self Service** > **Manage App Protection** policy.

4. Select one or both the following options:

   - **Anti-key logging**: Prevents keyloggers from capturing keystrokes.
   - **Anti-screen capturing**: Prevents users from taking screenshots and sharing their screen.

5. Click **Apply** and **OK**.

Expected Behavior:

The expected behavior depends upon the method by which you access the StoreFront that has the protected resources.

Using Global App Configuration service UI

Starting with Citrix Workspace app for Windows 2302 or Citrix Workspace app for Windows 2301 versions, Citrix Workspace app allows you to configure App Protection for authentication screens and self-service plug-in using Global App Configuration service (GACS).

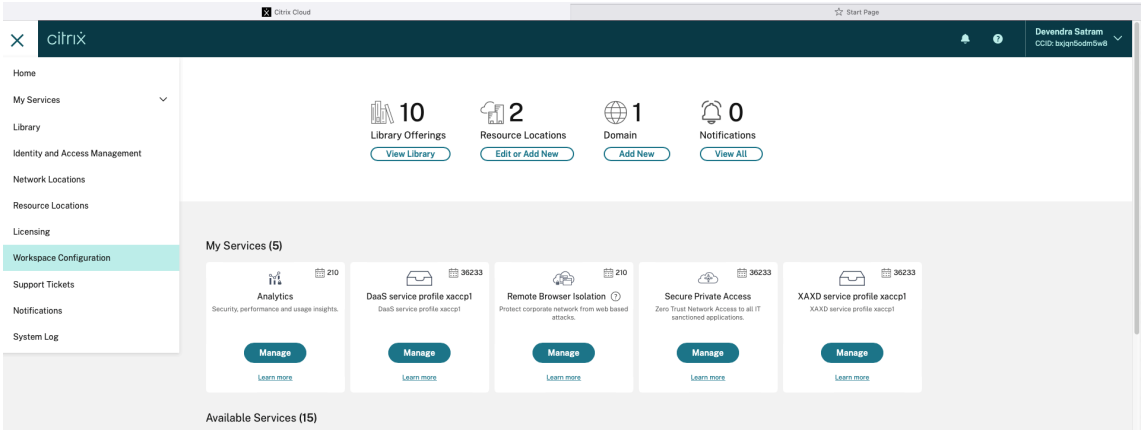
If you enable the anti-keylogging and the anti-screen capturing functionality using the GACS, they're applicable to both authentication and self-service plug-in screens.

> **Note:**
>
> - Configuring anti-keylogging or anti-screen capture for authentication and self-service plug-in using GACS is applicable for Citrix Workspace app for Windows and Citrix Workspace app for Mac. It isn't applicable for Citrix Workspace app for Linux.
> - The GACS configurations don't apply for Virtual App and Desktops, and web and SaaS apps. These resources continue to be controlled using the Delivery Controller and Citrix Secure Private Access.
> - Starting with the Citrix Workspace app for Mac 2311 version, you can configure App Protection for the Authentication and Self-Service plug-in using the Global App Configuration service UI for both cloud stores and on-premises. However, if you're using Citrix Workspace app for Mac earlier than the 2311 version, then you can configure it only for cloud stores.

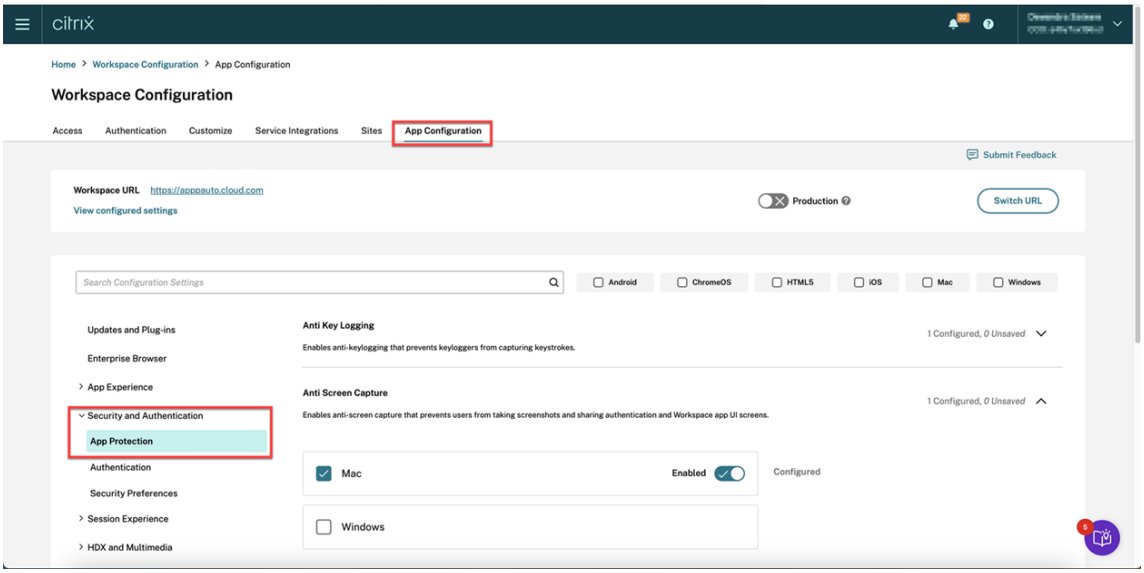
Administrators can configure App Protection using the Workspace Configuration UI:

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

1. Sign in to your Citrix Cloud account and select **Workspace Configuration**.

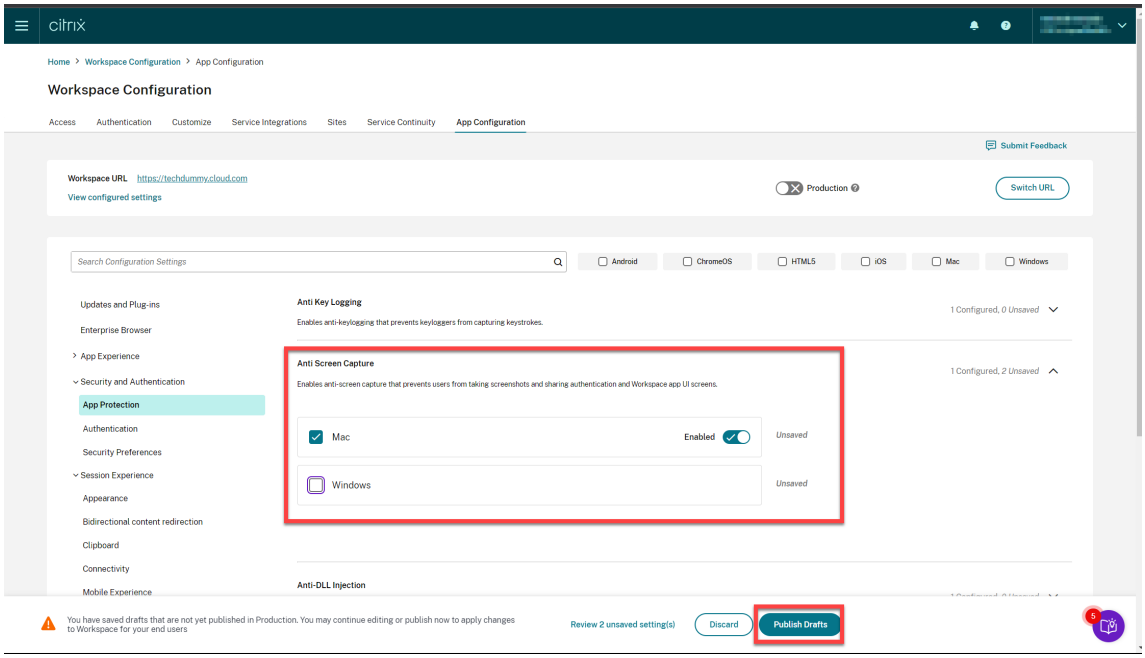


2. Select **App Configuration** > **Security and Authentication** > **App Protection**.

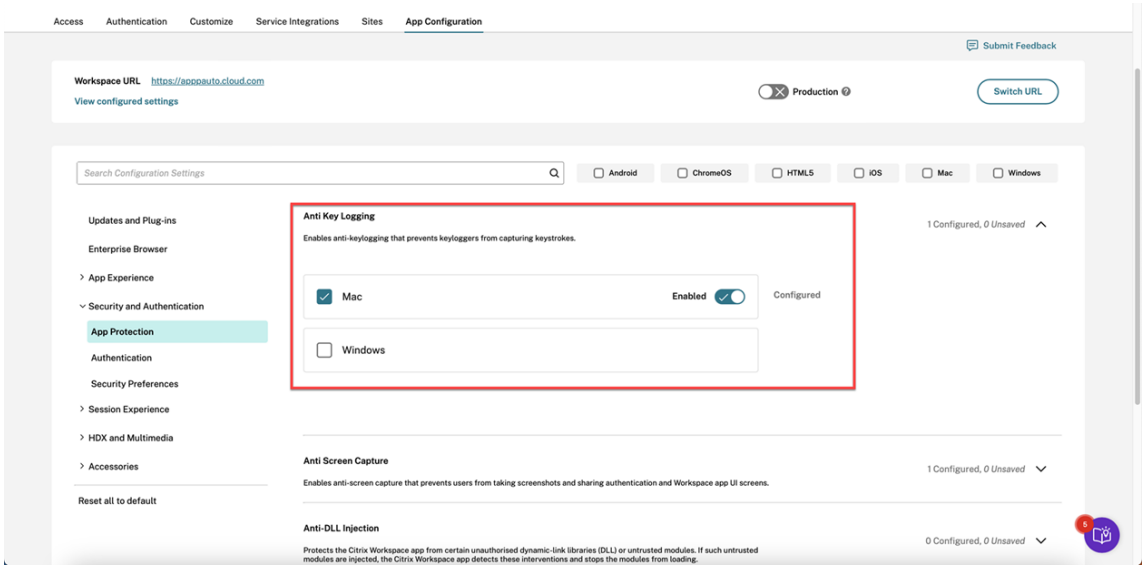


3. Click **Anti Screen Capture** and then select the relevant Operating System (Windows or Mac).
4. Click the **Enabled** toggle button and then click **Publish Drafts**.

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

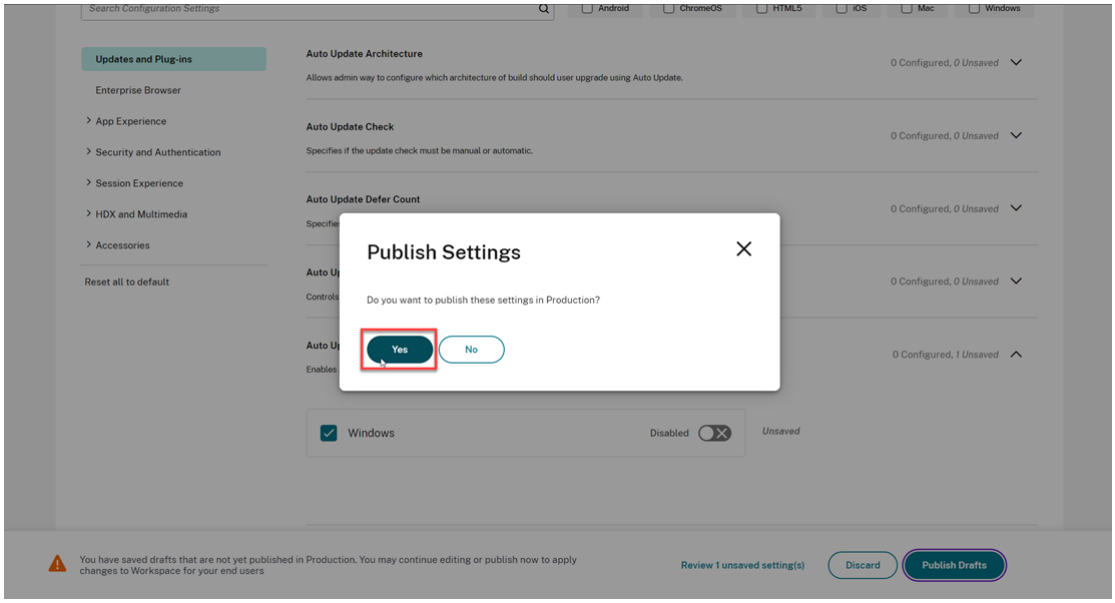


5. Click **Anti Key Logging** and then select the relevant Operating System (Windows or Mac).
6. Click the **Enabled** toggle button and then click **Publish Drafts**.



7. In the **Publish Settings** dialog box, click **Yes**.

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



Using Global App Configuration service API

The administrators can use the API to configure these App Protection features. The settings are as follows:

- **Setting to enable or disable anti-screen capturing:**

  “name”: “enable anti screen capture for auth and ssp”
  “value”: “true”or “false”

- **Setting to enable or disable anti-keylogging:**

  “name”: “enable anti key-logging for auth and ssp”
  “value”: “true”or “false”

Example: Following is a sample JSON file to enable anti-screen capture and anti-keylogging features for Citrix Workspace app in GACS:

```
{

        "category": "App Protection",

        "userOverride": true,

        "assignedTo": [

          "AllUsersNoAuthentication"

        ],

```

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

```
            "settings": [

              {


                "name": "enable anti screen capture for auth and ssp",

                "value": true

               }
 ,

              {


                "name": "enable anti key-logging for auth and ssp",

                "value": true

               }


            ] }
```

Using AuthManConfig.xml for an authentication manager

Navigate to `$ICAROOT/config/AuthManConfig.xml` and edit the file as follows:

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
   authmananti -A 1
    <key>AuthManAntiScreenCaptureEnabled</key>
    <value>true</value>
    <key>AuthManAntiKeyLoggingEnabled</key>
    <value>true </value>
```

Using AuthManConfig.xml for the Self-Service Plug-in interface

Navigate to `$ICAROOT/config/AuthManConfig.xml` and edit the file as follows:

```
/opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
   protection -A 4
<!-- Selfservice App Protection configuration -->
    <Selfservice>
      <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
      <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
    </Selfservice>
```

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

Configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops

Two policies provide anti-keylogging and anti-screen capturing functionality in a session. You can configure Anti-keylogging and Anti-screen capture for Virtual Apps and Desktops as follows:

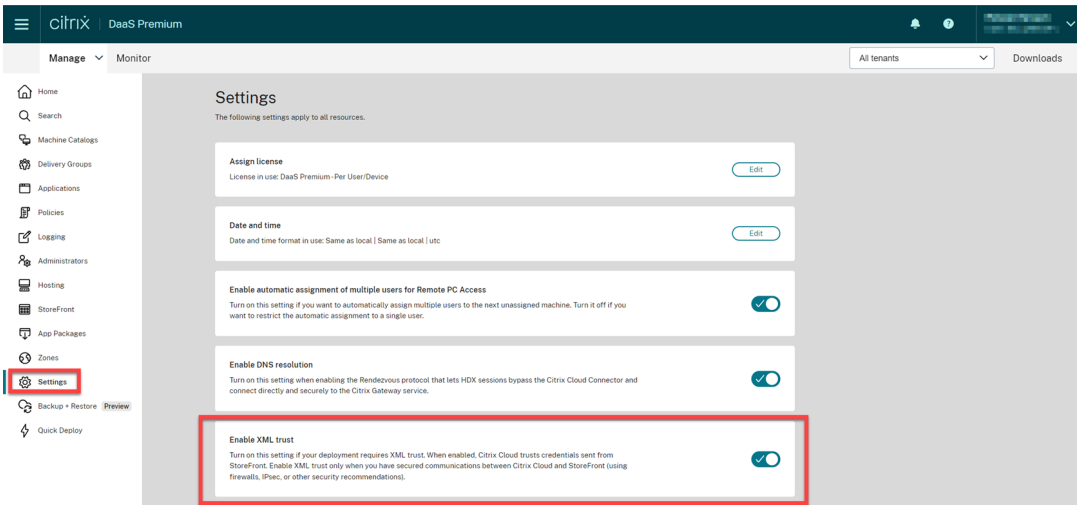
> **Note:**
>
> From version 2103, Citrix DaaS supports App Protection with StoreFront and Workspace.

Using Web Studio

To configure Anti-keylogging and Anti-screen capture for Citrix Virtual Apps™ or Desktops through Web Studio, do the following steps:

1. App Protection requires XML trust. To enable XML trust, do the following steps:

   a) Sign in to your Citrix DaaS™ account and go to **Manage** > **Settings** > **Enable XML trust**.

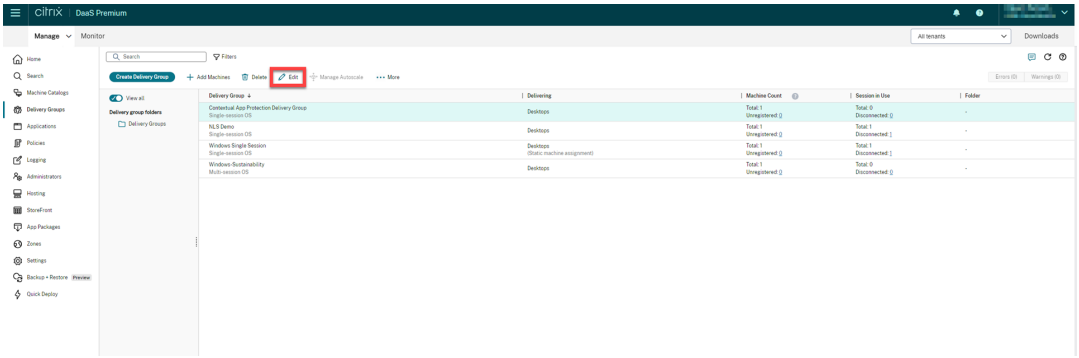
   b) Turn on the **Enable XML trust** toggle.

2. To choose an App Protection method for a delivery group, do the following steps:

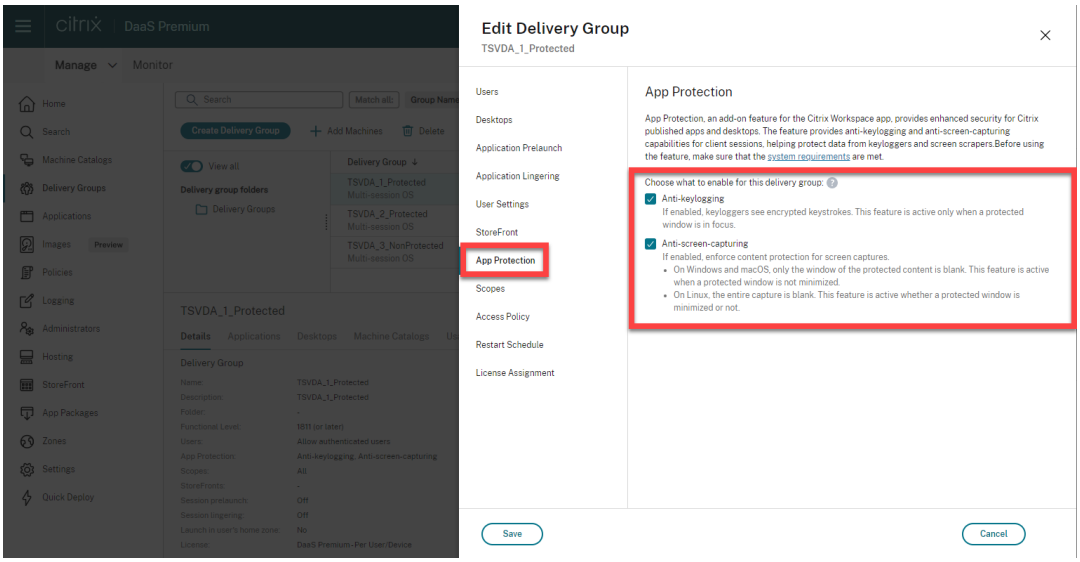
   a) In Citrix DaaS, go to **Manage** > **Delivery Groups**.

   b) Select a delivery group and then click **Edit** in the action bar.

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



c) Click **App Protection** and then select **Anti-keylogging** and **Anti-screen capturing** check-boxes.



d) Click **Save**.

Using PowerShell

> **Note:**
>
> In a Citrix DaaS environment, use the cmdlets in the Citrix Virtual Apps and Desktops Remote PowerShell SDK on any machine (apart from Citrix Cloud Connector machines) to issue the commands in this section.

Enable the following properties for the App Protection Delivery Group using the Citrix Virtual Apps and Desktops SDK on any installed Delivery Controller machine or on a machine with a stand-alone Studio installed that has the FMA PowerShell snap-ins installed.

- `AppProtectionKeyLoggingRequired`: `True`
- `AppProtectionScreenCaptureRequired`: `True`

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

You can enable each of these policies individually per Delivery Group. For example, you can configure keylogging protection only for DG1, and screen capture protection only for DG2. You can enable both policies for DG3.

Example:

To enable both policies for a Delivery Group naming **DG3**, run the following command on any Delivery Controller™ in the site:

```
Set-BrokerDesktopGroup -Name DG3 -AppProtectionKeyLoggingRequired
$true -AppProtectionScreenCaptureRequired $true
```

To validate the settings, run this cmdlet:

```
Get-BrokerDesktopGroup -Property Name, AppProtectionKeyLoggingRequired
, AppProtectionScreenCaptureRequired | Format-Table -AutoSize
```

Also, enable XML trust:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

Make sure that you secure the network between the StoreFront and the Broker. For more information, see Knowledge Center articles CTX236929 and Securing the XenApp and XenDesktop XML Service.

Configure Anti-keylogging and Anti-screen capture for Web and SaaS apps

Web and SaaS apps open in the Citrix Enterprise Browser for Citrix Workspace app for Windows and Citrix Workspace app for Mac. If the apps are configured to have the App Protection policies via the Citrix Secure Private Access, then App Protection is applied on a per tab basis.

Configure App Protection for Web and SaaS apps using the following:

- To configure App Protection for Web and SaaS apps for Workspace, see Citrix Secure Private Access for Citrix Workspace.
- To configure App Protection for Web and SaaS apps for StoreFront, see Citrix Secure Private Access support for StoreFront.

Configure Anti-DLL Injection

September 13, 2025

By default, the Anti-DLL Injection feature is disabled. You can enable this feature using the following:

- Group Policy Object (GPO)

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

- Global App Configuration service (GACS)

Configure using Group Policy Object

The following policies are added to configure the Anti-DLL Injection feature:

- Anti-DLL Injection
- Anti-DLL Injection Module Allow List

Using the Anti-DLL Injection policy

Use this policy to enable or disable the Anti-DLL Injection feature. When this policy is not configured, the Anti-DLL Injection feature is disabled. The possible values are:

- **Enabled** –The Anti-DLL Injection feature is enabled for Citrix Authentication Manager, Citrix Workspace app UI, and Citrix Virtual Apps and Desktops. Administrators can select the required components to enable the Anti-DLL Injection feature.
- **Disabled** –The Anti-DLL Injection feature is disabled for Citrix Authentication Manager, Citrix Workspace app UI, and Citrix Virtual Apps and Desktops.

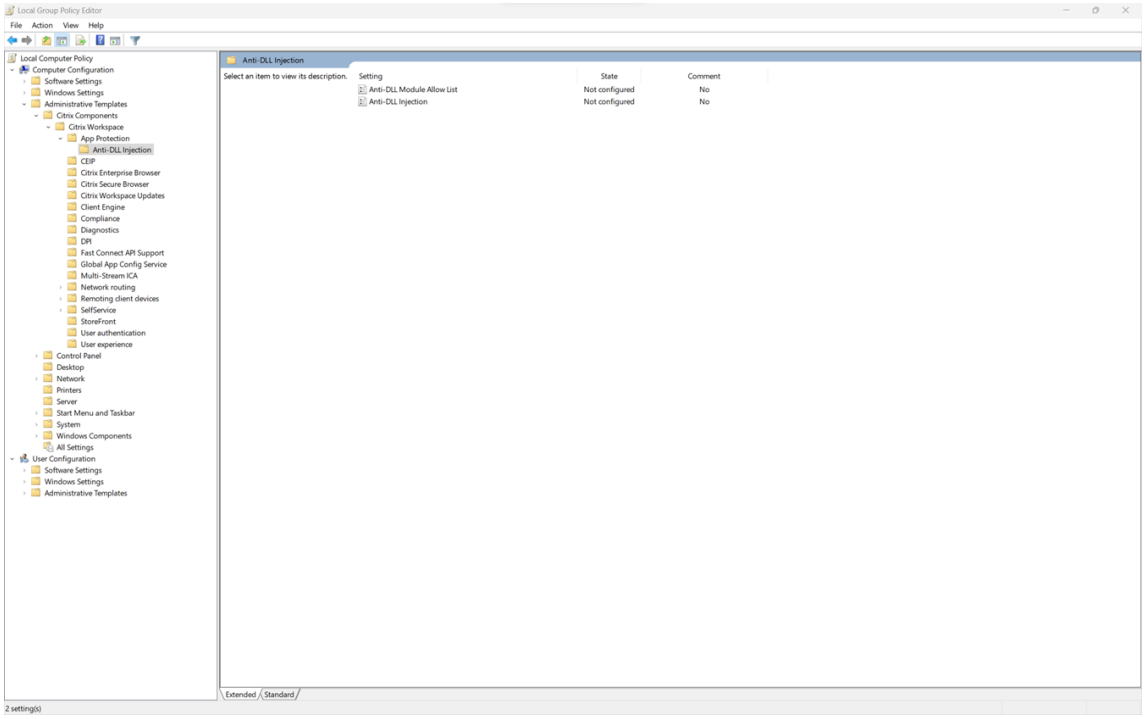
To enable the Anti-DLL Injection policy, do the following steps:

1. Open the Citrix Workspace app Group Policy Object administrative template by running the following command:

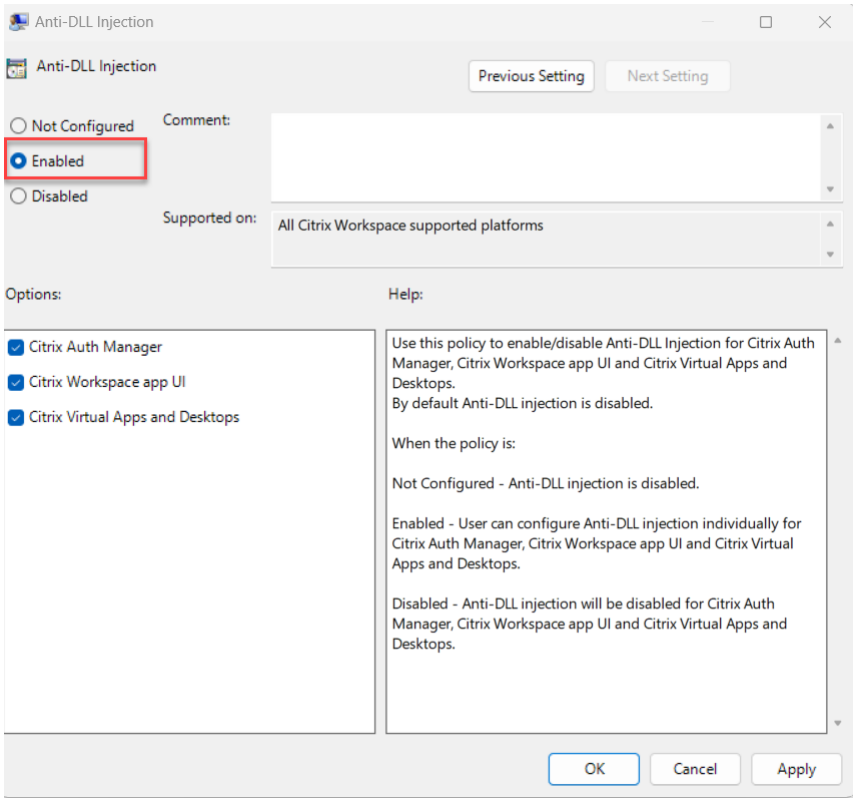
   ```
   gpedit.msc
   ```

2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **App Protection** > **Anti-DLL Injection**.

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



3. Click the **Anti-DLL Injection** policy and select **Enabled**. All the components are selected. However, you can modify the selection of the components from the Options section.



4. Click **OK**.

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

Using the Anti-DLL Injection Module Allow List policy

As an Administrator, you can use this policy to exclude any DLL from the Anti-DLL Injection feature. Citrix® recommends you to use this policy only to handle any exceptional scenario. When this policy is not configured, no DLL is part of the allow list. All the DLLs are included for the anti-DLL protection. The possible values are:

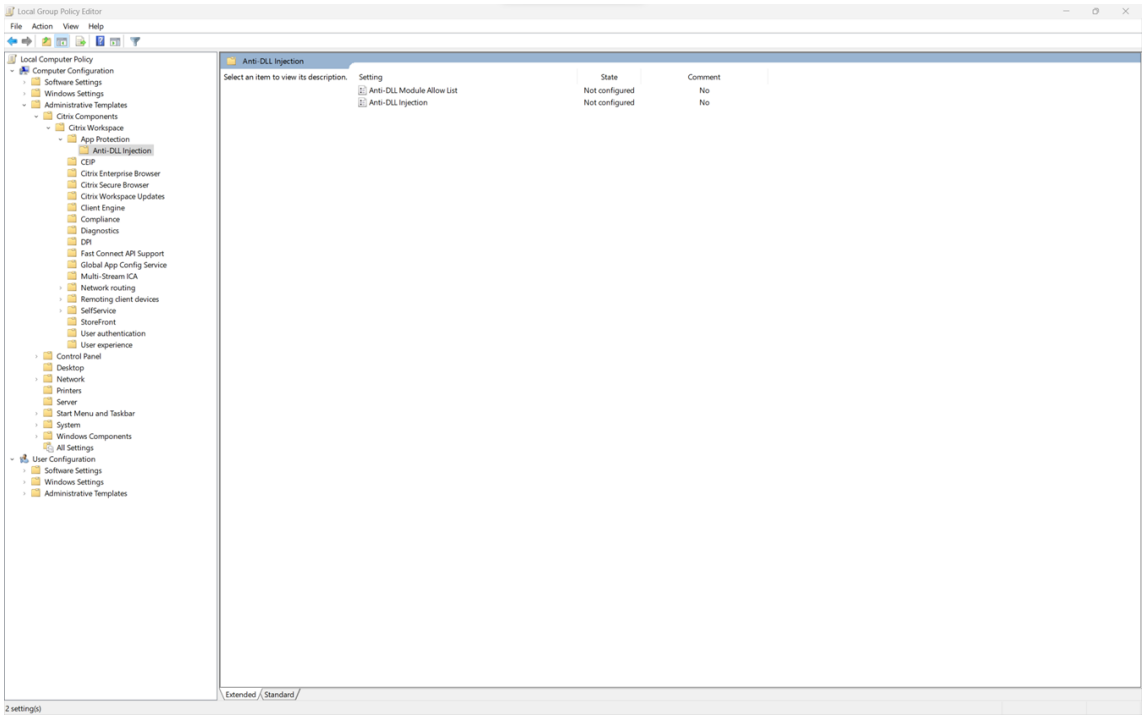
- **Enabled** - Excludes DLLs that are added in the allow list from the anti-DLL protection.
- **Disabled** - Clears the list of DLLs added to the allow list.

To enable the Anti-DLL Injection Module Allow List policy, do the following steps:

1. Open the Citrix Workspace app Group Policy Object administrative template by running the following command:

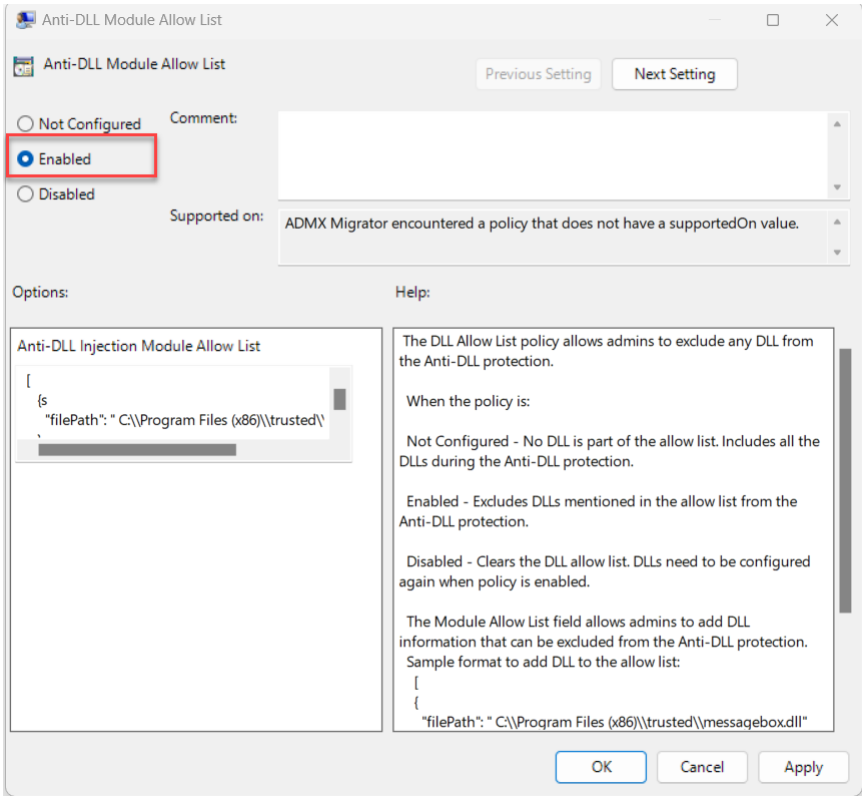
   ```
   gpedit.msc
   ```

2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **App Protection** > **Anti-DLL Module Allow List**.



3. Click the **Anti-DLL Module Allow List** policy and select **Enabled**.

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



4. Add the list of modules that you want to exclude from the anti-DLL protection in the **Anti-DLL Injection Module Allow List** field.
   Sample format to add DLL to the allow list:

```
[
    {

        "filePath":"C:\\Program Files (x86)\\trusted\\messagebox.
           dll"
     }
 ,
    {

        "filePath":"%PROGRAMFILES%\\trusted\\logging.dll"
     }

]
```

5. Click **OK**.

Configure using the Global App Configuration service

The Administrators can use GACS to configure the Anti-DLL Injection feature. The settings are as follows:

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

- anti dll injection –Add the required modules that you want to enable the anti-DLL Injection feature
- anti dll module allow list –Add the required DLLs that you want to exclude from the anti-DLL protection

For more information, see Global App Configuration service.

The following is a sample JSON file for enabling **anti dll injection** and **anti dll module allow list** for Citrix Workspace app for Windows in GACS:

```
{

  "serviceURL": {

    "url": "https://tuleshtest.cloudburrito.com:443"
   }
 ,
  "settings": {

    "appSettings": {

      "windows": [
        {

          "category": "App Protection",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "assignmentPriority": 0,
          "settings": [
            {

              "name": "anti dll injection",
              "value": [
                "Citrix Auth Manager",
                "Citrix Virtual Apps And Desktops",
                "Citrix Workspace app UI"
              ]
             }
 ,
            {

              "name": "anti dll module allow list",
              "value": [
                {

                  "filePath": "C:\\Program Files (x86)\\Citrix\\ICA
                     Client\\wfica32.exe"
                 }
 ,
                {
```

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

```
42
43                    "filePath": "C:\\Program Files (x86)\\Citrix\\ICA
                          Client\\AuthManager\\AuthManSvr.exe"
44                  }
45
46                ]
47               }
48
49             ]
50            }
51
52         ]
53       }
54   ,
55      "name": "name",
56      "description": "desc",
57      "useForAppConfig": true
58     }
59
60   }
```

Configure Policy Tampering Detection

January 6, 2026

Prerequisites

To configure Policy Tampering Detection feature, make sure that you have the following:

- For cloud deployments - Cloud Desktop Delivery Controller™ version 115 or later
- For on-premises deployments - Citrix Virtual Apps and Desktops™ version 2308 or later
- Windows Virtual Delivery Agent Installer version 2308 or later
- For Windows - Citrix Workspace app for Windows 2309 or later
- For Mac - Citrix Workspace app for Mac 2308 or later
- For Linux - Citrix Workspace app for Linux 2308 or later
- For Android - Citrix Workspace app for Android 25.3.0
- For iOS - Citrix Workspace app for iOS 24.9.0

> **Note:**
>
> From Citrix Virtual Apps and Desktops (CVAD) 2511, Policy Tampering Detection is enabled by default. No additional configuration is required.

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

For versions prior to CVAD 2511 to enable policy tampering detection the admin must start the **Citrix AppProtection Service** on the Ts/WS VDAs which are hosting the virtual app and desktops configured with aApp Protection. Do one of the following steps to enable Policy Tampering Detection:

- Using the command prompt:
    1. On the leftmost of the taskbar, click the **Search** icon. Type **cmd** and then click **Run as administrator**. The **Command Prompt** screen appears.
    2. Run the following commands:

```
sc config ctxappprotectionsvc start=auto
sc start ctxappprotectionsvc
```

- Using the user interface:
    1. On the leftmost of the taskbar, click the **Search** icon. Type **services.msc** and press **Enter**. The **Services** screen appears.
    2. Select **Citrix AppProtection Service** and then click **Start**.
    3. Right-click **Citrix AppProtection Service** and then select **Properties**.
    4. Select **General** > **Startup type** > **Automatic** and then click **OK** to make sure that the service starts automatically when the system starts.

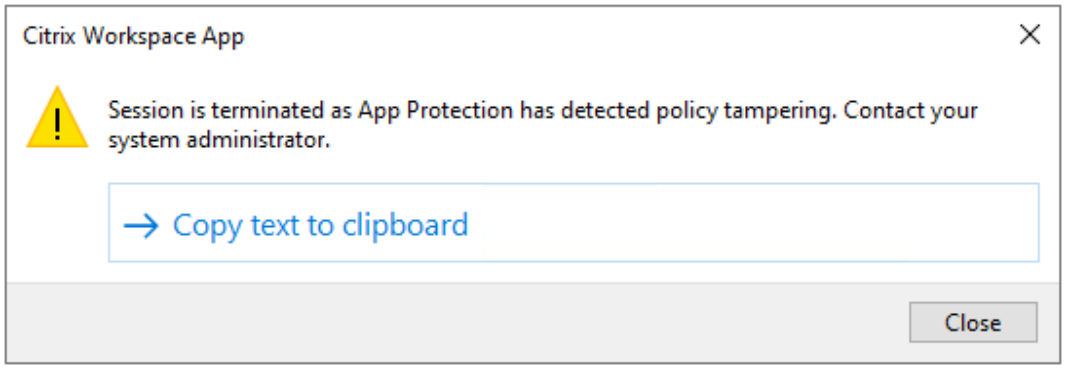
Policy Tampering Detection feature is enabled successfully.

To detect and block prior versions of Citrix Workspace app that do not support Policy Tampering Detection, configure App Protection Posture Check. For more information about App Protection Posture Check, see App Protection Posture Check.

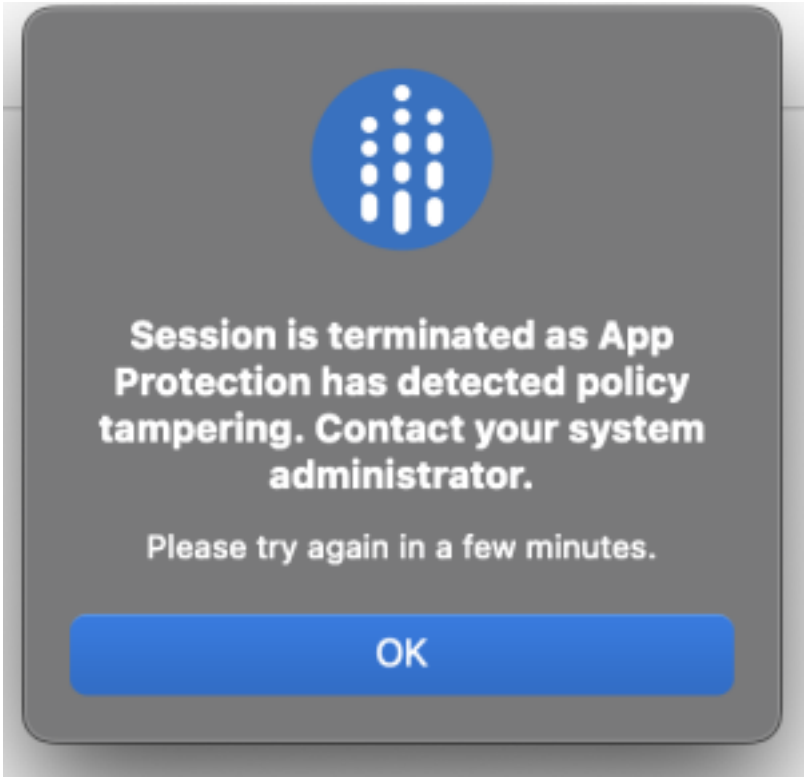
Expected behavior when App Protection detects Policy Tampering

- If the Policy Tampering Detection VDA Citrix Policy is enabled and you're using a Citrix Workspace™ app version that does not support the Policy Tampering Detection feature, then the session terminates without displaying any error message.
- If you're using a Citrix Workspace app version that supports the Policy Tampering Detection feature, then the session terminates displaying the following error message based on the OS you are using:
    - Windows:

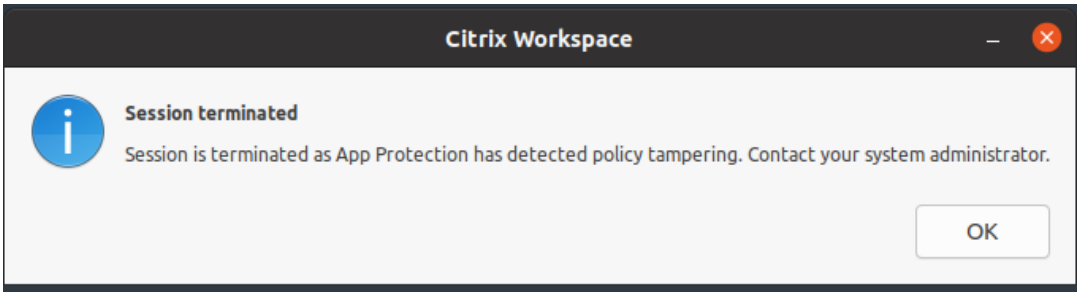
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Mac

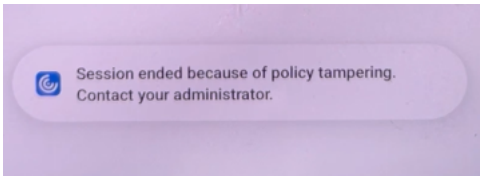


- Linux

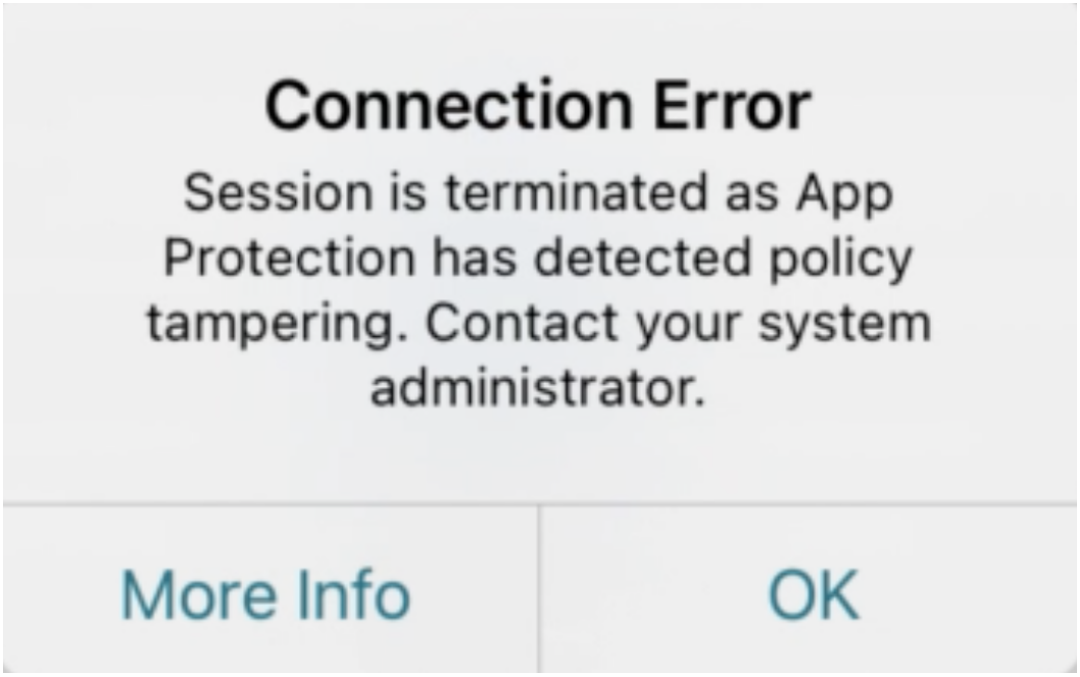


- Android

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



- iOS



Configure App Protection Posture Check

September 7, 2025

To enable App Protection Posture Check, configure the new VDA Citrix Policy that is related to this feature.

Prerequisites

Make sure that you have the following:

- For cloud deployments - Cloud Desktop Delivery Controller™ version 115 or later
- For on-premises deployments - Citrix Virtual Apps and Desktops™ version 2308 or later
- Windows Virtual Delivery Agent Installer version 2308 or later
- For Windows - Citrix Workspace app for Windows 2309 or later
- For Mac - Citrix Workspace app for Mac 2308 or later

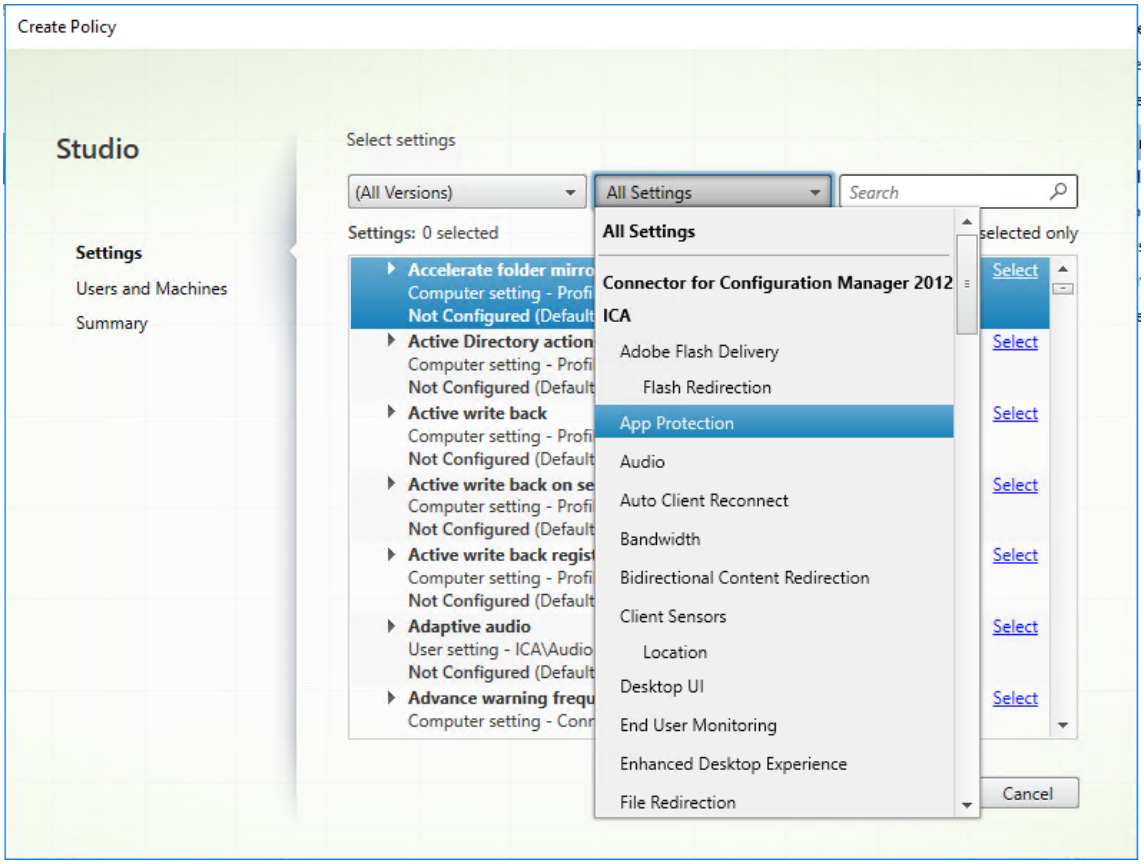
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For Linux - Citrix Workspace app for Linux 2308 or later
- For Android - Citrix Workspace app for Android 25.3.0
- For iOS - Citrix Workspace app for iOS 24.9.0

Configure the new VDA Citrix Policy for Posture Check as follows:

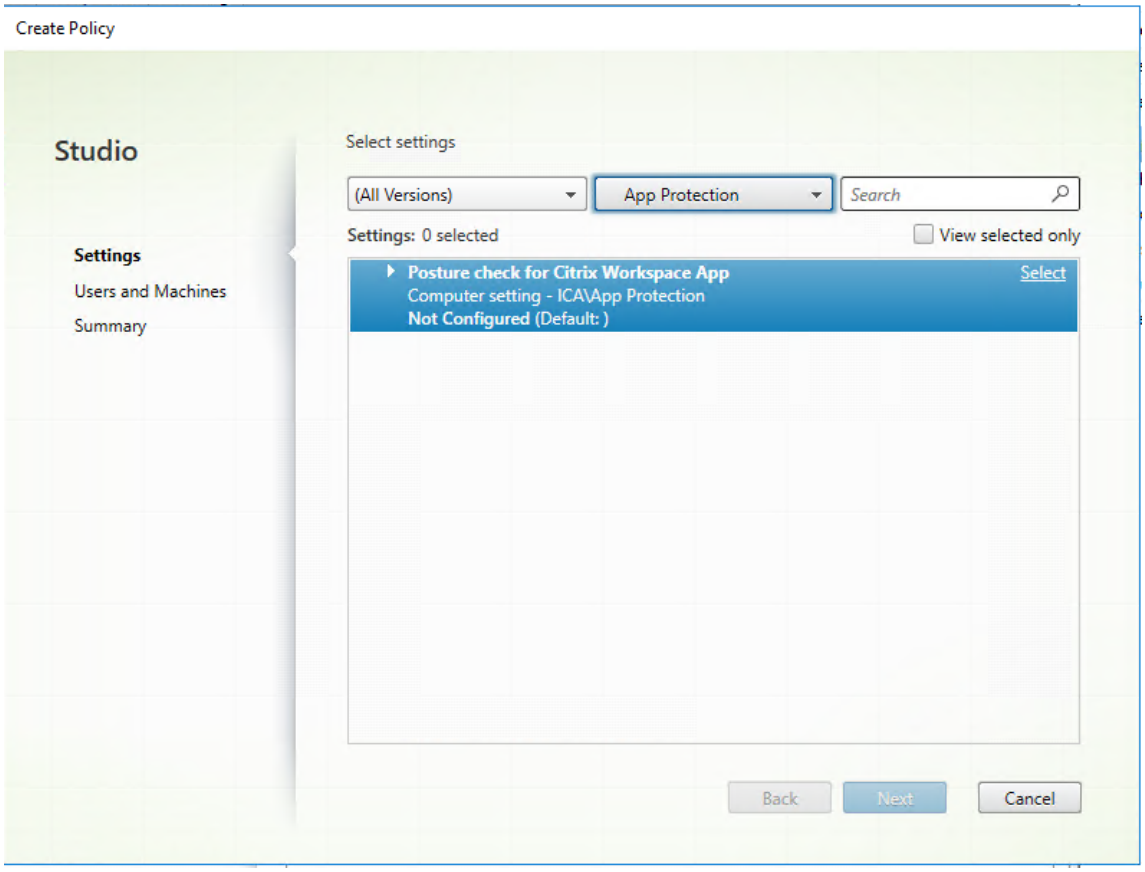
> **Note:**
>
> This new VDA Citrix Policy can be deployed using both Citrix Studio and Web Studio. The following procedure is deployed via Citrix Studio and you can use the same procedure for Web Studio also.

1. Open the Citrix Studio app on the Desktop Delivery Controller (DDC) for on-prem or Web Studio for Cloud deployments and then select **Policies**.
2. Under **Actions**, select **Policies** > **Create Policy**.
3. Click the **All Settings** drop-down menu and select **App Protection** under **ICA**.



4. Select **Posture check for Citrix Workspace app** and then click **Select**.

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



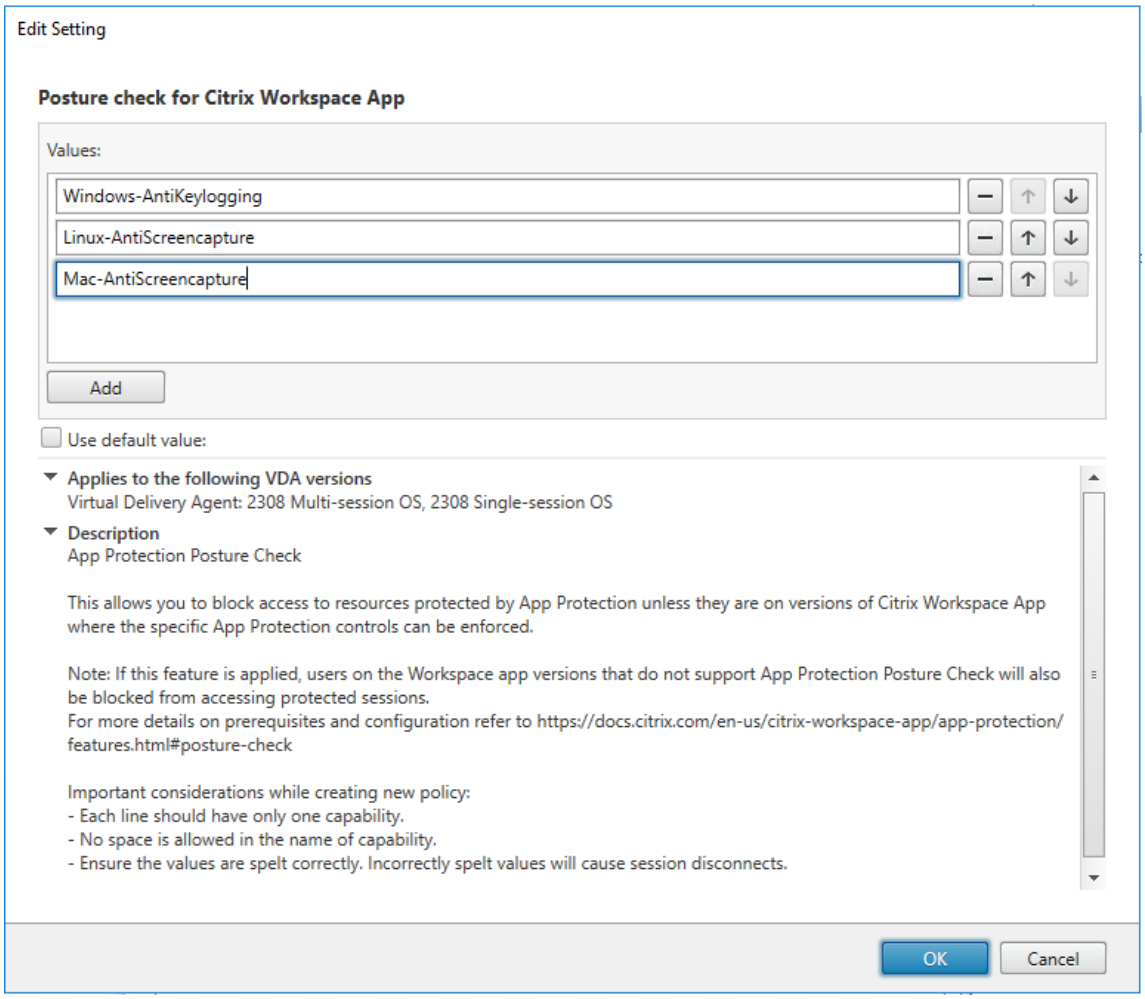
The **Edit Setting** window appears.

5. Clear the **Use default value** checkbox.
6. Click **Add** and enter the relevant values from the following:

    - Windows-AntiScreencapture
    - Windows-AntiKeylogging
    - Linux-AntiScreencapture
    - Linux-AntiKeylogging
    - Mac-AntiScreencapture
    - Mac-AntiKeylogging
    - Android-AntiScreencapture
    - iOS-AntiScreencapture
    - iOS-AntiKeylogging

    For example, If you've added "Windows-AntiScreencapture"and "Windows-AntiKeylogging" , then the Citrix Workspace app for Windows that supports Posture Check and has these capabilities is allowed to connect to the VDA.

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

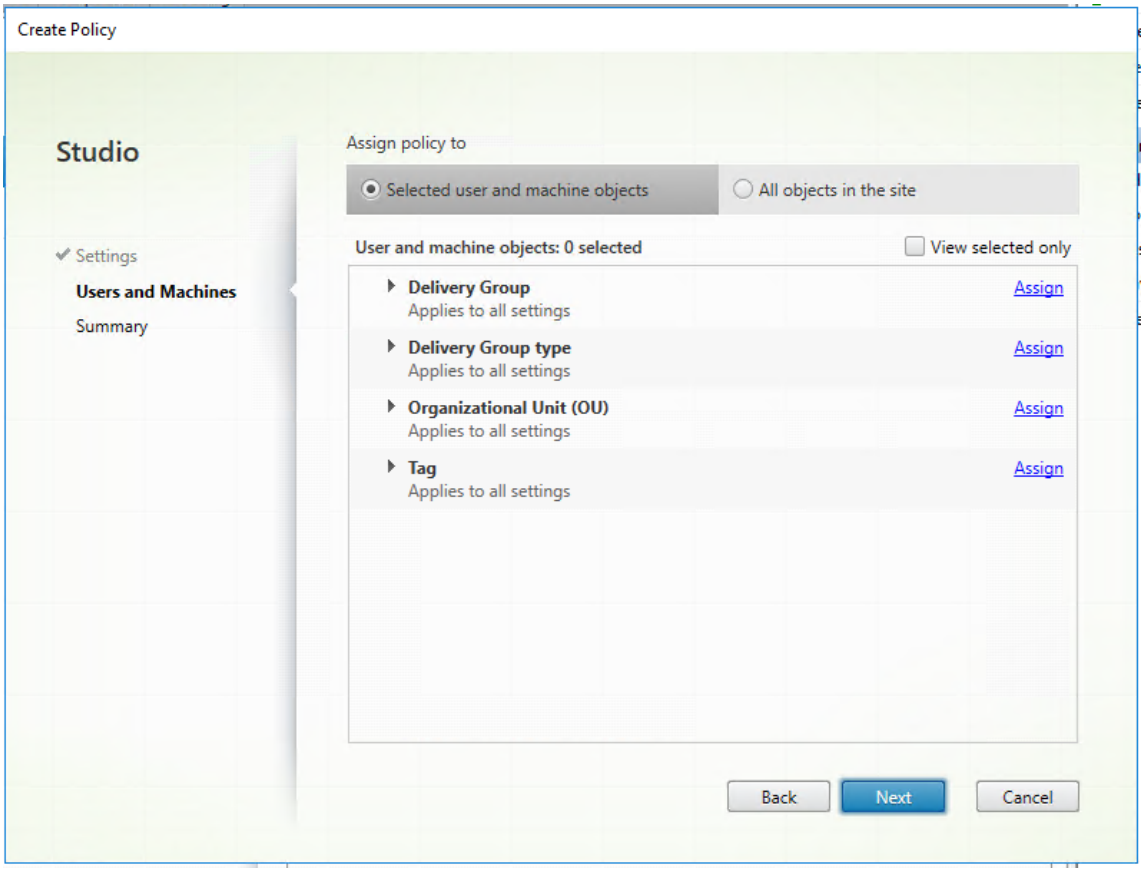


Note:

- Each entry must have only one capability.
- No space is allowed in the name of capability.
- Make sure that the values are spelt correctly. Incorrectly spelt values cause the session to terminate.
- Values that don't have the prefix Windows-, Linux-, Android-, iOS-, or Mac- are ignored.

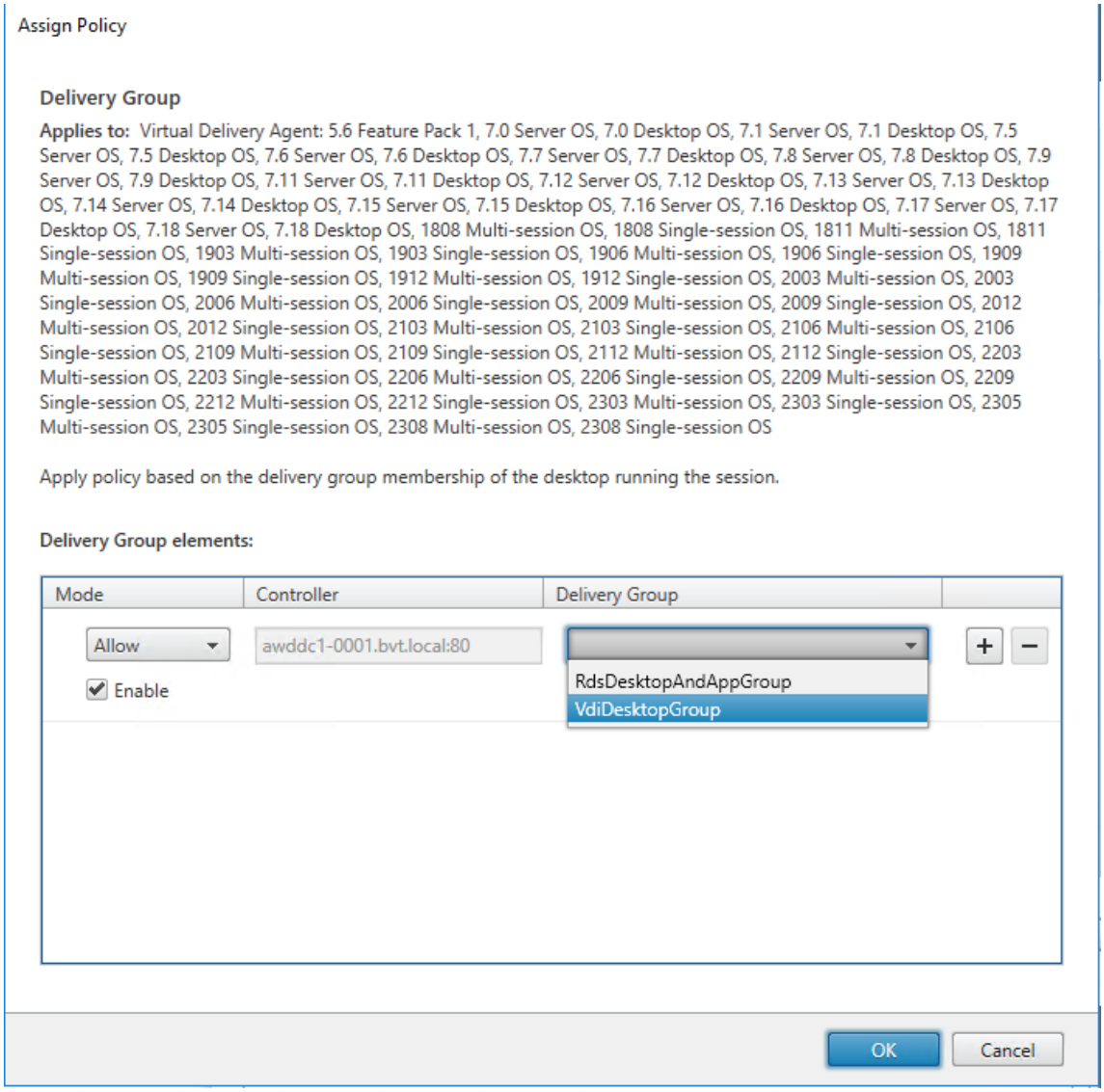
7. After adding all the required values, click **OK**.
8. Click **Next**.
9. Select **Assign Policy to** > **Selected users and machine objects**.

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



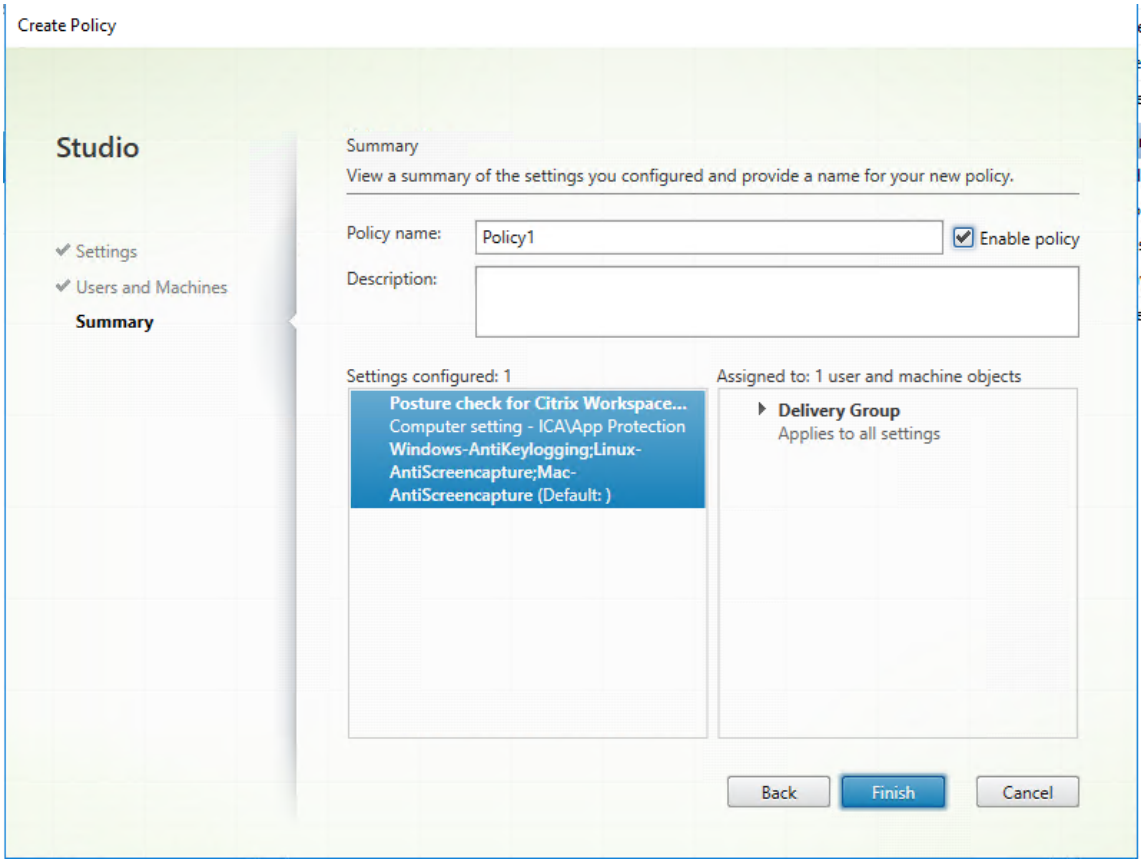
10. Select the required delivery groups where this policy must be deployed and then click **OK**.

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



11. Click **Next**.
12. Enter the policy name in the **Policy name** field and then select the **Enable policy** checkbox.

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



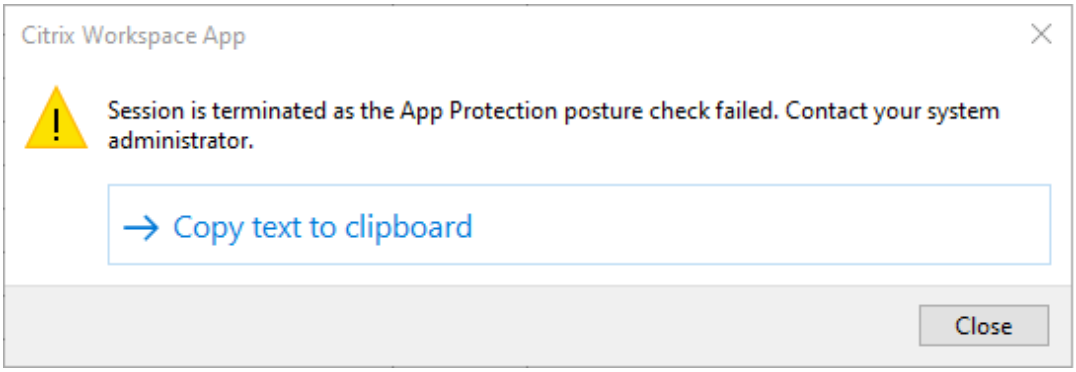
13. Click **Finish**.

A policy for posture check is created.

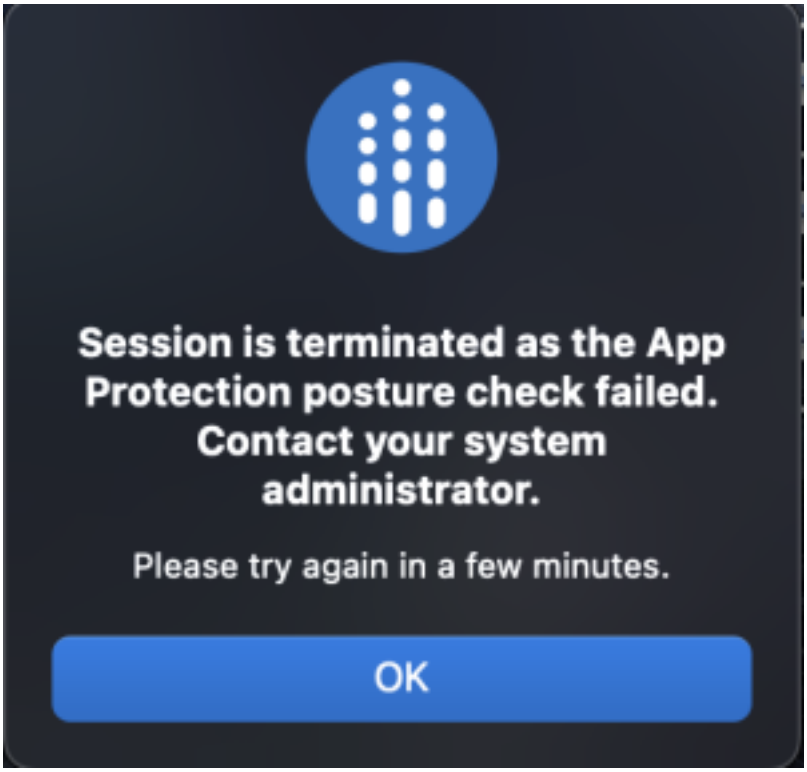
Expected behavior if App Protection Posture Check fails

- If the Posture Check VDA Citrix Policy is enabled and you're using a Citrix Workspace app version that does not support the Posture Check feature, then the session is terminated without displaying any error message.
- If you're using a Citrix Workspace app version that supports the Posture Check feature, then the session is terminated displaying the following error messages respectively:
    - Windows:

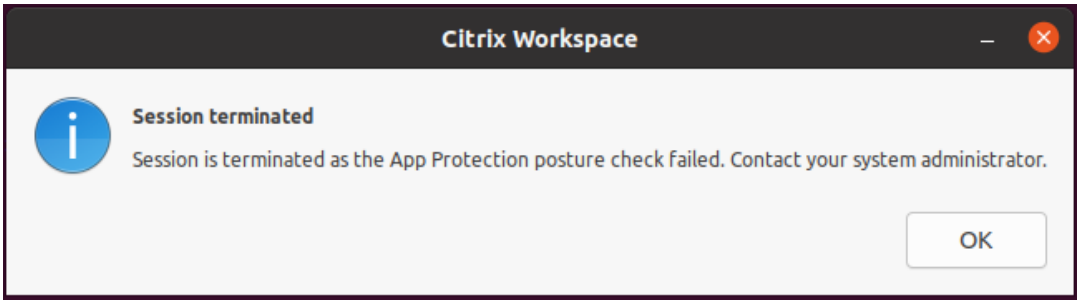
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- Mac

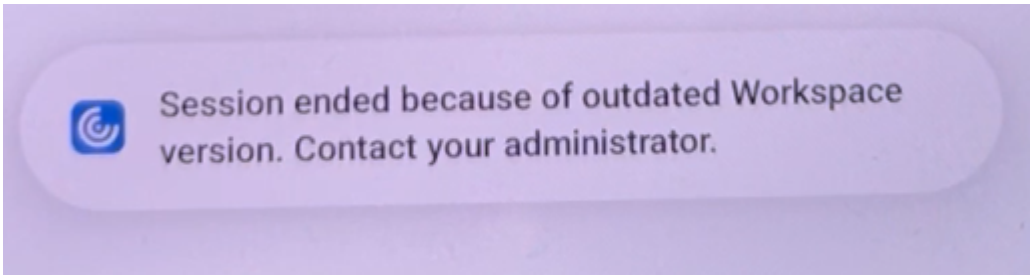


- Linux

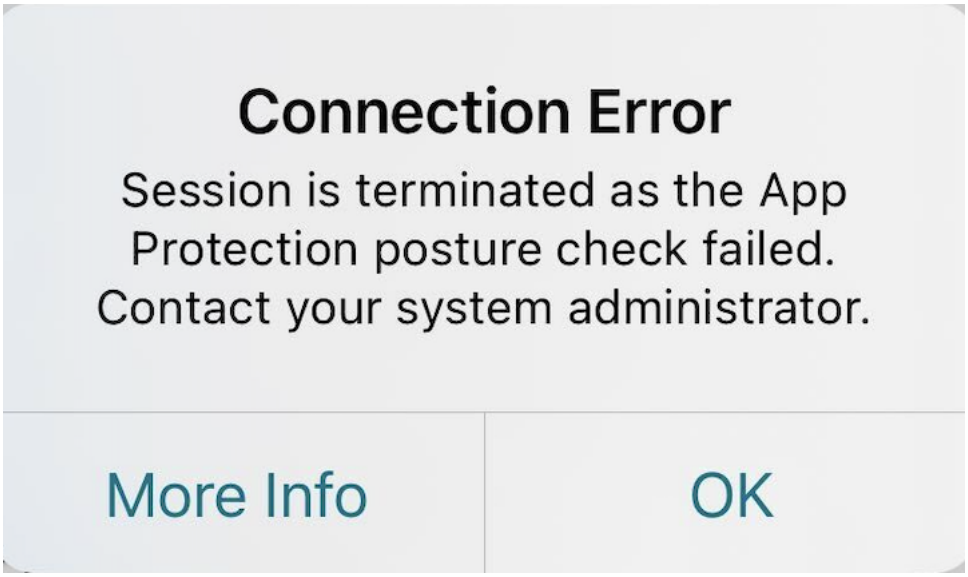


- Android

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



- iOS



Block DoubleHop Launch

September 7, 2025

You can block the opening of virtual apps, desktops, web apps, or SaaS apps enabled with App Protection feature in a double hop scenario.

Pre-requisites:

- To block opening of a virtual app or desktop, ensure that you're running Citrix Workspace app for Windows 2309 or later on the first hop.
- To block opening of web or SaaS apps, ensure that you are using Citrix Enterprise Browser version 123 or later.

Deploy the following configurations to all VDAs on the first hop:

1. Update the latest GPO policies. For more information, see Update latest GPO policies.

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

2. Launch **Group Policy Editor** and then go to **Computer Configuration** > **Administrative Templates** > **Citrix Components** > **Citrix Workspace** > **App Protection** > **Block DoubleHop Launch**.
3. Select **Enabled** and then click **OK**.

   Block DoubleHop Launch setting is enabled and you're blocked if you try to do double hop launch.

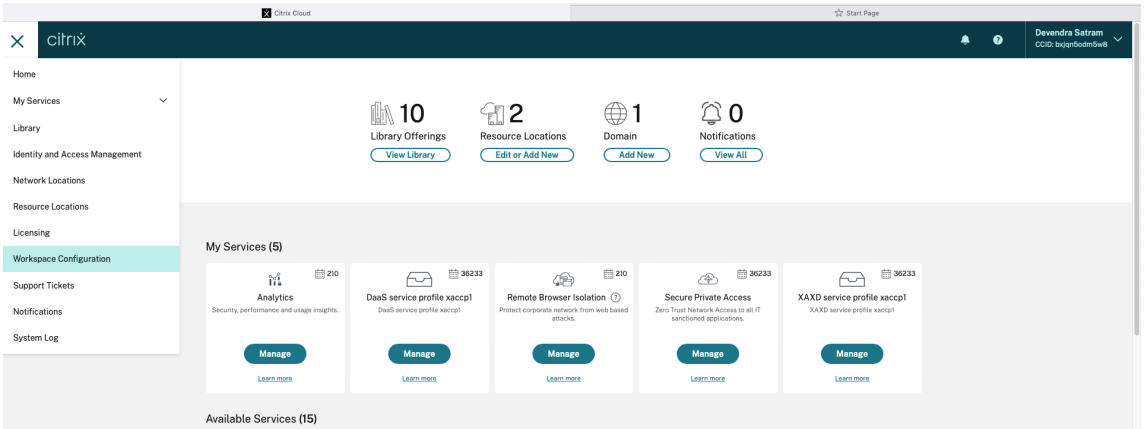
> **Note:**
>
> Windows Server OS doesn't support App Protection. So, the Virtual Apps and Desktops that are enabled with App Protection aren't displayed if you're running a Windows server OS on the first hop.

Configure Screen Capture Allow List

September 7, 2025

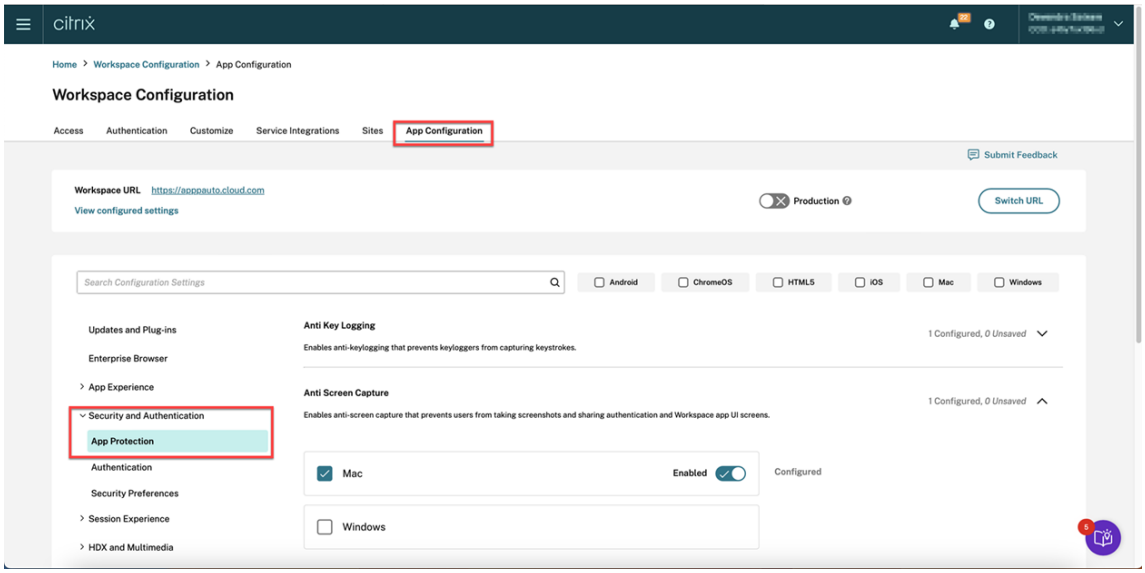
To add an app to the screen capture allow list, do the following steps:

1. Sign in to your Citrix Cloud™ account and select **Workspace Configuration**.

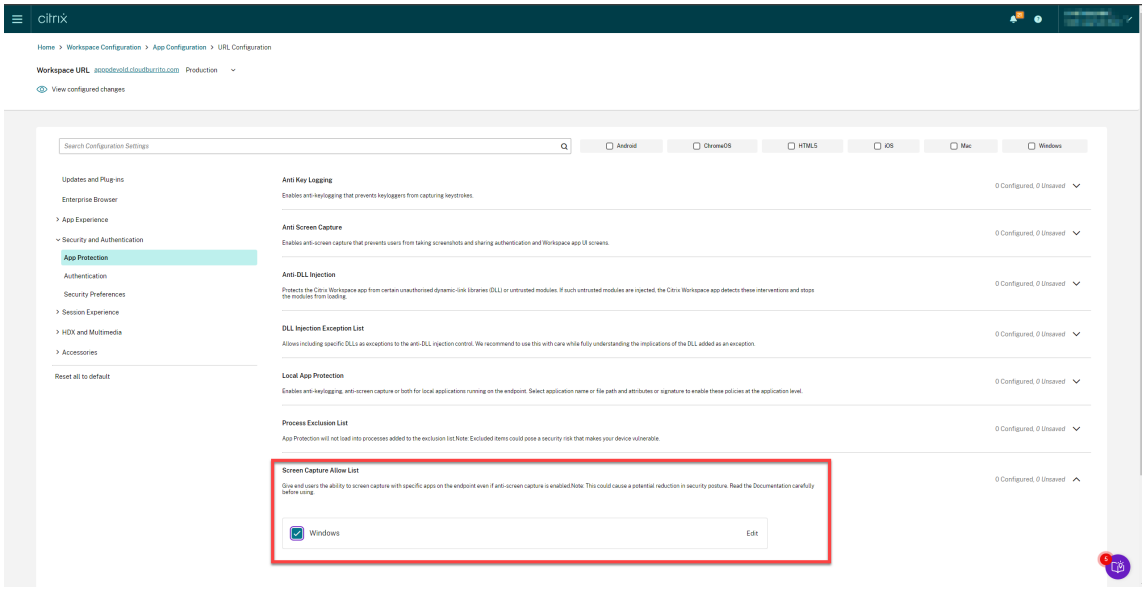


2. Select **App Configuration** > **Security and Authentication** > **Configure** > **App Protection**.

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



3. Click **Screen Capture Allow List** and select the **Windows** checkbox.



4. Click the **Edit** option.

   The **Manage settings for Windows** screen appears.

5. Add the information about the app that you want to add to the Screen Capture Allow List.

   For example,

```
[
 {

 "name": "ScreenshotTool_1.exe",
 "signature": "ScreenshotTool_1 Signature",
 "publisher": "ScreenshotTool_1 Publisher"
  }
```

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

