Citrix Workspace-App

Contents

Citrix Workspace-App

April 25, 2024

Info zur Citrix Workspace-App

Citrix Workspace-App bietet sofortigen, sicheren und nahtlosen Zugriff auf alle Ressourcen, die Endbenutzer benötigen, um produktiv zu sein. Die Citrix Workspace-App umfasst Zugriff auf virtuelle Desktops, virtuelle Apps, Web- und SaaS-Apps sowie Features wie eingebettetes Surfen und Single Sign-On (von überall und von jedem Gerät aus).

Citrix Workspace-App ist eine Clientanwendung, die geräteübergreifend in Cloud- und On-Premises-Umgebungen bereitgestellt werden kann. Sie baut auf den Funktionen von Citrix Receiver auf und umfasst Citrix Client-Technologien wie HDX, die Citrix Gateway-Plug-Ins und Secure Private Access.

Die Client-App ist für die Ausführung auf allen Client-Betriebssystemen wie Windows, macOS, Linux, iOS und Android optimiert. Sie kann auch über einen Browser aufgerufen werden. Weitere Informationen zu den unterstützten Browsern finden Sie unter Workspace Browser Compatibility.

Die Citrix Workspace-App, die auf dem Citrix-Protokoll und HDX (High Definition Experience) basiert, bietet leistungsstarke virtuelle App- und Desktopsitzungen. Sie wurde weiterentwickelt, um eine sichere Anmeldung und sicheres Surfen im Internet, die einfache Verwaltung Ihrer Apps und Desktops, erweiterte Suchfunktionen und vieles mehr zu bieten.

> **Hinweis:**
>
> Die Benutzeroberfläche der App kann variieren und hängt davon ab, ob Ressourcen in der Cloud durch Nutzung der Workspace-Plattform oder On-Premises durch Nutzung der StoreFront-Plattform bereitgestellt werden.

Informationen zu den Features in Citrix Workspace-Apps finden Sie unter Citrix Workspace-App - Featurematrix.

Informationen zu den Unterschieden zwischen LTSR und aktuellen Releases finden Sie unter Lifecycle Milestones for Citrix Workspace app.

Die Citrix Workspace-App ist für die folgenden Betriebssysteme verfügbar:

- Citrix Workspace-App für Android
- Citrix Workspace-App für ChromeOS
- Citrix Workspace-App für HTML5
- Citrix Workspace-App für iOS

- Citrix Workspace-App für Linux
- Citrix Workspace-App für Mac
- Citrix Workspace-App für Windows
- Citrix Workspace-App für Windows (Store)

> **Wichtig**
>
> **Daten, die für Citrix Workspace-App-Updates gesammelt wurden:**
>
> In Bezug auf Geräte, die mit dem Internet verbunden sind, sucht die Citrix Workspace-App möglicherweise ohne weitere Ankündigung nach Updates, die zum Herunterladen und Installieren auf dem Gerät verfügbar sind, und informiert den Benutzer über deren Verfügbarkeit. In diesem Fall werden nur nicht personenbezogene Informationen übertragen, außer in dem Umfang, in dem IP-Adressen in einigen Ländern als personenbezogen angesehen werden können.

Citrix Workspace-App mit dem Global App Configuration Service konfigurieren

Der Global App Configuration Service bietet eine zentrale Schnittstelle zum Konfigurieren der Citrix Workspace-App-Einstellungen für Endbenutzer. Sie können Einstellungen für Cloudstores und On-Premises-Stores über eine einzige Oberfläche konfigurieren. Diese Einstellungen gelten sowohl für verwaltete als auch für nicht verwaltete Geräte (BYOD). Weitere Informationen finden Sie unter Global App Configuration Service.

Sprachunterstützung

Citrix Workspace-Apps sind für die Verwendung in anderen Sprachen als Englisch angepasst. In diesem Abschnitt werden die unterstützten Sprachen für die neuesten Versionen der Citrix Workspace-Apps aufgeführt.

In der folgenden Tabelle sind die Sprachen aufgeführt, die für die Citrix Workspace-App auf verschiedenen Betriebssystemen oder Plattformen unterstützt werden. Ein ☑ bedeutet, dass die App in der jeweiligen Sprache verfügbar ist.

Sprache	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows Store
Englisch	☑	☑	☑	☑	☑	☑	☑	☑
Dänisch	☑			☑				
Niederländisch	☑	☑	☑	☑	☑	☑	☑	☑

Sprache	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows Store
Französisch	☑	☑	☑	☑	☑	☑	☑	☑
Deutsch	☑	☑	☑	☑	☑	☑	☑	☑
Italienisch	☑	☑	☑	☑	☑	☑	☑	☑
Japanisch	☑	☑	☑	☑	☑	☑	☑	☑
Koreanisch	☑	☑	☑	☑	☑		☑	☑
Portugiesisch (Brasilien)	☑	☑	☑	☑	☑	☑	☑	☑
Russisch		☑	☑		☑		☑	☑
Vereinfachtes Chinesisch	☑	☑	☑	☑	☑	☑	☑	☑
Spanisch	☑	☑	☑	☑	☑	☑	☑	☑
Schwedisch	☑			☑				
Traditionelles Chinesisch		☑	☑				☑	☑

Featureflag

In diesem Artikel werden die Verwaltung von Featureflags und die verschiedenen Citrix Workspace-Apps beschrieben, die Featureflags unterstützen.

Featureflags verwalten

Wenn ein Problem mit der Citrix Workspace-App in der Produktion auftritt, können wir ein betroffenes Feature dynamisch in der Citrix Workspace-App deaktivieren, auch nachdem das Feature bereitgestellt wurde. Hierfür verwenden wir Featureflags und den Drittanbieterdienst "LaunchDarkly". Sie müssen das Aktivieren des Datenverkehrs über LaunchDarkly nur dann konfigurieren, wenn Sie den ausgehenden Datenverkehr durch eine Firewall oder einen Proxyserver blockieren. In diesem Fall aktivieren Sie den Datenverkehr über LaunchDarkly Ihren Richtlinienanforderungen entsprechend über bestimmte URLs oder IP-Adressen.

In der folgenden Tabelle werden die verschiedenen Apps aufgeführt, die Featureflags unterstützen, und die Releaseversionen, in denen Featureflags in diesen Apps eingeführt wurden.

App	Unterstützung für Featureflags	Version	Dokumentation
Citrix Workspace-App für Android	Ja	10.7.5	Verwaltung von Featureflags für die Citrix Workspace-App für Android
Citrix Workspace-App für ChromeOS	Ja	1908	Verwaltung von Featureflags für die Citrix Workspace-App für ChromeOS
Citrix Workspace-App für HTML5	Ja	1908	Verwaltung von Featureflags für die Citrix Workspace-App für HTML5
Citrix Workspace-App für iOS	Ja	10.4.10	Verwaltung von Featureflags für die Citrix Workspace-App für iOS
Citrix Workspace-App für Linux	Ja	2109	Verwaltung von Featureflags für die Citrix Workspace-App für Linux
Citrix Workspace-App für Mac	Ja	2010	Verwaltung von Featureflags für die Citrix Workspace-App für Mac
Citrix Workspace-App für Windows	Ja	2012	Verwaltung von Featureflags für die Citrix Workspace-App für Windows

Wichtiges Update zu Citrix Receiver

Im August 2018 wurde Citrix Receiver durch die Citrix Workspace-App ersetzt. Sie können immer noch ältere Versionen von Citrix Receiver herunterladen; neue Funktionen und Verbesserungen werden jedoch nur für die Citrix Workspace-App veröffentlicht.

Die Citrix Workspace-App ist ein neuer Client von Citrix, der ähnlich wie Citrix Receiver funktioniert und vollständig abwärtskompatibel mit der Citrix-Infrastruktur Ihres Unternehmens ist. Die Citrix Workspace-App bietet alle Funktionen von Citrix Receiver und neue Funktionen, die auf der Citrix-Bereitstellung Ihres Unternehmens basieren.

Die Citrix Workspace-App basiert auf der Citrix Receiver-Technologie und ist vollständig abwärtskompatibel mit allen Citrix-Lösungen.

Weitere Informationen finden Sie auf der FAQ-Seite zur Workspace-App.

Citrix Workspace-Weberweiterungen

April 25, 2024

Mit der Citrix Workspace-Weberweiterung können Sie Ihre Workspace-Apps überall ohne eine `.ica`-Datei starten, was Ihr Benutzererlebnis sicherer und zuverlässiger macht. Wenn Sie Ihre Apps mit der Browsererweiterung öffnen, haben Sie alle Apps und Desktops an einem einzigen Ort, sodass Sie Ihre Arbeit einfach verfolgen und einen aufgeräumten Desktop genießen können. Die Citrix Workspace-Weberweiterung bietet außerdem Schutz vor Screenshot-Apps und nahtlose Servicekontinuität.

Citrix Workspace-Weberweiterungen installieren

Mit den folgenden Schritten installieren Sie die Citrix Workspace-Weberweiterung:

1. Navigieren Sie zum Webstore Ihres bevorzugten Browsers:
   - Chrome Web Store
   - Microsoft Edge Add-Ons
   - Mac App Store
2. Fügen Sie die Citrix Workspace-Weberweiterung über den App-Store Ihres bevorzugten Browsers hinzu und bestätigen Sie die Installation.
3. Bestätigen Sie ggf. in der Popupmeldung, dass Sie die Weberweiterung hinzufügen möchten.
4. (Optional) Wählen Sie das Puzzleteilsymbol oben rechts im Browser aus, um den Browser für schnellen Zugriff anzuheften.
5. Wählen Sie **Erweiterung hinzufügen** aus.
6. Wählen Sie das Reißzweckensymbol, um die Erweiterung anzuheften.

Die Citrix Workspace-Weberweiterung ist jetzt installiert.

Weitere Informationen zur Citrix Workspace-Weberweiterung finden Sie im Blog zur Citrix Workspace-Weberweiterung.

SaaS-Apps in Ihrer Citrix Workspace-Instanz öffnen

Wenn die Citrix Workspace-Weberweiterung auf Ihrer Workspace-Instanz nicht bereits aktiviert ist, gehen Sie wie folgt vor:

1. Wählen Sie im Workspace-Fenster Ihr Kontoprofil aus.
2. Wählen Sie im Profilmenü die Option **Erweitert** aus.
3. Wählen Sie im Fenster **Startpräferenz für Apps und Desktops** die Option **Webbrowser verwenden** aus.
4. Bestätigen Sie im Popupfenster **Citrix Workspace Launcher öffnen**.

Ihre SaaS-Apps werden jetzt im Fenster Ihrer Citrix Workspace-App geöffnet.

Citrix Workspace-App – Featurematrix

Die Citrix Workspace-App bietet vielfältige Features für verschiedene Plattformen bzw. Betriebssysteme. Dieser Featurematrix können Sie die Verfügbarkeit der Features auf verschiedenen Plattformen entnehmen.

Auf die Citrix Workspace-Weberweiterung kann von jedem Computer aus mit einem unterstützten Webbrowser und einer Internetverbindung zugegriffen werden. Um alle Features und Funktionen der Citrix Workspace-Weberweiterung nutzen zu können, werden die folgenden Browsertypen unterstützt:

Browsername	Version
Google Chrome	Aktuelle Version
Microsoft Edge	Aktuelle Version
Apple Safari	Aktuelle Version

App Protection

May 31, 2024

App Protection ist ein Feature für die Citrix Workspace-App und bietet erweiterte Sicherheit bei der Verwendung von in Citrix Virtual Apps and Desktops veröffentlichten Ressourcen. App Protection wird für die On-Premises-Version von Citrix Virtual Apps and Desktops und für Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) mit StoreFront und Workspace unterstützt. App Protection wird also in allen Cloud-Umgebungen, on-premises Umgebungen und Hybridumgebungen unterstützt. App Protection wird auch unterstützt, wenn Sie über ADC Gateway eine Verbindung zu StoreFront oder Workspace herstellen.

Zwei Richtlinien bieten Schutz vor Keylogging und Bildschirmerfassung für Citrix HDX-Sitzungen. Bei Verwendung mit der Citrix Workspace-App ab 2203.1 LTSR für Windows, der Citrix Workspace-App ab 2001 für Mac bzw. der Citrix Workspace-App ab 2108 für Linux können die Richtlinien zum Schutz von Daten vor Keylogging und Screen Scraping beitragen.

Bei Aktivieren von Keyloggingschutz:

- Der Keylogger sieht verschlüsselte Tastenanschläge.
- Das Feature ist nur aktiv, wenn ein geschütztes Fenster im Fokus ist.

Bei aktiviertem Schutz vor Bildschirmerfassung:

- Unter Windows und macOS ist bei Screenshots nur der Inhalt des geschützten Fensters leer. Das Feature ist aktiv, wenn ein geschütztes Fenster nicht minimiert ist. Unter Linux ist der gesamte Screenshot leer. Dieses Feature ist aktiv, unabhängig davon, ob ein geschütztes Fenster minimiert ist.
- Wenn Sie unter Windows mit der Schaltfläche **Bildschirm drucken** Screenshots erstellen, werden die Daten nicht in die Zwischenablage kopiert. Um Screenshots mit der Schaltfläche **Bildschirm drucken** zu erstellen, minimieren Sie alle geschützten Apps.

Sie können die Richtlinien über PowerShell oder Web Studio konfigurieren. Weitere Informationen finden Sie unter App Protection für virtuelle Apps und Desktops konfigurieren.

Stellen Sie nach dem Erwerb des Features sicher, dass Sie die Lizenz für App Protection aktivieren.

> **Haftungsausschluss:**
>
> Die App Protection-Richtlinien filtern den Zugriff auf erforderliche Funktionen des zugrunde liegenden Betriebssystems (spezifische API-Aufrufe für die Bildschirmerfassung oder das Aufzeichnen von Tastenanschlägen). Damit schützen sie auch vor benutzerdefinierten und speziell entwickelten Hackertools. Die Weiterentwicklung von Betriebssystemen kann jedoch immer wieder zu neuen Einfallstoren für das Keylogging oder die Bildschirmerfassung führen. Darum ist kein hundertprozentiger Schutz möglich, auch wenn wir diese Schwachstellen kontinuierlich identifizieren und korrigieren.
>
> Die Citrix App Protection-Richtlinien arbeiten effektiv mit zugrundeliegenden Betriebssystemkomponenten, einschließlich ICA-Dateien. Citrix kann keinen Support leisten, wenn

> vorsätzliche Manipulationen oder Änderungen der zugrundeliegenden Komponenten festgestellt werden, um die Integrität der angewandten Richtlinien zu gewährleisten.

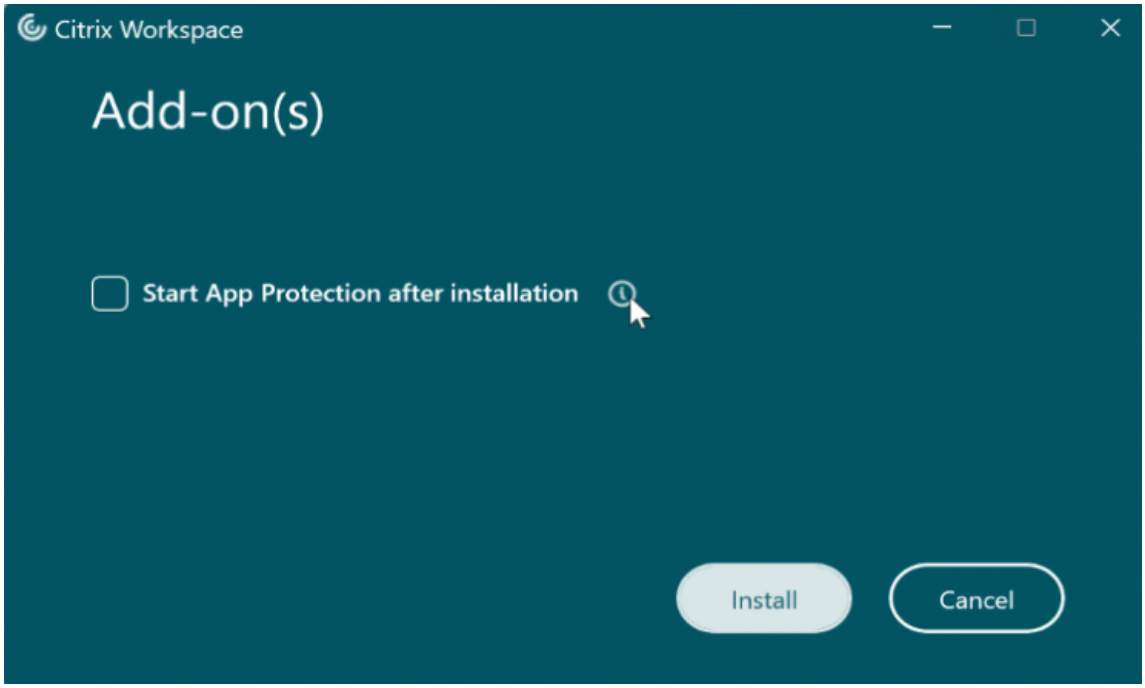
Prüfen Sie, ob App Protection installiert ist