```
  ,
  {

   "name": "Screenshottool_2.exe",
   "signature": "",
   "publisher": ""
   }

]
```

Manage settings for Windows

```
[
  {
    "name": "ScreenshotTool_1.exe",
    "signature": "ScreenshotTool_1_Signature",
    "publisher": "ScreenshotTool_1_Publisher"
  },
  {
    "name": "ScreenshotTool_2.exe",
    "signature": "",
    "publisher": ""
  }
]
```

Save draft Cancel

Note:

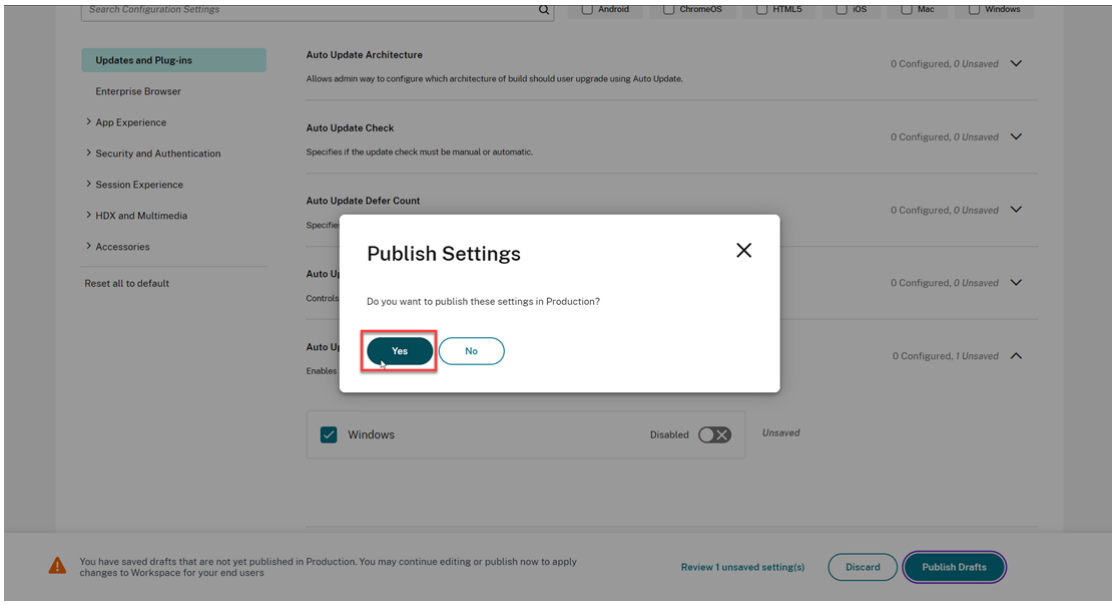
- The `name` has to be mandatorily filled. At the same time, the `publisher` and `signature` aren't mandatory. However, It's recommended to add the relevant`publisher` and `signature` to ensure that only the allow listed app can take the screenshots.
- Without `publisher` and `signature` values, a malicious application with the same

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

> name can capture screenshots.
> - Also, you can add multiple apps to the Screen Capture Allow-list by adding multiple entries in this block.

To get the `publisher` and `signature` information, see Get the `publisher` and `signature` information.

6. Click **Save draft** and then click **Publish Drafts**.
7. On the **Publish Settings** dialog box, click **Yes**.

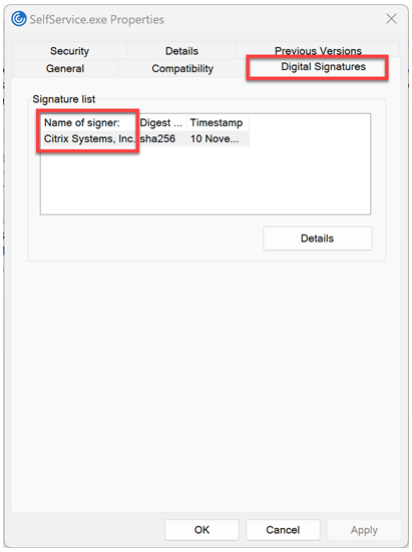


Get the `publisher` and `signature` information

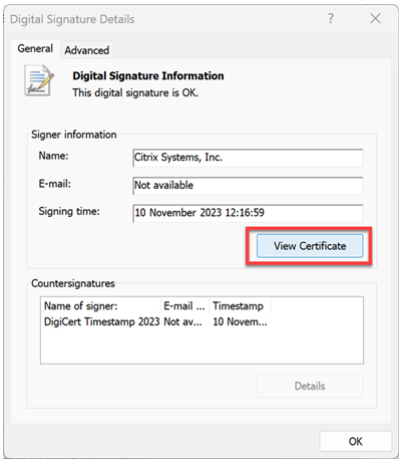
To get the `publisher` and `signature` information, do the following steps:

1. Open the file location where you have the relevant `.exe` file of the app.
2. Right-click on the `.exe` file and then click **Properties**. A properties pop-up screen appears.
3. Click **Digital Signatures**. The **Name of signer** is the `publisher` value.

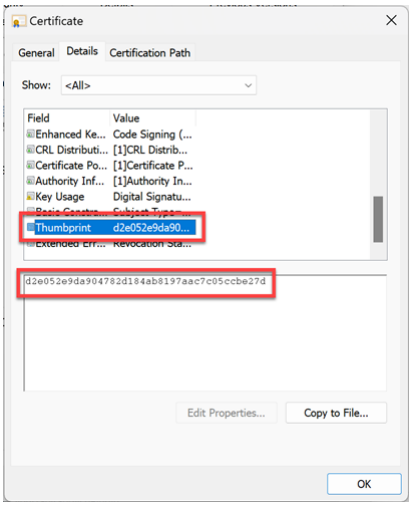
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click the first entry in the **Name of signer** and then click **Details** > **View Certificate**.



5. Click **Details** > **Thumbprint**. The content that appears in the textbox is the `signature`.



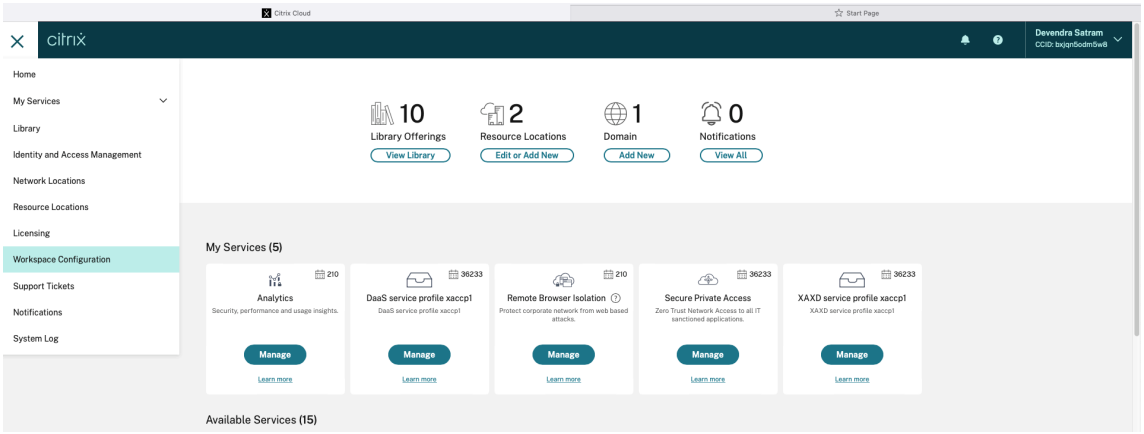
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Process exclusion list

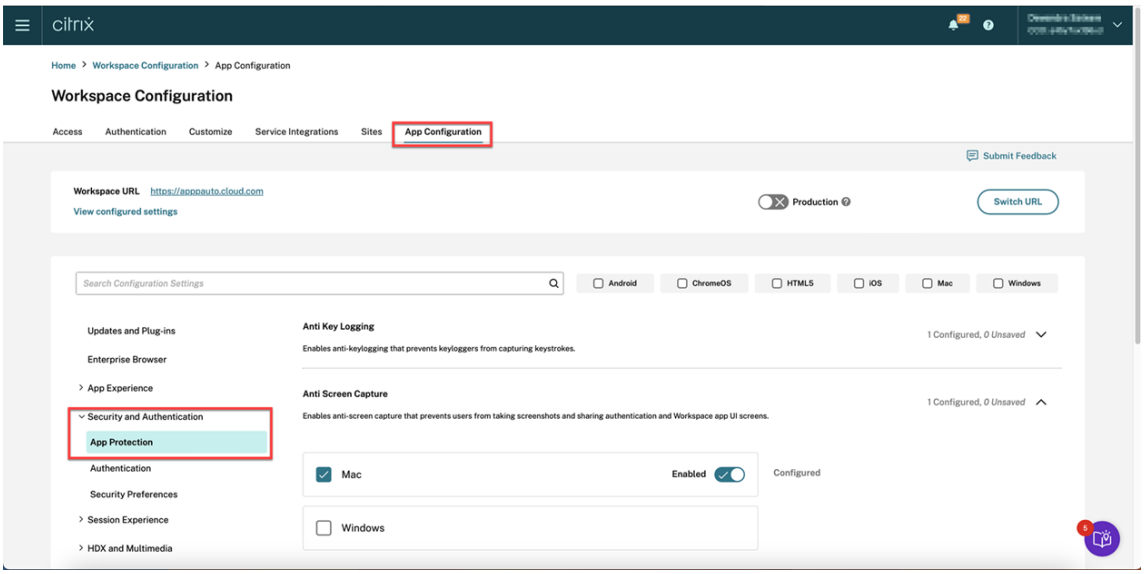
September 7, 2025

To add a process to the Process Exclusion List, do the following steps:

1. Sign in to your Citrix Cloud™ account and select **Workspace Configuration**.

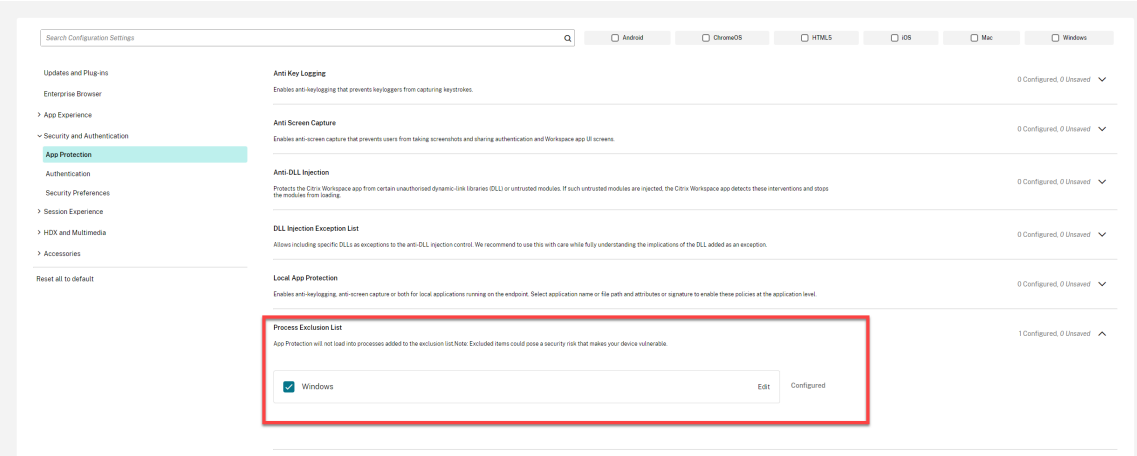


2. Select **App Configuration** > **Security and Authentication** > **Configure** > **App Protection**.



3. Click **Process Exclusion List** and then select the **Windows** checkbox.

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



4. Click the **Edit** option.

   The **Manage settings for Windows** screen appears.

5. Add the information about the process that you want to add to the Process Exclusion List.

   For example,

```
[
 {

  "name": "sample_program.exe",
  "publisher": "sample_publisher1",
  "signature": "sample_thumbprint1"
  }

]
```

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

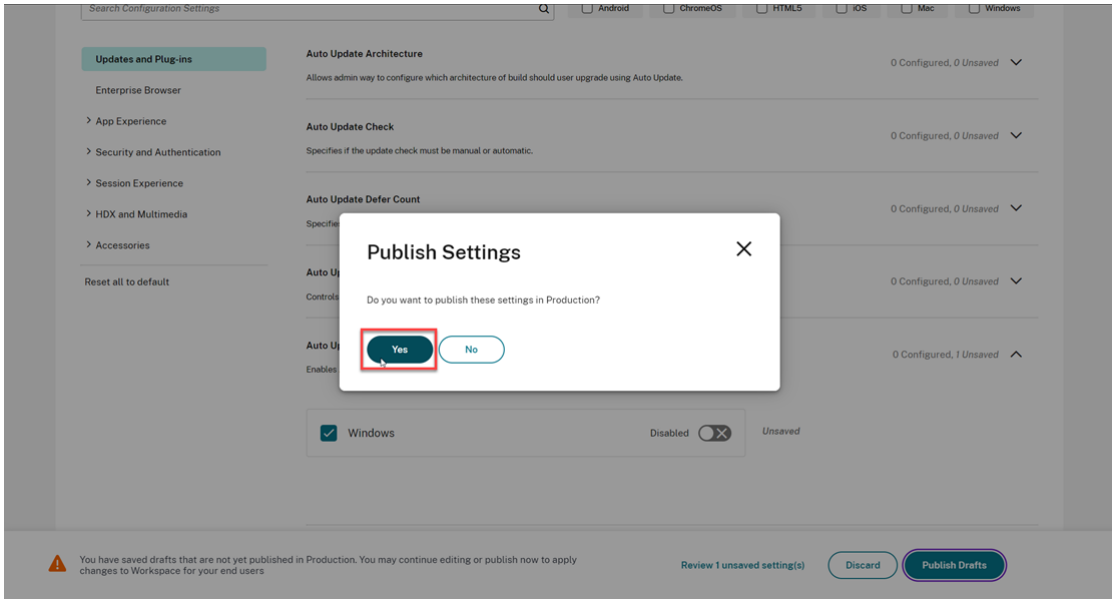


> **Note:**
>
> - The `name` has to be mandatorily filled. At the same time, the `publisher` and `signature` aren't mandatory. However, It's recommended to add `publisher` and `signature` to ensure that the correct process is added to the list.
> - Also, you can add multiple processes to the Process Exclusion List by adding multiple entries in this block.

To get the `publisher` and `signature` information, see Get the `publisher` and `signature` information.

6. Click **Save draft** and then click **Publish Drafts**.
7. On the **Publish Settings** dialog box, click **Yes**.

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



8. Restart Citrix Workspace app.

Configure USB Filter Driver Exclusion List

September 7, 2025

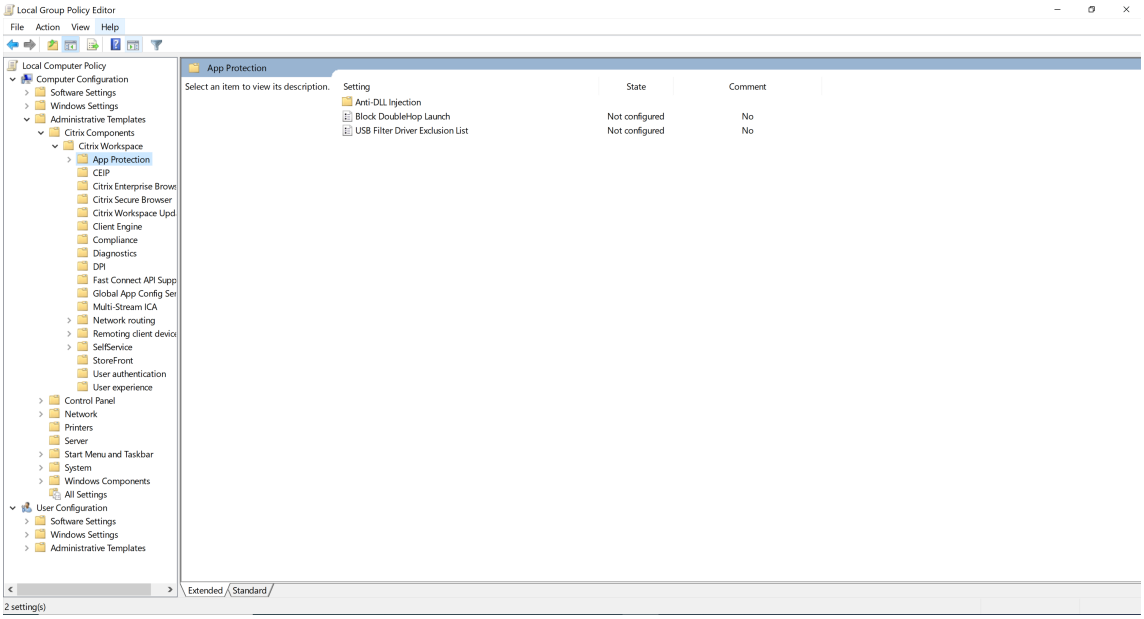
You can add a USB device to the USB Filter Driver Exclusion List using one of the following methods:

- Using Group Policy Object
- Using the Global App Configuration Service UI

Using Group Policy Object

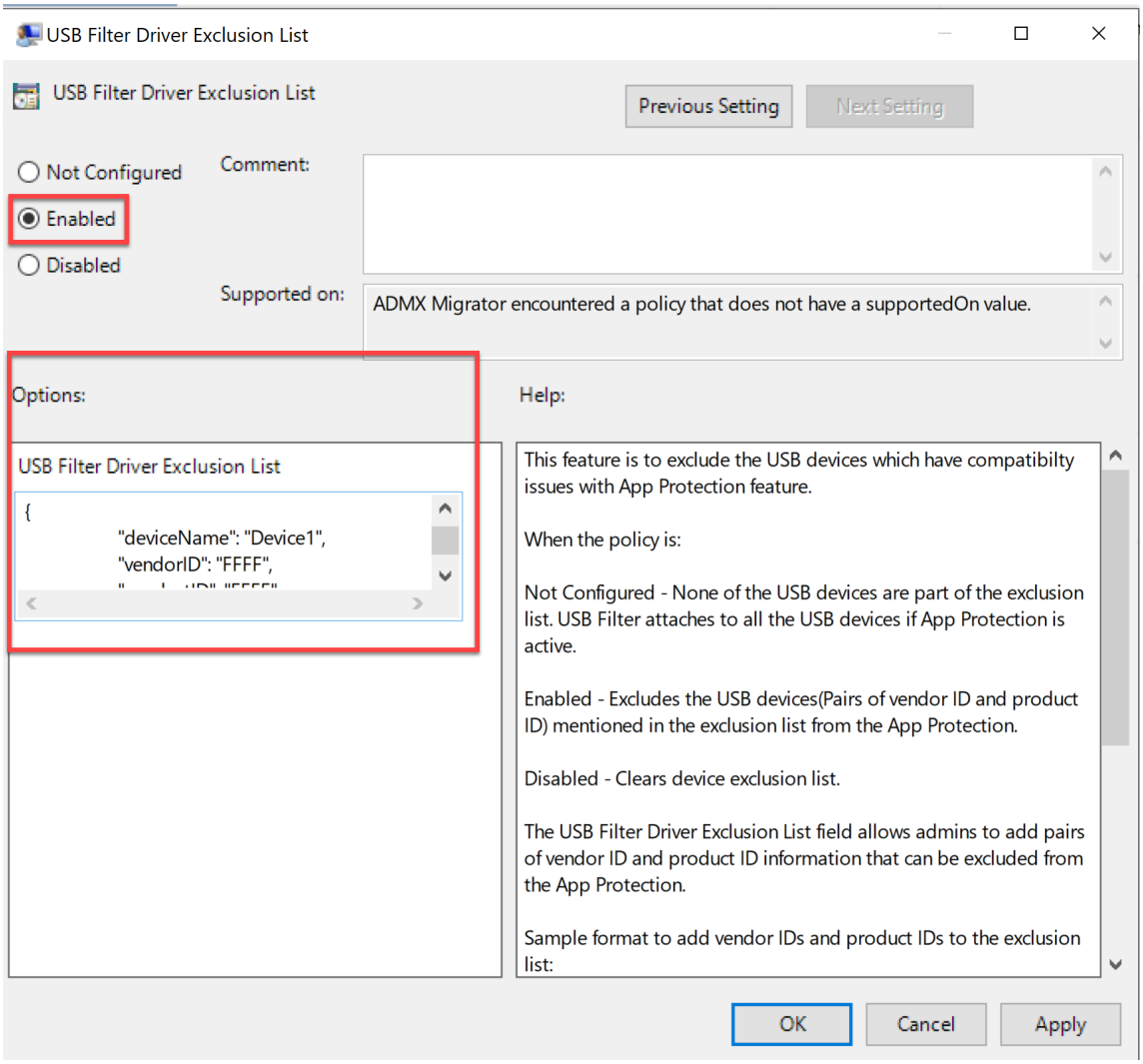
1. Open the Citrix Workspace app Group Policy Object administrative template by running `gpedit.msc`. For more information, see Group Policy Object.
2. Under the **Computer Configuration** node, go to **Administrative Templates** > **Citrix Components** > **Citrix Workspace™** > **App Protection** > **USB Filter Driver Exclusion List**.

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



3. Select **Enabled** and enter the **Vendor ID** and **Product ID** of the USB device you want to exclude in the **Options** text box.

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



> **Note:**
>
> - The `productID` and `vendorID` must be mandatorily filled. At the same time, the `deviceName` isn't mandatory.
> - Also, you can add multiple USB devices to the exclusion list by adding multiple entries in this block.

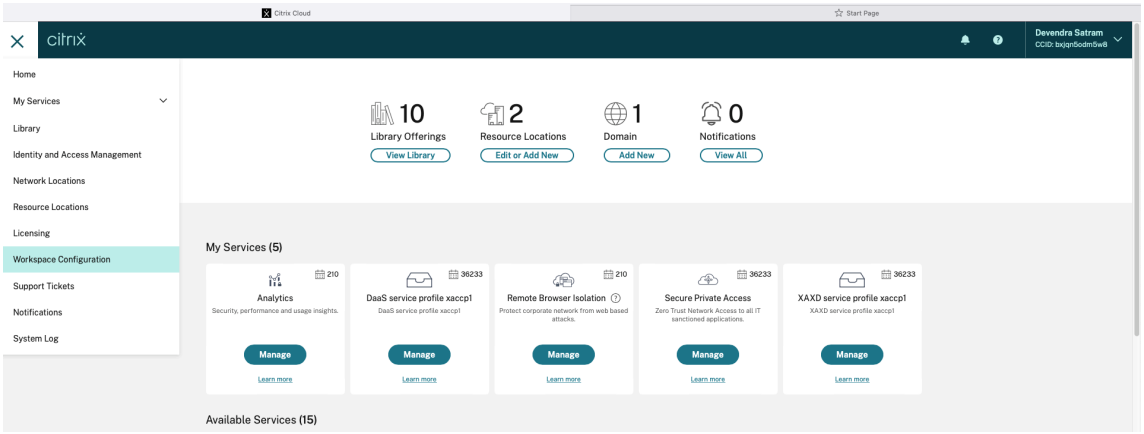
To get the `productID` and `vendorID`, see Get the `productID` and `vendorID`.

4. Click **OK**.

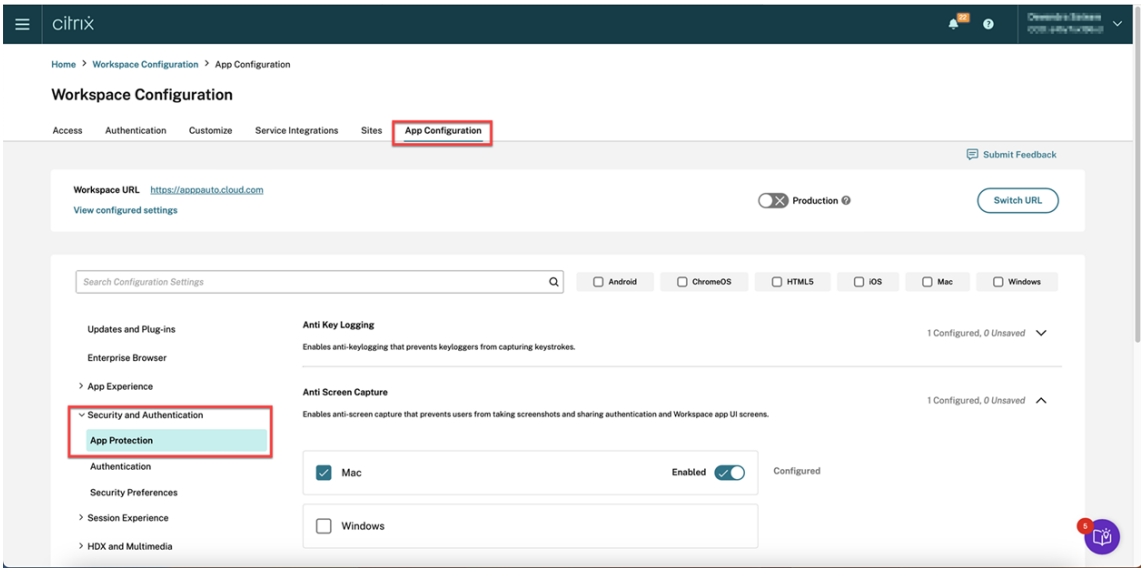
Using the Global App Configuration Service UI

1. Sign in to your Citrix Cloud™ account and select **Workspace Configuration**.

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

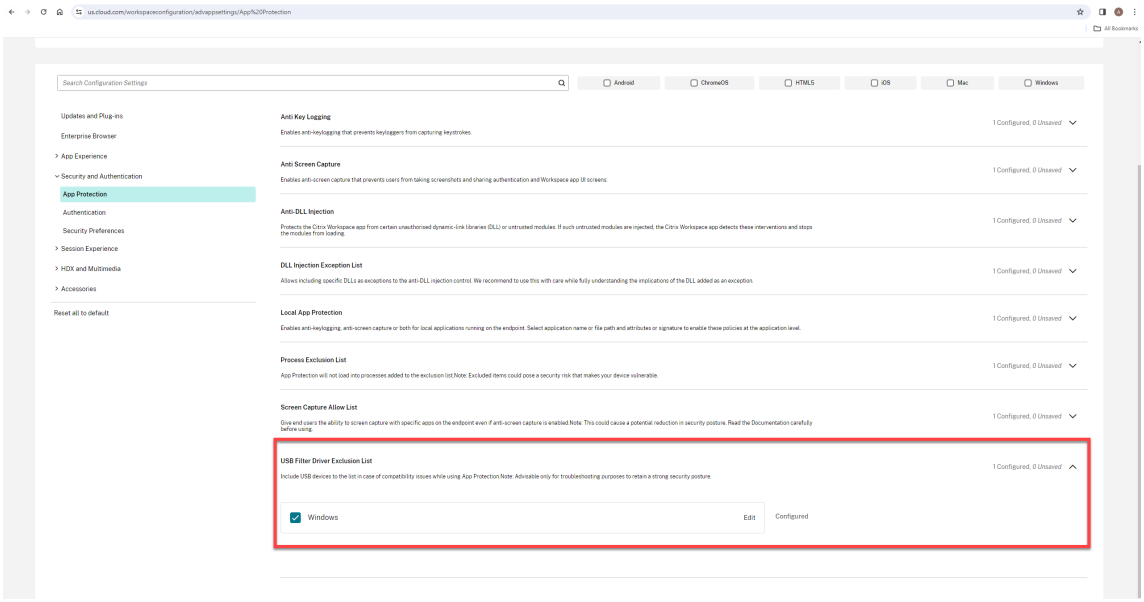


2. Select **App Configuration** > **Security and Authentication** > **Configure** > **App Protection**.



3. Click **USB Filter Driver Exclusion List** and then select the **Windows** checkbox.

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



4. Click the **Edit** option.

   The **Manage settings for Windows** screen appears.

5. Add the information about the process or app that you want to add to the USB Filter Driver Exclusion List.

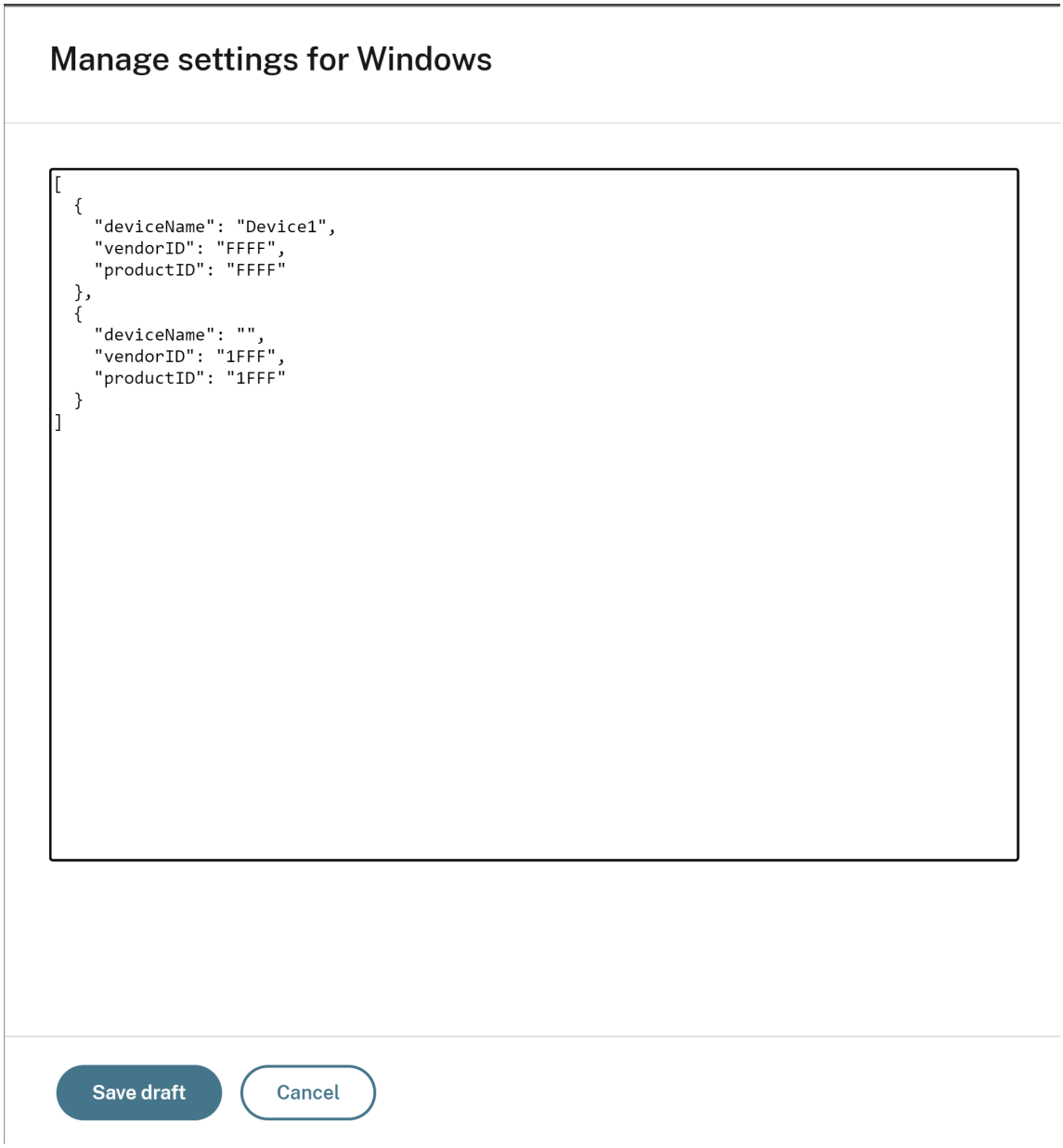
   For example,

```
[
 {

  "deviceName": "Device1",
  "vendorID": "FFFF",
  "productID": "FFFF"
  }

]
```

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



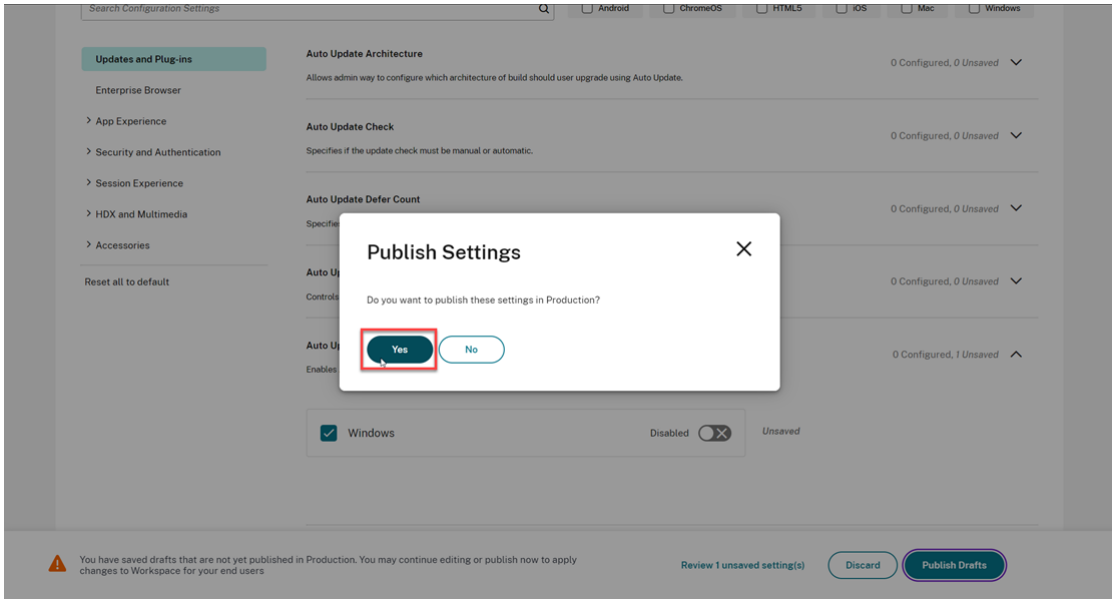
Note:

- The `productID` and `vendorID` must be mandatorily filled. At the same time, the `deviceName` isn't mandatory.
- Also, you can add multiple USB devices to the exclusion list by adding multiple entries in this block.

To get the `productID` and `vendorID`, see Get the `productID` and `vendorID`.

6. Click **Save draft** and then click **Publish Drafts**.
7. On the **Publish Settings** dialog box, click **Yes**.

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



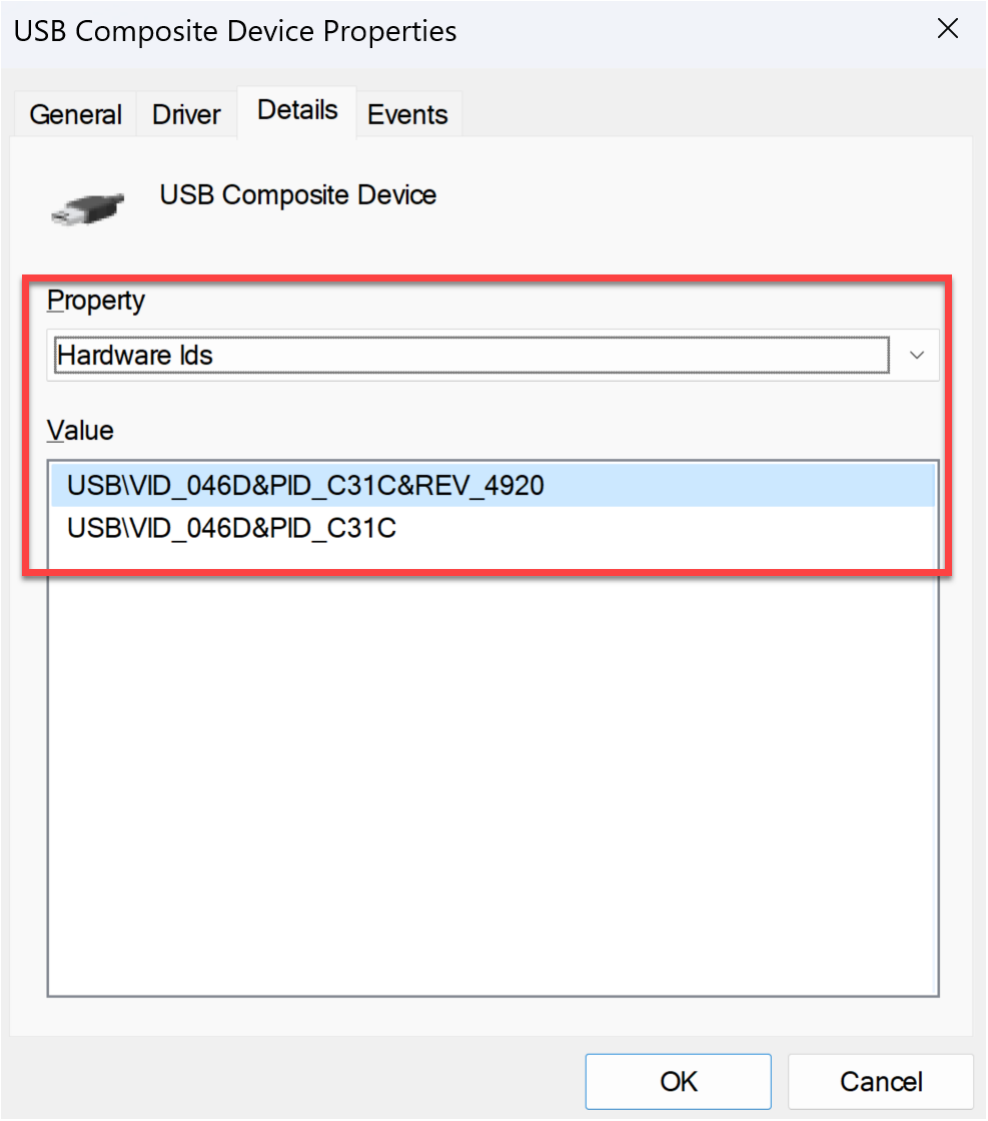
8. Restart Citrix Workspace app.

Get the `productID` and `vendorID`

To get the `productID` and `vendorID`, do the following steps:

1. Open **Device Manager** and find the device that you want to add to the exclusion list.
2. Right-click on the device name and then click **Properties**. A properties pop-up screen appears.
3. Click **Details** and then select the **Hardware Ids** option from the **Property** list.
4. In the **Value** field, the value with prefix of `VID_` is the `vendorID` and the value with prefix of `PID_` is the `productID`.

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



Configure allow list for the apps which use LD_PRELOAD functionalities

June 24, 2026

> **Note:**
>
> Configuring allow list using LD_PRELOAD functionality is only available for Citrix Workspace™ app for Linux.

App protection blocks the launch of a protected session if other apps running use LD_PRELOAD. If there are genuine apps or if approved by the admin, you can use the allow list feature. To permit the use of other apps which use LD_PRELOAD, you must configure the allow list.

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

App protection stops a protected session from starting if other apps using LD_PRELOAD are running. But if there are legitimate apps or if the admin approves, you can use the allow list feature. To allow these apps to run, you need to set up the allow list.

You can add apps with preload functionalities to the allow list using the following steps:

1. Identify the process that is blocking the protected VDA/App session from starting.
2. Create a configuration file for the allow list and add the identified process.

Identify the process preventing protected VDA launch

When AppProtection prevents the launch of a protected VDA due to LD_PRELOAD usage, verify processes using LD_PRELOAD. Genuine processes can be added to the allow list.

To identify processes using `LD_PRELOAD`, use the following script. Save it with a `.sh` extension and run it as `sudo` in a terminal window:

```
#!/bin/bash

declare -A map

append_kv() {

  local key="$1"
  local val="$2"
  local sep="$3"

  if [[ -v "map[$key]" && -n "${
 map[$key] }
 " ]]; then
    map["$key"]+="$sep$val"
  else
    map["$key"]="$val"
  fi
 }


escape_json_string() {

    local str="$1"
    # Escape backslashes first, then quotes, then other control
       characters
    str="${
 str//\\/\\\\ }
 "     # \ → \\
    str="${
 str//\"/\\\" }
 "     # " → \"
    str="${
 str//$'\t'/\\t }
```

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

```
 "   # tab → \t
    str="${
 str//$'\n'/\\n }
 "   # newline → \n
    str="${
 str//$'\r'/\\r }
 "   # carriage return → \r
    printf '%s' "$str"
 }


print_procs_JSON() {

    printf "{
 \n"
    first=true
    for key in "${
 !map[@] }
 "; do
        if [ "$first" = true ]; then
            first=false
        else
            printf ",\n"
        fi
        printf "  \"%s\": \"%s\"" "$(escape_json_string "$key")" "$(
            escape_json_string "${
 map[$key] }
 ")"
    done
    printf "\n }
 \n"
 }


validate_json() {

    local json="$1"

    if command -v jq >/dev/null 2>&1; then
        printf '%s' "$json" | jq -e . >/dev/null 2>&1
        return $?
    fi

    if command -v python3 >/dev/null 2>&1; then
        printf '%s' "$json" | python3 -c 'import json, sys; json.load(
            sys.stdin)' >/dev/null 2>&1
        return $?
    fi

    # No validator available on PATH.
    return 2
 }

```

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

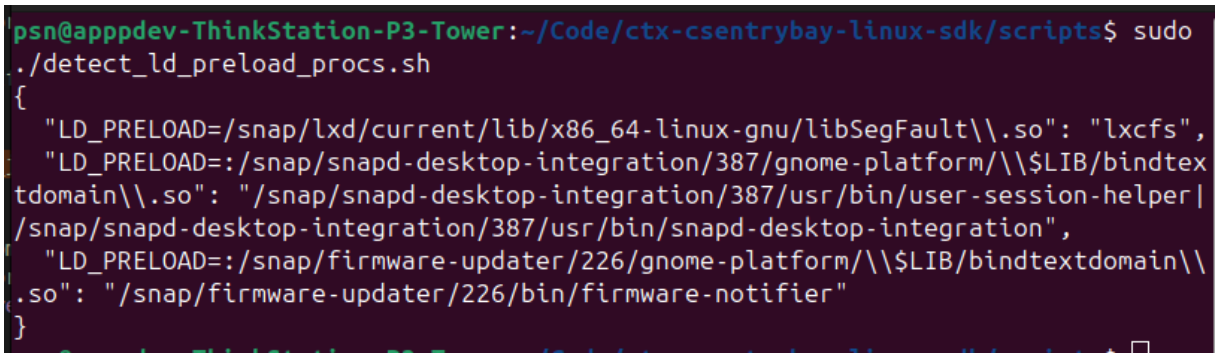
```
84
85  for pid in /proc/*/; do
86      pid=${
87   pid%*/ }
88
89      pid=${
90   pid##*/ }
91
92
93      # Only numeric /proc entries are process IDs.
94      [[ "$pid" =~ ^[0-9]+$ ]] || continue
95
96      environ_file="/proc/$pid/environ"
97      cmdline_file="/proc/$pid/cmdline"
98
99      if [[ ! -r "$environ_file" || ! -r "$cmdline_file" ]]; then
100         continue
101     fi
102
103     # Check if the process has the LD_PRELOAD environment variable set
104     ld_preload=$(cat "$environ_file" 2>/dev/null | tr '\0' '\n' | grep
            '^LD_PRELOAD=' | cut -d '=' -f 2-)
105     if [ -n "$ld_preload" ]; then
106         # Keep only argv[0] (the executable path/name) from cmdline.
107         cmdline=$(cat "$cmdline_file" 2>/dev/null | tr '\0' '\n' | head
                -n 1)
108         [ -n "$cmdline" ] || continue
109         # Output the LD_PRELOAD value and the process cmdline in JSON
              format
110         append_kv "LD_PRELOAD=$ld_preload" "$cmdline" "|"
111     fi
112 done
113
114 # Generate and validate JSON output before printing.
115
116 json_output="$(print_procs_JSON)"
117
118 if ! validate_json "$json_output"; then
119     status=$?
120     if [ "$status" -eq 2 ]; then
121         echo "Warning: could not validate JSON (no jq/python3 found)."
                >&2
122         printf '%s\n' "$json_output"
123         exit 0
124     fi
125
126     echo "Error: generated invalid JSON output." >&2
127     exit 1
128 fi
129
130 printf '%s\n' "$json_output"
```

Based on the output of the preceding script, identify the processes that are causing the protected VDA

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

launch to fail and add those processes to the allow list.

Here is a sample image displaying the output with a list of apps with a preload list.



Creating the allow list configuration file

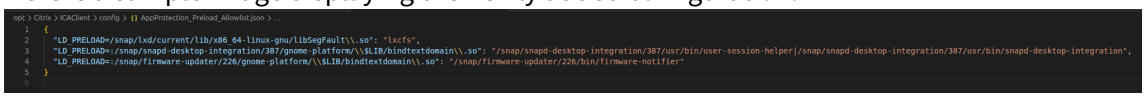
The process allow list configuration file isn't installed by default for security reasons. You need to create this configuration file the first time it's needed.

1. Create an empty file named AppProtection_Preload_Allowlist.json in the "$ICAROOT/config/" folder.
2. Add the process details in the following format. The second entry describes how to manage multiple processes that use the same library in LD_PRELOAD.

```
{

    "LD_PRELOAD_PATH1" : "PROCESS_PATH1",
    "LD_PRELOAD_PATH2" : "PROCESS_PATH2|PROCESS_PATH3"
 }
```

   Here is a sample image displaying the newly added configuration:



3. Save the file and then set the permissions to the AppProtection_Preload_Allowlist.json file using the following command.

```
sudo chmod 644 $ICAROOT/config/AppProtection_Preload_Allowlist.json
```

> **Note:**
>
> Minimal regex expressions are allowed in configuration entries to prevent redundancy. Special regex characters must be checked and escaped with a double backslash (\\).

- For example, consider that the script output is as follows:

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

```
LD_PRELOAD=:/snap/firmware-updater/226/gnome-platform/\\$LIB/bindtextdomain
\\.so": "/snap/firmware-updater/226/bin/firmware-notifier
```

- To use variable elements like the number 126, regex expressions can be used for a more generic allow list entry:

```
LD_PRELOAD=:/snap/firmware-updater/\\d+/gnome-platform/\\$LIB/bindtextdomain
\\.so": "/snap/firmware-updater/226/bin/firmware-notifier
```

- You can see that the output includes '.', '$'which are special characters in regex patterns, and have been escaped:

```
LD_PRELOAD=:/snap/firmware-updater/226/gnome-platform/\\$LIB/bindtextdomain
\\.so": "/snap/firmware-updater/226/bin/firmware-notifier
```

- If there are other special characters like " (quotation mark) or ^ (caret), escape them in the same way.

Disable App Protection

September 7, 2025

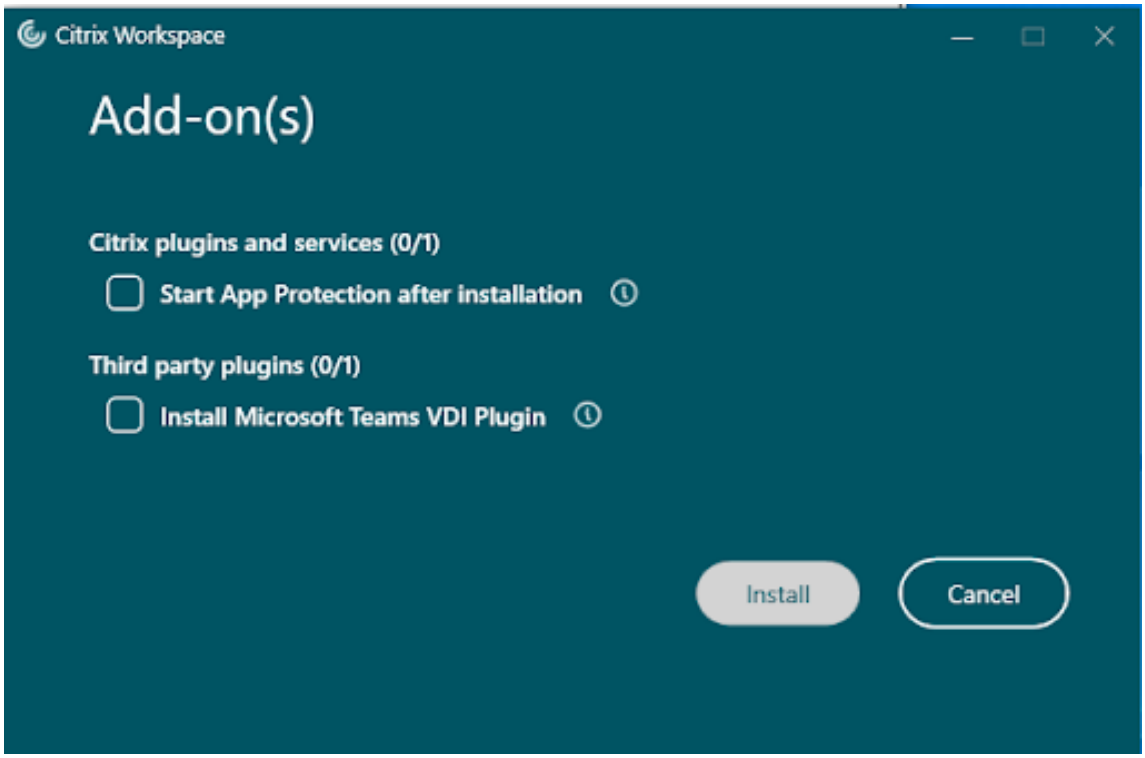
Steps to disable App Protection on Windows

Once App Protection is running, disabling App Protection is not supported. The only recommended solution is to reinstall the Citrix Workspace app and not passing the **Start App Protection** options to the installer.

To disable App Protection, please perform the following steps:

1. Uninstall the Workspace app.
2. Reboot the machine after completing the uninstallation.
3. Install the Workspace app again.
    - For UI-based installation, ensure the **Start App Protection after installation** checkbox is unchecked.

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

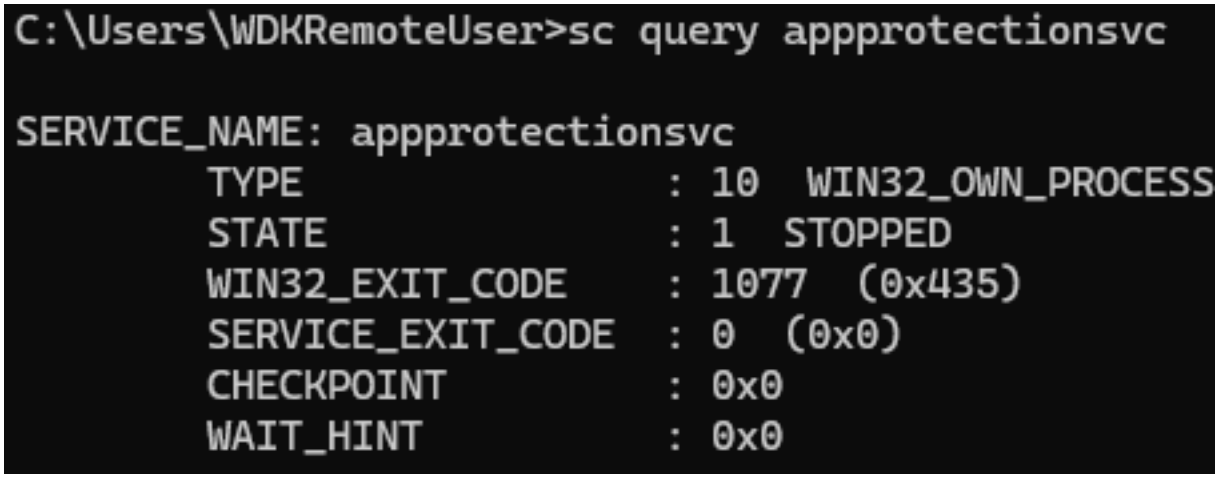


- For command line based installation make sure installation is started without having the `/startAppProtection` commandline option added.

  ex: `PS C:\Users\WDKRemoteUser\Downloads> .\CitrixWorkspaceApp.exe`

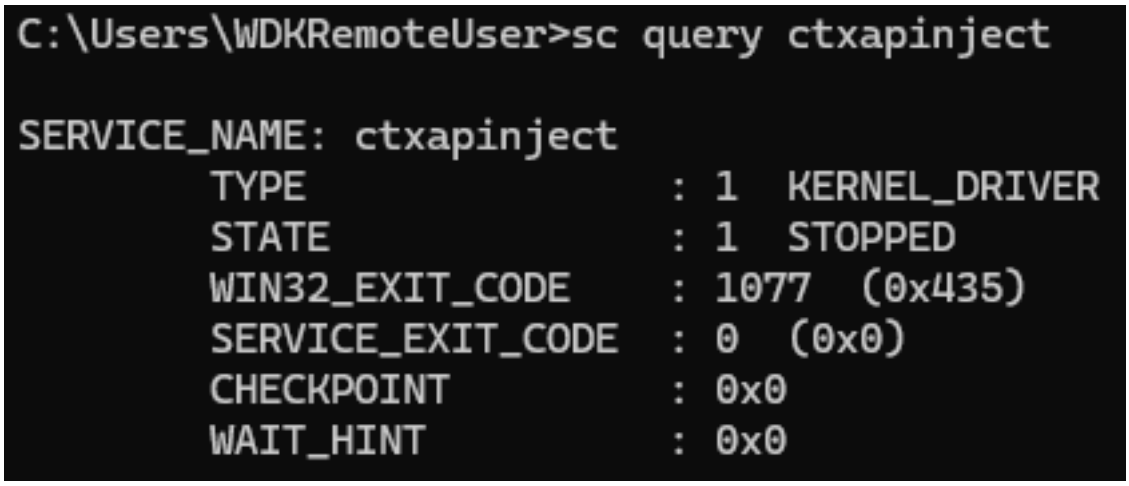
4. After completing the installation, confirm if App Protection is in a stopped state. Check if all the four components are in "Stopped"state by running the following commands in the command prompt. For each component, the status should display **STATE: 1 STOPPED**, as shown in the corresponding visual representations.

- `sc query appprotectionsvc`

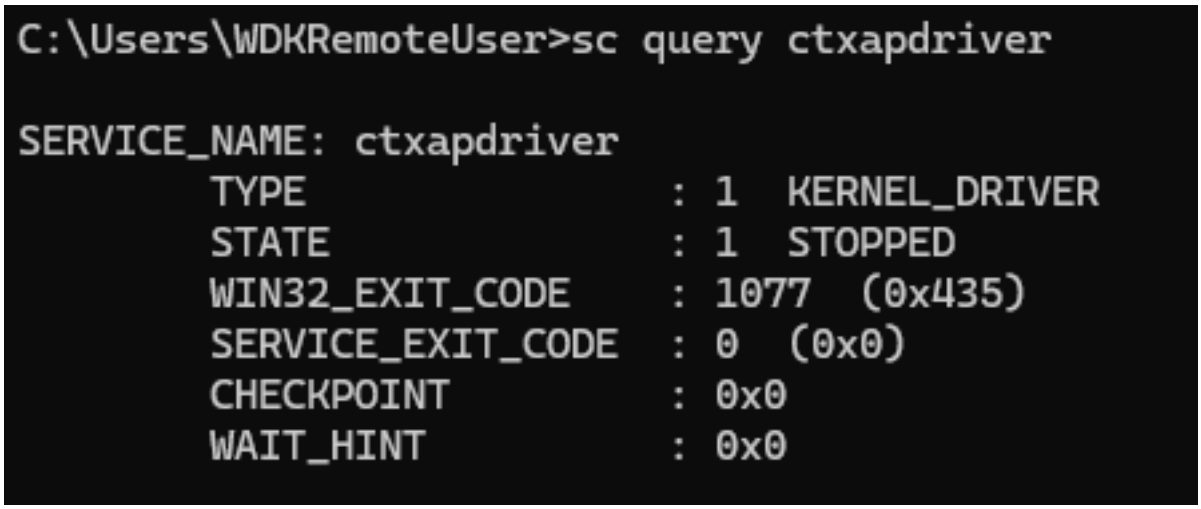


© 1997–2026 Citrix Systems, Inc. All rights reserved.

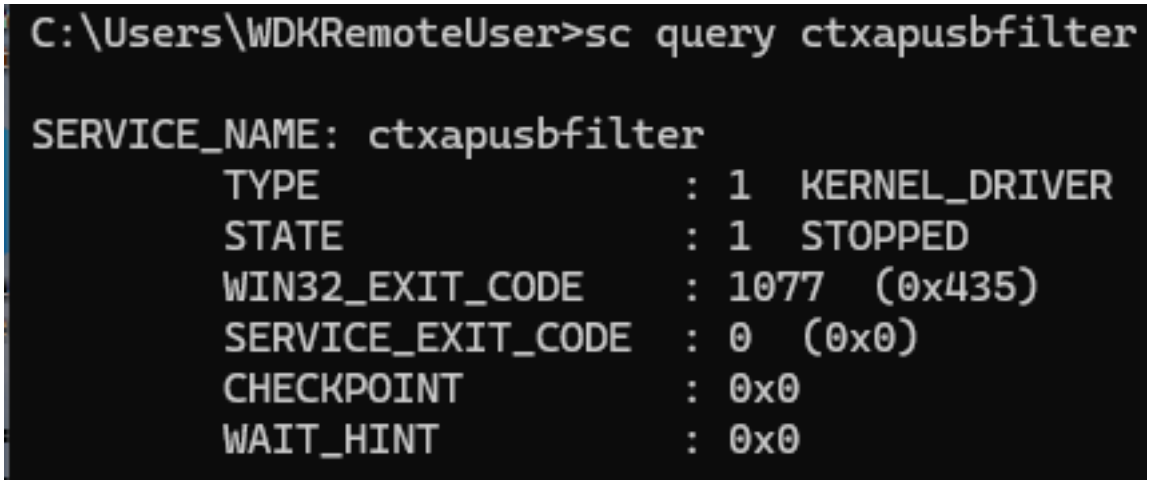
- `sc query ctxapinject`



- `sc query ctxapdriver`



- `sc query ctxapusbfilter`



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

> **Note:**
>
> Just keeping the `Start App Protection after installation` check box unchecked OR installing without the `/startAppProtection` command line option will not continue to keep App Protection in a stopped or dormant state. If any resource (Virtual app, Virtual Desktop, Auth, Web/Saas Apps) enabled with App Protection is launched, it will move all the App Protection services to Running state. Ensure that all App Protection configurations are set to "disabled" if you want to keep App Protection in a dormant state. For steps to disable various components, refer here.

Disable Screen Capture Notifications

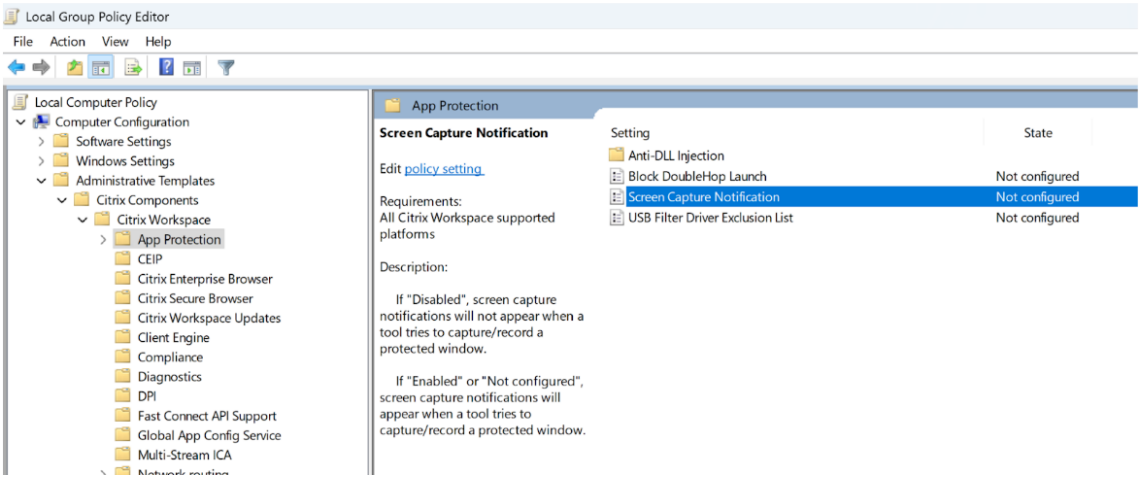
September 8, 2025

This document describes how to disable screen capture notifications.

You can disable screen capture notifications on Windows using the following method:

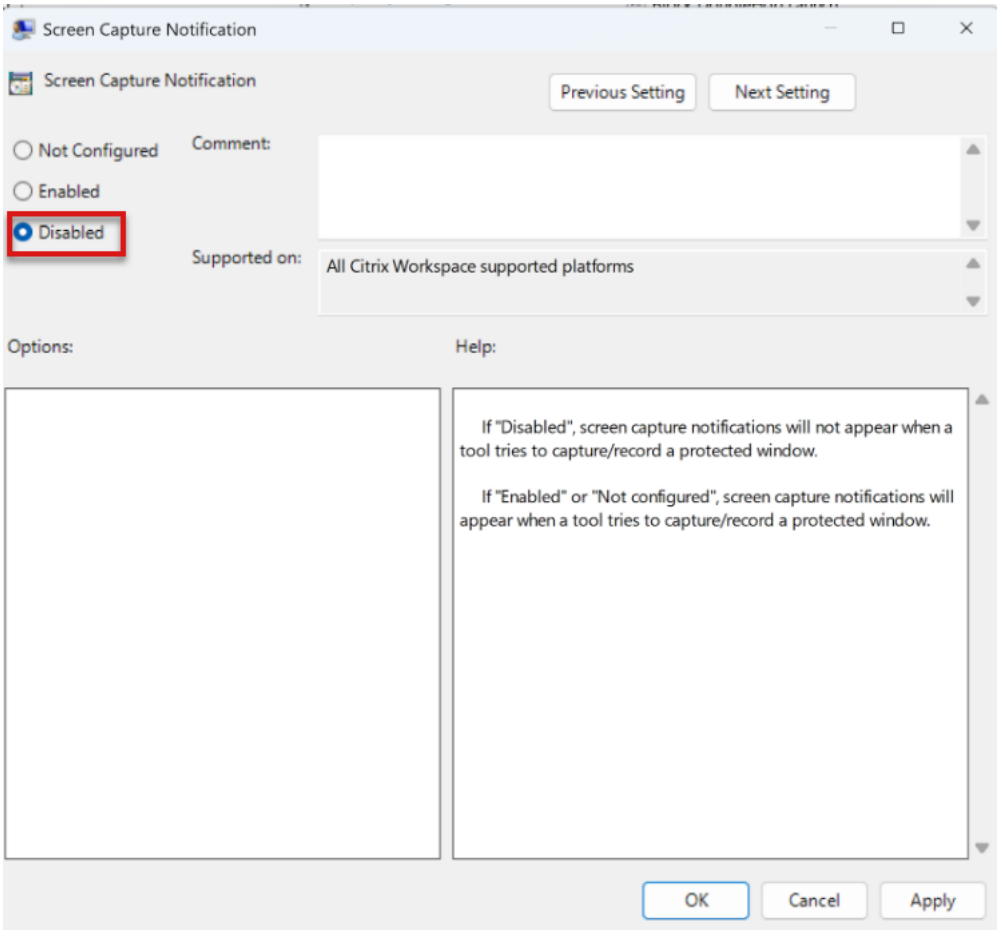
Disable Screen Capture Notification through GPO Setting

1. Open Group Policy Editor.
2. Navigate to **Computer Configuration** > **Administrative Templates** > **Citrix Components** > **Citrix Workspace™** > **App Protection** > and select **Screen Capture Notification**.



3. Select **Disabled** in the launched setting.

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



4. Select **Apply**.

Behavior Upon Disablement

Upon disablement, screen capture notifications do not appear when a user attempts to capture a protected resource.

> **Note:**
>
> If a screen capture allowlisted app is launched while this setting is configured, the screen capture notification setting is disregarded, and end users will begin to see notifications.

Troubleshoot

September 7, 2025

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

This article explains how to troubleshoot App Protection on different platforms for Citrix Workspace app.

For troubleshooting scenarios, see the following:

- Generic troubleshooting scenarios
- Policy Tampering Detection
- App Protection Posture Check

Check if App Protection is installed

Citrix Workspace app for Windows

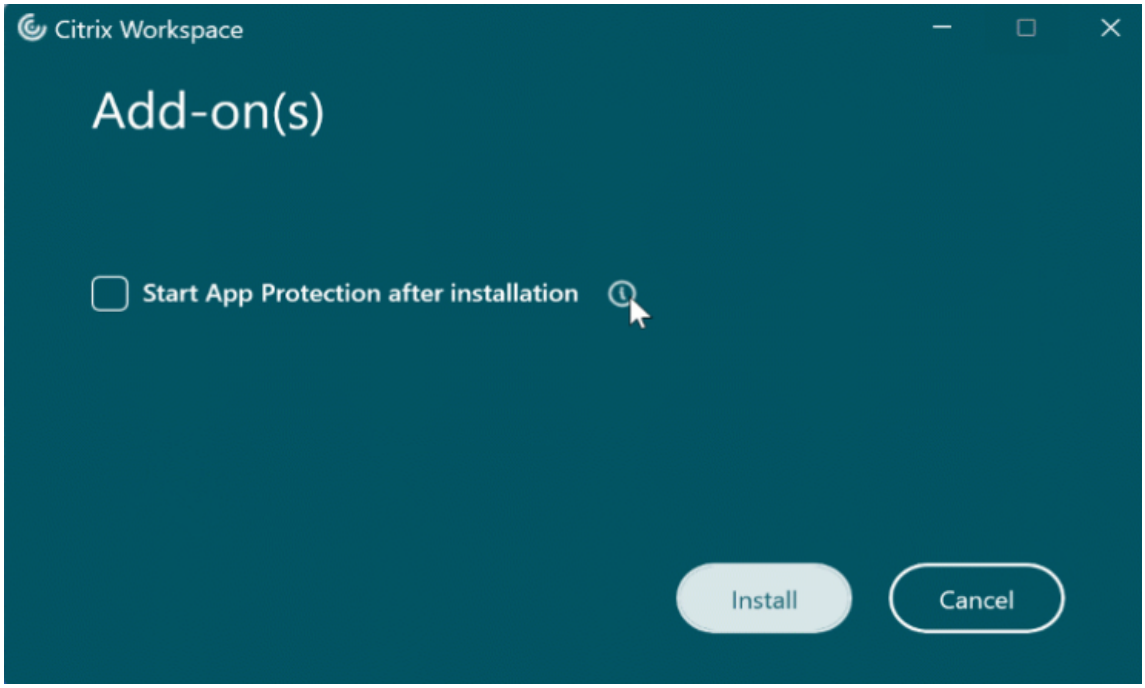
Starting with Citrix Workspace app version 2212, App Protection is installed by default. However, the component might be in an active or dormant state depending on whether the user selected the **Start App Protection after installation** checkbox.

- For Citrix Workspace app versions before 2311:



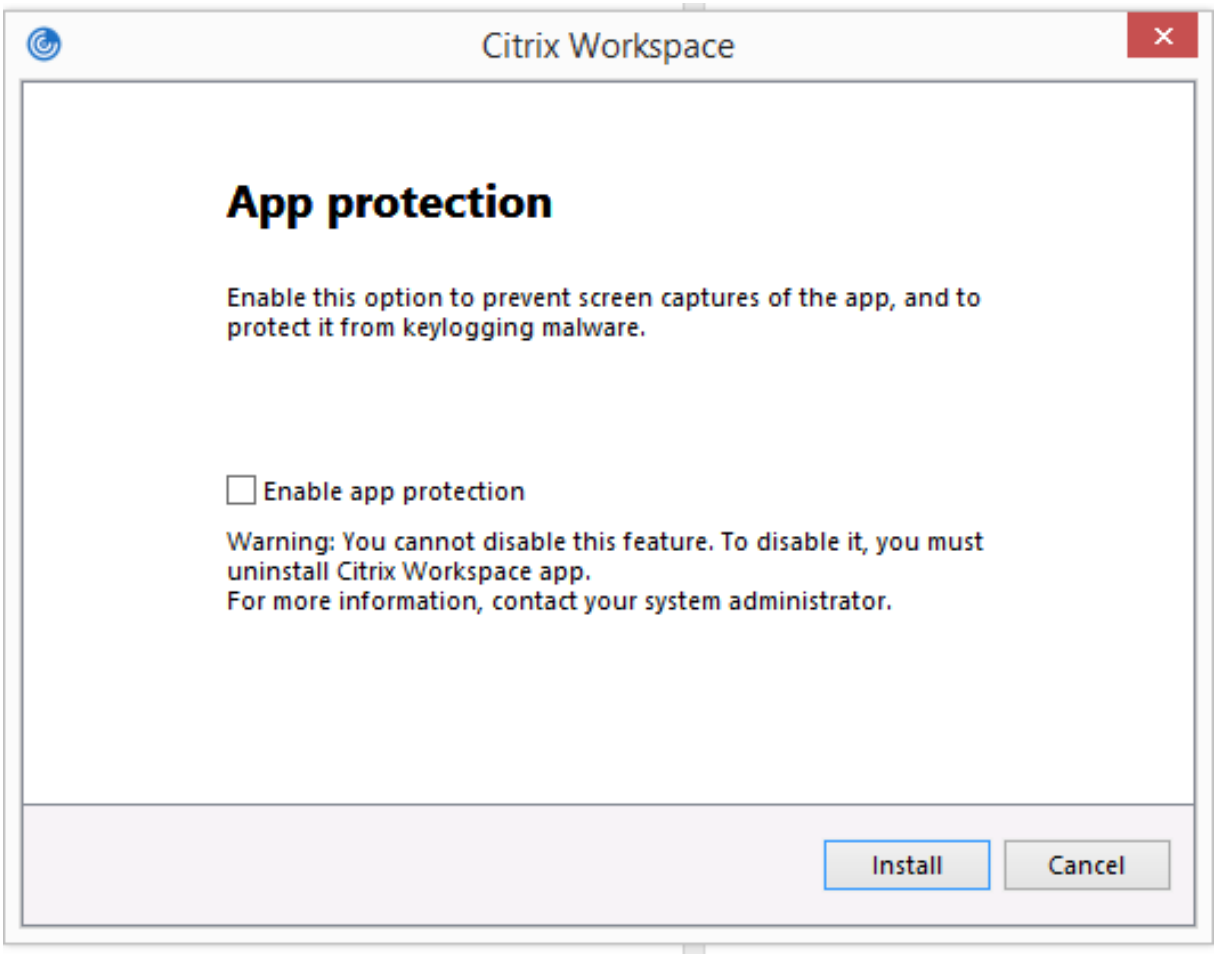
- From Citrix Workspace app version 2311 onwards:

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



For Citrix Workspace app versions before 2212, App Protection is installed and be in the active state only if you select the **Enable App Protection** checkbox while installing Citrix Workspace app.

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

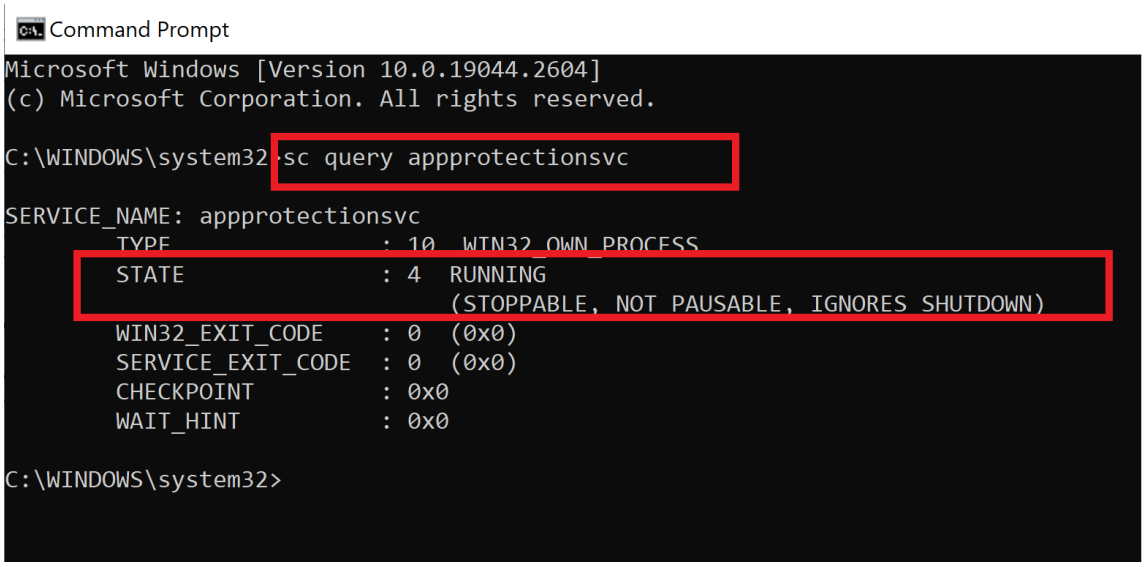


App Protection can either be in the **STOPPED** state or **RUNNING** state.
To check the status of the service, do one of the following steps:

- For Citrix Workspace app version 2206 or later, run the following command:

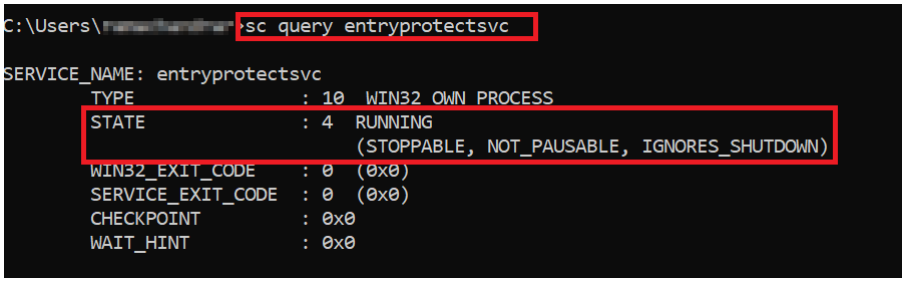
```
sc query appprotectionsvc
```

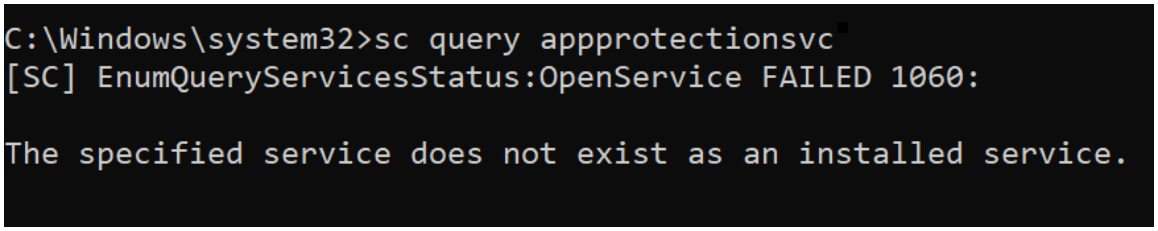
© 1997–2026 Citrix Systems, Inc. All rights reserved.



- For Citrix Workspace app versions before 2206, run the following command:

```
sc query entryprotectsvc
```



> **Note:**
>
> In Citrix Workspace app versions before 2212, if you didn't select the **Enable App Protection** checkbox while installing Citrix Workspace app and run the preceding command to check the status, then it displays the following error message:
>
> 
>

Citrix Workspace app for Windows

1. Collect logs as described in log collection.
2. Press **Win + R** to open the Run box > type cmd > Select **Enter**.

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

3. Run the following commands:

    - If you are using a Citrix Workspace app for Windows version before 2311, then run the following commands:

        - `sc query appprotectionsvc`
        - `sc query entryprotectdrv`
        - `sc query epinject6`
        - `sc query epusbfilter`

    - If you are using Citrix Workspace app for Windows version 2311 or later, then run the following commands:

        - `sc query appprotectionsvc`
        - `sc query ctxapdriver`
        - `sc query ctxapinject`
        - `sc query ctxapusbfilter`

Provide the results along with the traces collected from the log collection tool.

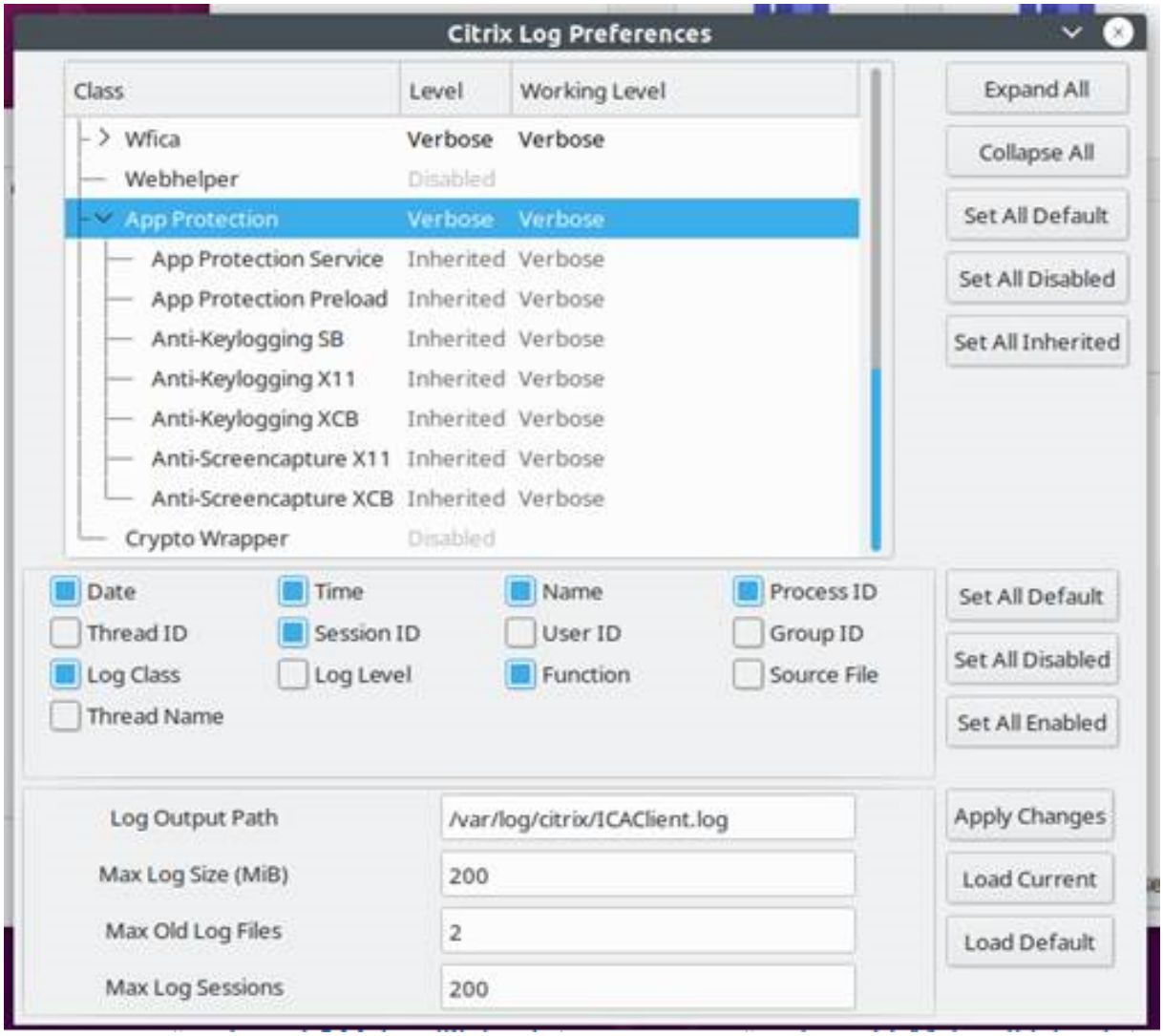
Citrix Workspace app for Mac

Provide the logs by collecting them as described in log collection.

Citrix Workspace app for Linux

1. Run the set log executable found in the *util* folder of the installation. For example, `/opt/Citrix/ICAClient/util/setlog`.
2. Click **Set All Disabled** (This step is optional, and makes sure that only the required logs are collected).
3. Go to App Protection logging.
4. Set App Protection log level to Verbose by right-clicking and selecting Verbose (only warnings and errors are logged).
5. Expand the App Protection class and right-click its child element. Select **Group > Inherited**.
6. Enable logs for **wfica**. Right-click **wfica** and select **Verbose**. If App Protection is not installed or not detectable by **wfica**, then you get the log as **[NCS] < P3563 > citrix-wfica: App Protection is not installed**.
7. When you launch the session, the logs are recorded in the file that is mentioned in the *Log output Path* of the set log.

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



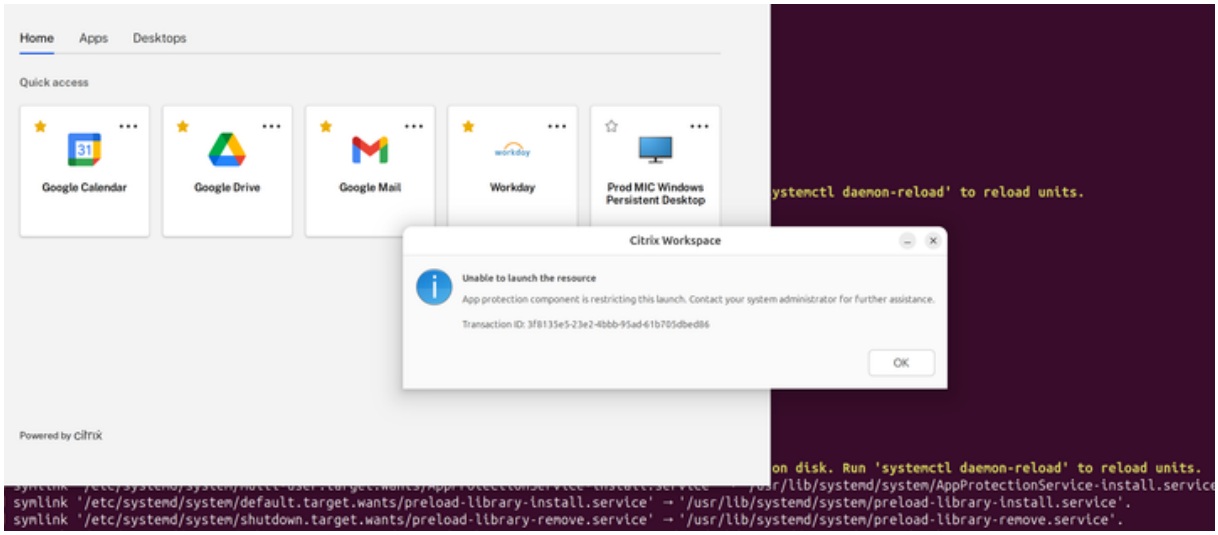
Generic troubleshooting

September 7, 2025

App Protection component restricting launch

Users encounter the following error when another application using preload is running on Citrix Workspace™ app for Linux:

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



To resolve the issue, follow these steps:

1. Verify that the App Protection service is running using the following command:

```
systemctl status AppProtectionService-install.service
```

2. Restart the machine and try again.
3. If the issue persists after the reboot, identify the process causing the issue using the script provided at Identify the process preventing protected VDA launch.
4. Close the interfering process and retry.
5. If the application is essential, consider using the LD_PRELOAD allowlist. For configuration details, see LD_PRELOAD allowlist configuration.
6. If the issue persists, collect the relevant logs and reach out to support. For more information, see Log collection.

Resources enabled with App Protection policies aren't displayed on native apps

If the resources enabled with App Protection policies aren't displayed on the native apps, then do the following steps:

1. Update your Citrix Workspace app to any higher version if it's older than the following:
   - Citrix Workspace app 2002 for Windows
   - Citrix Workspace app 2305.1 for Windows (Store)
   - Citrix Workspace app 2203.1 LTSR for Windows
   - Citrix Workspace app 2001 for Mac
   - Citrix Workspace app 2108 for Linux

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

- Citrix Workspace app for 24.7.0 for Android
- Citrix Workspace app for 24.9.0 for iOS

2. Make sure that you haven't installed the Citrix Workspace app in a Windows Multisession Operating System such as Windows 2K16 or Windows 2K22.
3. If the preceding conditions are met but still the resources aren't displayed, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

Resources enabled with App Protection policies aren't displayed on the browser while using the on-premises store

If the resources enabled with App Protection policies aren't displayed on the browser while using the on-premises store, then do the following steps:

1. Make sure that your Delivery Controller™ version isn't before version 1912.

   > **Note:**
   >
   > App Protection isn't supported if you're using a Delivery Controller before version 1912.

2. If you're using StoreFront versions between 1912 and 2203, verify if you've enabled the StoreFront customization. For more information about enabling StoreFront customization, see Enable StoreFront customization.
3. If you're using StoreFront version 2308 or later, you don't need to enable the StoreFront customization. Verify if you've enabled App Protection for hybrid launch on StoreFront correctly using Hybrid launch through StoreFront version 2308 or later.
4. Verify if you've enabled the App Protection features for the delivery group correctly.
5. If the preceding conditions are met but the resources are still not displayed, collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Collect Logs for Citrix Workspace app and Collect Logs for StoreFront.

Unable to establish a secure environment when launching App Protection-enabled resources

For the Citrix Workspace app for Windows, the **Start App Protection after installation** checkbox must be enabled during the installation to make sure that the App Protection services are started and the secure environment is established. If you didn't enable the **Start App Protection after installation** checkbox during the installation, the App Protection service starts automatically when you launch a resource enabled with App Protection policies. Based on the system load, App Protection might take

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

time to start. Sometimes, it might start or time out. So, selecting the **Start App Protection after installation** checkbox during installation is recommended. Usually, re-launch the resource enabled with App Protection and the secure connection must be established. However, if you are still not able to launch the resource enabled with App Protection, then do the following steps:

1. Open Command Prompt as Admin and run the following command and check if the App Protection service is running:

```
sc query AppProtectionSvc
```

2. If the App Protection service is not running, then start the service by running the following command:

```
sc start AppProtectionSvc
```

3. If you continue to get the error, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

Unable to enable or disable App Protection

If you aren't able to enable or disable App Protection for a delivery group for On-premises or Cloud using either Web Studio or PowerShell, then do the following steps:

1. Check if you have the required license. If the required licenses aren't available, then you can't enable the App Protection.
2. If the necessary licenses aren't available, then fetch the required licenses and add the licenses.
3. After adding the licenses, restart the license server and try enabling App Protection again.
4. If valid licenses are available but still you aren't able to enable or disable the App Protection, then check if the `TrustRequestsSentToTheXmlServicePort` is enabled by running the following command:

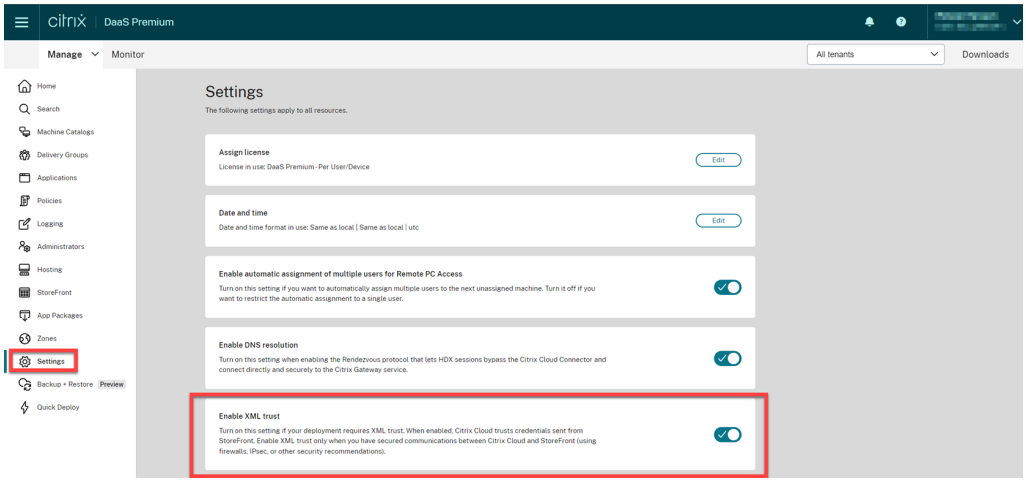
```
Get-BrokerSite | Select-Object
    TrustRequestsSentToTheXmlServicePort
```

5. If the `TrustRequestsSentToTheXmlServicePort` isn't enabled, then enable the XML Trust using one of the following methods:

    - **Using Web Studio:**

        a) Sign in to your Citrix DaaS™ account and go to **Manage** > **Settings** > **Enable XML trust**.

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



b) Turn on the **Enable XML trust** toggle.

- **Using PowerShell:** Run the following command to enable XML trust:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

6. After enabling the `TrustRequestsSentToTheXmlServicePort`, enable App Protection again.
7. If the preceding conditions are met but you're still not able to enable or disable App Protection, then contact Citrix Technical Support.

App Protection policies are not applied properly

1. Make sure that the following conditions are met:
   - You're using a supported version of the Citrix Workspace app.
   - The Delivery Group has the proper features enabled.
   - The feature is installed on the endpoint.
   - The Citrix Workspace app was installed with the `/includeappprotection` switch enabled.
2. If the preceding conditions are met but still App Protection policies aren't applied properly, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Collect Logs for Citrix Workspace app

Screenshots not working on non-Citrix windows:

- Minimize or close the protected Citrix windows, including the Citrix Workspace app.

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

Unable to boot to OS when Citrix Workspace app is installed with App Protection on Linux

1. If you're using Citrix Workspace app earlier than version 2204, the App Protection feature does not support the operating systems that use `glibc` 2.34 or later.
2. If you do install it, the OS boot might fail on restarting the system. To recover from the OS boot failure, do one of the following:
    - Reinstall the OS.
    - Go to Recovery mode of the OS and uninstall the Citrix Workspace app using the terminal.
    - Boot through the live OS and remove the `rm -rf /etc/ld.so.preload` file from the existing OS.

Troubleshoot Policy Tampering Detection

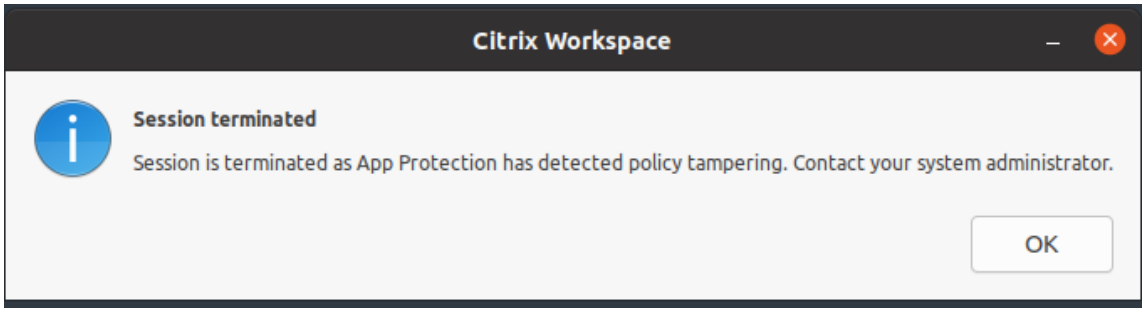
September 7, 2025

The following section describes some of the issues that you might face and how to troubleshoot them:

The ICA® file is tampered and the session is still running

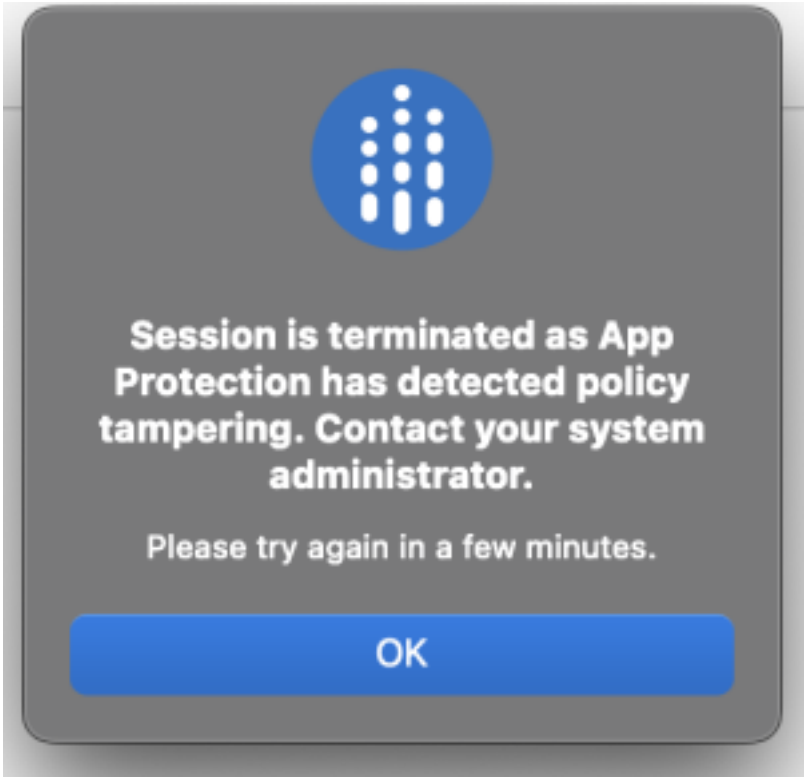
If the ICA file of a virtual app or desktop session that is enabled with the App Protection Policy Tampering Detection feature is tampered with, then the session must be terminated displaying one of the following error messages:

- Citrix Workspace app for Linux

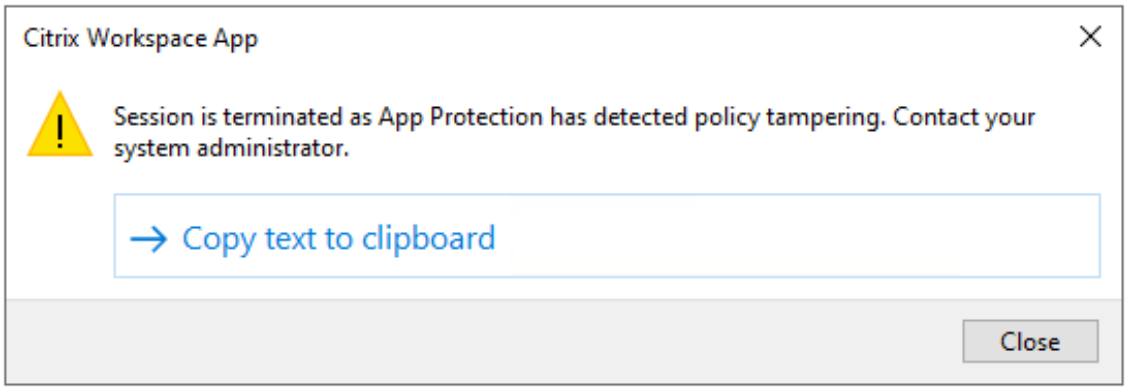


- Citrix Workspace app for Mac

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



- Citrix Workspace app for Windows



However, if the session is running even if the ICA file is tampered with and Policy Tampering Detection is enabled, then do the following steps:

1. In the Virtual Delivery Agent, do the following:

   a) Run the following command and check if the `ctxappprotectionsv` service is running:

   ```
   sc query ctxappprotectionsvc
   ```

   b) If the `ctxappprotectionsvc` service isn't running, then do the following steps to start the service:

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

i. Change the startup type of the `ctxappprotectionsvc` service to automatic by running the following command:

```
sc config ctxappprotectionsvc start=auto
```

ii. Start the service by running the following command:

```
sc start ctxappprotectionsvc
```

2. In the client, do the following:

a) Check if the *vdappp.dll* file is in the installation location of the Citrix Workspace app. The default installation location of the Citrix Workspace app is as follows:

- Windows - C:\Program Files (x86)\Citrix\ICA Client
- Linux - /opt/Citrix/ICAClient
- Mac - Not applicable

b) For Citrix Workspace app for Windows, use *procexp.exe* and check if the *vdappp.dll* file is loaded in *wfica32.exe*.

c) For Citrix Workspace app for Linux, check if the *vdappp.dll* file is loaded in *wfica.exe*.

3. If the session is still running, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

Policy Tampering Detection stops working after rebooting Virtual Delivery Agent

If you reboot the Virtual Delivery Agent and the Policy Tampering Detection feature stops working, then it might be because the App Protection service isn't running after reboot. Do the following steps on the Virtual Delivery Agent:

1. Run the following command and check if the `ctxappprotectionsvc` service is running and set to **automatic**:

```
sc query ctxappprotectionsvc
```

2. If the `ctxappprotectionsvc` service isn't running, then do the following steps to start the service:

a) Change the startup type of the `ctxappprotectionsvc` service to **automatic** by running the following command:

```
sc config ctxappprotectionsvc start=auto
```

b) Start the service by running the following command:

```
sc start ctxappprotectionsvc
```

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

3. If the Policy Tampering Detection feature is still not working, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

Troubleshooting App Protection Posture Check

February 28, 2024

The following section describes some of the issues that you might face and how to troubleshoot them:

The session terminated without any error message

If your virtual app or desktop session terminates abruptly without displaying any error message, then do the following steps:

1. Check if your Citrix Workspace app version is earlier than one of the following versions:
   - Citrix Workspace app for Windows 2309
   - Citrix Workspace app for Mac 2308
   - Citrix Workspace app for Linux 2308

   > **Note:**
   >
   > If the Citrix Workspace app version is earlier than the versions listed in step 1 and the App Protection Posture Check feature is enabled, then the virtual app or desktop session terminates without displaying any error message. However, if the Citrix Workspace app version is greater than or equal to the versions listed in step 1 and the App Protection Posture Check feature is enabled, then the virtual apps or desktop session terminates displaying an error message.

2. Check whether the App Protection Posture Check feature is enabled.
3. If the Citrix Workspace app version is greater than or equal to the preceding versions and the Posture Check feature is also active, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

App Protection Posture Check is enabled but the session is not terminated for older versions

Generally, if the App Protection Posture Check feature is enabled and you are connecting through an older version of Citrix Workspace app, then the session must be terminated.

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

But if the session is not terminated, then do the following steps:

1. In the Virtual Delivery Agent, do the following:

    a) Run the following command and check if the `ctxappprotectionsvc` service is running:

    ```
    sc query ctxappprotectionsvc
    ```

    b) If the `ctxappprotectionsvc` service is not running, then do the following steps to start the service:

        i. Change the startup type of the `ctxappprotectionsvc service` to **automatic** by running the following command:

        ```
        sc config ctxappprotectionsvc start=auto
        ```

        ii. Start the service by running the following command:

        ```
        sc start ctxappprotectionsvc
        ```

2. Check if the Posture Check values that you have entered have one of the following prefixes:

    - For Citrix Workspace app for Windows, `windows-`
    - For Citrix Workspace app for Linux, `linux-`
    - For Citrix Workspace app for Mac, `mac-`

3. Check if the Posture Check values are correctly added as per the relevant platform as they are platform-specific.

4. Check the `reg` location (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) to verify if the Posture Check is synced with the Virtual Delivery Agent.

5. If all the preceding conditions are met and the session is still connected for the older versions of Citrix Workspace app, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

App Protection Posture Check is working on one platform but not working on another

Sometimes, the App Protection Posture Check feature might work on one platform and not on another. For example, the App Protection Posture Check feature is working on Citrix Workspace app for Windows but not on Citrix Workspace app for Linux.

In scenarios like these, do the following steps:

1. Check if the Posture Check values that you have entered have one of the following prefixes:

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

- For Citrix Workspace app for Windows, `windows-`
- For Citrix Workspace app for Linux, `linux-`
- For Citrix Workspace app for Mac, `mac-`

2. Check if the Posture Check values are correctly added as per the relevant platform as they are platform-specific.
3. Check the `reg` location (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) on the Virtual Delivery Agent to verify if the Posture Check is synced with the Virtual Delivery Agent. They must match with what was configured on Studio.
4. If all the preceding conditions are met and the session is still connected for the older versions of Citrix Workspace app, then collect the logs and contact Citrix Technical Support. For more information about collecting logs, see Log collection.

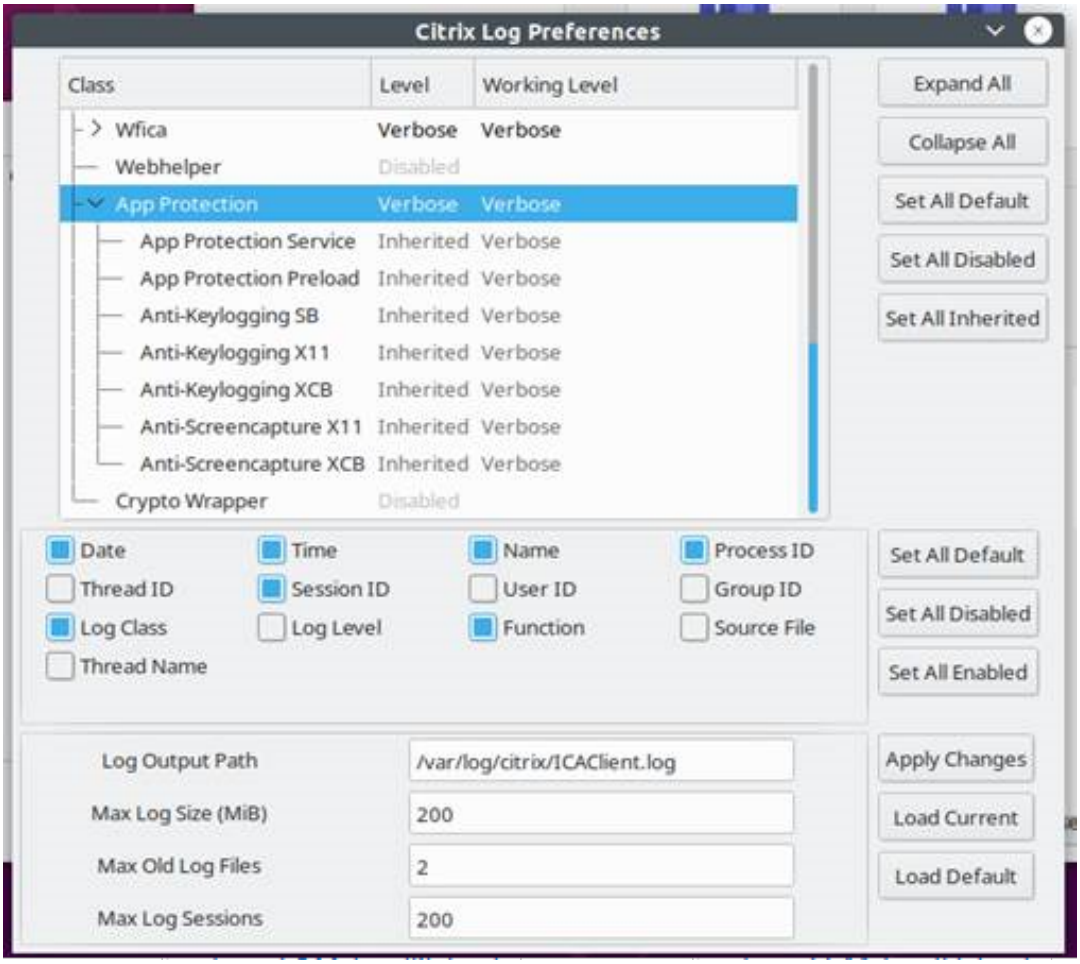
Log collection

July 24, 2024

- To collect logs for Citrix Workspace app for Windows, see Log collection for Windows.
- To collect logs for Citrix Workspace app for Mac, see Log collection for Mac.
- To collect logs for Citrix Workspace app for Android, see How to collect logs.
- To collect logs for Citrix Workspace app for Linux, do the following steps:
    1. Run the set log executable found in the *util* directory of the installation. For example, */opt/Citrix/ICAClient/util/setlog*.
    2. (Optional) Click **Set All Disabled** and make sure that only the required logs are collected.
    3. Go to App Protection logging.
    4. Set the App Protection log level to Verbose by right-clicking and selecting **Verbose** (only warnings and errors are logged).
    5. Expand the App Protection class and right-click its child element. Select **Group** > **Inherited**.
    6. Use the linux logging utility (from *install dir*, launch *util/setlog*) and change the logging level for the virtual channel to Verbose.
    7. Enable logs for **wfica**. Right-click **wfica** and select **Verbose**. If App Protection isn't installed or not detectable by **wfica**, then you get the log as **[NCS] < P3563 > citrix-wfica: App Protection is not installed**.

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

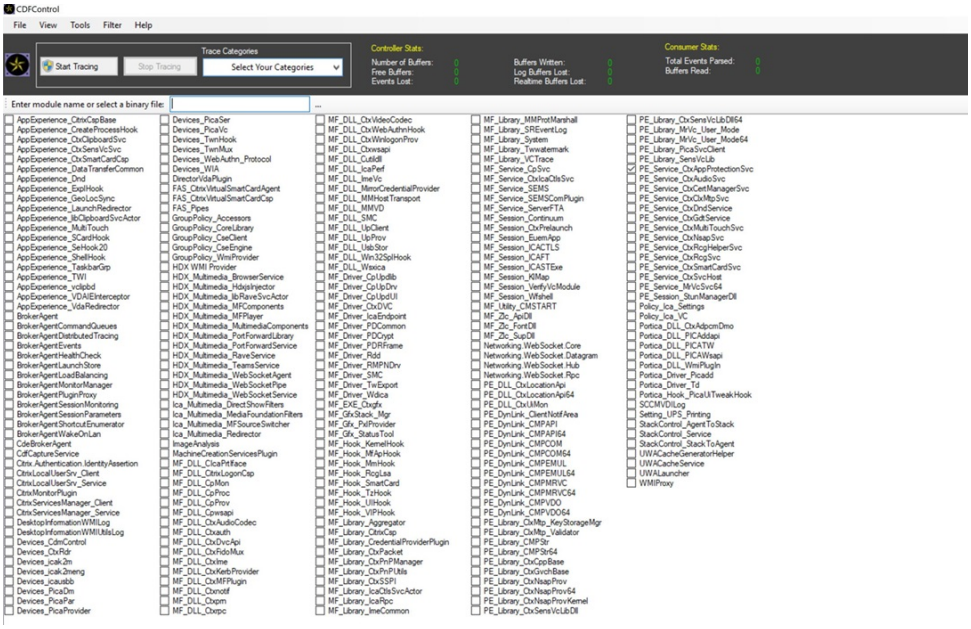
8. Click **wfica** and change the logging level for **winstation driver** to **Verbose**.
9. When you launch the session, the logs are recorded in the file that is mentioned in the log output Path of the set log.



- To collect logs for the Virtual Delivery Agent, do the following steps:

1. To get traces from the App Protection service through CDF control, select all the modules.

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



2. In certain cases, we might have to capture cdf traces from a different machine. To collect cdf traces, see CTX237216.

Advanced Troubleshooting on Windows

May 14, 2025

The following guide provides a systematic approach to gathering issue-specific logs, reducing communication between the end user and the engineer responsible for triaging the issue.

Application is unresponsive after installing CWA with App Protection

1. Collect Citrix Workspace app logs as mentioned in the log collection section.
2. Collect **System details** as mentioned in the System details section.
3. Collect **Issue Environment** as mentioned in the Issue Environment section.
4. Collect **Environment Details** as mentioned in the Environment Details section.
5. Collect **Other details** as mentioned in the Other details section.
6. For performance issues like process hang, capture a full memory dump of the concerned process using:
   - `procdump -ma 1234 C:\dumps\myprocess.dmp`
   - `1234` is the process ID of the concerned app.
   - `C:\dumps\myprocess.dmp` is the path to the dump file.
7. Save all the logs collected in a zip file and upload it in Citrix Support case.

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

Application crashes after installing CWA with App Protection

1. Collect Citrix Workspace app logs as mentioned in the log collection section.
2. Collect **System details** as mentioned in the System details section.
3. Collect **Issue Environment** as mentioned in the Issue Environment section.
4. Collect **Environment Details**as mentioned in the Environment Details section.
5. Collect **Other details** as mentioned in the Other details section.
6. Configure Windows to capture full memory dumps for crashing applications. Refer to MSDN for details Collecting User-Mode Dumps
7. Save all the logs collected in a zip file and upload it in Citrix Support case.

System encounters BSOD when CWA is installed with AppProtection

1. Collect Citrix Workspace app logs as mentioned in the log collection section.
2. Collect **System details** as mentioned in the System details section.
3. Collect **Issue Environment** as mentioned in the Issue Environment section.
4. Collect **Environment Details** as mentioned in the Environment Details section.
5. Collect **Other details** as mentioned in the Other details section.
6. Note down the **Stop error code** displayed on the BSOD page
7. Configure Windows to collect a full memory dump for BSOD. Follow the link for guidance Generate a Kernel or Complete Crash Dump
8. Save all the logs collected in a zip file and upload it in Citrix Support case.

Application is not behaving in the expected way after installing CWA with App Protection

If the application exhibits unexpected behavior, such as slowness, graphical corruption, or keyboard issues, follow the following steps:

1. Collect Citrix Workspace app logs as mentioned in the log collection section.
2. Collect **System details** as mentioned in the System details section.
3. Collect **Issue Environment** as mentioned in the Issue Environment section.
4. Collect **Environment Details** as mentioned in the Environment Details section.
5. Collect **Other details** as mentioned in the Other details section.
6. Save all the logs collected in a zip file and upload it in Citrix Support case.

System Details

1. To obtain advanced system details, run the following command and provide the resulting .nfo file:

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

- msinfo32 /nfo `C:\path\to\output\systeminfo.nfo`
- Save the `.nfo` file to be shared across with Citrix

2. Use the following PowerShell command to list installed applications and save the output to a file:

```
Get-WmiObject -Query "SELECT * FROM Win32_Product"| Select-Object
 -Property Name, Version | Out-File -FilePath "C:\path\to\your\
installed_apps.txt"
```

3. Save the `installed_apps.txt` file, which is to be shared with Citrix.

Issue Environment

1. **Upgrade Details**: Include information on recent OS, CWA, or software upgrades, specifying previous and updated patch or version details.
2. **Upgrade Method**: Indicate whether the upgrade was manual or via auto-update.
3. **System Restart**: Confirm if the system was restarted post-installation.
4. **Software-Specific Issues**: Provide comprehensive details if the issue relates to specific software.
5. **Configuration Settings**: Include relevant configurations such as GACS, MDM, SPA, GPIO, Director-Monitor, or App Protection.
6. **Reproduction Steps**: Offer detailed steps for reproducing the issue.
7. **Issue Frequency**: Specify how often the issue occurs (for example, Always, Once, 1/10, 5/10).

Environment Details

1. **Setup Type**: Specify if the environment is On-premises, Cloud, or Hybrid.
2. **Gateway Details**: Provide information on any gateways in use.
3. **CVAD Version**: State the version of Citrix Virtual Apps and Desktops.
4. **Broker Version**: Mention the broker version in use.
5. **StoreFront/WSP Version**: Include the version details of StoreFront or Workspace Services Platform.
6. **Anti-virus and Anti-malware**: List installed security software with version information.
7. **Virtualization Software**: Mention any virtualization software in use.
8. **Video Recording**: Provide a recording of the issue for better analysis.

Other Details

1. **Test Setup and Credentials**: Provide access to a test environment with credentials for accurate issue replication and testing.

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

2. **Customer Contact for Debugging**: Share the contact details of a knowledgeable customer representative to assist in troubleshooting.
3. **Compatibility and Vendor Collaboration**: Share support tickets for compatibility issues with other vendors to facilitate collaboration.
4. **Impacted Devices**: Report the number of affected devices to prioritize and allocate resources for resolution.

App Protection Health Checker

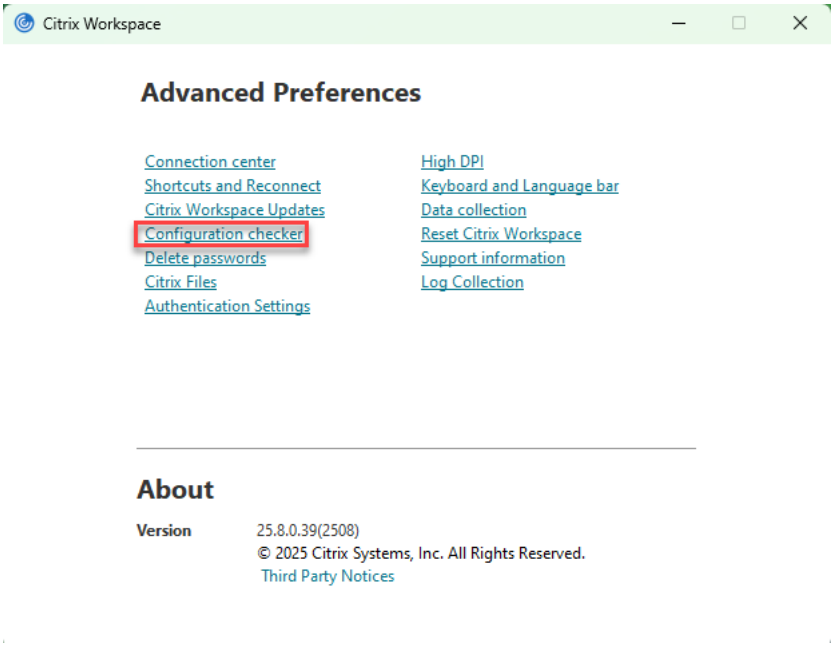
September 15, 2025

The **App Protection Health Checker** is part of the Citrix Workspace app (CWA) Advanced Preferences. You can find it in the Configuration Checker. This tool helps you check the health and setup of your AppProtection environment from your local CWA client. Use it to spot issues early and keep your experience smooth.

How to Access the App Protection Health Checker

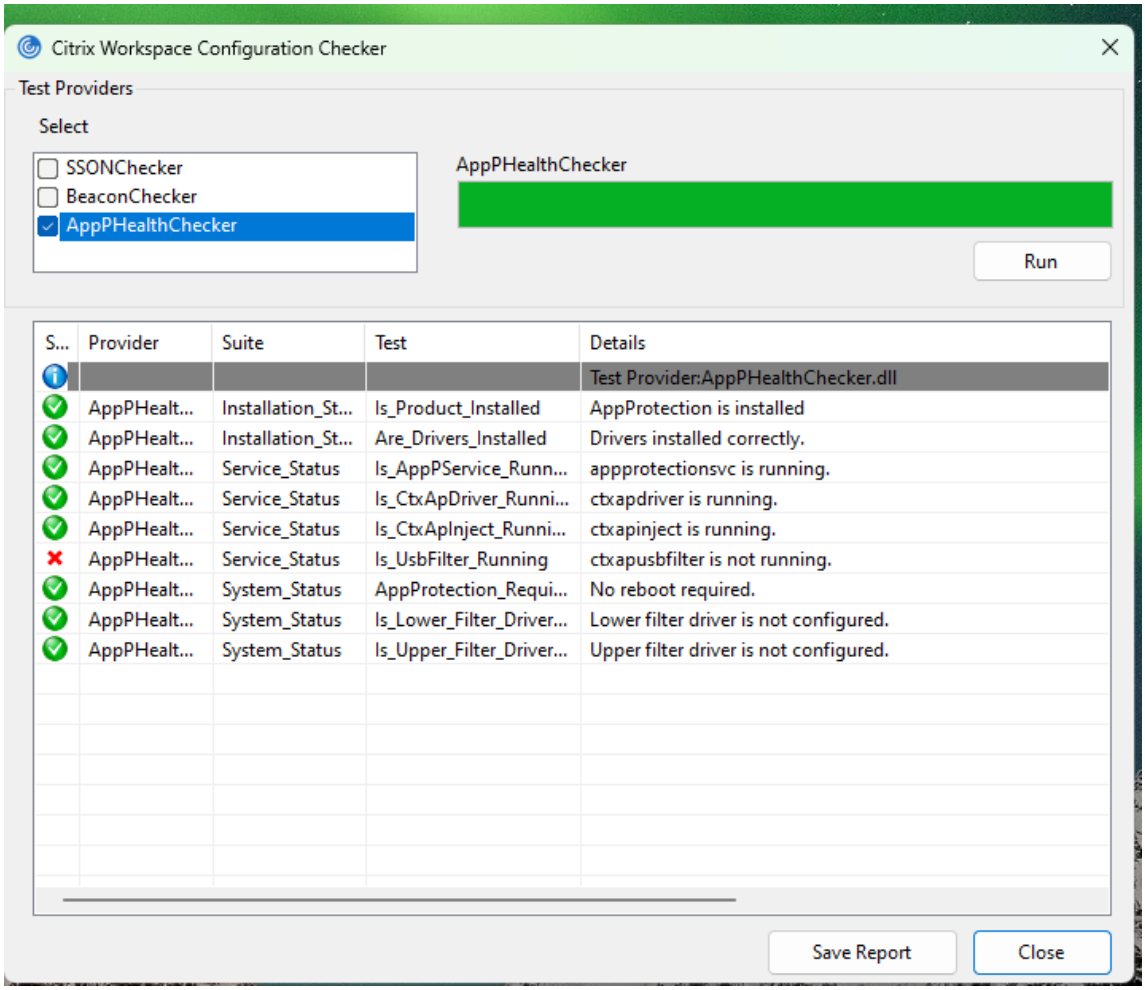
You can access this feature through the CWA Advanced Preferences by following the steps below:

1. Open the Citrix Workspace app.
2. Go to **Advanced Preferences**.
3. Select the **Configuration Checker** section.



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

4. The App Protection Health Checker is available within this section.



Using the App Protection Health Checker

The App Protection Health Checker runs diagnostic checks on your system's AppProtection configuration and operational status. This tool provides insights into your environment's health. It helps you identify potential configuration discrepancies or operational issues.

> **Note:**
>
> The tool does not automatically repair issues. However, its output provides diagnostic information for troubleshooting. Using this diagnostic information enhances application performance and reliability.

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

Contextual App Protection for Workspace

September 7, 2025

Contextual App Protection provides the granular flexibility to apply the App Protection policies conditionally for a subset of users - based on users, their device, and the network posture.

Implementing contextual App Protection

You can implement contextual App Protection using the connection filters defined in the Broker Access policy rule. The Broker Access policies define the rules controlling a user's access to delivery groups. The policy comprises a set of rules. Each rule relates to a single delivery group, and has a set of connection filters and access right controls.

Users gain access to a delivery group when their connection's details match the connection filters of one or more rules in the Broker Access policy. Users don't have access to any delivery group within a site by default. You can create more Broker Access policies based on requirements. Multiple rules can apply to the same delivery group. For more information, see New-BrokerAccessPolicyRule.

The following parameters in the Broker Access policy rule provide the flexibility to enable App Protection contextually if the user's connection matches the connection filters defined in the access policy rule:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Use the Smart Access policies referenced in the Broker Access policy rules to further refine the connection filters. Refer to the scenarios explained in this article to understand how to use the Smart Access policies to set up contextual App Protection.

Contextual App Protection scenarios

Following are some of the scenarios about how you can enable Contextual App Protection:

- Enable App Protection for External users coming through the Access gateway
- Enable App Protection for Untrusted Devices
- Enable App Protection based on Device Posture results
- Enable App Protection for specific user groups

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

Prerequisites

February 28, 2024

Make sure that you have the following:

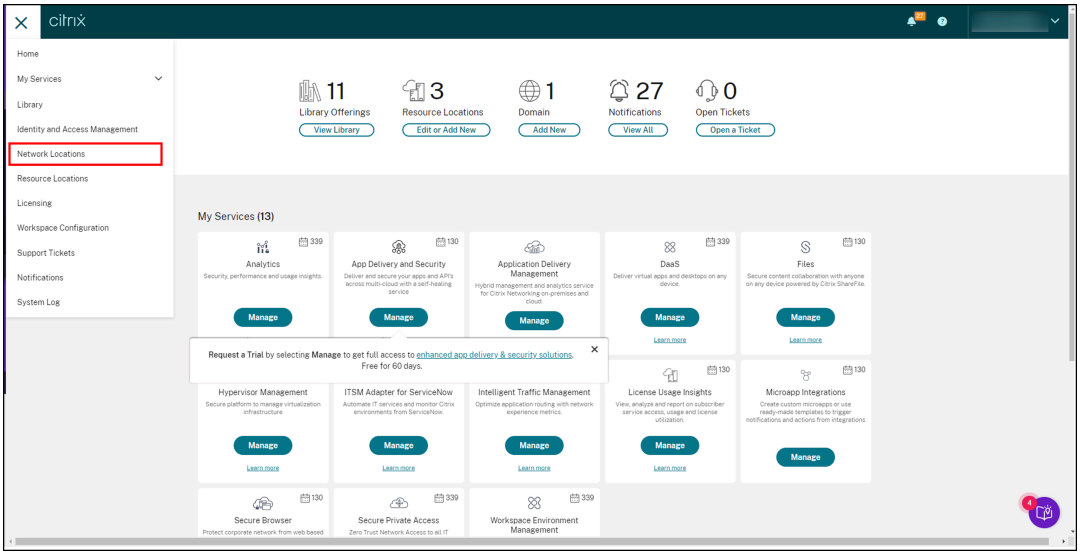
- Network location service (NLS) for scenarios based on the user's network location
- Licensing requirements -
  - App Protection for DaaS
  - Adaptive Authentication entitlement for scenarios with Smart Access policies.

Scenario 1

September 13, 2025

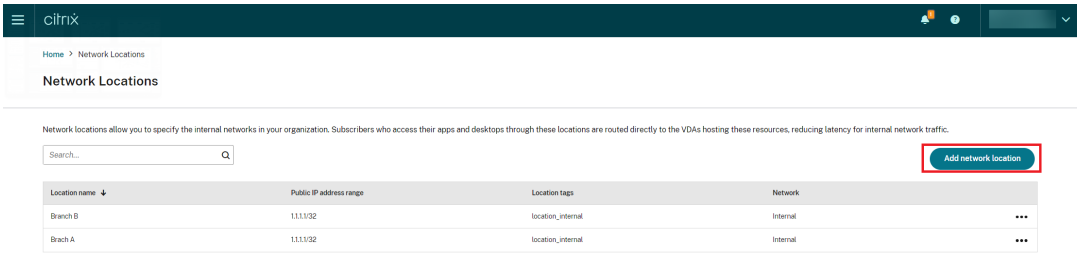
This scenario covers how to enable App Protection for external users coming through the Access Gateway.

1. Configure Adaptive Authentication.
2. Configure adaptive access based on your network location,
   a) Sign in to Citrix Cloud and navigate to **Network Locations**.



   b) Click **Add Network location**.

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



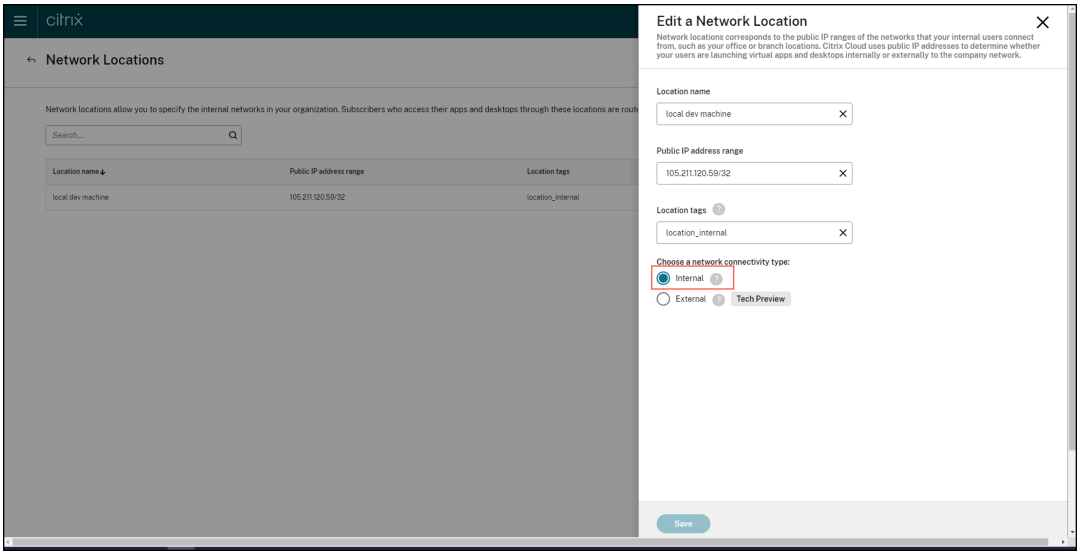
Add a Network Location screen appears.

c) In the **Location name** field, enter the relevant location name.

d) In the **Public IP address range** field, enter the network IP address or subnet that you want to consider as an internal network.

e) In the **Location tags** field, enter **location_internal**. For more information about the location tag, see Location tags.

f) Under **Choose a network connectivity type**, select *Internal*.



If you sign in to the Cloud store from a device whose IP address is configured as *Internal* under **Choose a network connectivity type** setting, then the connection is considered as an internal connection.

3. Configure Broker Access policy rules

   For every delivery group, two broker access policies are created by default. One policy is for connections coming through the Access gateway, and the other policy is for direct connections. You can enable App Protection only for the connections coming through the Access gateway, which is the external connections. Use the following steps to configure the Broker Access policy rules:

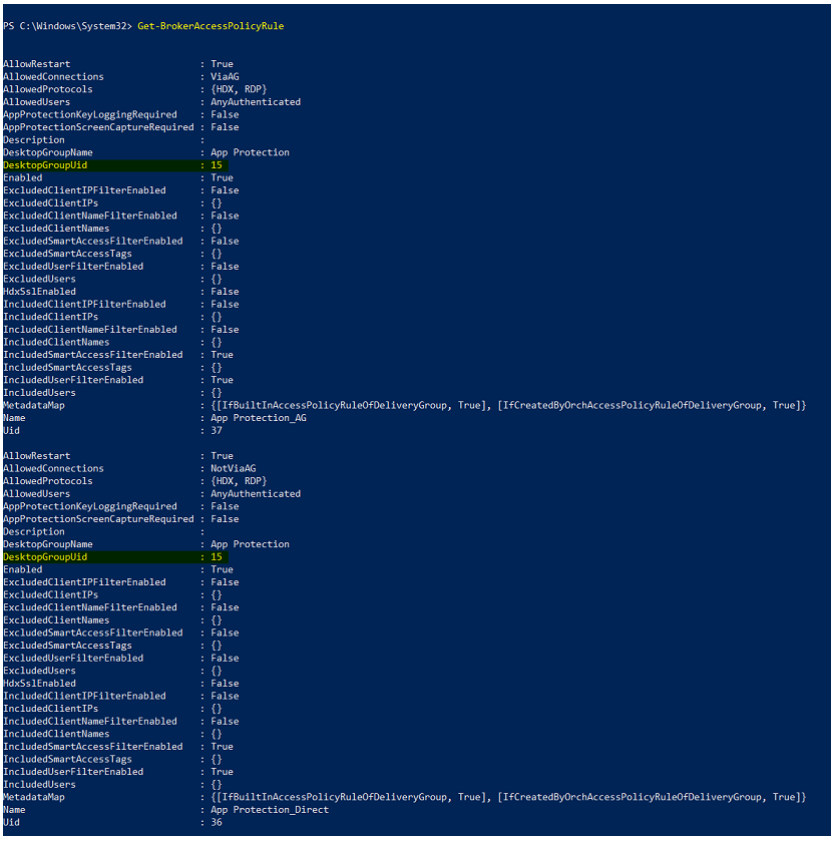
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a) Install the Citrix PowerShell SDK and connect to the cloud API as explained in the Citrix blog Getting started with PowerShell automation for Citrix Cloud.

b) Run the command `Get-BrokerAccessPolicyRule`.

A list of all the broker access policies for all the delivery groups that are present is displayed.

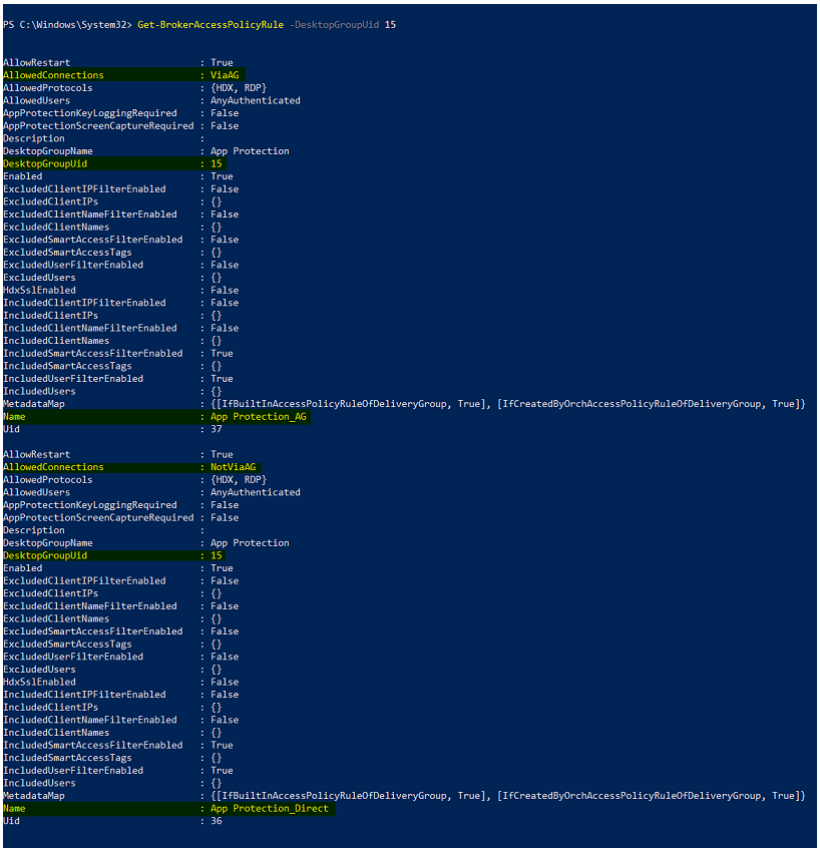
c) Find the **DesktopGroupUid** for the delivery group that you want to change.



d) Run the following command using the **DesktopGroupUid** to fetch policies applicable to the delivery group. There are at least two policies, one where *AllowedConnections* has *ViaAG* and another which has *NotViaAG*.

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 15
```

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



In the screenshot, you see two policies:

- App Protection_AG - *AllowedConnections* with *ViaAG*, which is the policy for connections via the access gateway
- App Protection_Direct –*AllowedConnections* with *NotViaAG*, which is the policy for connections not via the access gateway

4. Enable App Protection policies only for external connections and disable for internal connections using the following commands:

   - `Set-BrokerAccessPolicyRule "App Protection_AG"-IncludedSmartAccessFilt $true -IncludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequ $false`
   - `New-BrokerAccessPolicyRule "App Protection_AG_Exclude"-ExcludedsmartAc $true -ExcludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $true -AppProtectionKeyLoggingRequi $true -DesktopGroupUid 15 -AllowedConnections ViaAG -AllowedProtocols HDX, RDP`
   - `Remove-BrokerAccessPolicyRule "App Protection_Direct”`

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

5. Verification:

   Sign out of Citrix Workspace app and sign in again. Launch the protected resource from an external connection. You see that the App Protection policies are applied. Launch the same resource from an internal connection, a device from within the IP Address range configured in the first step. You see that the App Protection policies are disabled.

Scenario 2

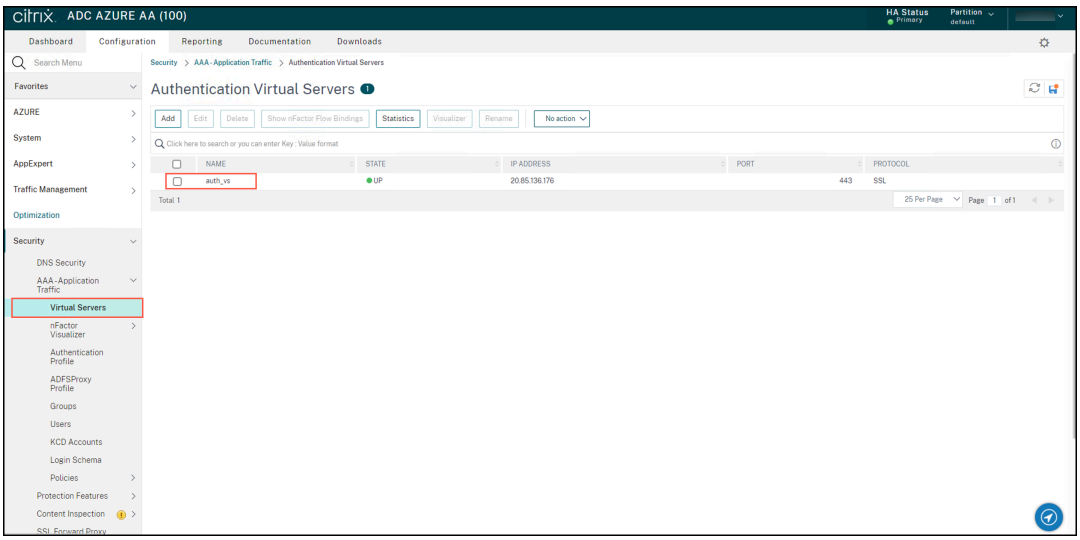
September 13, 2025

This scenario covers how to enable App Protection for untrusted devices.

There are many definitions for trusted and untrusted devices. For this scenario, let's consider a device trusted if the Endpoint analysis (EPA) scan is successful. All other devices are considered untrusted devices.

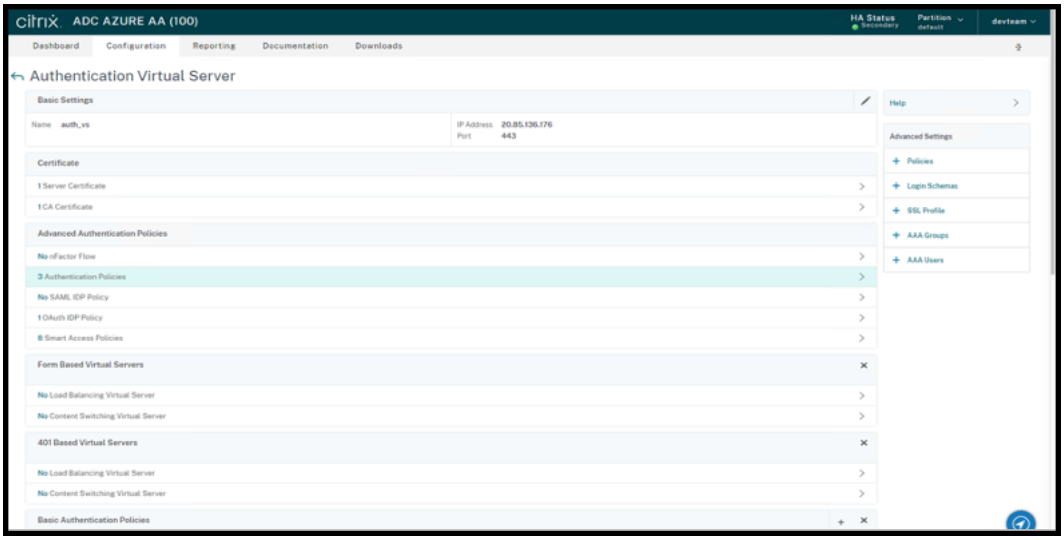
1. Configure Adaptive Authentication.
2. Create an Authentication policy with the EPA scan using the following steps:

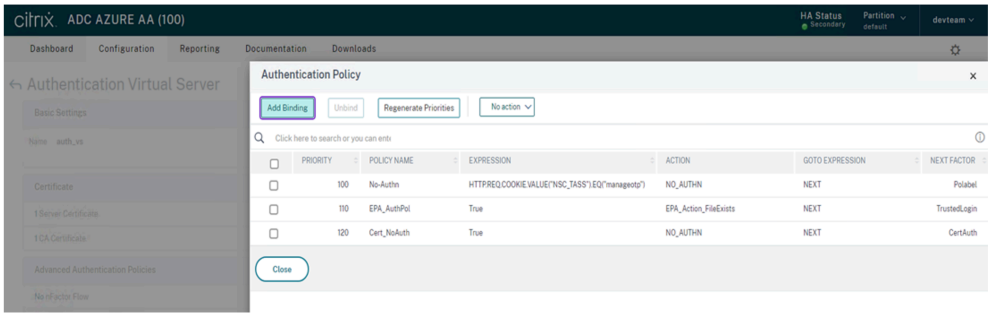
   a) Sign in to Citrix ADC Administration UI. In the **Configuration** tab, navigate to **Security > AAA-Application Traffic > Virtual Servers**. Click the virtual server that you want to use, *auth_vs* in this case.



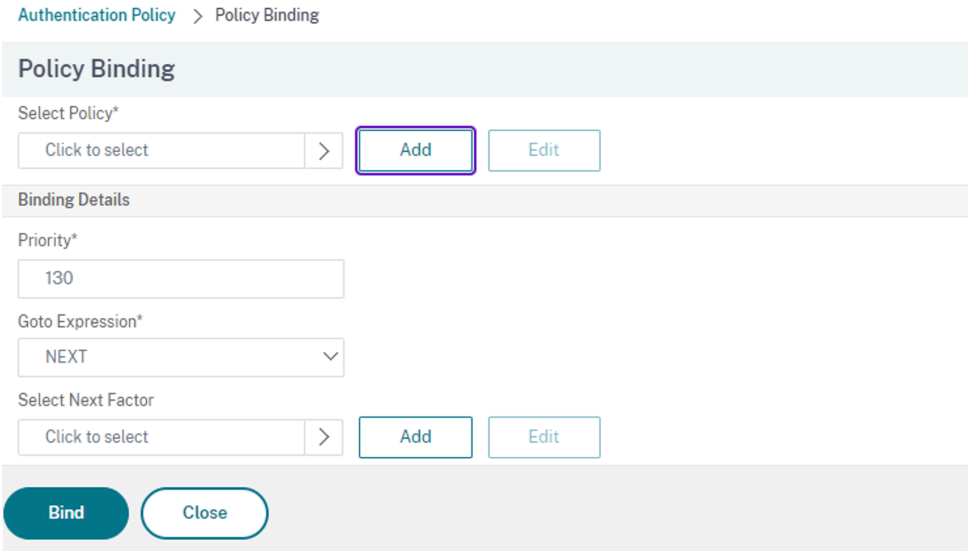
   b) Navigate to **Authentication Policies > Add Binding**.