Citrix Workspace-App für Windows

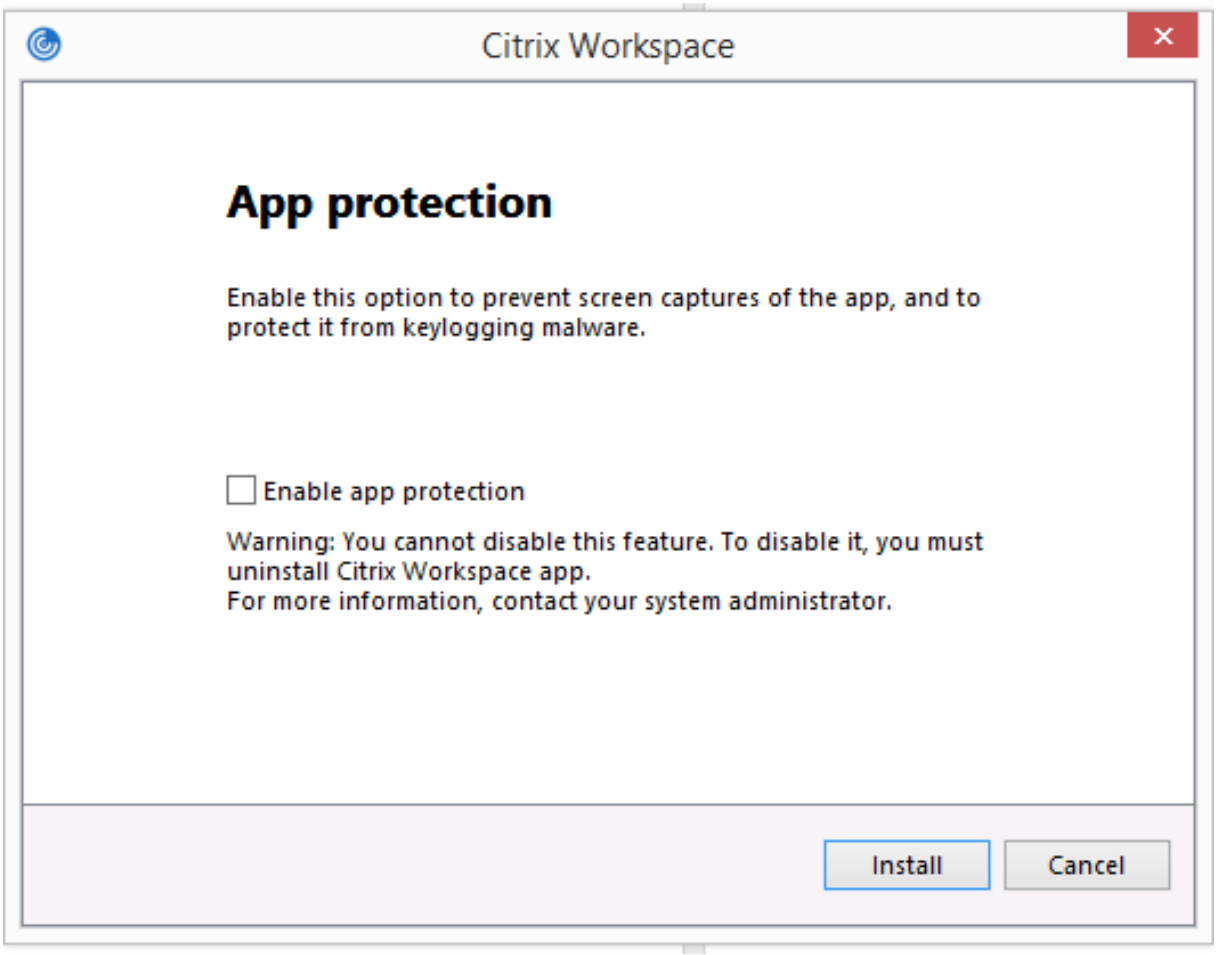
Ab Version 2212 der Citrix Workspace-App ist App Protection standardmäßig installiert. Die Komponente kann sich jedoch im aktiven oder inaktiven Zustand befinden, je nachdem, ob der Benutzer das Kontrollkästchen **App Protection nach der Installation starten** aktiviert hat.

- Für Citrix Workspace-App-Versionen vor 2311:

- Ab Version 2311 der Citrix Workspace-App:



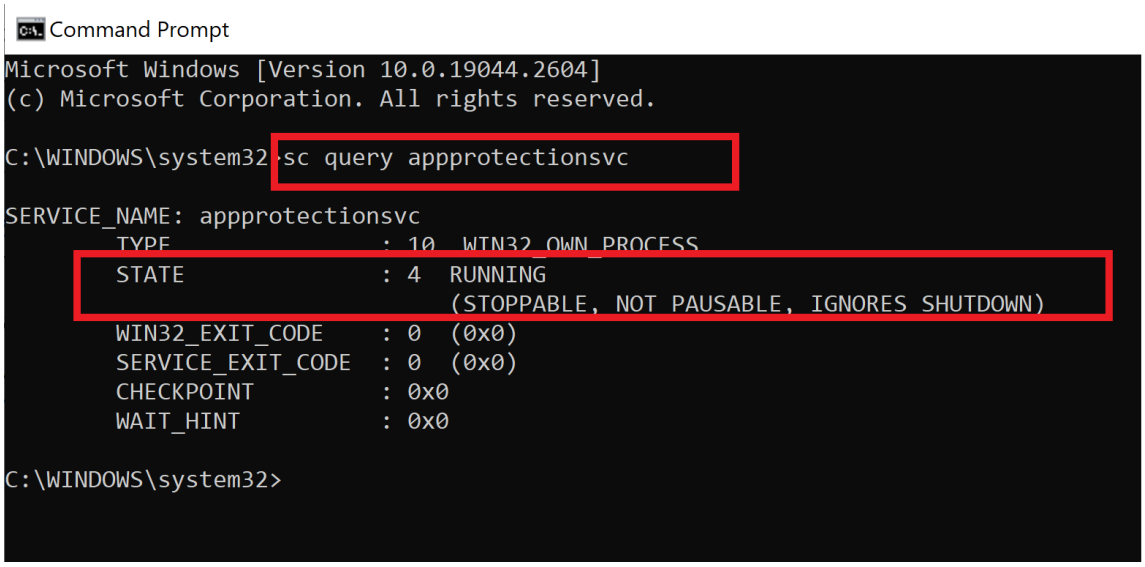
Bei älteren Versionen der Citrix Workspace-App (vor Version 2212) wird App Protection nur dann installiert und aktiviert, wenn Sie bei der Installation der Citrix Workspace-App das Kontrollkästchen **App Protection aktivieren** wählen.



App Protection kann im Status **BEENDET** oder **WIRD AUSGEFÜHRT** vorliegen.
Führen Sie einen der folgenden Schritte aus, um den Status des Dienstes zu überprüfen:

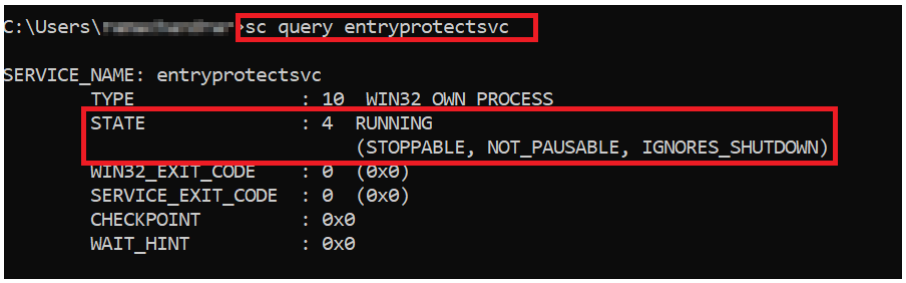
- Ab Version 2206 der Citrix Workspace-App führen Sie folgenden Befehl aus:

```
sc query appprotectionsvc
<!--NeedCopy-->
```

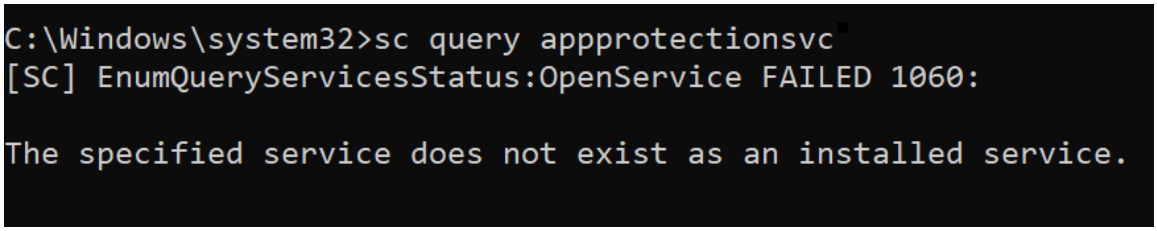



- Vor Version 2206 der Citrix Workspace-App führen Sie folgenden Befehl aus:

```
sc query entryprotectsvc
<!--NeedCopy-->
```



> **Hinweis:**
>
> Wenn Sie bei der Installation der Citrix Workspace-App vor Version 2212 das Kontrollkästchen **App Protection aktivieren** nicht aktivieren und dann den zuvor genannten Befehl zur Statusprüfung ausführen, wird folgende Fehlermeldung angezeigt:



Verhalten von App Protection in unterschiedlichen Umgebungen

Das Verhalten von App Protection hängt vom Zugriff auf die mit App Protection-Richtlinien konfigurierten Ressourcen ab. Zu diesen Ressourcen gehören Virtual Apps and Desktops, interne Web-Apps

und SaaS-Apps. Sie können mit einem unterstützten nativen Client der Citrix Workspace-App oder mit einem Webbrowser auf diese Ressourcen zugreifen. App Protection funktioniert in verschiedenen Umgebungen unterschiedlich:

- **Nicht unterstützte Citrix Receiver oder Citrix Workspace-Apps**: Die mit App Protection-Richtlinien konfigurierten Ressourcen sind nicht verfügbar.
- **Unterstützte Versionen der Citrix Workspace-App**: Die mit App Protection-Richtlinien konfigurierten Ressourcen sind verfügbar und werden ordnungsgemäß gestartet.
- **Hybridstart mit Workspace-Store-URL**: Die mit App Protection-Richtlinien konfigurierten Ressourcen sind immer verfügbar. Informationen zum erfolgreichen Ressourcenstart in einem Webbrowser mit der Workspace Store-URL finden Sie unter App Protection für Hybridstart in Workspace.
- **Hybridstart mit StoreFront-Store-URL**: Die mit App Protection-Richtlinien konfigurierten Ressourcen sind nicht verfügbar, wenn die StoreFront-Anpassung nicht bereitgestellt ist. Informationen zum erfolgreichen Ressourcenstart in einem Webbrowser mit der StoreFront-Store-URL finden Sie unter App Protection für Hybridstart mit StoreFront.

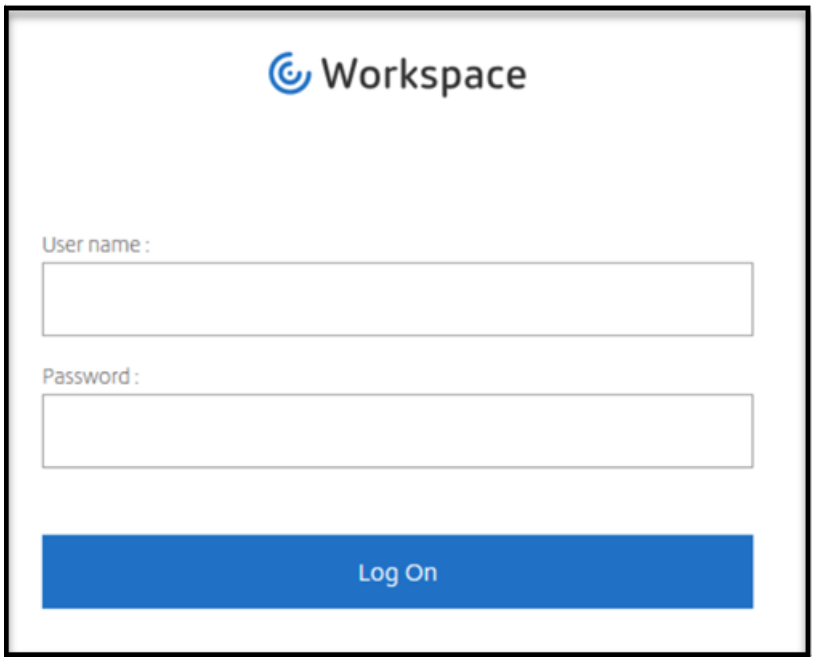
Der Schutz wird unter folgenden Bedingungen angewendet:

- **Screenshotschutz**: Für Citrix Workspace-App für Windows und Citrix Workspace-App für Mac ist das Feature aktiviert, wenn ein geschütztes Fenster auf dem Bildschirm sichtbar ist. Um den Schutz zu deaktivieren, minimieren Sie alle geschützten Fenster. Für die Citrix Workspace-App für Linux ist er aktiviert, wenn ein geschütztes Fenster aktiv ist. Um den Schutz zu deaktivieren, schließen Sie alle geschützten Fenster.
- **Keyloggingschutz**: aktiviert, wenn ein geschütztes Fenster im Fokus steht. Um den Schutz zu deaktivieren, verschieben Sie den Fokus auf ein anderes Fenster.

Was wird durch App Protection geschützt?

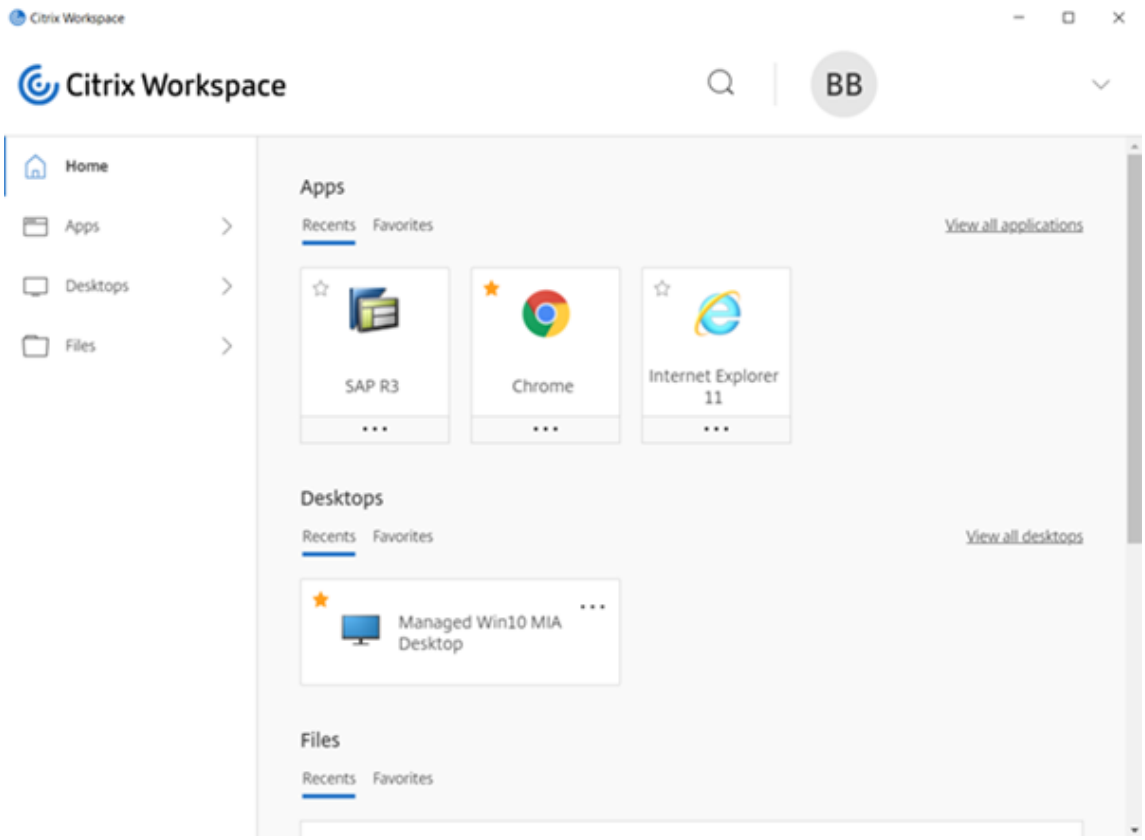
Folgende Citrix-Fenster sind durch App Protection geschützt:

- Citrix-Anmeldefenster

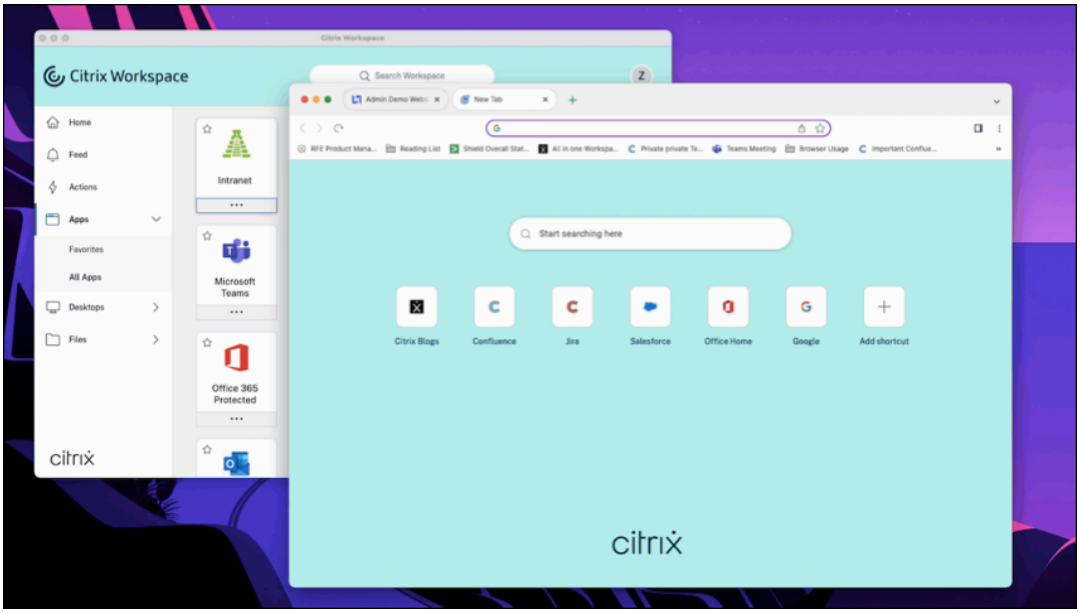


- HDX-Sitzungsfenster der Citrix Workspace-App (Beispiel: verwalteter Desktop)

- Fenster des Self-Service-Store



- Web- und SaaS-Apps
  - Citrix Workspace-App für Windows und Citrix Workspace-App für Mac − Web- und SaaS-Apps werden im Citrix Enterprise Browser geöffnet. Wenn die Apps so konfiguriert sind, dass die App Protection-Richtlinien über Citrix Secure Private Access angewendet werden, wird App Protection pro Registerkarte angewendet.