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



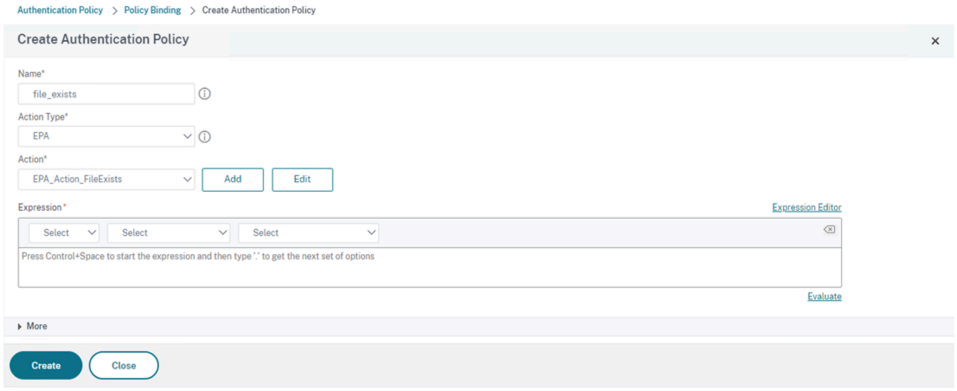


c) Click **Add** to create a policy.

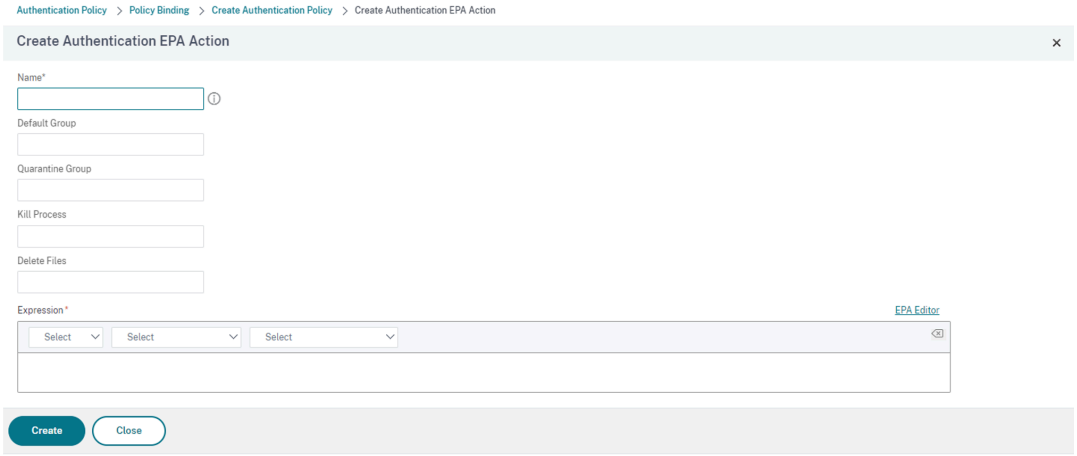


d) Create an authentication policy based on the EPA scan. Enter the name of the policy. Select **Action Type** as *EPA*. Click **Add** to create action.

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



Create Authentication EPA Action screen appears.



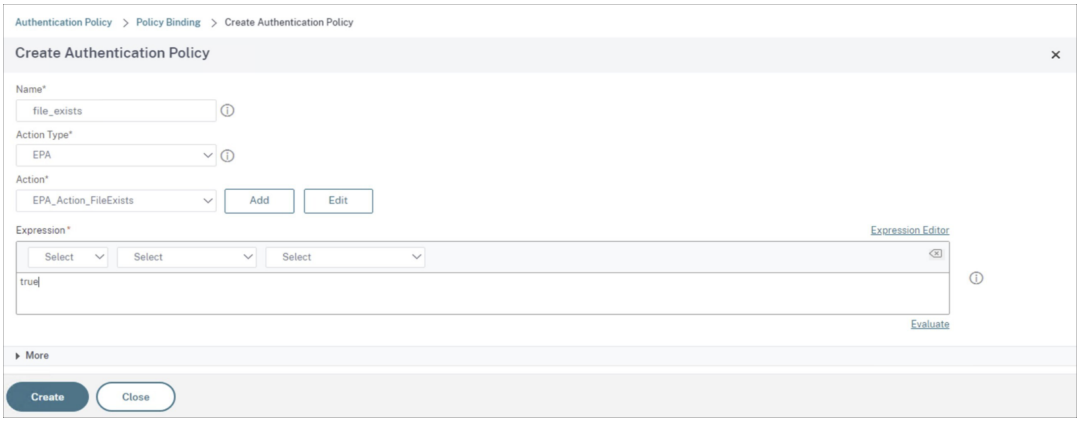
e) On the **Create Authentication EPA Action** screen, enter the following details and click **Create** to create an action:

- **Name**: Name of the EPA action. In this case *EPA_Action_FileExists*.
- **Default Group**: Enter the default group name. If the EPA expression is *True*, users are added to the default group. The **Default Group** in this case is *FileExists*.
- **Quarantine Group**: Enter the quarantine group name. If the EPA expression is *False*, users are added to the quarantine group.
- **Expression**: Add the EPA expression that you want to scan. In this example, we consider the EPA scan to be successful if a particular file is present: `sys.client_expr("file_0_C:\\\\\epa\\\\\avinstalled.txt")`

You return to the **Create Authentication Policy** screen.

f) Enter **true** in the Expression editor, and click **Create**.

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



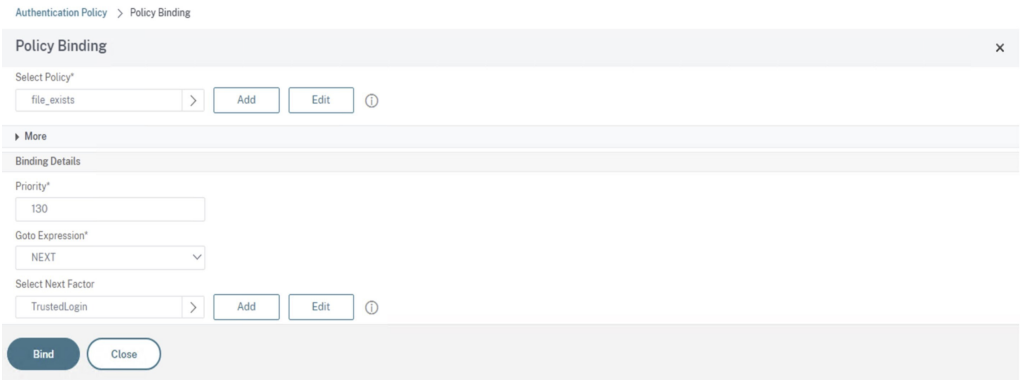
You return to the **Policy Binding** screen.

g) On the **Policy Binding** screen, do the following:

i. Select the **Goto Expression** as **NEXT**.

ii. In the **Select Next Factor** section, select the LDAP policy that you've configured for the authentication in the Application Delivery Controller™ (ADC).

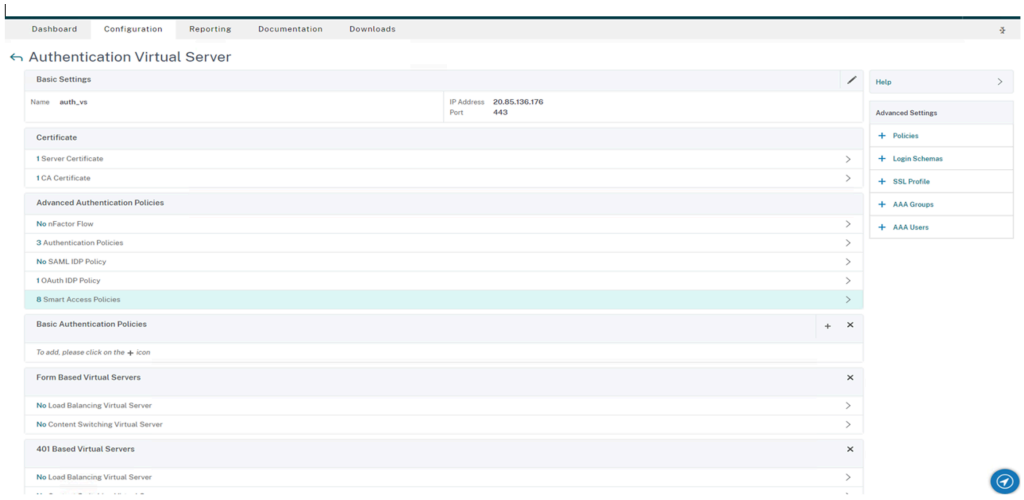
iii. Click **Bind**.



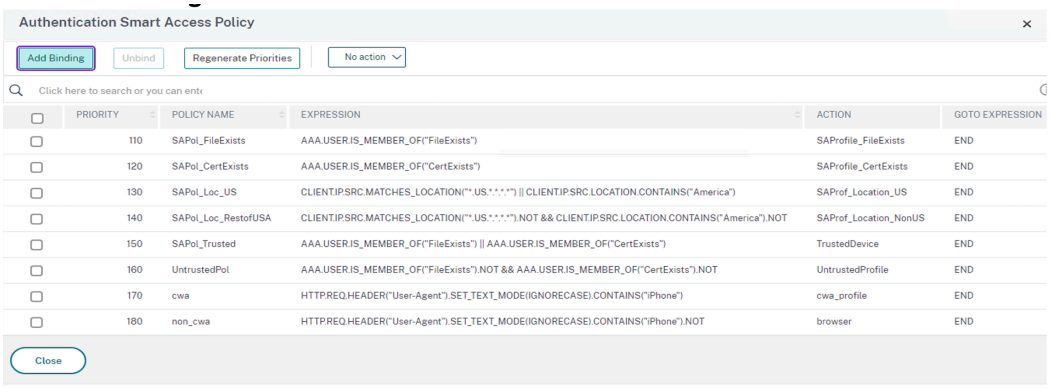
3. Create a Smart Access Policy for trusted devices:

a) Select **Smart Access Policies** on the **Authentication Virtual Server** page of the *auth_vs* server.

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



b) Click **Add Binding**.

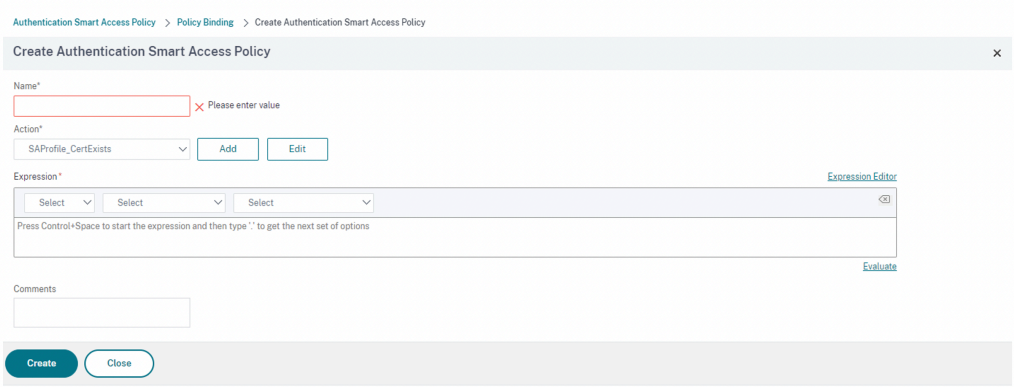


c) On the **Policy Binding** screen, click **Add** in the **Select Policy** section.



The **Create Authentication Smart Access Policy** screen appears.

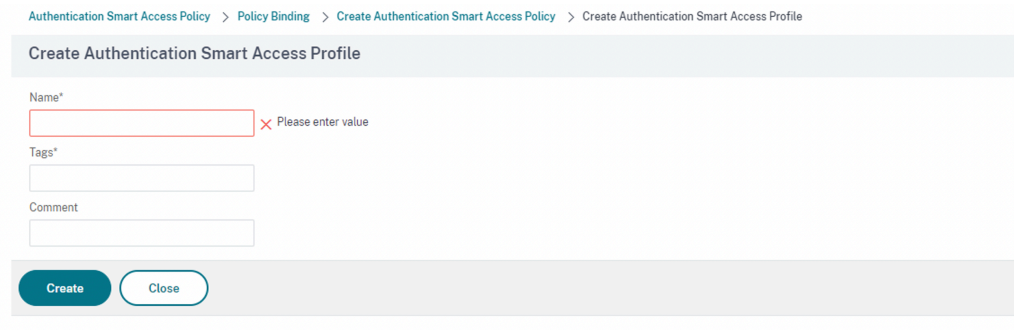
© 1997–2026 Citrix Systems, Inc. All rights reserved.



d) On the **Create Authentication Smart Access Policy** screen, enter **Name** for the Smart Access Policy and click **Add** to create a Smart Access Profile.

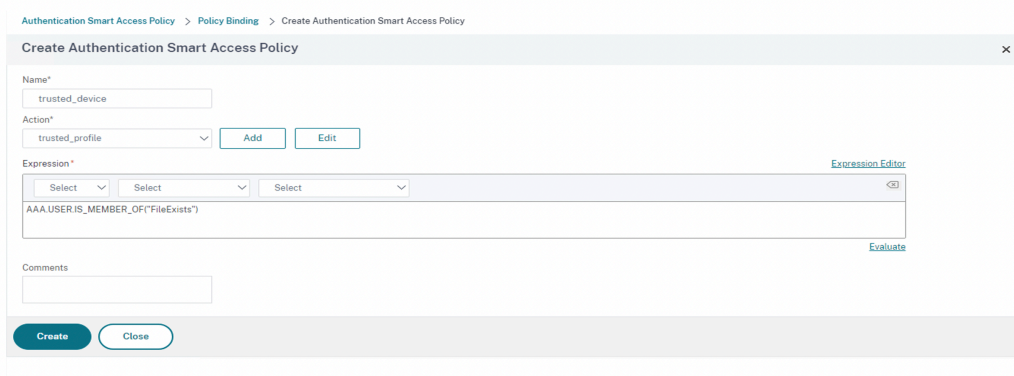
The **Create Authentication Smart Access Profile** screen appears.

e) Add **Name** for the action. Enter *trusted* in **Tags**. The tag is later referenced in the Broker Access Policy rule for configuring. Click **Create**.



You return to the **Create Authentication Smart Access Policy** screen.

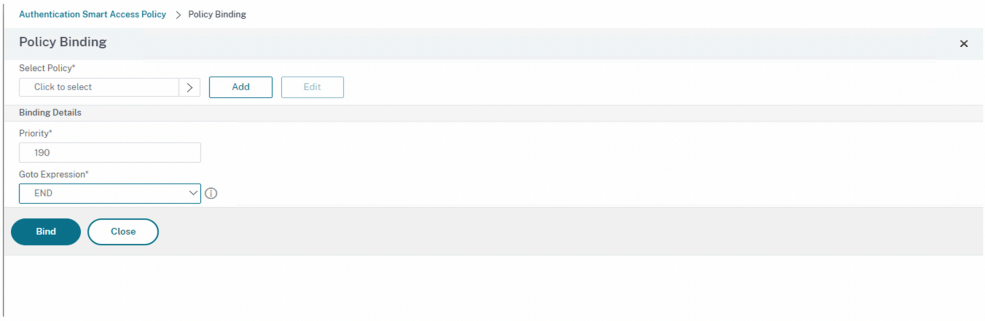
f) In the **Expression** section, enter the expression for which you want to push the tag. In this case, since the tag is pushed for trusted devices, enter `AAA.USER.IS_MEMBER_OF("FileExists")`. Click **Create**.



You return to the **Policy Binding** screen.

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

g) Select the **Goto Expression** as *End* and Click **Bind**.



4. Create a Smart Access Policy for untrusted devices:

   a) Follow the instructions of the previous step, except sub-steps **v** and **vi**.

   b) For the sub-step **v**, on the **Create Authentication Smart Access Profile** screen, add **Name** for the action. Enter *untrusted* in **Tags**. The tag is later referenced in the Broker Access Policy rule for configuring. Click **Create**.

   c) For the sub-step **vi**, in the **Expression** section of the **Create Authentication Smart Access Policy** screen, enter the expression for which you want to push the tag. In this case, since the tag is pushed for untrusted devices, enter `AAA.USER.IS_MEMBER_OF("FileExists").NOT`.

5. Configure the Broker Access policy rules:

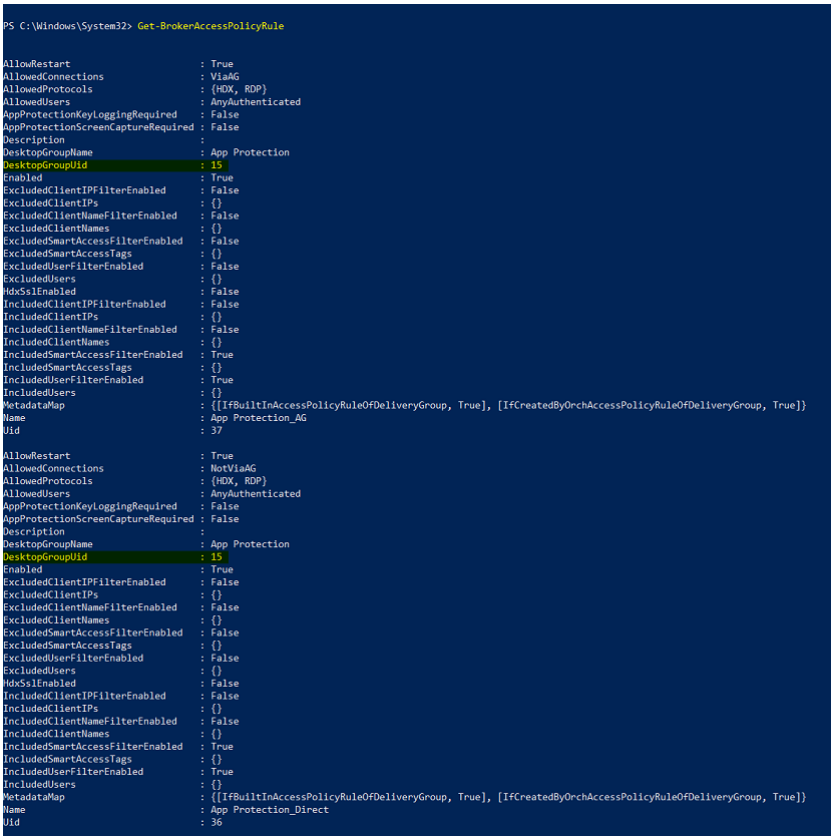
   a) Install the Citrix PowerShell SDK and connect to the cloud API as explained in the Citrix blog Getting started with PowerShell automation for Citrix Cloud.

   b) Run the command `Get-BrokerAccessPolicyRule`.

      A list of all the broker access policies for all the delivery groups which are present is displayed.

   c) Find the **DesktopGroupUid** for the delivery group that you want to change.

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



d) Get the policies that are applied only to a particular delivery group using the command:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) To filter users using trusted devices, create another Broker Access policy using the command:

```
New-BrokerAccessPolicyRule -Name CAP_Desktops_AG_Trusted-
DesktopGroupUid 7 - AllowedConnections ViaAG -AllowedProtocols
 HDX, RDP -AllowedUsers AnyAuthenticated - AllowRestart $true
 -Enabled $true-IncludedSmartAccessFilterEnabled $true
```

f) To disable App Protection for trusted devices and enable App Protection for untrusted devices, use the following command:

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG_trusted -IncludedSmartAcces
 Workspace:trusted -AppProtectionKeyLoggingRequired $false -
AppProtectionScreenCaptureRequired $false
```

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG -IncludedSmartAccessTags
 Workspace:untrusted -AppProtectionKeyLoggingRequired $true -
AppProtectionScreenCaptureRequired $true
```

6. Verification:

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

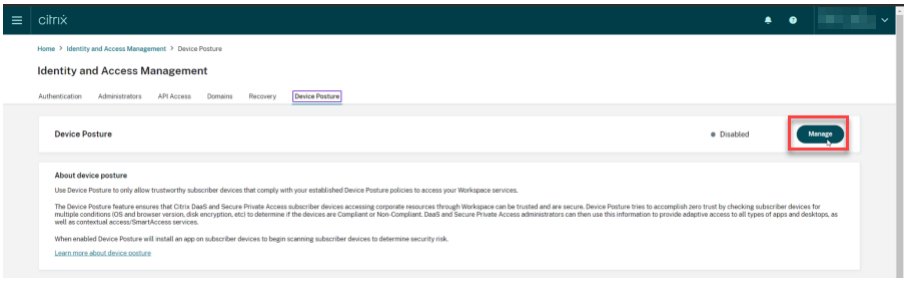
Sign out of Citrix Workspace app and sign in again. Launch the protected resource from a trusted device, one that meets the EPA scan condition. You see that the App Protection policies are not applied. Launch the same resource from an untrusted device. You see that the App Protection policies are applied.

Scenario 3

February 28, 2024

This scenario covers how to enable App Protection based on Device Posture results.

1. Configure Device Posture service:
   a) Sign in to Citrix Cloud.
   b) Navigate to **Identity and Access Management** > **Device Posture** and click **Manage**.



   c) Click **Create device policy**.

      Create devicy policy page appears.

   d) Under **Policy rules**, click the **Select Rule** drop-down menu and select *Citrix Workspace app Version*.
   e) Click the **Select a rule** drop-down menu and select *Greater or equal to* >=.
   f) Enter the Citrix Workspace app version that you want to set as the condition. In this example, it is *23.7.0.19*.
   g) Under **Policy result**, select **Compliant**.
   h) In the **Name** field, enter a name for the policy.
   i) In the **Priority** field, enter the priority of the policy.
   j) Select the **Enable when created** checkbox to enable the policy since you created it.
   k) Click **Create**.
2. Configure the Broker Access policy rules:

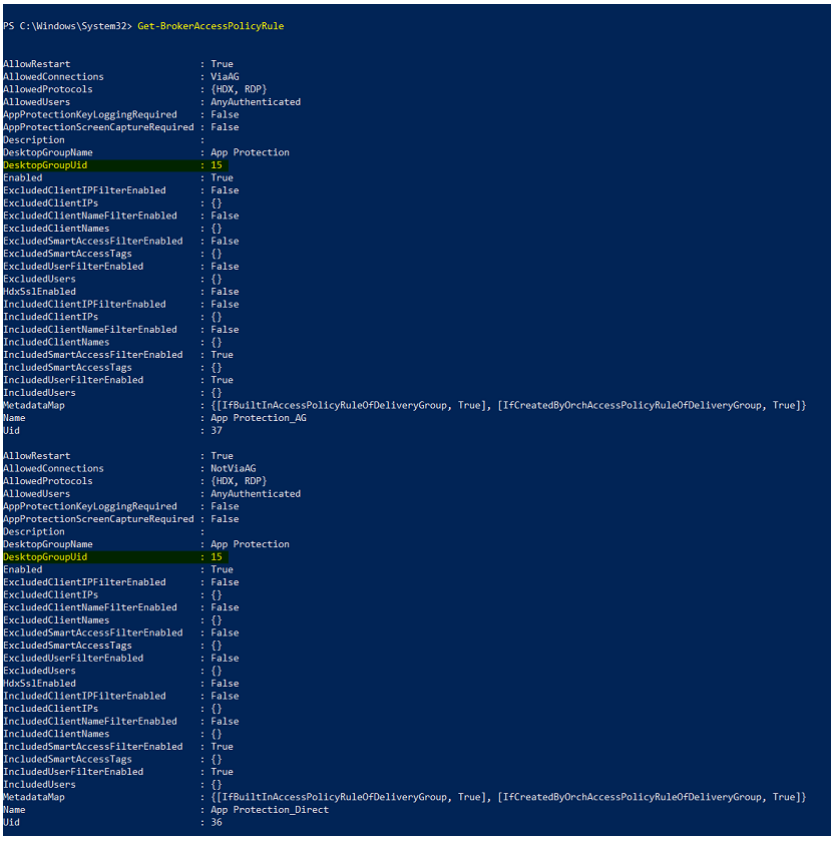
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a) Install the Citrix PowerShell SDK and connect to the cloud API as explained in the Citrix blog Getting started with PowerShell automation for Citrix Cloud.

b) Run the command `Get-BrokerAccessPolicyRule`.

A list of all the broker access policies for all the delivery groups which are present is displayed.

c) Find the **DesktopGroupUid** for the delivery group that you want to change.



d) Get the policies that are applied only to a particular delivery group using the command:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) To apply App Protection to the compliant devices, run the following command:

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG"-IncludedSmartAccessFilterEnabled $true -IncludedSmartAccess
 Workspace:COMPLIANT
```

f) To apply App Protection to the non-compliant devices, run the following command:

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG_NonCompliant"-DesktopGroupUid 7 -AllowedConnections
 ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
```

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

```
$true -ExcludedSmartAccessFilterEnabled $true -ExcludedSmartAccessTag
Workspace:COMPLIANT-IncludedSmartAccessFilterEnabled $true
```

3. Verification:

   Sign out of Citrix Workspace app. Sign in from a Citrix Workspace app version that is compliant with the device policy. You see that the App Protection policies are not applied. Again, sign out from the Citrix Workspace app and sign in from a Citrix Workspace app version that is not complaint with the device policy. You see that the App Protection policies are applied.

Scenario 4

February 28, 2024

This scenario covers how to enable App Protection for specific user groups.

The following steps allow you to enable App Protection for users of a specific group:

1. Select the Active Directory user group for which you want to enable the App Protection policies for the users. In this example, the Active Directory user group is **ProductManagers**.
2. Configure the Broker Access policy rules:

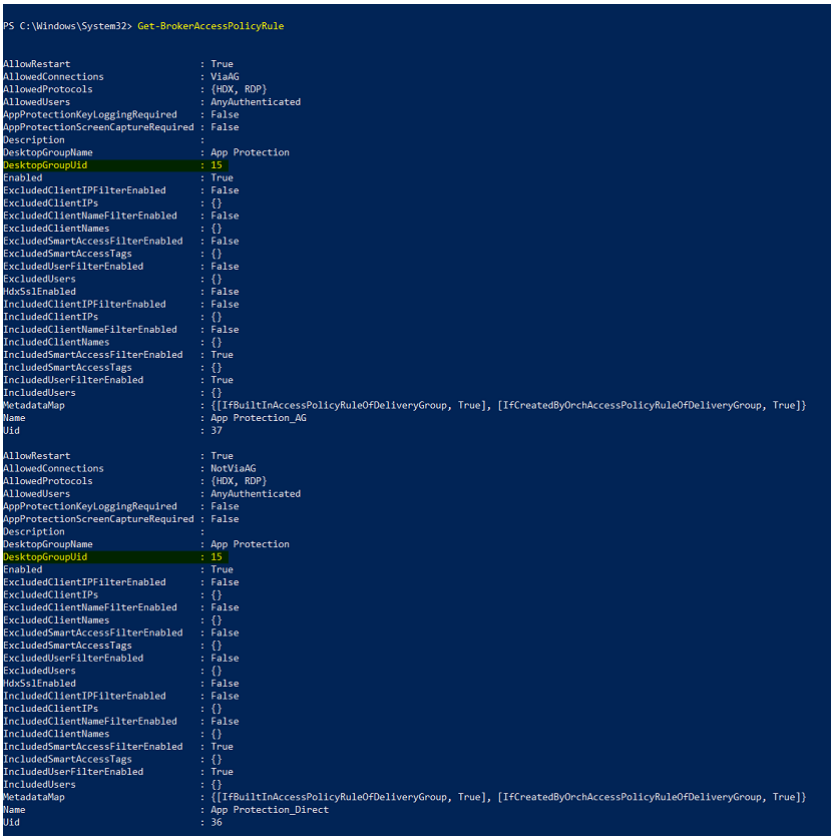
   a) Install the Citrix PowerShell SDK and connect to the cloud API as explained in the Citrix blog Getting started with PowerShell automation for Citrix Cloud.

   b) Run the command `Get-BrokerAccessPolicyRule`.

   A list of all the broker access policies for all the delivery groups which are present is displayed.

   c) Find the **DesktopGroupUid** for the delivery group that you want to change.

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



d) Get the policies that are applied only to a particular delivery group using the command:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) To enable App Protection policies for the users in the **ProductManagers** user group, run the following commands:

```
New-BrokerAccessPolicyRule "Example Rule Name_1"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $true -IncludedUserFilte
 $true -IncludedUsers domain.com\ProductManagers
```

f) To disable App Protection policies for the users who are not a part of the the **ProductManagers** user group, run the following commands:

```
New-BrokerAccessPolicyRule "Example Rule Name_2"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $false-ExcludedUserFilte
 $true -ExcludedUsers domain.com\ProductManagers
```

3. Verification:

   Sign out of Citrix Workspace app, if already open. Sign in to Citrix Workspace app as a user in the **ProductManagers** Active Directory user group. Launch the protected resource and you see

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

that App Protection is disabled. Sign out of Citrix Workspace app and Sign in again as a user who is not part of the **ProductManagers** Active Directory user group. Launch the protected resource and you see that App Protection is enabled.

Contextual App Protection for StoreFront

September 7, 2025

Contextual App Protection provides the granular flexibility to apply the App Protection policies conditionally for a subset of users - based on users, their device, and the network posture.

Implementing Contextual App Protection

You can implement contextual App Protection using the connection filters defined in the Broker Access policy rule. The Broker Access policies define the rules controlling a user's access to delivery groups. The policy comprises a set of rules. Each rule relates to a single delivery group, and has a set of connection filters and access right controls.

Users gain access to a delivery group when their connection's details match the connection filters of one or more rules in the Broker Access policy. Users don't have access to any desktop group within a site by default. You can create more Broker Access policies based on requirements. Multiple rules can apply to the same delivery group. For more information, see New-BrokerAccessPolicyRule.

The following parameters in the Broker Access policy rule provide the flexibility to enable App Protection contextually if the user's connection matches the connection filters defined in the access policy rule:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Use the Smart Access filters referenced in the Broker Access policies to refine the connection filters. For information on configuring Smart Access filters, see this CTX227055. Refer to the following scenarios to understand how to use the Smart Access policies to set up Contextual App Protection.

> **Note:**
>
> If App Protection is enabled on the Delivery Group, then Contextual App Protection cannot be applied by default. Disable App Protection on the Delivery Group by using the following command:

```
1 Set-BrokerDesktopGroup -Name "Admin Desktop" -
```

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

```
        AppProtectionKeyLoggingRequired $false -
        AppProtectionScreenCaptureRequired $false
```

Prerequisites

To enable Contextual App Protection for StoreFront, make sure that you meet the requirements mentioned in the Prerequisites section.

Enable Contextual App Protection

- **For CVAD Versions Beyond 2209:**

  Contextual App Protection is enabled by default. No additional configuration is required.

- **For CVAD 2209 and Earlier Versions:**

  Follow these steps to enable Contextual App Protection for CVAD 2209 and earlier versions.

  - Download the Contextual App Protection policies (feature table) for your Citrix Virtual Apps and Desktops version from the Citrix Downloads page.
  - Run the following PowerShell command in the delivery controller™:

    ```
    asnp Citrix*
    Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
    ```

  - Run the following command to enable contextual App Protection in the delivery controller:

    ```
    Import-ConfigFeatureTable <path to the downloaded feature
       table>
    ```

    For example,

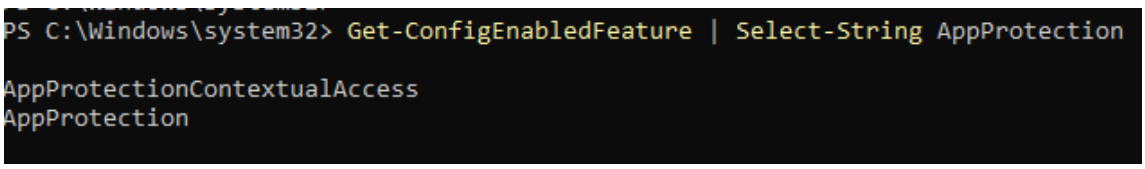
    ```
    Import-ConfigFeatureTable\Downloads\FeatureTable.OnPrem.
       AppProtContextualAccess.xml
    ```

To verify the feature status

1. Run the following command to check if Contextual App Protection is enabled:

   `Get-ConfigEnabledFeature | Select-String AppProtection`

2. If enabled, you should see `AppProtectionContextualAccess` in the output.



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

Contextual App Protection scenarios

Following are some of the scenarios about how you can enable or disable Contextual App Protection:

- Disable App Protection for certain device types
- Disable App Protection for connections started from browser-based access and enable App Protection for connections from Citrix Workspace app
- Disable App Protection for users in a specific Active Directory group
- Enable App Protection for devices based on the EPA scan results
- Enable App Protection for specific user groups

Prerequisites

September 13, 2025

Make sure that you have the following:

- Citrix Virtual Apps and Desktops™ version 2109 or later
- Delivery Controller™ version 2109 or later
- StoreFront version 1912 LTSR or later
- VPN virtual server or gateway and authentication virtual server configurations
- Successful connection between NetScaler and StoreFront. For more information, see Integrate NetScaler Gateway with StoreFront
- XML table import is required up to Citrix Virtual Apps and Desktops version 2006
- Contextual App Protection feature table import is required up to Citrix Virtual Apps and Desktops version 2209
- Enable Smart Access on NetScaler Gateway, for scenarios that require Smart Access tags. For more information, see this support article.
- Licensing requirements -
  - App Protection On-premises license
  - Citrix Gateway Universal license for scenarios with Smart Access tags

Scenario 1

September 13, 2025

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

This scenario covers how to disable App Protection for certain device types.

The following are the steps to disable App Protection for iPhone users on a delivery group called `Win10Desktop`:

1. Create a Smart Access policy:

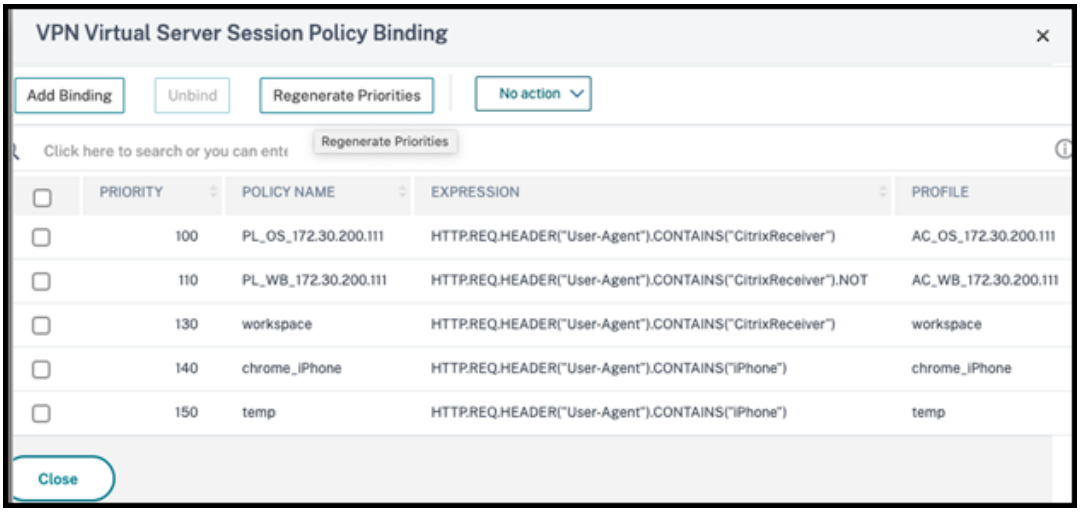
   a) Sign in to the Citrix ADC Administration UI.

   b) On the left navigation menu, go to **Citrix Gateway** > **Virtual Servers**.

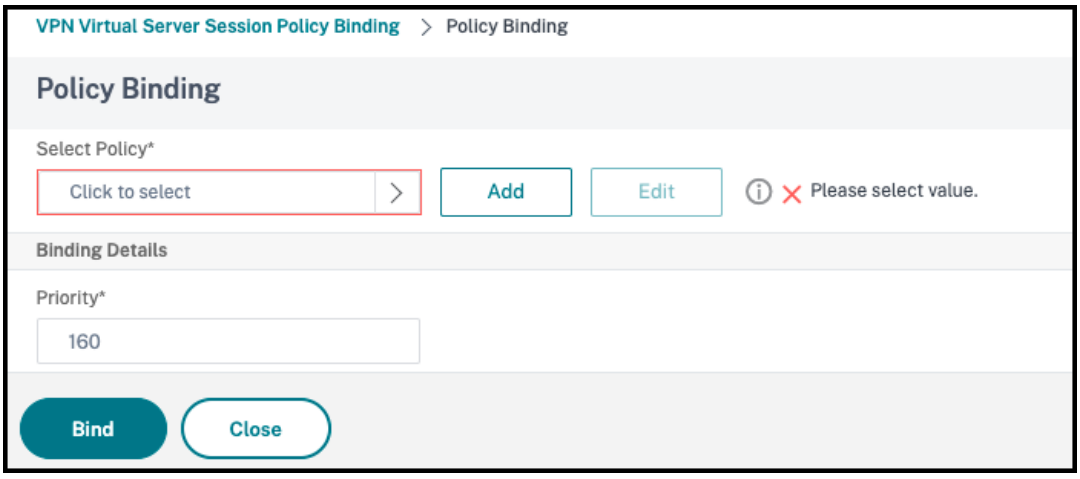
   Note the VPN Virtual Server name, which is needed to configure the Broker Access Policy later on.

   c) Click **VPN Virtual Server**. Scroll to the bottom of the page and click **Session policies**. A list of session policies appears.

   d) Click **Add Binding**.

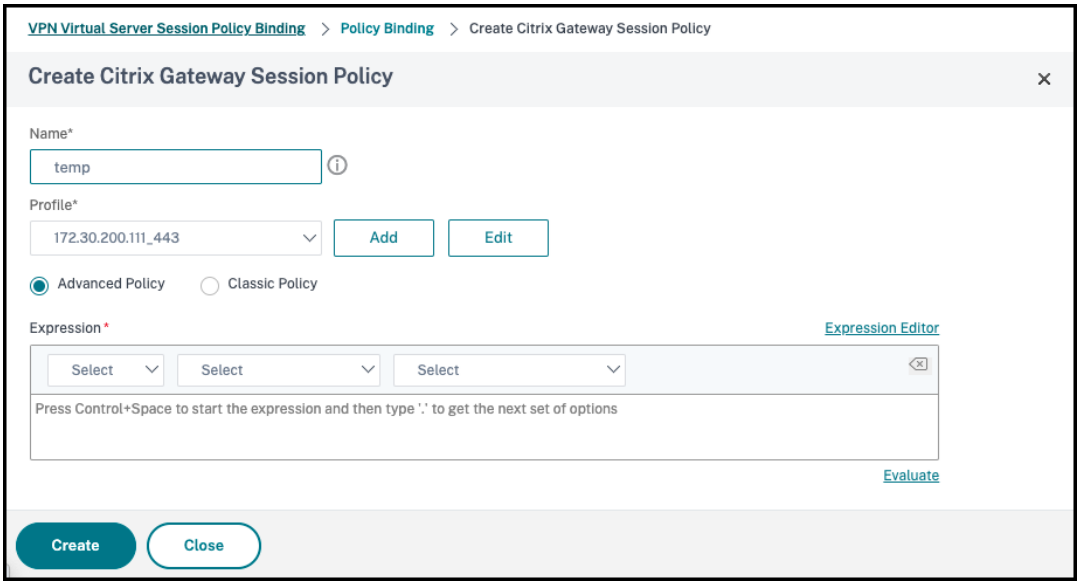


   e) Click **Add to create a session policy**.

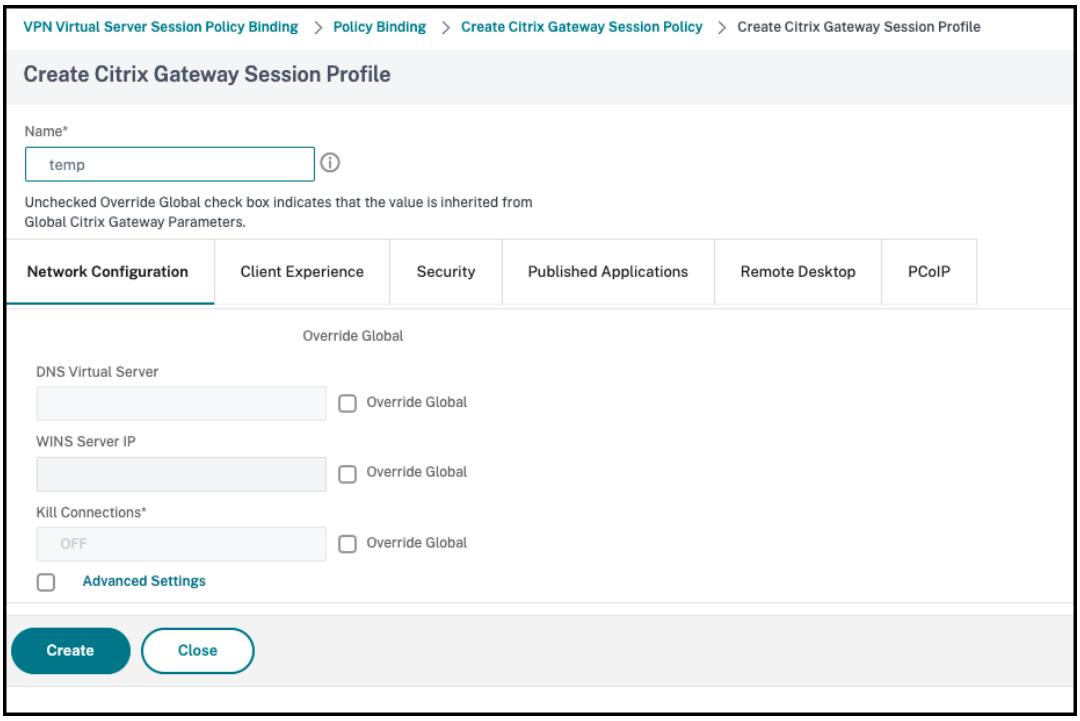


   f) Enter a name for the session policy. In this scenario, it is *temp*.

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



g) Click **Add** next to Profile to specify a Profile name. Click **Create**.



h) Click **Expression Editor** from the Session policy window.

i) Create the following expression to check for *iPhone* in the **User Agent** string:

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
```

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



j) Click **Bind** to create the session policy.

2. Create Broker access policy rules:

   To apply the policy for iPhone users accessing `Win10Desktop` through the access gateway, do the following steps:

   a) Run the following command in the Delivery controller™ (DDC):

   ```
   1 Get-BrokerAccessPolicyRule
   ```

   which lists all the Broker Access policies defined in the DDC. In this scenario, the Broker Access policies for the delivery group `Win10Desktop` are `Win10Desktop_AG` and `Win10Desktop_Direct`. Note the desktop group UID of the delivery group for the next step.

   b) Create a broker access policy rule for `Win10Desktop` to filter iPhone users coming through the access gateway using the following command:

   ```
   1 New-BrokerAccessPolicyRule -Name Win10Desktop_AG_iPhone -
       DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
       ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
       AnyAuthenticated -AllowRestart $true -
       AppProtectionKeyLoggingRequired $false -
       AppProtectionScreenCaptureRequired $false -Enabled $true -
       IncludedSmartAccessFilterEnabled $true
   ```

   Uid_of_desktopGroup is the DesktopGroupUID of the delivery group got by running the GetBrokerAccessPolicy Rule in step 1.

   c) To disable App Protection for `Win10Desktop` iPhone users coming through the access gateway, reference the Smart Access tag *temp* created in Step 1. Create Smart Access policy using the following command:

   ```
   1 Set-BrokerAccessPolicyRule Win10Desktop_AG_iPhone -
       IncludedSmartAccessTags Primary_HDX_Proxy:temp -
       AppProtectionScreenCaptureRequired $false -
       AppProtectionKeyLoggingRequired $false
   ```

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

Primary_HDX_Proxy is the VPN virtual server name from earlier in Step 1, Create Smart Access Policy.

d) To enable App Protection policies for the rest of the `Win10desktop` users, use the following command:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
```

3. **Verification**

For iPhone: Sign out of the Citrix Workspace app, if already open on the iPhone. Sign in to Citrix Workspace app externally through the access gateway connection. You can see the required resources in StoreFront and App Protection has to be disabled.