  - Citrix Workspace-App für Linux - Citrix Enterprise Browser wird nicht unterstützt.

Was wird durch App Protection nicht geschützt?

- Die folgenden Elemente unter dem Symbol der Citrix Workspace-App in der Navigationsleiste:
  - Connection Center
  - Alle Links unter "Erweiterte Einstellungen"
  - Personalisieren
  - Nach Updates suchen
  - Abmelden
- Wenn Sie einen virtuellen Desktop mit Screenshotschutz schützen, können Benutzer weiterhin Screenshots von Apps innerhalb des virtuellen Desktops teilen. Von Apps außerhalb des virtuellen Desktops können jedoch keine Screenshots erstellt bzw. der virtuelle Desktop kann nicht aufgezeichnet werden.

Einschränkungen

Die folgenden Einschränkungen sind designbedingt:

- Virtuelle Apps und Desktops, für die App Protection aktiviert ist, können nicht gestartet werden, wenn sie innerhalb von RDP-Sitzungen aufgerufen werden.
- In der RDP-Sitzung wird App Protection in den Web- und SaaS-Anwendungen, die mit dem Citrix Enterprise Browser geöffnet wurden, nicht unterstützt.
- App Protection wird in Double-Hop-Szenarien und Multiple-Hop-Szenarien nicht unterstützt.
- App Protection wird nicht unterstützt, wenn Sie eine nicht unterstützte Version der Citrix Workspace-App oder von Citrix Receiver verwenden. In diesem Fall werden Ressourcen verborgen.
- Wenn die App Protection-Features auf virtuelle Apps und Desktops angewendet werden, kann bei der Verwendung von Optimierung die ausgehende Bildschirmübertragung beeinträchtigt werden.
- Die Citrix Workspace-App mit App Protection ist möglicherweise nicht mit anderen Sicherheitslösungen oder Apps kompatibel, die eine ähnliche Technologie verwenden.
- App Protection wird nicht unterstützt, wenn Sie Ressourcen im Citrix Secure Browser oder mit Remote Browser Isolation starten.
- In der Citrix Workspace-App für Linux können Sie keine Anwendungen andocken, wenn App Protection installiert ist.

Kontextbezogenes App Protection

Kontextbezogenes App Protection ermöglicht es, App Protection-Richtlinien flexibel und granular nur auf bestimmte Benutzergruppen anzuwenden –basierend auf Benutzern, ihrem Gerät und der Netzwerkstruktur. Weitere Informationen finden Sie in den folgenden Artikeln:

- Kontextbezogenes App Protection für StoreFront
- Kontextbezogenes App Protection für Workspace

App Protection für Hybridstart

Beim Hybridstart von Citrix Virtual Apps and Desktops melden Sie sich über den Browser (Citrix Workspace für Web) bei der Citrix Workspace-App an und verwenden die Anwendungen über die native Citrix Workspace-App. Der Begriff "hybrid"verweist darauf, dass Benutzer eine Kombination aus Citrix Workspace-App für Web und nativer Citrix Workspace-App verwenden, um eine Verbindung herzustellen und die Ressourcen zu verwenden. App Protection unterstützt den Hybridstart in Workspace und StoreFront. Weitere Informationen finden Sie in den folgenden Artikeln:

- App Protection für Hybridstart in Workspace
- App Protection für Hybridstart mit StoreFront

Systemanforderungen und Kompatibilität

April 29, 2024

Systemanforderungen

Als Voraussetzung müssen Sie die Citrix Workspace-App mit Administratorrechten installiert haben.

Mindestversionen von Citrix Komponenten

- Citrix Workspace-App 2108 für Linux
- Citrix Workspace-App 2203.1 LTSR für Windows
- Citrix Workspace-App 2002 für Windows
- Citrix Workspace-App 2305.1 für Windows (Store)
- Citrix Workspace-App 2001 für Mac
- StoreFront 1912 LTSR
- Delivery Controller 1912

- Gültige Citrix-Lizenzen Weitere Informationen erhalten Sie von Ihrem Citrix Vertriebsmitarbeiter oder Citrix Partner.

> **Hinweis:**
>
> Wenn Benutzer Geräte oder Workspace-App-Versionen verwenden, die App Protection nicht unterstützen, können sie nicht auf die geschützten Ressourcen zugreifen. Zu den geschützten Ressourcen gehören Virtual Apps and Desktops sowie Web- und SaaS-Apps.

Lizenzen

Im folgenden Abschnitt werden die verschiedenen Lizenztypen erläutert, die für App Protection je nach Produkt, Plattform und Anwendungsfall verfügbar sind.

IT-verwaltete VDI Für alle Editionen von IT-verwalteter VDI ist App Protection als Add-On verfügbar. Weitere Informationen finden Sie unter IT-verwaltete VDI.

Citrix DaaS für Hyperscaler

- Azure
- Google
- AWS

Citrix DaaS Navigieren Sie unter Feature Matrix for Citrix DaaS zu **DaaS cloud services > Security and Monitoring > App Protection**.

Citrix Secure Private Access App Protection ist als eigenständige Komponente für Citrix Secure Private Access verfügbar. Weitere Informationen finden Sie unter Service Descriptions for Citrix Services > **Citrix Cloud Services > Citrix Secure Private Access**.

Citrix Universal-Abonnement App Protection ist in den folgenden Services enthalten:

- Citrix Universal Premium
- Citrix Universal Premium Plus

Es ist als Add-On mit den folgenden Editionen verfügbar:

- Citrix Universal Advanced
- Citrix Universal Advanced Plus

Weitere Informationen finden Sie in diesem Artikel.

Betriebssystemplattformen

Die App Protection-Richtlinien werden auf dem Endpunkt installiert und ausgeführt, von dem die Verbindung *ausgeht* und nicht auf dem VDA, an dem die Verbindung *eingeht*. Daher ist nur die Betriebssystemversion des Endpunkts von Bedeutung. App Protection kann eine Verbindung zu VDAs unter allen unterstützten Betriebssystemen (siehe Systemanforderungen für Citrix Virtual Apps and Desktops) herstellen.

App Protection wird auf Endpunkten mit folgenden Betriebssystemen unterstützt:

- **Windows:**
  - Windows 11 (64-Bit-Edition)
  - Windows 10 (32-Bit- und 64-Bit-Edition)

    > **Hinweis:**
    >
    > App Protection wird auf Geräten mit der Arm64-Edition des Windows-Betriebssystems nicht unterstützt.

- **macOS:**
  - High Sierra (10.13) und höher
- **Linux:**
  - 64-Bit-Ubuntu 22.04
  - 64 Bit RHEL 9
  - ARM64 Raspberry Pi OS (basierend auf Debian 11 (Bullseye))

> **Hinweis:**
>
> Die Citrix Workspace-App für Linux erfordert Gnome Display Manager sowie ein unterstütztes Betriebssystem für App Protection.

Kompatibilitätsmatrix

Kompatibilitätsmatrix für Citrix Cloud-basierte Produkte

Mit Citrix Cloud-basierten Produkten kompatible App Protection-Features:

Feature	Citrix Cloud	Citrix Cloud Japan
Keyloggingschutz und Screenshotschutz für virtuelle Apps und Desktops	Ja	Ja
Keyloggingschutz und Screenshotschutz für Web- oder SaaS-Apps	Ja	Nein
DLL-Einschleusungsschutz für Windows	Ja	Ja, über Gruppenrichtlinienobjekt (GPO)
Positivliste für DLL-Einschleusungsschutz	Ja	Ja, über GPO
Global App Configuration Service (GACS)	Ja	Nein
Authentifizierungs- bzw. Self-Service-Plug-in-Bildschirmschutz für Linux	Ja	Ja über AuthManConfig.xml
Authentifizierungs- bzw. Self-Service-Plug-in-Bildschirmschutz für Mac	Ja, über GACS	Ja, über GACS
Authentifizierungs- bzw. Self-Service-Plug-in-Bildschirmschutz für Windows	Ja	Ja, über GPO
CAS App Protection – ScreenShot-Ereignisse	Ja	Nein
Kontextbezogenes App Protection	Ja	Ja, auf Benutzerbasis
Erkennung von Richtlinienmanipulationen	Ja	Ja
App Protection Posture Check	Ja	Ja
Positivliste/Filter lokale App für Windows	Ja	Ja, über GPO
Lokale App Protection – Windows	Ja	Ja, über GPO

App Protection-Funktionen

June 19, 2024

In diesem Artikel werden die App Protection-Funktionen beschrieben, die von der Citrix Workspace-App für Windows, der Citrix Workspace-App für Linux und der Citrix Workspace-App für Mac unterstützt werden.

Keyloggingschutz

Bei Verschlüsselung verschlüsseln die App Protection-Funktionen zum Keyloggingschutz den Text, den Benutzer auf der physischen bzw. Bildschirmtastatur eingeben. Der Keyloggingschutz verschlüsselt den Text, bevor ein Keylogging-Tool von der Kernel- oder Betriebssystemebene aus darauf zugreifen kann. Ein auf dem Client-Endpunkt installierter Keylogger, der die Daten vom Betriebssystem oder Treiber liest, erfasst Hash-Text anstelle der vom Benutzer eingegebenen Tastatureingaben. App Protection-Richtlinien sind nicht nur für veröffentlichte Anwendungen und Desktops aktiv, sondern auch für Dialogfelder zur Citrix Workspace-Authentifizierung. Ihre Citrix Workspace-App ist geschützt, sobald Ihre Benutzer das erste Dialogfeld zur Authentifizierung öffnen. App Protection verschlüsselt Tastatureingaben und gibt nicht entschlüsselbaren Text an Keylogger zurück.

Administratoren können den Keyloggingschutz für folgende Ressourcentypen aktivieren:

- Virtual Apps and Desktops
- Interne Web- und SaaS-Apps
- Authentifizierungsbildschirme
- Bildschirme des Self-Service-Plug-Ins (SSP)

Screenshotschutz

Der Screenshotschutz verhindert, dass Apps in einer Sitzung mit virtueller App oder virtuellem Desktop den Bildschirm aufnehmen oder aufzeichnen können. Die Software zur Screenshotaufnahme kann keine Inhalte innerhalb des Aufnahmebereichs erkennen. Der von der App ausgewählte Bereich ist ausgegraut, oder die App erfasst nichts anstelle des Bildschirmausschnitts, der kopiert werden soll. Der Screenshotschutz gilt für
Snip & Sketch, das Snipping-Tool und den Tastaturbefehl **Umschalt+Strg+Druck** unter Windows.

Ein weiterer Anwendungsfall für den Screenshotschutz ist die verhinderte Weitergabe vertraulicher Daten in virtuellen Besprechungs- oder Webkonferenzanwendungen wie GoToMeeting, Microsoft Teams oder Zoom. App Protection verhindert eine unbeabsichtigte Freigabe, indem in Webkonferenzen bei geschützten Apps ein leerer Bildschirm angezeigt wird. Dieses Feature sorgt dafür,

dass vertrauliche Daten nicht versehentlich aus dem Unternehmen gelangen. Es kann in regulierten Branchen zur Einhaltung der Vorschriften beitragen, da die Absicht bei der Offenlegung einer Datenschutzverletzung nicht berücksichtigt wird.

Administratoren können wählen, ob der Screenshotschutz für die folgenden Ressourcentypen aktiviert werden soll:

- Virtual Apps and Desktops
- Interne Web- und SaaS-Apps
- Authentifizierungsbildschirme
- Bildschirme des Self-Service-Plug-Ins (SSP)

> **Hinweis:**
>
> Wenn Sie zwei virtuelle Desktops gestartet haben und auf einem der virtuellen Desktops die Screenshotschutzfunktion aktiviert ist und auf dem anderen virtuellen Desktop nicht, dann gilt die Screenshotschutzfunktion für beide virtuellen Desktops. Sie können von keinem der virtuellen Desktops Screenshots erstellen.
>
> Falls Sie den virtuellen Desktop, für den der Screenshotschutz aktiviert ist, minimiert haben, gilt die Screenshotschutzfunktion weiterhin für den virtuellen Desktop, bei dem die Screenshotschutzfunktion nicht aktiviert ist.

Erkennung und Benachrichtigung bei Screenshot

In der Citrix Workspace-App können Sie eine Benachrichtigung anzeigen, wenn versucht wird, einen Screenshot einer geschützten Ressource zu erstellen. Weitere Informationen zu den von App Protection geschützten Ressourcen finden Sie unter Was wird durch App Protection geschützt?

Die Benachrichtigung wird in folgenden Fällen angezeigt:

- Versuch der Erstellung eines Screenshots oder Videos über ein Screenshot-Tool
- Versuch der Erstellung eines Screenshots über die Taste “Druck/S-Abf”

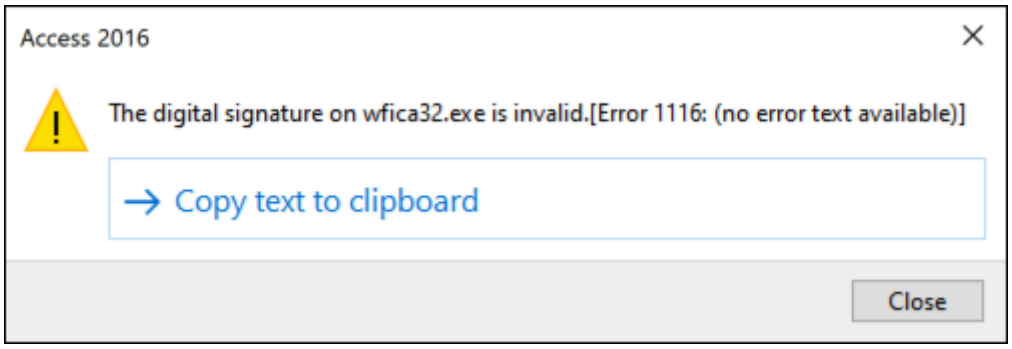
> **Hinweis:**
>
> - Die Benachrichtigung wird nur einmal pro ausgeführter Instanz des Screenshot-Tools angezeigt. Die Benachrichtigung wird erneut angezeigt, wenn Sie das Tool neu starten und versuchen, den Bildschirm aufzuzeichnen.
> - In der Citrix Workspace-App für Windows 2212 und höher sind Anmeldefenster und Fenster des Self-Service-Store standardmäßig nicht geschützt.

DLL-Einschleusungsschutz

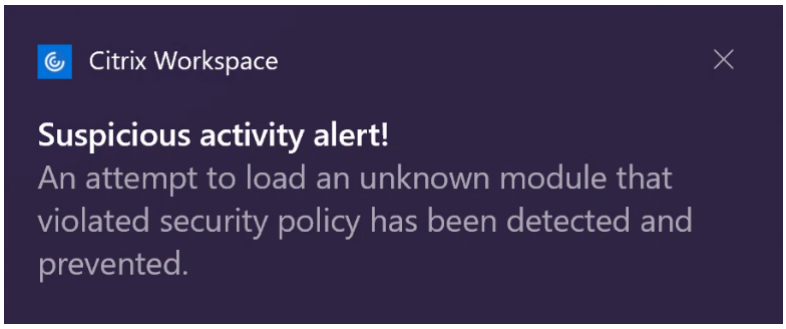
Der DLL-Einschleusungsschutz schützt die Citrix Workspace-App vor bestimmten nicht autorisierten Dynamic-Link-Bibliotheken (DLL) und nicht vertrauenswürdigen Modulen. Wenn ein solches nicht vertrauenswürdiges Modul eingeschleust wird, erkennt die Citrix Workspace-App den Eingriff und stoppt das Laden des Moduls. Wenn vor dem Start der Sitzung eine nicht vertrauenswürdige oder bösartige DLL erkannt wird, blockiert App Protection den Sitzungsstart und zeigt eine Fehlermeldung an. Beim Schließen der Fehlermeldung wird die virtuelle App- und Desktop-Sitzung beendet.

Dieses Feature gilt für alle geschützten virtuellen Apps und Desktops sowie für den Authentifizierungsbildschirm der Citrix Workspace-App (On-Premises-Bereitstellung/StoreFront).

Mit dieser Verbesserung wird die Sitzung sofort beendet, wenn bestimmte nicht vertrauenswürdige oder schädliche DLLs in der geschützten Komponente vorhanden sind.



Es wird jetzt eine Benachrichtigung angezeigt, wenn eine nicht vertrauenswürdige oder schädliche DLL blockiert wird. Beim Schließen der Meldung wird die virtuelle App- und Desktop-Sitzung beendet.



Hinweis: Diese Funktion filtert den Zugriff auf erforderliche Funktionen des zugrunde liegenden Betriebssystems (spezifische API-Aufrufe zum Laden von DLLs). Damit schützt es sogar vor bestimmten benutzerdefinierten und speziell entwickelten Hackertools. Die Weiterentwicklung von Betriebssystemen öffnet jedoch immer wieder neue Einfallstore für das Laden von DLLs. Darum ist kein hundertprozentiger Schutz möglich, auch wenn wir diese Schwachstellen kontinuierlich identifizieren und korrigieren.

Dieses Feature unterstützt die Citrix Workspace-App für Windows ab Version 2206.