For devices other than the iPhone: Sign out of the Citrix Workspace app, if already open on the device. Sign in to Citrix Workspace app externally through an access gateway connection. You can see the required resources in the StoreFront and App Protection has to be disabled.

Scenario 2

September 13, 2025

This scenario covers how to disable App Protection for connections started from browser-based access and enable App Protection for connections started from Citrix Workspace app.

The following are the steps to disable App Protection for a delivery group called `Win10Desktop` when connections are started from a browser and enable App Protection for connections from Citrix Workspace app:

1. Create Smart Access policies:

a) Create a Smart Access policy to filter the connections started from the Citrix Workspace app, as defined in the preceding scenario **Disable App Protection for certain device types**. Create the following expression, to check for **CitrixReceiver** in the **User Agent** string:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
```

In this scenario, the Smart Access policy is `cwa`.

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



b) Create another Smart Access policy to filter the connections that aren't started from the Citrix Workspace app, `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT`. In this case, this Smart Access policy is *browser*.



2. Create Broker Access policy rules:

a) Run `GetBrokerAccessPolicyRule` to view the two broker access policies for `Win10Desktop`. For the delivery group `Win10Desktop`, the broker access policies are `Win10Desktop_AG` and `Win10Desktop_Direct`. Note the Desktop Group UID of `Win10Desktop`.

b) Create a Broker Access policy for `Win10Desktop` to filter connections started from the Citrix Workspace app by using the following command:

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_CWA -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
    AnyAuthenticated -AllowRestart $true -Enabled $true -
    IncludedSmartAccessFilterEnabled $true
```

Uid_of_desktopGroup is the DesktopGroupUID of the delivery group got by running the GetBrokerAccessPolicy Rule in step 1.

c) Use the following command to enable App Protection policies only for connections coming through CWA by referencing the Smart Access tag `cwa`:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_CWA -
    IncludedSmartAccessTags Primary_HDX_Proxy:cwa -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
```

Primary_HDX_Proxy is the VPN virtual server name noted down earlier in Step 1, Create Smart Access Policy.

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

d) Use the following command to disable App Protection policies for the rest of the connections coming through the browser:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    IncludedSmartAccessTags Primary_HDX_Proxy:browser -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
```

3. **Verification**

   Sign out of Citrix Workspace app, if already open. Sign in to Citrix Workspace app again and launch the required resource from an external connection through an access gateway. You can see that the App Protection policies are enabled for the resource. Launch the same resource from the browser through an external connection and you can see that the App Protection policies are disabled.

Scenario 3

September 13, 2025

This scenario covers how to disable App Protection for users in a specific Active Directory group.

Following are the steps to disable App Protection for `Win10Desktop` users who are part of the Active Directory group **xd.local\sales**:

1. Run `Get-BrokerAccessPolicyRule` to view the two broker access policies for `Win10Desktop`. For a delivery group `Win10Desktop` there are two broker access policies, `Win10Desktop_AG` and `Win10Desktop_Direct`. Make a note of the Desktop Group UID of the `Win10Desktop`.
2. Create a Broker access policy rule for `Win10Desktop` to filter connections from users in the Active Directory group `xd.local\sales`.

   ```
   New-BrokerAccessPolicyRule -Name Win10Desktop_AG_Sales_Group -
       DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections ViaAG
        -AllowedProtocols HDX, RDP -AllowedUsers Filtered -
       AllowRestart $true -Enabled $true
   ```

   Uid_of_desktopGroup is the DesktopGroupUID of the delivery group got by running the Get-BrokerAccessPolicy Rule in step 1.
3. Use the following command to disable App Protection policies for the Windows 10 Desktop users, part of the AD group **xd.local\sales**:

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

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_Sales_Group -
    AllowedUsers Filtered -IncludedUsers xd.local\sales -
    IncludedUserFilterEnabled $true -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
```

4. Use the following command to enable App Protection policies for the rest of the gateway connections except for the users from **xd.local\sales**:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -AllowedUsers
    Anyauthenticated -ExcludedUserFilterEnabled $true -
    ExcludedUsers xd.local\sales -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
```

5. **Verification**

   Sign out of the Citrix Workspace app, if already open. Sign in to the Citrix Workspace app as a user in the **xd.local\sales** Active Directory group. Launch the protected resource and you see that App Protection is disabled.

   Sign out of the Citrix Workspace app and sign in again as a user who is not part of **xd.local\sales**. Launch the protected resource and you see that App Protection is enabled.

Scenario 4

February 28, 2024

This scenario covers how to enable App Protection for devices based on the EPA scan results.

Following are the steps to enable App Protection for the devices that pass the EPA scans:

Prerequisites:

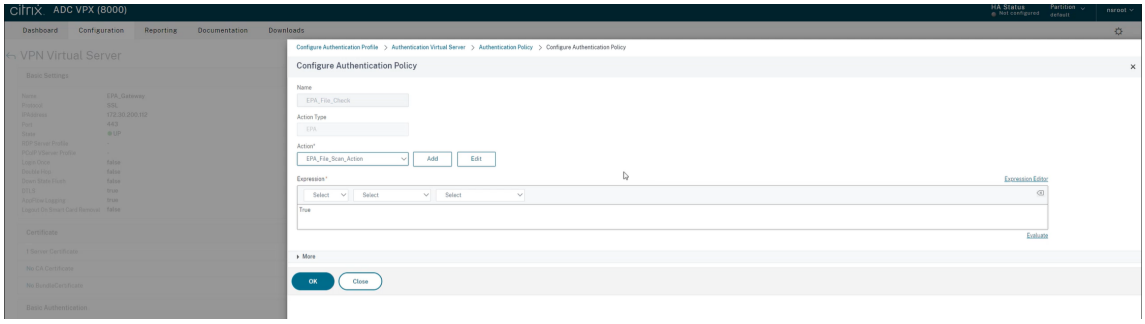
Make sure that you have the following:

- Authentication, authorization, and auditing user groups (for default and quarantined user groups) and associated policies
- LDAP server configurations and associated policies

1. Sign in to Citrix ADC and go to **Configuration** > **Citrix Gateway** > **Virtual Servers**.
2. Select the relevant Virtual Server and click **Edit**.
3. Edit the existing Authentication Profile.
4. Select the relevant Virtual Server and click **Edit**.

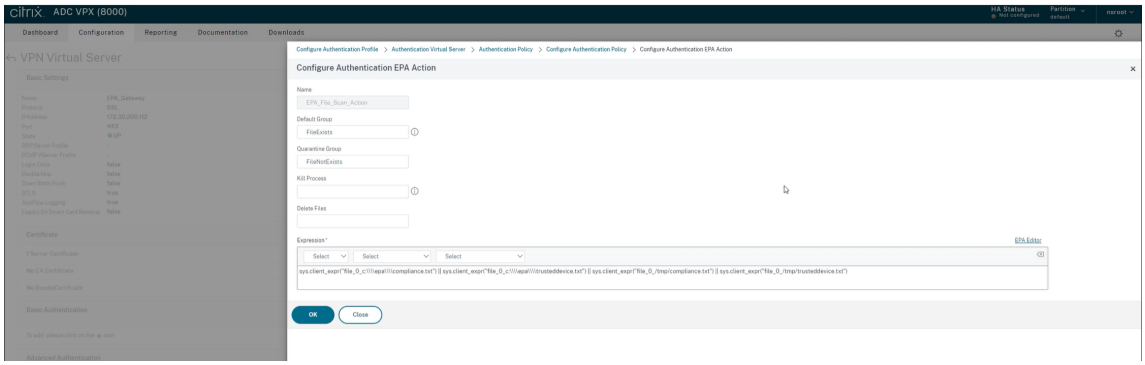
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Click **Authentication Policies** > **Add Binding**.
6. Under **Select Policy**, click **Add**.
7. In the **Name** field, enter the name of the Authentication Policy.
8. In the **Action Type** drop-down list, select **EPA**.
9. In the **Expression** field, enter `True`.



10. Under **Action**, click **Add**.
11. In the **Name** field, enter the name of the EPA Action.
12. Enter the **Default Group** and **Quarantine Group** names. In this scenario, **Default Group** name is **FileExists** and **Quarantine Group** name is **FileNotExists**.
13. In the **Expression** field, enter the following value:

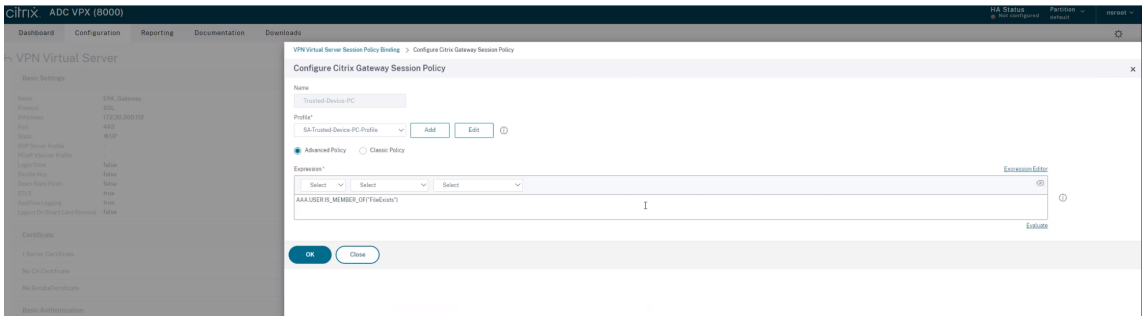
```
sys.client_expr("file_0_c:\\\\epa\\\\compliance.txt") || sys.
    client_expr("file_0_c:\\\\epa\\\\trusteddevice.txt") || sys.
    client_expr("file_0_/tmp/compliance.txt") || sys.client_expr("
    file_0_/tmp/trusteddevice.txt")
```



14. Click **Create** and then click **Bind**.
15. Click **Session Policies** > **Add Binding**.
16. Under **Select Policy**, click **Add**.
17. In the **Name** field, enter the name of the Session Policy.
18. In the **Expression** field, enter the following value:

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

```
AAA.USER.IS_MEMBER_OF("FileExists")
```



19. Click **Create** and then click **Bind**.
20. On the leftmost side of the taskbar, click the **Search** icon.
21. Type **Powershell** and open **Windows Powershell**.
22. Use the following command to disable App Protection policies for devices that have passed the EPA scans by referencing the **Smart Access tag"EPA_GW:Trusted-Device-PC"**:

    ```
    Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
        Group_AG" -IncludedSmartAccessFilterEnabled $true -
        IncludedSmartAccessTags EPA_GW:Trusted-Device-PC -
        AppProtectionScreenCaptureRequired $false
    ```

    where, *EPA_GW* is the VPN Virtual Server name.

23. Use the following command to enable App Protection policies for devices that have failed the EPA scans by referencing the **Smart Access tag"EPA_GW:Trusted-Device-PC"**:

    ```
    New-BrokerAccessPolicyRule "Contextual App Protection Delivery
        Group_AG_NonCompliant"-DesktopGroupUid 17 -AllowedConnections
        ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
        $true -ExcludedSmartAccessFilterEnabled $true -
        ExcludedSmartAccessTags EPA_GW:Trusted-Device-PC -
        IncludedSmartAccessFilterEnabled $true -
        AppProtectionScreenCaptureRequired $true
    ```

24. **Verification**

    Sign out of the Citrix Workspace app, if already open. Sign in to the Citrix Workspace app from a trusted device. Launch the protected resource and you see that App Protection is disabled.

    Sign out of the Citrix Workspace app and Sign in again from an untrusted device. Launch the protected resource and you see that App Protection is enabled.

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

Scenario 5

December 27, 2023

This scenario covers how to enable App Protection for specific user groups.

To enable App Protection for users of a specific group, see Enable App Protection for specific user groups

App Protection support for hybrid launch through Workspace

March 27, 2026

Hybrid launches of Citrix Virtual Apps and Desktops are when you sign in to Citrix Workspace for Web by typing the store URL in the native browser, and launching the virtual apps and desktops through the native Citrix Workspace app and its HDX engine. The term hybrid is the result of using the combination of Citrix Workspace app for Web and the native Citrix Workspace app to connect and use the resources.

> **Note:**
>
> When no native Citrix Workspace app components are installed on the endpoint, it's a zero-install configuration where both the Citrix Workspace store and the HDX engine are within the browser. This scenario is known as the Citrix Workspace app for HTML5, which is hosted either on Citrix Workspace or Citrix StoreFront. This document does not address that scenario.

Prerequisites

- Make sure that you're on a browser that supports the Citrix Workspace Web extension.
- Make sure that you're on one of the following versions of Citrix Workspace app:
  - Citrix Workspace app for Windows 2106 or later
  - Citrix Workspace app for macOS 2106 or later
- If you are using a Custom Domain as your Workspace URL instead of the default cloud.com domain:
  - Ensure that the Citrix Web Extension is greater than or equal to version 24.4.0.
  - The workspace URL has "Citrix"in it. Eg: `prod.mycompany.com/xyz/Citrix/*`.

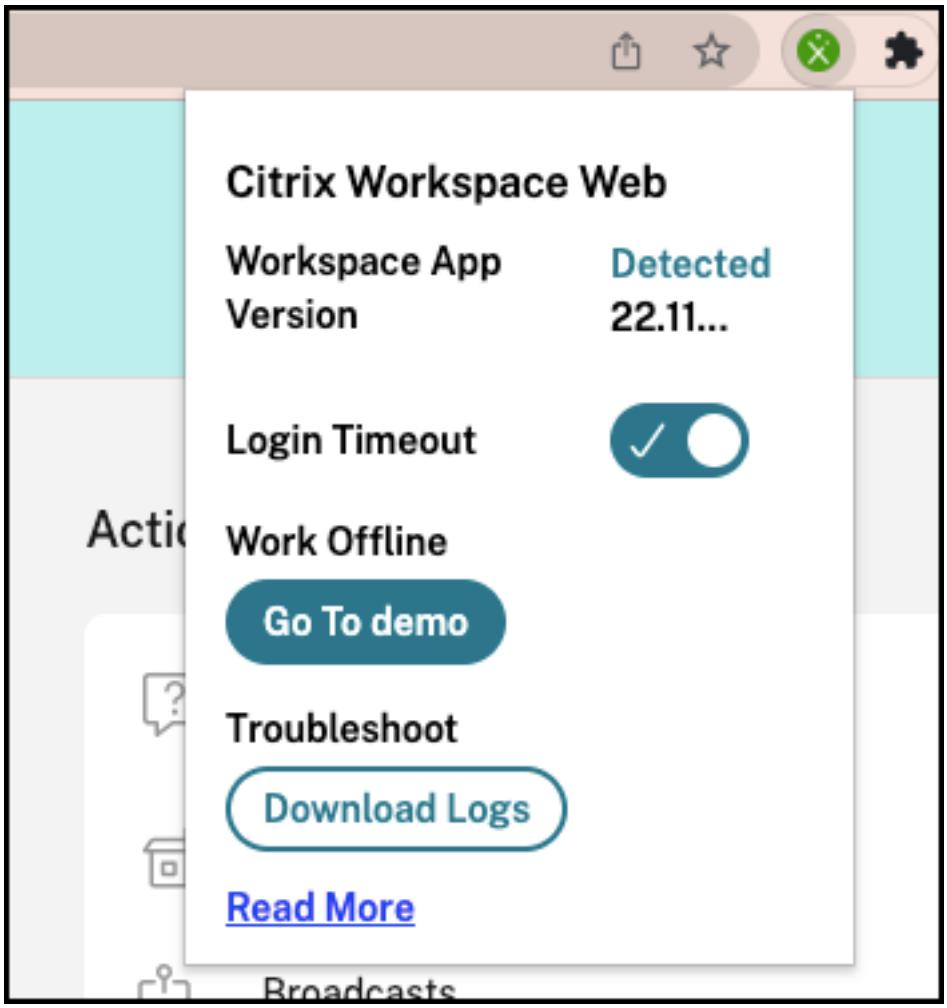
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Enable App Protection for hybrid launch

1. Install the Citrix Workspace Web extension for your browser before adding the store. Use one of the following links based on your browser:

   - Chrome
   - Edge Chromium

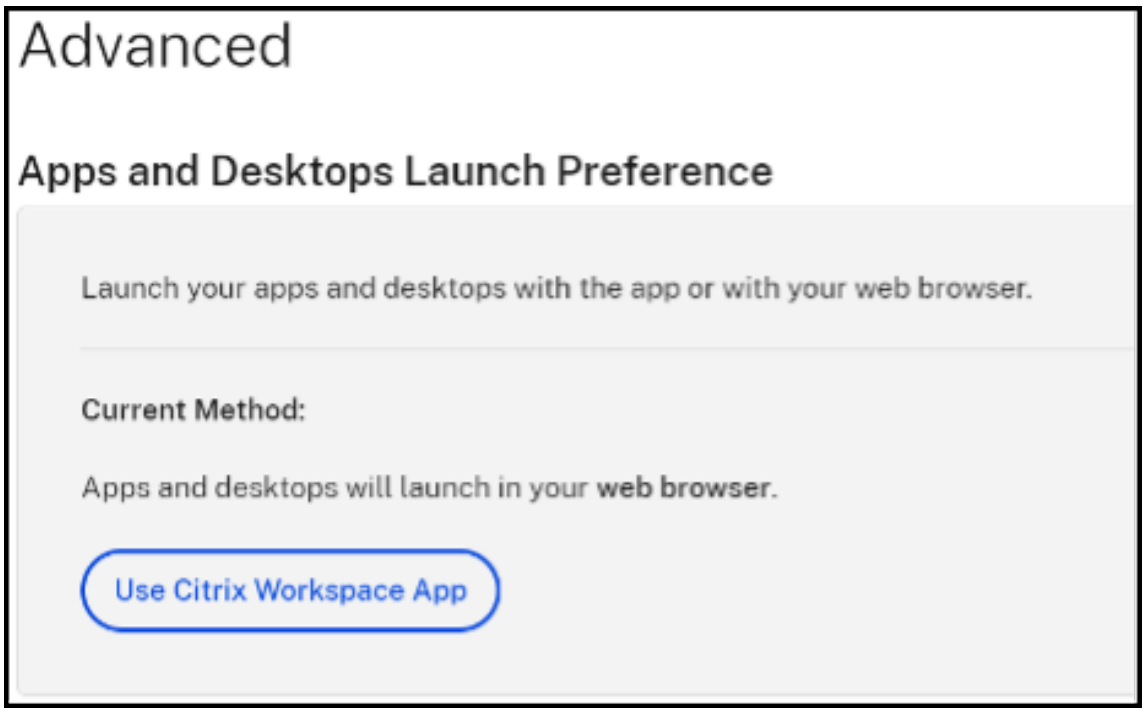
   Once you install the extension, you see it in the extensions section of your browser.



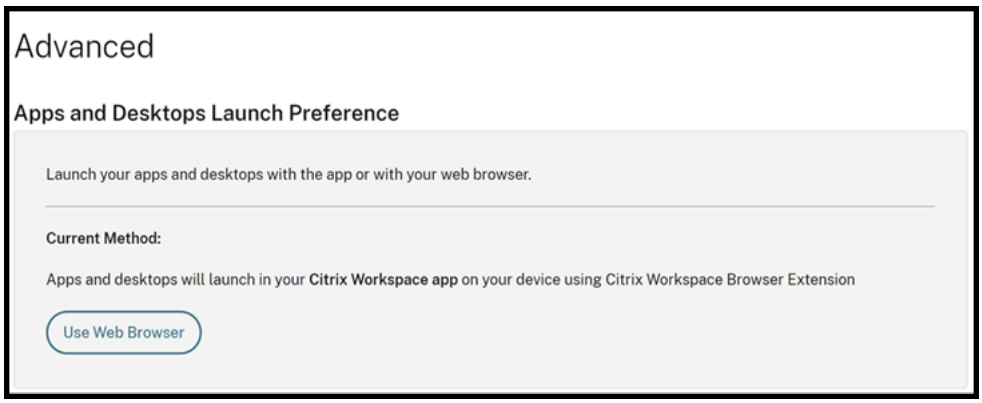
2. Sign in to the store from your native browser.
3. Navigate to your **Profile > Account Settings > Advanced**.

   In the **Apps and Desktops Launch Preference** section, you can see the current method in which the apps and desktops currently launch in your web browser. Click **Use Citrix Workspace app**.

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



If you're using the Citrix Workspace app to launch the resources, you see the following option. In such a case, no changes are required.



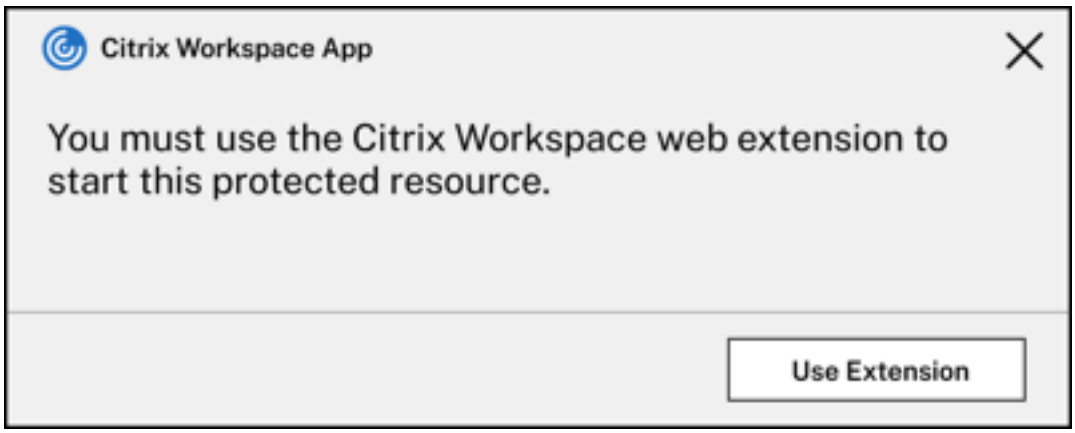
4. You can now launch your protected virtual app or desktop.

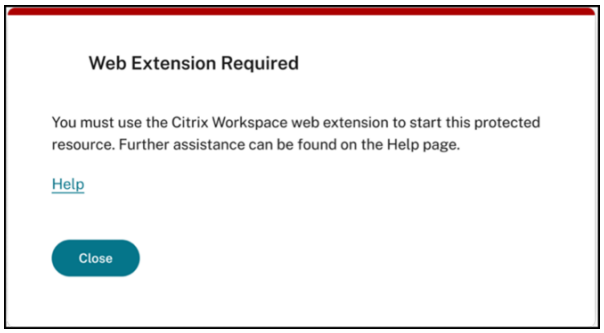
Common failure scenarios

Here are some scenarios to demonstrate failure in launches and how to fix them.

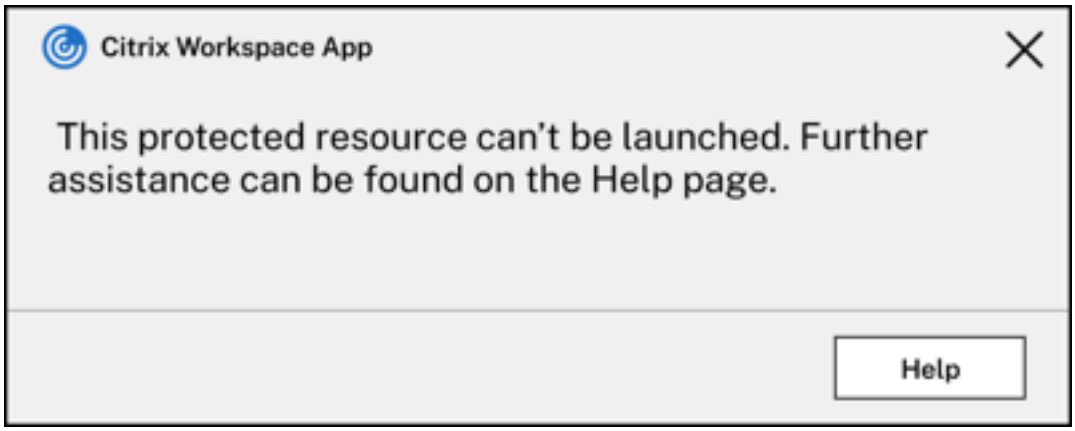
- You get one of the following errors when you disable or uninstall the Citrix Workspace Web extension before launching the protected application. To avoid it, install the extension before you log in to Citrix Workspace for Web.

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

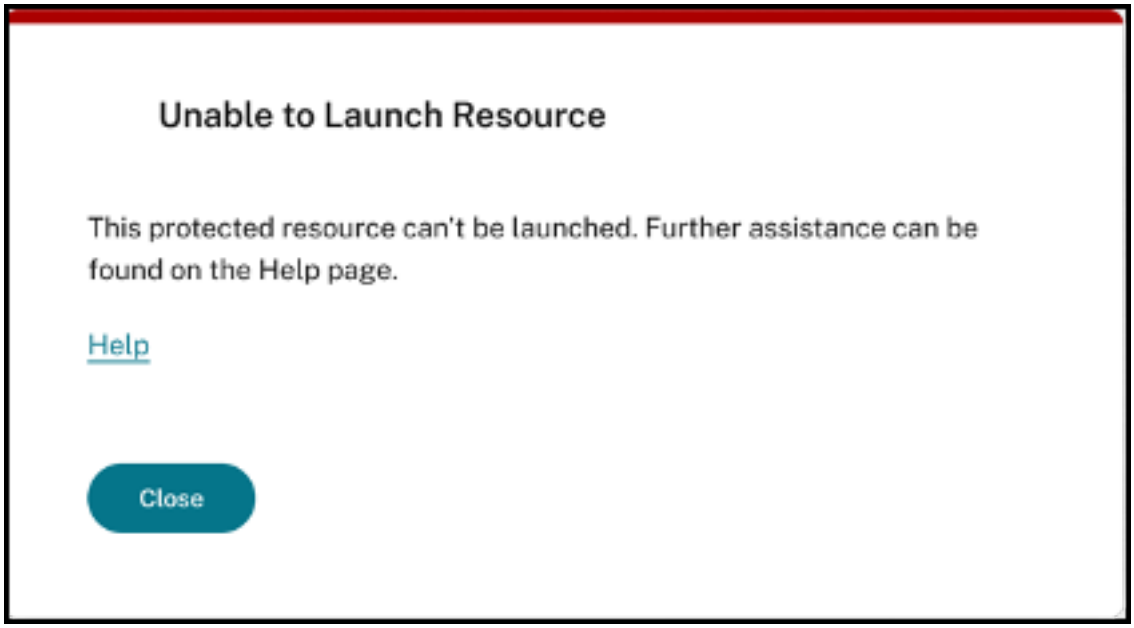




- You get one of the following errors when the launch preference is set as **Web Browser**. Change the launch preference to **Use Citrix Workspace app** to resolve this error. For more information, see this support article.



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



App Protection support for hybrid launch through StoreFront

September 7, 2025

Hybrid launch of Citrix Virtual Apps and Desktops is when you sign in to StoreFront for Web by typing the store URL in the native browser and launch the virtual apps and desktops through the native Citrix Workspace app and its HDX engine. The term hybrid is the result of using the combination of StoreFront for Web and the native Citrix Workspace app to connect and use the resources.

> **Note:**
>
> When no native Citrix Workspace app components are installed on the endpoint, it's a zero-install configuration where both the Citrix Workspace store and the HDX engine are within the browser. This scenario is known as Citrix Workspace app for HTML5, which is hosted either on Citrix Workspace or Citrix StoreFront. This document does not address that scenario.

App Protection support for hybrid launch through StoreFront provides the ability for App Protection enabled resources to be displayed and launched from browsers.

> **Note:**
>
> If you select the options **Use light version** (which uses the HTML5 client) or **Already installed**, then the App Protection enabled sessions are blocked as Citrix Workspace app isn't detected successfully in the browser.

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

If you're using StoreFront 2308 or later, then you can access the apps and desktops that are enabled with App Protection policies using a web browser if StoreFront is configured appropriately and the browser successfully detects the native Citrix Workspace app. If you're using versions between StoreFront 1912 and 2203, then you must apply the customization as described in the How to deploy section.

> **Limitation:**
>
> StoreFront determines the Citrix Workspace app version when you sign in to the website for the first time. If you later install a different version of Citrix Workspace app, then StoreFront isn't aware of the change. So, it might incorrectly allow or disallow the launching of virtual apps and desktops enabled with App Protection policies. Citrix recommends configuring App Protection Posture Check which blocks launching virtual apps and desktops from previous versions of Citrix Workspace app that do not support App Protection. For more information about Posture Check, see App Protection Posture Check.

Hybrid launch through StoreFront version 2308 or later

StoreFront versions 2308 include support for hybrid launch of virtual apps and desktops enabled with App Protection policies but this is disabled by default. For more information about enabling App Protection for hybrid launch on StoreFront 2308 or later, see App Protection for hybrid launch via StoreFront.

Hybrid launch through StoreFront versions between 1912 and 2203

StoreFront versions between 1912 and 2203 supports the enabling of hybrid launch of virtual apps and desktops that are enabled with App Protection policies using a customization as follows:

Citrix recommends removing this customization when upgrading to StoreFront 2308 or later.

Prerequisites

For information about the required versions of Citrix components for App Protection, see System requirements.

How to deploy

1. Download the Zip file named *stf-customization-AppP.zip*, which has all the required files that you must deploy to the StoreFront server machine. Download the file from Citrix Downloads. The file includes the following:

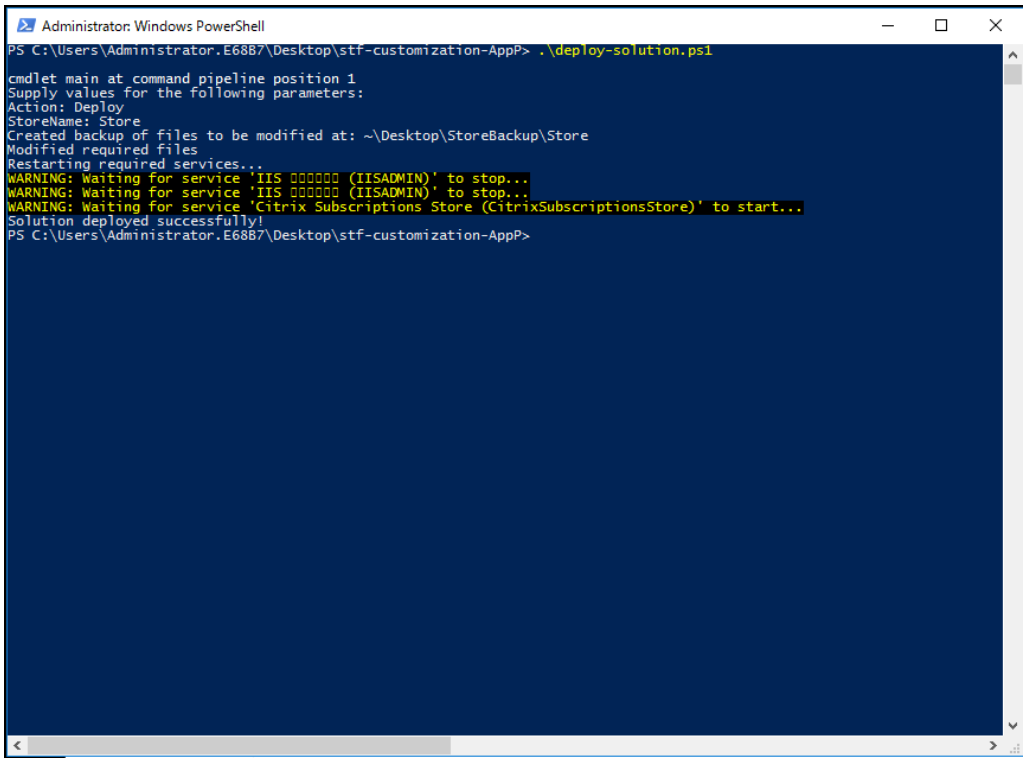
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DLLs that you must copy to the store's bin folder
- JavaScript files and other files required for the solution to work
- *deploy-solution.ps1* PowerShell script, which the StoreFront admin uses to deploy the solution

2. Unzip the *stf-customization-AppP.zip* file and open a new administrator PowerShell where the files are extracted. Run the `deploy-solution.ps1` command, which takes the following arguments:

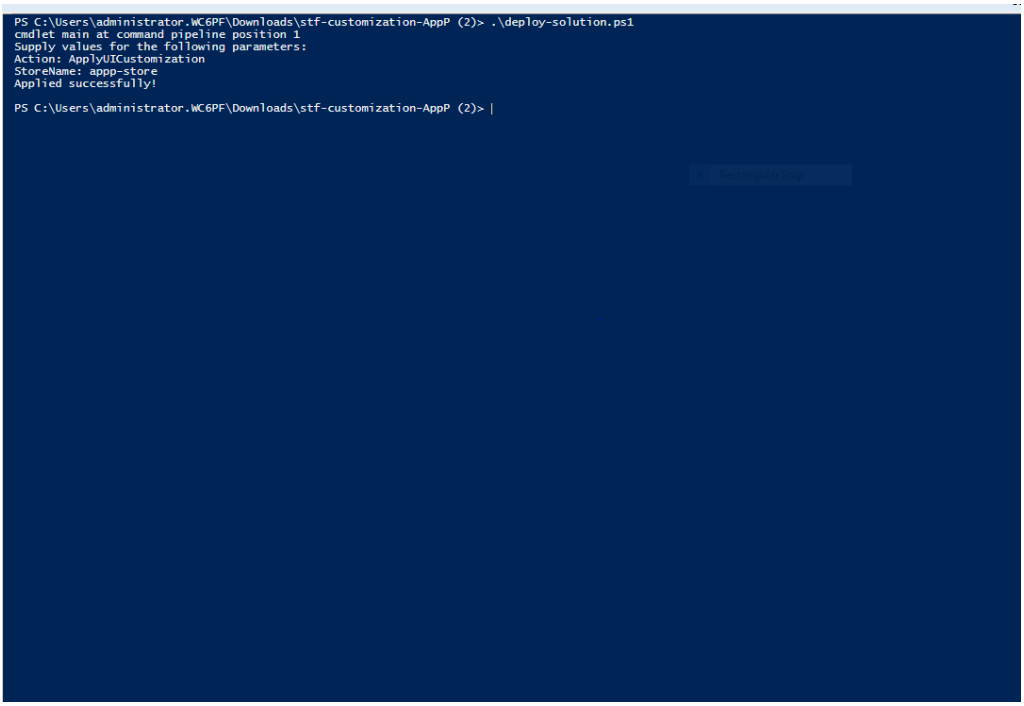
   - `-Action`: The action that the script takes. The allowed values are as follows:

     - The `Deploy` action deploys the solution in a seamless manner. It creates a backup of files that this solution changes, copies the solution files, and restarts the services. The following screenshot describes the command to deploy the solution on the StoreFront server:



     - The `ApplyUICustomization` action applies a customization on the store UI so that you don't see the **Already installed** and **Use light version** options. This action enforces detection of the native Citrix Workspace app in the browser and makes sure that you bypass the blocked or unsupported scenarios.

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



  - The `RemoveUICustomization` action undoes the action of `ApplyUICustomization` and the **Already Installed** and **Use light version** options appear again.
- `-StoreName`: The name of the store for which the action must be taken. This parameter is mandatory and it must be passed along with the `Deploy` action.
- `-BackupDir`: Parameter that can be passed with the `Deploy` action to create a backup at the required directory. If not passed, the backup is created on the desktop. This parameter is an optional parameter.

> **Note:**
>
> If there are any existing customizations in *StoreCustomization_Input.dll* or *StoreCustomization_Launch.dll*, deploying this solution overrides them.

The App Protection enabled apps and desktops will only display after deploying the customizations. Without the deployment, the apps and desktops don't display.

How to revert StoreFront customization

Do the following steps to revert the preceding StoreFront customization:

1. Go to *\Desktop\StoreBackup<store name>* directory and copy the following files to the respective directories:
   - *StoreCustomization_Input.dll* and *StoreCustomization_Launch.dll* files to the *IISINETPub\Citrix<store name>\bin* directory

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

- *web.config* file to the *IISINETPub\Citrix\StoreWeb* directory
- **.js* and *style.css* files to the *IISINETPub\Citrix\StoreWeb\Custom* directory

> **Note:**
>
> If there are customization files other than the preceding files in the \Desktop\StoreBackup<store name> directory, copy those files and directories to the relevant directories as needed.

2. Open PowerShell.
3. Stop the **IISADMIN** and **CitrixSubscriptionsStore** services by running the following commands:

```
sc stop IISADMIN
sc stop CitrixSubscriptionsStore
```

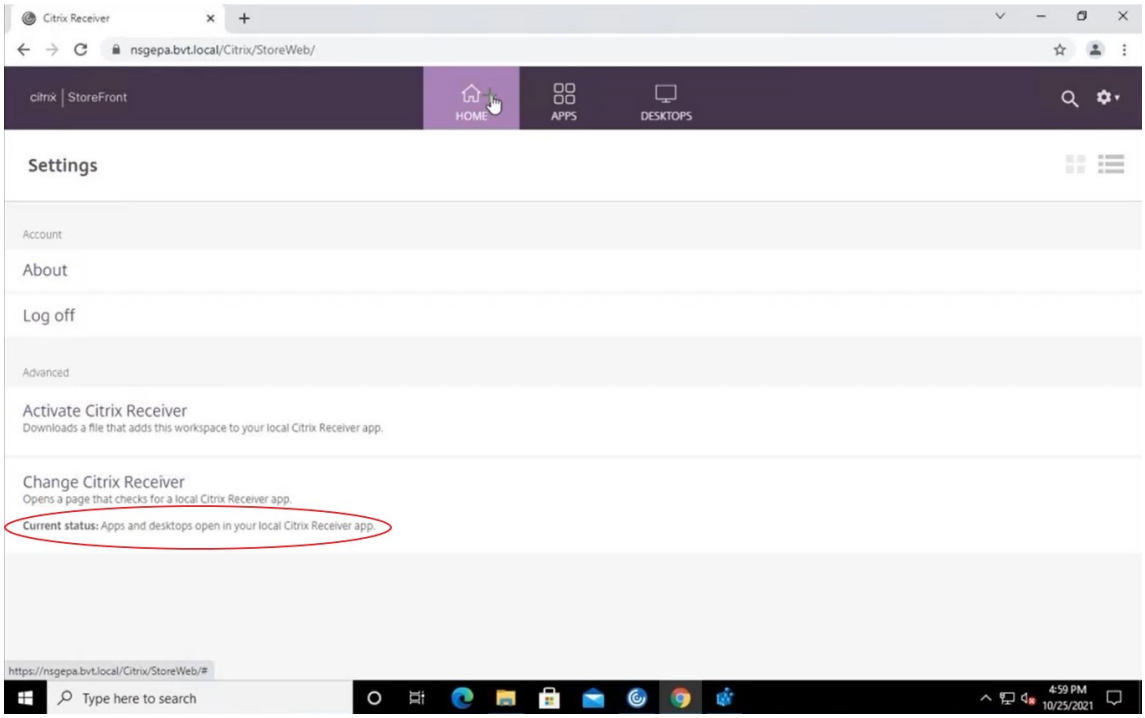
4. Start the **IISADMIN** and **CitrixSubscriptionsStore** services again by running the following commands:

```
sc start IISADMIN
sc start CitrixSubscriptionsStore
```

End user experience of hybrid launch for protected resources

1. After the deployment of the solution by the admin on the StoreFront server, sign in to your store on the client side and then access StoreFront using the URL in a web browser.
2. To see if Citrix Workspace app is successfully detected in the browser, check the **Current status** in your **Account Settings**.

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



After Citrix Workspace app is detected, you can see and launch all the virtual apps and desktops that are enabled with App Protection.

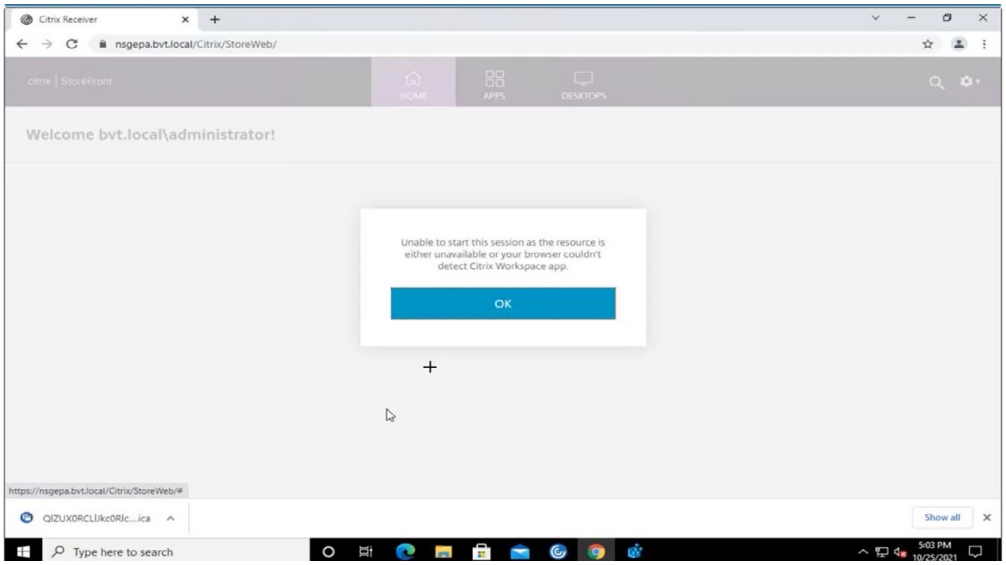
Enable tracing on StoreFront

To enable tracing in StoreFront, see the StoreFront documentation. This trace can be used to verify whether the configured NetScaler Gateway session policy labels are passed down to the store properly.

Troubleshooting

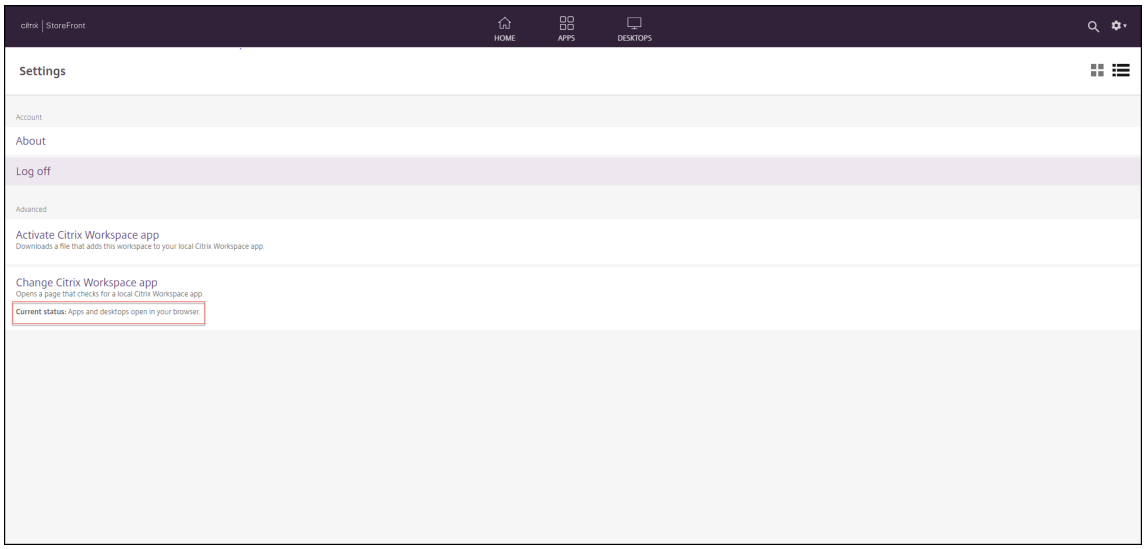
When you launch the App Protection enabled sessions, you might sometimes face the following error:

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



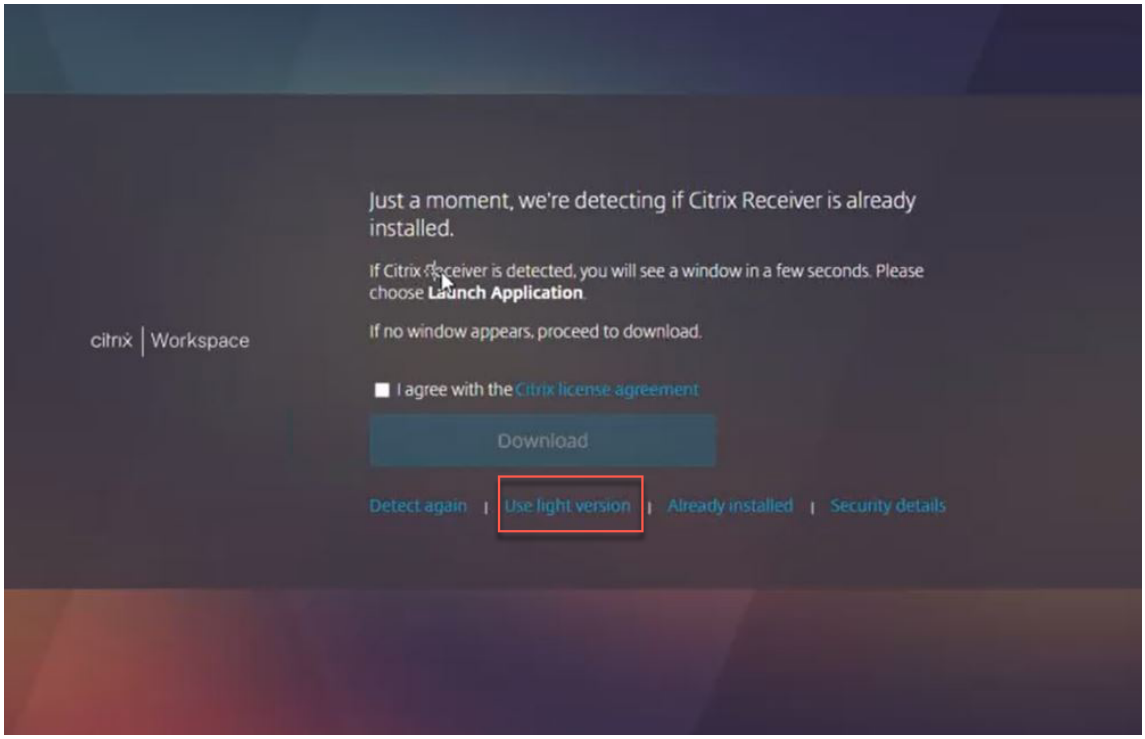
The possible reasons for this error are as follows:

- The apps and desktops are configured to open in a browser.

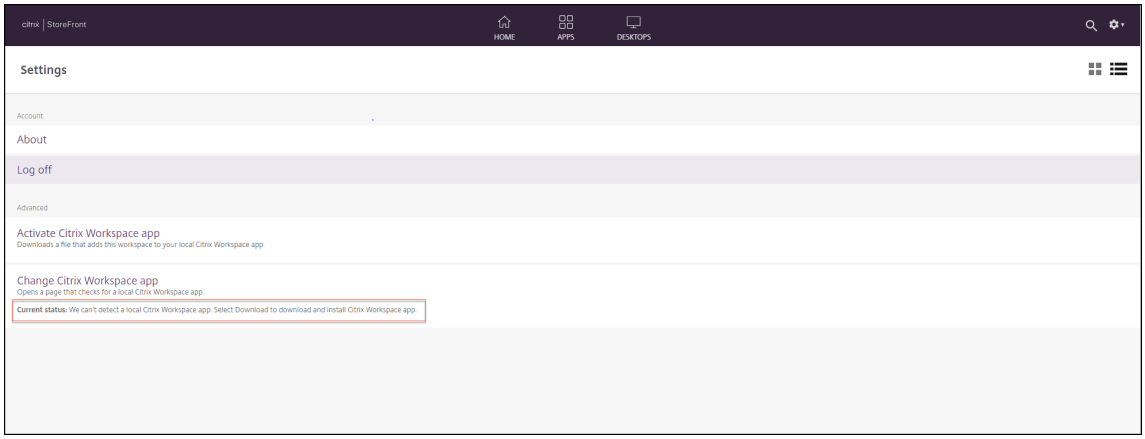
  

  You face this scenario if you clicked **Use light version** during Citrix Workspace app detection as shown in the following screen:

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

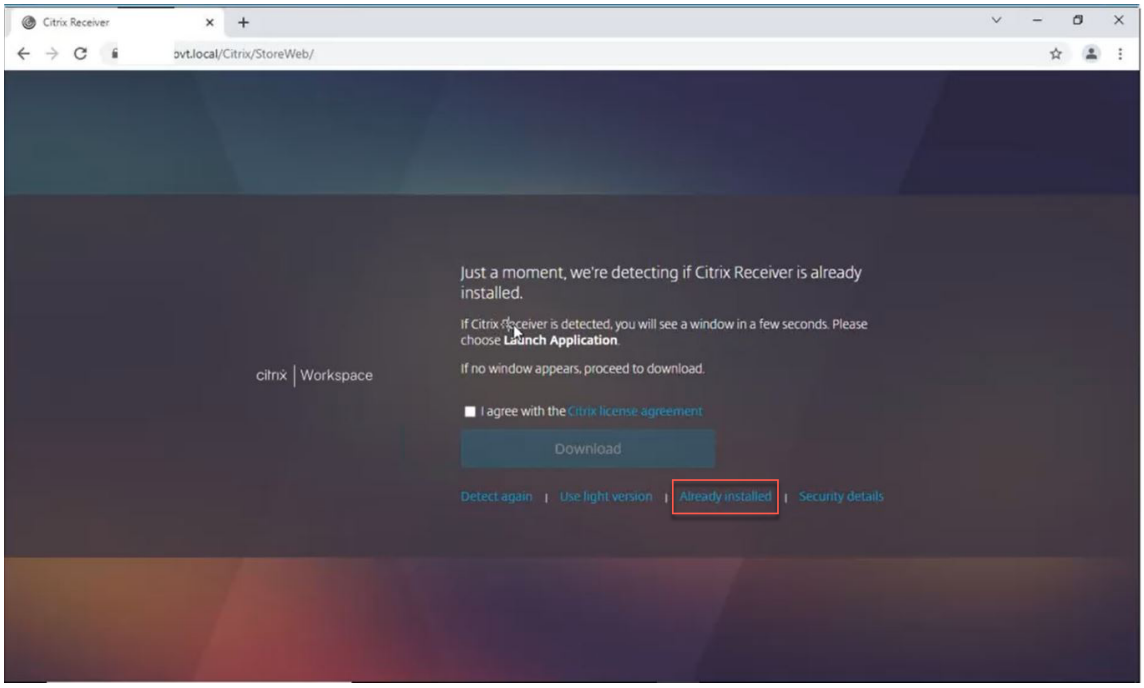


- The browser doesn't detect Citrix Workspace app.



You face this scenario if you clicked **Already installed** during Citrix Workspace app detection as shown in the following screen:

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



Solution: To correct the preceding scenarios and launch the App Protection enabled sessions, click **Change Citrix Workspace app** in **Account Settings** and wait for Citrix Workspace app to be detected.

Optimization

Citrix Workspace app detection is mandatory to launch the App Protection enabled sessions. To avoid failures during hybrid launches for protected sessions, the StoreFront admins can use the `ApplyUICustomization` action of the `deploy-solution.ps1` command and hide the **Use light version** and **Already installed** options.

Blocking of Screen Capture from AI-Powered tools

September 7, 2025

As AI powered tools and agents become more common on endpoints, screen capture capabilities often used by large language models (LLMs) can inadvertently expose sensitive data. This risk is especially significant in regulated industries where compliance and data protection are critical.

App Protection helps safeguard sensitive information by detecting and blocking unauthorized screen capture attempts, including those from advanced AI driven features like Microsoft Recall. By integrating these protections, Citrix helps secure virtualized applications and maintain data security across all user environments.

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

> **Note:**
>
> To use Citrix App Protection's Anti-Screen Capture feature, ensure that all prerequisites are met for the following components -
>
> - Citrix Workspace app for Windows LTSR 2203.1 and above, Citrix Workspace app for Windows CR 2305.1 and above
> - Citrix Workspace app for iOS 24.9.0 and above
> - Citrix Workspace app for Linux 2108 and above
> - Citrix Workspace app for Mac 2001 and above
> - Citrix Workspace app for Android 24.7.0 and above
> - Citrix Workspace app 1912 and above

Blocking screen capture attempt by Microsoft Recall

Citrix Workspace app for Windows 2507 will support arm64 based devices in emulation mode. Leveraging app protection anti-screen capture policy will detect and block attempts by Microsoft Recall to capture screen content on arm64 based Copilot+ PCs.

App Protection events to Director and Monitor

July 9, 2026

Introduction

Citrix Workspace app (CWA) for Windows introduces built-in security checks that automatically detect high-risk conditions on endpoints—such as **Microsoft Recall**—without requiring manual configuration. These detections provide real-time visibility by reporting events to Citrix Director and Monitor, enabling administrators to quickly assess risk and apply protective measures like App Protection policies.

While detection for select events (for example, Microsoft Recall) is automatic, protection from these events requires manual configuration of App Protection policies by the administrator.

By utilizing proactive risk management and policy reconfiguration, administrators can strengthen endpoint security in their environment and reduce exposure to emerging threats. This proactive approach furthers the Citrix® commitment to secure application delivery by helping organizations identify and respond to threats in real time.

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

> **Note:**
>
> Citrix Workspace app collects telemetry data about user and device usage through the product for license entitlement enforcement as well as to operate, manage, measure and improve the software, including the following:
>
> - Device ID
> - User name
> - Timestamp
> - IP address

Prerequisites

- **Citrix Virtual Delivery Agent**: VDA version 2507 or later.
- **Citrix Director**: Citrix Virtual Apps and Desktops 2603 or later.
- **Citrix Monitor**: DDC version 128 or later.
- **Citrix Workspace app (CWA) for Windows**: Version 2603 or later is required on the endpoint.
    - For protection events, the administrator must configure the relevant App Protection policies (for example, Anti-screen capture, Anti-DLL injection) through Citrix policy.

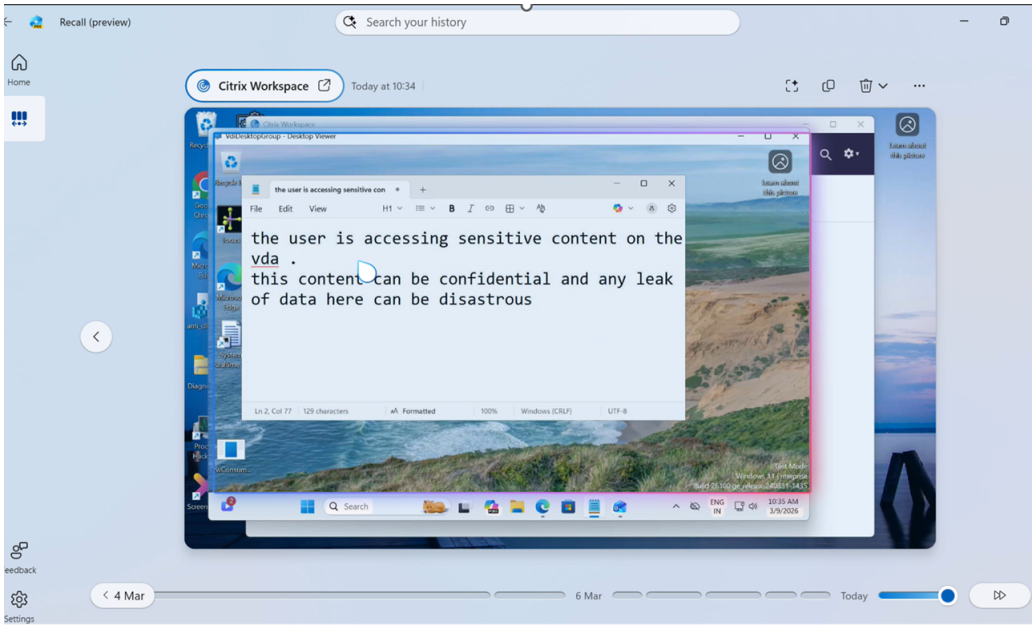
Event Types

Microsoft Recall Detection

Windows Recall is an AI agent running on the endpoint that continuously captures and stores snapshots of the user's screen content locally for analysis. These snapshots can include sensitive information such as:

- Corporate credentials entered during sign-in.
- Confidential application data displayed in virtual desktops or published apps.
- Proprietary documents and intellectual property visible during a session.

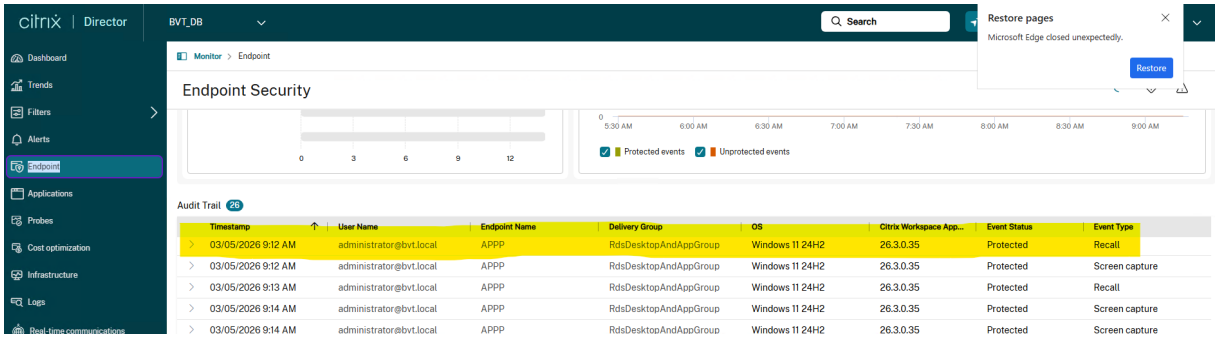
© 1997–2026 Citrix Systems, Inc. All rights reserved.



If exploited, this feature could allow attackers or unauthorized users to retrieve sensitive data from the device, even after the session ends.

When is this event sent? During session launch, CWA automatically detects whether Windows Recall is active on the endpoint.

- **Detection Event**: Sent if Recall is detected and the session does **not** have the Anti-screen capture policy enabled.
- **Protection Event**: Sent if Recall is detected and the session **has** the Anti-screen capture policy enabled.



Event-Specific Data

This event uses only the common fields; it includes no additional fields beyond `resourceType` and `resourceName`.

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

Screen Capture Detection

A screen capture event is raised when a user or tool attempts to take a screenshot of the endpoint desktop. If the App Protection Anti-screen capture policy is enabled, the content of the session is blacked out for the capture tool. The tool can still capture the desktop region outside the session, but the session content itself is obscured.

When is this event sent? A `screenCaptureEvent` is sent when CWA detects a screen capture tool actively attempting to capture the screen while a session with Anti-screen capture policy is enabled and running. The event includes the name and path of the tool, along with its signing status.



DLL Injection Detection

A DLL (Dynamic Link Library) is an executable library. DLL Injection occurs when a process injects DLLs into Citrix processes. These DLLs could be injected for various reasons —both genuine (e.g., graphics drivers, antivirus software) and malicious (e.g., intercepting network traffic, intercepting credentials).

App Protection Anti-DLL Injection prevents unsigned DLLs from being injected into specific Citrix processes. An unsigned DLL being injected into a Citrix process is considered a DLL injection event.

When is this event sent? A DLL injection event is sent when CWA detects an unsigned DLL being injected into a protected Citrix process while the Anti-DLL injection policy is enabled.



Details of Data and Events

Common Event Schema

All endpoint security events share a common envelope reported to Director and Monitor:

Field	Description	Example
`deviceName`	Endpoint computer name.	`WORKSTATION-01`
`username`	Logged-in user (UPN format).	`john@example.com`

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

Field	Description	Example
`timestamp`	Unix epoch timestamp in milliseconds.	`1733805466000`
`osVersion`	Endpoint operating system version.	`Windows 11 Pro`
`cwaVersion`	Citrix Workspace app version on the endpoint.	`25.3.2.196`
`ipAddress`	Endpoint IP address.	`123.45.67.89`
`version`	Event schema version.	`1.0`
`eventType`	Identifier for the security event type.	`recallEvent`
`payloadType`	0 = Detection (threat identified); 1 = Protection (mitigated).	`0`
`component`	CWA component that generated the event.	`AppProtection`

Every event also includes an **EndpointSecurityAdditionalData** object containing:

Field	Description	Example
`resourceType`	Type of resource associated with the event.	`ICA session`
`resourceName`	Friendly name of the published resource.	`Prod_Win11_Session`

Screen Capture Event-Specific Data

In addition to common fields, `EndpointSecurityAdditionalData` includes:

Field	Description	Example
`screenCaptureToolName`	Executable name of the detected tool.	`obs64.exe`
`screenCaptureToolPath`	Full file-system path to the tool executable.	`C:\Program Files\obs-studio\bin\64bit`
`signed`	Whether the detected executable is digitally signed.	**`true`**

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

DLL Injection Event-Specific Data

In addition to common fields, administrators can see the path of the DLL:

Field	Description	Example
`dllPath`	Full file-system path to the injected unsigned DLL.	`C:\Program Files\abc.dll`

Citrix Workspace app release timelines

September 7, 2025

This release timeline illustrates the target release cadence and dates of Citrix Workspace app releases. Although exact dates might change, we want to help you plan ahead. We also want to make it easier for you to manage Citrix Workspace app deployments.

You can download new releases from the Citrix Workspace app Downloads page. Citrix Workspace app for Android, Citrix Workspace app for iOS, and Citrix Workspace app for Windows (Store) are also available for download from their respective app stores. If you have enabled Citrix Workspace Updates for Citrix Workspace app for Mac or Windows, you're notified to accept the download and install the update. Consider subscribing to our RSS feed to receive alerts when new releases become available.

For details about the features available in each Citrix Workspace app, see Citrix Workspace app feature matrix.

For lifecycle information, see Lifecycle Milestones for Citrix Workspace app.

Target release cadence

The following Citrix Workspace app platforms follow a quarterly release cadence:

- Linux
- Mac
- Windows
- ChromeOS
- HTML5

The following Citrix Workspace app platforms follow a monthly release cadence:

- Android

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

- iOS

> **Note:**
>
> Citrix Workspace app for Windows, Citrix Workspace app for Mac, Citrix Workspace app for Android, and Citrix Workspace app for iOS going forward will be having major and minor releases in a quarter. Minor releases will be denoted as '.10'and these releases will include minor enhancements around quality and performance improvements. The minor '.10'release isn't expected to have any major features.

Target release dates for desktop apps

Citrix Workspace™ app	Jan 2025	Feb 2025	Mar 2025	Apr 2025	May 2025	Jun 2025	Jul 2025	Aug 2025	Sep 2025	Oct 2025	Nov 2025	Dec 2025
Windows	☒	-	☑	☒	-	-	☑	-	☒	-	☑	☒
Windows LTSR	-	-	☒	-	-	☒	☑	-	-	☒	-	-
Mac	-	-	☑	☒	☑	☒	-	☑	☒	-	☑	☒
ChromeOS	☑	-	-	☑	-	☑	-	☑	-	☑	-	
HTML5	-	☑	-	-	☑	-	-	-	☑	-	☑	-
Linux	-	-	☑	-	☑	-	-	☑	-	-	☑	-

Note: The ☑ symbol denotes major releases and the ☒ symbol denotes minor releases. The ☒ symbol denotes cumilative updates (CUs).

Target release dates for mobile and tablet apps

Citrix Workspace app for Android and Citrix Workspace app for iOS follow a monthly release cadence.

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

Citrix Workspace app	Jan	Feb	Mar 2025	Apr 2025	May 2025	Jun 2025	Jul 2025	Aug 2025	Sep 2025	Oct 2025	Nov 2025	Dec 2025
Android and iOS	☑	☒	☑	☒	☑	☒	☑	☒	☑	☒	☑	☒

Note: The ☑ symbol denotes major releases and the ☒ symbol denotes minor releases. Minor releases are optional releases tailored to meet specific requirements or improvements.

> **Disclaimer:**
>
> The development, release, and timing described for our products remains at our sole discretion and is subject to change without notice or consultation. The data provided is for informational purposes only and is not a commitment, promise, or legal obligation to deliver any material, code, or functionality and should not be relied upon in making purchasing decisions or incorporated into any contract.

Citrix Workspace app feature matrix

October 8, 2026

Citrix Workspace app provides a gamut of features distributed across different platforms or operating systems. With this feature matrix, you can clearly understand the availability of the features across different platforms. In each section, along with the feature matrix, you can find the feature definition table that describes every feature in brief.

Citrix Workspace

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Citrix Virtual Apps	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Citrix Virtual Desktops	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Citrix Secure Private Access	Yes	Yes	No	Yes	Yes	Yes	No	No	No
Citrix Enterprise Browser (formerly Citrix Workspace Browser)	Yes	Yes(5)	Yes	Yes	No	No	No	No	No
Web/SaaS apps with SSO	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Citrix Mobile Apps	No	No	No	No	Yes	Yes	No	No	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
App Personalization service	Yes	No	No	Yes	Yes	Yes	No	No	No
Auto launch desktops and apps	No	No	No	No	Yes	No	No	No	No

Feature	Definition
Citrix Virtual Apps	Access Citrix Virtual Apps through Citrix DaaS or Citrix Virtual Apps and Desktops™ entitlement.
Citrix Virtual Desktops™	Access Citrix Virtual Desktops through Citrix DaaS or Citrix Virtual Apps and Desktops entitlement.
Citrix Virtual Apps	Access Citrix Virtual Apps through Citrix DaaS or Citrix Virtual Apps and Desktops™ entitlement.
Citrix Virtual Desktops™	Access Citrix Virtual Desktops through Citrix DaaS or Citrix Virtual Apps and Desktops entitlement.

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

Feature	Definition
Citrix Secure Private Access	With the Citrix Secure Private Access IT admins can govern access to approved SaaS apps. Also, with a simplified single sign-on experience admins can protect the organization's network and end-user devices from malware and data leaks by filtering access to specific websites and website categories.
Citrix Enterprise Browser(5)	Browser delivered with the Citrix Workspace app to access SaaS and Web Apps securely.
Web/SaaS apps with SSO	Access SaaS/Web Apps configured using Secure Workspace Access with SSO.
Citrix Mobile apps	Access Citrix Mobile Apps aggregated by Citrix Endpoint Management formerly known as XenMobile.
Citrix Mobile App Upgrades	Access Citrix Mobile Apps aggregated by Citrix Endpoint Management formerly known as XenMobile.
App Personalization service	Allows to have a personalized corporate experience. You can have a custom app name and a co-branded icon for your Citrix Workspace app across the app workflow.
Auto launch desktops and apps	Configurable by admin, launches desktop or apps automatically upon login based on geo-location or user behavior analysis.
Auto launch desktops and apps	Configurable by admin, launches desktop or apps automatically upon login based on geo-location or user behavior analysis.

Workspace Management

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Auto configure using DNS for email discovery	Yes	Yes	No	Yes	Yes	Yes	No	No	No
Centralized Management settings	Yes	Yes	Yes	No	No	No	No	Yes	Yes
Global App Config service (Workspace)	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Global App Config service (StoreFront)	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
App Store updates	No	No	No	No	Yes	Yes	No	No	No
Citrix Auto updates	Yes	Yes	No	Yes	No	No	No	No	No
Client App Management	Yes	No	No	No	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

Feature	Definition
Auto configure using DNS for email discovery	Enable Citrix Workspace app to be configured via auto-discovered settings.
Centralized Management settings	App setting from a centralized service, for example, Google Chrome management or GPOs.
Global App Config service (Workspace)	The Global App Configuration service for Citrix Workspace allows a Citrix administrator to deliver Workspace service URLs and Citrix Workspace app settings through a centrally managed service.

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

Feature	Definition
Global App Config service (StoreFront)	The Global App Configuration service for Citrix StoreFront allows a Citrix administrator to deliver Citrix Workspace app settings through a centrally managed service.
App Store updates	Updates from vendor application store
Citrix Auto updates	Updates for Windows and Mac through Citrix Auto-upgrade functionality
Client App Management	Enables Citrix Workspace app to become a single client app that is required on the end point to install and manage agents such as Secure Access Agent and End Point Analysis (EPA) plug-in. With this feature, administrators can easily deploy and manage required agents from a single management console.
App Store updates	Updates from vendor application store
Citrix Auto updates	Updates for Windows and Mac through Citrix Auto-upgrade functionality
Client App Management	Enables Citrix Workspace app to become a single client app that is required on the end point to install and manage agents such as Secure Access Agent and End Point Analysis (EPA) plug-in. With this feature, administrators can easily deploy and manage required agents from a single management console.

User interface

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Desktop Viewer/Toolbar	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multi-tasking	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Follow Me Sessions (Workspace Control)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Connection Strength Indicator Phase 2	No	No	No	No	Yes	No	No	No	No

Feature	Definition
Desktop Viewer/Toolbar	Enables in session control of session functions like sending Ctrl+Alt+Del via a toolbar.
Multi-tasking	Enables multiple apps and desktops to be used at the same time.
Follow Me Sessions (Workspace Control)	Allows users to move between devices and automatically connect to all of their sessions.

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

Feature	Definition
Connection Strength Indicator Phase 2	Displays enhanced session details, including CPU and memory usage, connection history, scored metrics, and actionable recommendations to help users and administrators assess and improve session performance.
Connection Strength Indicator Phase 2	Displays enhanced session details, including CPU and memory usage, connection history, scored metrics, and actionable recommendations to help users and administrators assess and improve session performance.

HDX™ Host Core

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Adaptive transport	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
HDX adaptive throughput	Yes	Yes	No	No	No	No	Yes	Yes	Yes
SDWAN support	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Session reliability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Auto-client Reconnect	Yes	Yes	Yes	Yes	No	Yes	No	Yes	No
Session sharing	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multi-port ICA®	Yes	Yes	Yes	No	No	No	No	No	No

Feature	Definition
Adaptive transport	Enables EDT transport for HDX for improved throughput independent of network conditions.
SDWAN support	Enables SDWAN acceleration for QoS, TCP, compression, and de-duplication.
Session reliability	Keeps sessions active and on the user's screen when network connectivity is interrupted.
Auto-client Reconnect	Prompts and reconnects the session on connection interruption.
Session Sharing	Enables the published app to run over the same connection as other published applications when already running on the same server.
Multi-port ICA	Allows support for multiple TCP ports for HDX traffic to improve the Quality of Service.

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

HDX IO / Devices / Printing

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2402 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Local printing	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Generic USB redirection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Client drive mapping / File transfer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TWAIN 2.0	Yes	No	No	No	No	No	No	No	No

Feature	Definition
Local printing	Enables users to print documents via shared or local printers.
Generic USB redirection	Enables use of USB devices inside the session. For example, keyboard, mouse, external webcam and so on.
Generic USB redirection	Enables use of USB devices inside the session. For example, keyboard, mouse, external webcam and so on.

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

Feature	Definition
Client drive mapping / File Transfer	Enables use of client drives inbuilt or attached for data storage.
TWAIN	Allows mapping client TWAIN devices, such as digital cameras or scanners.
TWAIN	Allows mapping client TWAIN devices, such as digital cameras or scanners.

HDX integration

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Local App Access	Yes	Yes	No	No	No	No	No	No	No
Multi-touch	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Mobility pack	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No
HDX Insight	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
HDX Insight with NSAP VC	Yes	Yes	Yes	Yes	Yes *(3)*	Yes *(3)*	No	No	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
EUEM experience matrix	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No
Bidirectional content redirection	Yes	Yes	Yes	Yes	No	No	No	No	No
Legacy Host-to-Client Redirection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Browser content redirection	Yes	Yes	Yes	Yes	No	No	No	Yes	No
File open in Citrix Workspace app	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Location Based Services (Location available via API-description)	Yes	Yes	No	No	Yes	Yes	No	No	No

Feature	Definition
Local App Access	Access the local application on a client device inside the session.
Multi-touch	Enables 10 finger multi-touch control of Windows/Linux desktops and apps.
Mobility pack	Enables native device experience features (for example, auto popup keyboard and local device UI controls) and tablet-optimized desktops.
HDX insight	Provides visibility into the session startup/end times using ICA network performance metrics.
HDX insight with NSAP VC	Provide visibility into the session startup/ end time using the NetScaler App Experience or NSAP Virtual channel to get HDX insights.

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

Feature	Definition
EUEM experience matrix	Provides Citrix admins visibility into the logon duration metrics via the Citrix Virtual Desktop that was formerly known as XenDesktop® 7 Director.
EUEM experience matrix	Provides Citrix admins visibility into the logon duration metrics via the Citrix Virtual Desktop that was formerly known as XenDesktop® 7 Director.
Bi-directional Content redirection	Enables client to host and host to client URL redirection.
Legacy Host-to-Client Redirection	Allows URLs, embedded as hyperlinks in applications running on a Citrix® session, to open using the corresponding application on the user endpoint device.
Legacy Host-to-Client Redirection	Allows URLs, embedded as hyperlinks in applications running on a Citrix® session, to open using the corresponding application on the user endpoint device.
Browser content redirection	Enables an entire webpage (a browser's viewport) to be redirected to the endpoint for local rendering, offloading the server.
File open in Citrix Workspace app	Allows opening a local file in Citrix Workspace app using a hosted application (Client to Server Content Redirection).
Location Based Services (Location available via API-description)	Enables location information to be used by applications delivered by Citrix Virtual Desktop earlier known as XenDesktop.

HDX multimedia

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Audio playback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bi-directional Audio (VoIP)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Webcam redirection	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Video playback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Teams optimization	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes
Skype for Business Optimization Pack	Yes	Yes	Yes	Yes	No	No	No	No	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Cisco Jabber unified communications optimization	Yes	Yes	Yes	No	No	No	No	No	No
Windows Multimedia redirection	Yes	Yes	Yes	No	No	No	No	No	No
UDP audio	Yes	Yes	Yes	No	No	No	No	No	No
Unified Communications SDK	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes

Feature	Definition
Audio Playback	Enables server rendered audio playback.
Bi-directional audio (VoIP)	Enables use of hosted softphone / voice chat collaboration applications.

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

Feature	Definition
Webcam redirection	Enables use of video chat collaboration applications using a local webcam.
Video playback	Enable viewing of recorded videos.
Microsoft Teams optimization	Offloads Microsoft Teams media processing from the Citrix server to the user device.
Skype for Business optimization	Offloads Skype for Business media processing from the Citrix server to the user device. For Citrix Workspace app for Android, we support only on Chrome devices.
Cisco Jabber unified communications optimization	Offloads Jabber media processing from the Citrix server to the user device.
Windows Multimedia redirection	Enables Windows Multimedia to be rendered on the user device, offloading the server.
UDP audio	Support for audio input and output over UDP.
Unified Communications SDK	Allows integration of unified communications features (such as voice and video) into supported desktop and browser-based applications using Citrix Workspace.
Unified Communications SDK	Allows integration of unified communications features (such as voice and video) into supported desktop and browser-based applications using Citrix Workspace.

Security

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
TLS 1.3	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
TLS 1.2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TLS 1.0/1.1	No	No	No	Yes	No	No	Yes	Yes	Yes
DTLS 1.0	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
DTLS 1.2	Yes	Yes	Yes	Yes	No	No	No	No	No
SHA2 Cert	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Smart Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote Access via Citrix Gateway	Yes *(1)*	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Workspace for Web Access	Yes	Yes	Yes	Yes	Via ICA file	Yes	Yes	Yes	Yes
IPV6	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
App Protection	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Lockdown mode (iPad and iPhone)	No	No	No	No	Yes	No	No	No	No

Feature	Definition
TLS 1.3	Successor to SSL, strong communication channel security.
TLS 1.2	Successor to SSL, strong communication channel security.
TLS 1.0/1.1	Successor to SSL, strong communication channel security.
DTLS 1.0	DTLS is a derivation of the SSL protocol. It provides the same security services (integrity, authentication, and confidentiality) but under the UDP protocol.
DTLS 1.2	DTLS is a derivation of the SSL protocol. It provides the same security services (integrity, authentication, and confidentiality) but under the UDP protocol.
SHA2 Cert	Ability to use SHA2 certificates.
Smart access	Controls access to available apps by using Gateway policies and filters.
Remote access via Gateway	Provides users with secure access to enterprise apps, virtual desktops, and data anywhere without a VPN client.

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

Feature	Definition
Workspace for Web access	Access to hosted applications or virtual desktops using a browser.
IPV6	Enables use on IPV6 networks.
Lockdown mode (iPad and iPhone)	Enhanced security mode that limits device functionalities with some web-based feature restrictions.
Lockdown mode (iPad and iPhone)	Enhanced security mode that limits device functionalities with some web-based feature restrictions.

HDX graphics

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
H.264-enhanced SuperCodec	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Client hardware acceleration	Yes	Yes	Yes	Yes	No	Yes	No	No	No
3DPro graphics	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
External monitor support	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Desktop composition redirection	Yes	Yes	No	No	No	No	No	No	No
True Multi-monitor	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes

Feature	Definition
H.264-enhanced SuperCodec	Enables streamlined delivery of applications using XenApp/Desktop 7.X H264-enhanced Supercodec.
Client hardware acceleration	Enables hardware acceleration for HDX features like graphics, webcam. The use of hardware capability varies with different Citrix Workspace apps.
3DPro Graphics	Enables use of 3D professional graphics applications hosted in the data center.
External monitor support	Enables use of an external monitor.

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

Feature	Definition
Desktop composition redirection	Enables graphics command that is remote to the client for rendering to make sure server scalability. Deprecated in Receiver for Mac 12.9 version.
True Multi-monitor	XenApp® or XenDesktop creates the same number of monitors as supported by the client.
True Multi-monitor	XenApp® or XenDesktop creates the same number of monitors as supported by the client.

Authentication

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Federated authentication (SAML/Azure AD)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ADC full VPN	Yes	Yes	Yes	Yes	No	No	No	No	No
RSA soft token	No	No	No	No	Yes	Yes	No	No	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Challenge response SMS (Radius)	Yes	Yes	No	Yes	No	No	No	No	No
User Cert Auth via Gateway (via native Workspace app)	No	No	No	No	Yes	Yes	Yes	Yes	No
User Cert Auth via Gateway (via browser)	Yes *(4)*	Yes *(4)*	No	Yes	No	No	Yes	Yes	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Smart card (CAC, PIV, and so on)	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Proximity/Contactless card	Yes	Yes	Yes	No	No	No	No	Yes	No
Credential insertion (for example, Fast Connect, Store-browse)	Yes	Yes	Yes	No	No	No	No	Yes	No
Pass through authentication	Yes	Yes	No	No	No	No	No	No	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Save credentials *On-prem and only StoreFront	Yes	Yes	No	Yes	No	No	No	No	No
ADC nFactor authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
ADC Native OTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Biometric authentication (Touch ID, Face ID)	No	No	No	No	Yes	No	No	No	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Single sign-On to Citrix Mobile apps	No	No	No	No	Yes	Yes	No	No	No
Anonymous store access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Feature	Definition
Federated Authentication (SAML/Azure AD)	Enables the FAS server for the user authentication that delegates the Microsoft ADFS server (or other SAML-aware IdP) either by Azure AD or SAML.
ADC (NetScaler®) Full VPN	Builds full VPN tunnel for Gateway.
ADC (NetScaler®) Full VPN	Builds full VPN tunnel for Gateway.
RSA Soft Token	Enables simplified authentication when using RSA Soft Tokens.
Challenge Response SMS (Radius)	Enables a use of challenge response authentication for example the use of SMS pass codes.
User Cert Auth via Gateway (via browser only)	Enables use of users certificates as one factor for authentication with Gateway, which is for browser-based authentication on Windows.

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

Feature	Definition
Smart Card (CAC, PIV, and so on)	Enables use of a standard PC/SC compatible cryptographic smart card for authentication and signing.
Proximity/Contactless Card	Enables users to use Citrix apps or desktops by authenticating with proximity or contactless smart card.
Credential insertion (for example, Fast Connect, Storebrowse)	Enables users to use Citrix apps or desktops by authenticating with a proximity or contactless smart card. Storebrowse is a command-line utility tool available with Citrix Workspace app for Windows. You can use Storebrowse to customize Citrix Workspace app by scripting the Storebrowse utility.
Pass through authentication	Passes user credentials to a web interface site and then to the Citrix Virtual Apps and Desktops servers. This process prevents users to explicitly authenticate at any point during the Citrix app launch process.
Save credentials *On-prem and only StoreFront	Enables save credentials for on-prem and only using Citrix StoreFront.
Gateway native OTP	Gateway supports one-time passwords (OTPs) without having to use a third-party server, by keeping the entire configuration on the NetScaler appliance.
NetScaler nFactor authentication	nFactor authentication enables dynamic authentication flows based on the user profile. Sometimes, these flows can be simple flows to be intuitive to the user. The minimum version of NetScaler required is 12.1.49.x.
Biometric authentication (Touch ID, Face ID)	Enables Biometric authentications such as Touch ID and Face ID.
Single sign-on to Citrix Mobile apps	Enables single sign-on to Citrix Mobile apps.
Anonymous store access	Support access for unauthenticated (anonymous) users.

Input experience

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Keyboard layout sync - client to VDA (Windows VDA)	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Keyboard layout sync - client to VDA (Linux VDA)	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Keyboard layout sync - VDA to client (Windows VDA)	No	No	No	No	No	No	No	No	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Keyboard layout sync - VDA to client (Linux VDA)	No	No	No	No	No	No	No	No	No
Unicode keyboard layout mapping	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
Keyboard input mode - unicode	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
Keyboard input mode - scancode	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No
Server IME	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Generic client IME (CTXIME) for CJK IMEs	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Command line interface	Yes	Yes	No	No	No	No	No	No	No
Keyboard sync setting UI and configurations	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Input mode setting UI and configurations	No	No	Yes	Yes	Yes	No	No	No	No

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

Feature	Windows 2603.20 CR(32bit and 64bit) and Windows Store 2508.10	Windows 2507.1 LTSR	Linux 2601	Mac 2511.1	iOS 26.9.0	Android 26.7.0	HTML5 2603.10	ChromeOS 2603.60	CWA for IWA - Tech Preview
Language bar setting UI and configurations	Yes	Yes	No	Yes	No	No	No	No	No

Feature	Definition
Keyboard layout sync - client to VDA (Windows VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the client device. The keyboard layout on the client device gets automatically set on the Windows VDA.
Keyboard layout sync - client to VDA (Linux VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the client device. The keyboard layout on the client device gets automatically set on the Linux VDA.
Keyboard layout sync - VDA to client (Windows VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the Windows VDA. The keyboard layout on the Windows VDA gets automatically set on the client device.

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

Feature	Definition
Keyboard layout sync - VDA to client (Linux VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the Linux VDA. The keyboard layout on the Linux VDA gets automatically set on the client device.
Unicode keyboard layout mapping	Supports Unicode keyboard layout mapping for Windows VDA with non-Windows Citrix Workspace app.
Keyboard input mode - unicode	Unicode input mode sends the key from the client-side keyboard to VDA and VDA generates the same character in the VDA. Applies client-side keyboard layout.
Keyboard input mode - scancode	Scancode input mode sends the key position from the client-side keyboard to VDA and VDA generates the corresponding character. Applies server-side keyboard layout.
Server IME	Provides service (or VDA) side Input Method Editor (IME) usability and experience.
Generic client IME (CTXIME) for CJK IMEs	Provides enhanced Client IME usability and improved seamless experience for East Asian languages (Chinese, Japanese, Korean).
Command line interface	Users can enable or disable client IME using the command-line interfaces.
Keyboard sync setting UI and configurations	Users can choose different keyboard layout synchronization options using the GUI.
Input mode setting UI and configurations	Users can choose different keyboard input mode options using the GUI.
Language bar setting UI and configurations	Users can choose to show or hide the remote language bar in a VDA app session using the GUI. The language bar displays the preferred input language in a session.
Keyboard layout sync GPO administrative template	Administrators can override the keyboard layout synchronization configurations by deploying the corresponding policies from the Citrix Workspace app Group Policy Object administrative template.

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

Feature	Definition
Keyboard layout sync - client to VDA (Windows VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the client device. The keyboard layout on the client device gets automatically set on the Windows VDA.
Keyboard layout sync - client to VDA (Linux VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the client device. The keyboard layout on the client device gets automatically set on the Linux VDA.
Keyboard layout sync - VDA to client (Windows VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the Windows VDA. The keyboard layout on the Windows VDA gets automatically set on the client device.
Keyboard layout sync - VDA to client (Linux VDA)	Enables users to synchronize active keyboard layouts or switch among preferred keyboard layouts on the Linux VDA. The keyboard layout on the Linux VDA gets automatically set on the client device.
Unicode keyboard layout mapping	Supports Unicode keyboard layout mapping for Windows VDA with non-Windows Citrix Workspace app.
Keyboard input mode - unicode	Unicode input mode sends the key from the client-side keyboard to VDA and VDA generates the same character in the VDA. Applies client-side keyboard layout.
Keyboard input mode - scancode	Scancode input mode sends the key position from the client-side keyboard to VDA and VDA generates the corresponding character. Applies server-side keyboard layout.
Server IME	Provides service (or VDA) side Input Method Editor (IME) usability and experience.
Generic client IME (CTXIME) for CJK IMEs	Provides enhanced Client IME usability and improved seamless experience for East Asian languages (Chinese, Japanese, Korean).
Command line interface	Users can enable or disable client IME using the command-line interfaces.

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

Feature	Definition
Keyboard sync setting UI and configurations	Users can choose different keyboard layout synchronization options using the GUI.
Input mode setting UI and configurations	Users can choose different keyboard input mode options using the GUI.
Language bar setting UI and configurations	Users can choose to show or hide the remote language bar in a VDA app session using the GUI. The language bar displays the preferred input language in a session.
Keyboard layout sync GPO administrative template	Administrators can override the keyboard layout synchronization configurations by deploying the corresponding policies from the Citrix Workspace app Group Policy Object administrative template.

Table indicators

Indicator	Description
1	StoreFront only
2	HDX 3D Pro reverts to JPEG for these Citrix Workspace apps. 3 Mbps is recommended compared to 1.5 Mbps with H.264 Deep Compression.
3	For NSAP VC, the Workspace app for iOS/Android supports, but for ADC/ADM, the support is still pending.
4	User Cert Auth via Gateway (via browser only) method of authentication doesn't support Citrix Workspace app client detection. You can open a virtual app or desktop using Citrix Workspace app only if the ICA file is downloaded.

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

Indicator	Description
5	Citrix Enterprise Browser can be used with Citrix Workspace app LTSR as a compatible component. However, it isn't installed by default. To install Citrix Enterprise Browser, add install switch `InstallEmbeddedBrowser=Y` or `Addlocal` parameter `CitrixEnterpriseBrowser` as part of the command-line installation.
4	User Cert Auth via Gateway (via browser only) method of authentication doesn't support Citrix Workspace app client detection. You can open a virtual app or desktop using Citrix Workspace app only if the ICA file is downloaded.
5	Citrix Enterprise Browser can be used with Citrix Workspace app LTSR as a compatible component. However, it isn't installed by default. To install Citrix Enterprise Browser, add install switch `InstallEmbeddedBrowser=Y` or `Addlocal` parameter `CitrixEnterpriseBrowser` as part of the command-line installation.

> **Note:**
>
> The development, release, and timing of any features or functionality described for our products remains at our sole discretion. The information provided here is for informational purposes only and is not a commitment, promise, or legal obligation to deliver any material, code, or functionality and should not be relied upon in making purchasing decisions or incorporated into any contract. The development, release, and timing of any features or functionality described for our products remains at our sole discretion and are subject to change without notice or consultation.

© 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.