> **Hinweis:**
>
> Bisher wurden der Screenshotschutz und der Keyloggingschutz für Citrix Authentifizierung und Citrix Workspace-App-Bildschirme standardmäßig erzwungen. Ab Release 2212 sind diese Funktionen standardmäßig deaktiviert und müssen über das Gruppenrichtlinienobjekt konfiguriert werden. Informationen über die GPO-Konfiguration finden Sie unter Verbesserung der Konfiguration von App Protection.

Kompatibilität mit HDX-Optimierung für Microsoft Teams

Optimiertes Microsoft Teams unterstützt die Bildschirmfreigabe nur, wenn die Citrix Workspace-App mit aktiviertem App Protection im Desktop Viewer-Modus ist. Wenn Sie in Microsoft Teams auf **Inhalt freigeben** zeigt die Bildschirmauswahl folgende Optionen an:

- Option **Fenster** zum Freigeben geöffneter Apps: Diese Option wird nur angezeigt, wenn die VDA-Version 2109 oder höher ist.
- **Desktop**-Option zum Freigeben der Inhalte auf Ihrem VDA-Desktop: Diese Option wird nur für die folgenden Versionen der Citrix Workspace-App angezeigt:
  - Citrix Workspace-App für Linux, Version 2311 oder später
  - Citrix Workspace-App für Mac Version 2308 oder später
  - Citrix Workspace-App für Windows Version 2309 oder später

> **Hinweis:**
>
> Für die Citrix Workspace-App für Linux ist die Option zur Desktopfreigabe standardmäßig deaktiviert. Um sie zu aktivieren, fügen Sie Ihrer *config.json*-Datei den Parameter `UseGbufferScreenSharing` wie folgt hinzu:

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

      "UseGbufferScreenSharing":1
 }

<!--NeedCopy-->
```

Optimiertes Microsoft Teams mit aktivierter App Protection unterstützt auch das virtuelle Citrix Anzeigelayout zur separaten Freigabe jedes virtuellen Bildschirms.

> **Einschränkung:**
>
> - Optimiertes Microsoft Teams mit App Protection unterstützt keine Bildschirmfreigabe auf veröffentlichten Desktops mit lokalem App-Zugriff (LAA).

- Am Client (z. B. per Browserinhaltsumleitung) angezeigte Inhalte können nicht erfasst oder freigegeben werden. Wenn Sie versuchen, einen Screenshot zu erstellen, wird dieser schwarz angezeigt.

Hinweis:

Dieses Feature ist für die Citrix Workspace-App für Linux als Technical Preview verfügbar.

Lokales App Protection (Preview)

App Protection bietet erhöhte Sicherheit zum Schutz der Kunden vor Keyloggern und versehentlicher oder böswilliger Screenshoterstellung auf Endpunkten. Derzeit wird App Protection nur für Workspace-Ressourcen angeboten. Mit diesem Feature werden die App Protection-Funktionen auf lokale Apps auf Endpunkten erweitert. Ab Citrix Workspace-App 2210 für Windows kann App Protection auf lokale Apps auf Windows-Geräten angewendet werden.

Registrieren Sie sich mit dem Podio-Formular für die Vorschau dieses Features.

Erkennung von Richtlinienmanipulationen

Das Feature zur Erkennung von Richtlinienmanipulationen verhindert den Benutzerzugriff auf eine virtuelle App- oder Desktopsitzung, wenn die Richtlinien zu Screenshotschutz und Keyloggingschutz in App Protection manipuliert wurden. Wenn eine Richtlinienmanipulation festgestellt wurde, wird die virtuelle App- oder Desktopsitzung beendet.

Hinweis:

Das Feature zur Erkennung von Richtlinienmanipulationen wird ab einer zukünftigen Version standardmäßig aktiviert sein.

Informationen zum Konfigurieren der Erkennung von Richtlinienmanipulationen finden Sie unter Erkennung von Richtlinienmanipulationen konfigurieren.

Posture Check

Aktivieren Sie App Protection Posture Check, um den Start virtueller Apps und Desktops zu erkennen und zu blockieren, wenn die verwendeten App Protection-Richtlinien aus einer Citrix Workspace-Appversion stammen, die die Erkennung von Richtlinienmanipulationen nicht unterstützt.

Hinweis:

> Wenn Posture Check aktiviert ist und Sie die Version der Citrix Workspace-App verwenden, die Posture Check nicht unterstützt, werden Sitzungen mit App Protection-Richtlinien beendet.

Informationen zur Konfiguration von Posture Check finden Sie unter Posture Check konfigurieren.

> **Einschränkung:**
>
> Posture Check funktioniert sporadisch nicht, wenn Sie Windows Workstation-VDAs verwenden, die auf Microsoft Azure mit VDA 2308 gehostet werden. Diese Einschränkung wurde in VDA-Version 2311 und höher behoben.

App Protection und Double-Hop-Szenario

App Protection-Features werden in Double-Hop-Szenarien nicht unterstützt. Double Hop bezieht sich auf eine Citrix Virtual Apps- oder Virtual Desktops-Sitzung, die innerhalb einer Citrix Virtual Desktops-Sitzung ausgeführt wird. Sie konnten virtuelle Apps und Desktops mit aktivierten App Protection-Richtlinien in einem Double-Hop-Szenario starten, die App Protection-Funktionen wurden jedoch nicht angewendet.

Ab Citrix Workspace-App für Windows Version 2309 gestattet eine neue Windows-Gruppenrichtlinie das Unterbinden des Startens virtueller Apps und Desktops mit aktivierten App Protection-Richtlinien in einem Double-Hop-Szenario. Weitere Informationen zur Aktivierung der Einstellung DoubleHop-Start blockieren finden Sie unter **Einstellung "DoubleHop-Start blockieren"aktivieren**.

Citrix Analytics Service für App Protection

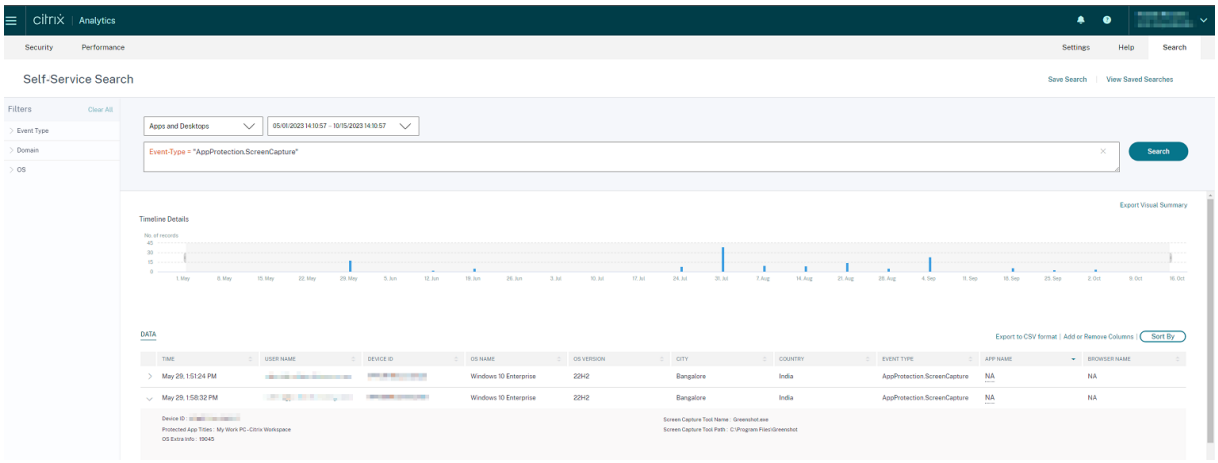
Wenn Sie Citrix Virtual Apps and Desktops verwenden, werden Benutzerereignisse generiert, die den Aktivitäten und Aktionen der Benutzer entsprechen. Citrix Analytics für Sicherheit verfügt über ein Feature namens **Self-Service-Suche**, die diese Benutzerereignisse aufzeichnet und Ihnen Einblicke in sie bietet. Mithilfe der **Self-Service-Suche** können Sie diese Benutzerereignisse finden, filtern und untersuchen, sodass Sie nachvollziehen können, welches Benutzerereignis stattgefunden hat, und je nach Schweregrad des Ereignisses Maßnahmen ergreifen. Weitere Informationen zur **Self-Service-Suche** finden Sie unter Self-Service-Suche.

Die **Self-Service-Suche für Virtual Apps and Desktops** hat den Ereignistyp `AppProtection.ScreenCapture`, mit dem Sie feststellen können, ob versucht wird, Screenshots der virtuellen Apps oder Desktops zu erstellen, für die App Protection-Richtlinien aktiviert sind. Weitere Informationen zur Suche nach einem Benutzerereignis finden Sie unter Suchabfrage zum Filtern von Ereignissen angeben.

Dieser Service bietet die folgenden Informationen:

- Geräte-ID

- Geschützte App-Titel
- Zusätzliche Informationen zum Betriebssystem
- Name des Screenshot-Tools
- Pfad zum Screenshot-Tool



Positivliste für Screenshots

Wenn für die Citrix Workspace-App, Virtual Apps and Desktops oder SaaS-Apps die Screenshotschutz-Richtlinie von App Protection aktiviert ist, können für sie keine Screenshots mit beliebigen Screenshot-Tools aufgenommen werden.

Ab der Version 2402 der Citrix Workspace-App für Windows können Sie jedoch mit dem Feature „Positivliste für Screenshots“eine App zur Positivliste für Screenshots hinzufügen. Dieses Feature ermöglicht die Verwendung der App auf der Positivliste zum Aufnehmen von Screenshots für die Ressource, für die die Screenshotschutz-Richtlinie von App Protection aktiviert ist. Informationen zum Hinzufügen einer App zur Positivliste für Screenshots finden Sie unter Positivliste für Screenshots konfigurieren.

> **Wichtig:**
>
> Es wird nicht empfohlen, eine App, die auf der Positivliste steht, über einen längeren Zeitraum auf Ihrem Gerät auszuführen, da dies die Sicherheit beeinträchtigt. Sie können die Apps auf der Positivliste verwenden, um Ihren Bildschirm vorübergehend in Szenarien wie der Fehlerbehebung zu teilen. Es wird empfohlen, die folgenden Bedingungen einzuhalten:
>
> - Führen Sie die App auf der Positivliste für einen kurzen Zeitraum zusammen mit der Ressource aus, für die das Screenshotschutz-Feature von App Protection aktiviert ist.
> - Beenden Sie die App auf der Positivliste sofort, nachdem die erforderliche Aufgabe abgeschlossen ist.
> - Fügen Sie ein Wasserzeichen hinzu, wenn Sie den Bildschirm teilen und gleichzeitig die

> Ressource verwenden, für die das Screenshotschutz-Feature von App Protection aktiviert ist, um mehr Sicherheit zu gewährleisten.

Ausschlussliste für Prozesse

Wenn Sie einen Prozess oder eine Anwendung auf Ihrem Gerät starten, werden App Protection-DLLs in jeden Prozess eingefügt, sofern App Protection aktiviert ist. Manchmal kann dies dazu führen, dass der Prozess oder die Anwendung aufgrund von Kompatibilitätsproblemen mit der DLL nicht funktioniert.

Ab der Version 2402 der Citrix Workspace-App für Windows können Sie jeden Prozess zur Prozessausschlussliste hinzufügen, um zu verhindern, dass die App Protection-DLL in diesen bestimmten Prozess eingeschleust wird, und um alle Kompatibilitätsprobleme zu beheben, die durch das Vorhandensein von App Protection-DLLs verursacht wurden. Informationen zum Konfigurieren der Prozessausschlussliste finden Sie unter Prozessausschlussliste konfigurieren.

> **Wichtig:**
>
> Es wird nicht empfohlen, Prozesse auszuschließen, da dies die Sicherheit beeinträchtigt. Sie können dieses Feature verwenden, um die Nutzung der Anwendung vorübergehend zu entsperren und ein Support-Ticket für weitere Untersuchungen zu erstellen.

Ausschlussliste für USB-Filtertreiber

Wenn Sie spezielle externe Tastaturen wie Gaming-Tastaturen mit der Citrix Workspace-App verwenden, kann der USB-Filtertreiber von App Protection manchmal Kompatibilitätsprobleme verursachen und Sie daran hindern, die Tastatur zu verwenden.

Ab der Version 2402 der Citrix Workspace-App für Windows können Sie mit dem Feature „Ausschlussliste für USB-Filtertreiber“jedes USB-Gerät ausschließen, das Kompatibilitätsprobleme mit der Citrix Workspace-App hat, indem Sie die Anbieter-ID und die Produkt-ID verwenden. Informationen zum Hinzufügen eines Geräts zur Ausschlussliste für USB-Filtertreiber finden Sie unter Ausschlussliste für USB-Filtertreiber konfigurieren.

> **Hinweis:**
>
> Es wird nicht empfohlen, Geräte dauerhaft auszuschließen. Verwenden Sie dieses Feature, um den Benutzer vorübergehend zu entsperren, damit er das Gerät nutzen und ein Support-Ticket erstellen kann, um das Kompatibilitätsproblem weiter zu untersuchen.

App Protection konfigurieren

April 10, 2024

App Protection erhöht die Sicherheit bei der Verwendung der Citrix Workspace-App. Es verringert das Risiko, dass Clients durch Keylogging und Screenshot-Malware kompromittiert werden. App Protection verhindert das Exfiltrieren vertraulicher Informationen wie Benutzeranmeldeinformationen und sensible Informationen, die auf dem Bildschirm angezeigt werden. Die Funktion verhindert, dass Benutzer und Angreifer Screenshots erstellen und Keylogger verwenden, um vertrauliche Informationen zu lesen und zu nutzen.

In diesem Artikel wird erläutert, wie Sie App Protection in der Citrix Workspace-App auf verschiedenen Plattformen konfigurieren.

App Protection ist in der Citrix Workspace-App für folgende Plattformen verfügbar:

- Citrix Workspace-App für Windows
- Citrix Workspace-App für Linux
- Citrix Workspace-App für Mac

> **Haftungsausschluss**
>
> App Protection-Richtlinien filtern den Zugriff auf erforderliche Funktionen des zugrunde liegenden Betriebssystems. Spezifische API-Aufrufe sind für Screenshots oder das Aufzeichnen von Tastenanschlägen erforderlich. Damit schützen sie auch vor benutzerdefinierten und speziell entwickelten Hackertools. Die Weiterentwicklung von Betriebssystemen kann jedoch immer wieder zu neuen Einfallstoren für das Keylogging oder die Bildschirmerfassung führen. Darum ist kein hundertprozentiger Schutz möglich, auch wenn wir diese Schwachstellen kontinuierlich identifizieren und korrigieren.

Citrix Workspace-App für Windows

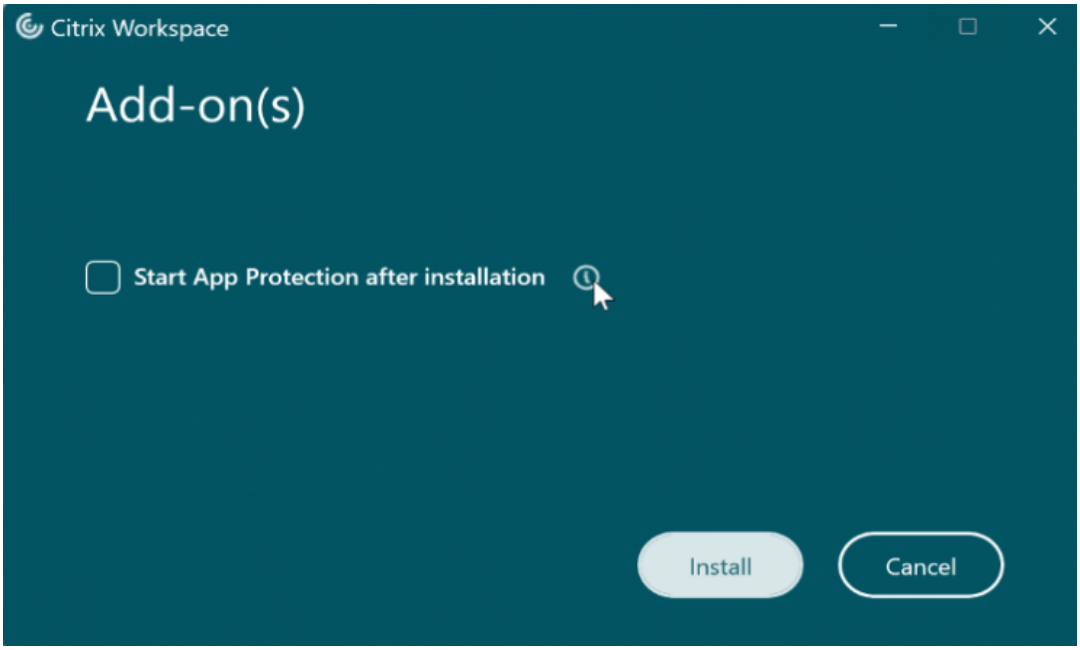
Voraussetzungen

- Citrix Virtual Apps and Desktops Version 1912 LTSR oder höher.
- StoreFront Version 1912 LTSR oder Workspace.
- Citrix Workspace-App Version 2203.1 LTSR oder höher.
- Eine gültige App Protection-Lizenz
- Ab Citrix Workspace-App 2212 wird App Protection bei der Installation der Citrix Workspace-App standardmäßig installiert.

Das bei der Installation angezeigte Kontrollkästchen **App Protection aktivieren** wurde durch **App Protection nach der Installation starten** ersetzt.

- Für Citrix Workspace-App-Versionen vor 2311:

- Ab Version 2311 der Citrix Workspace-App:



Wenn Sie dieses Kontrollkästchen aktivieren, wird App Protection sofort nach der Installation gestartet.

> **Hinweis:**
>
> Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird App Protection automatisch beim ersten Start einer geschützten Ressource oder Komponente für Kunden gestartet, die Anspruch auf App Protection haben.

Konfigurieren

Konfigurieren Sie die folgenden App Protection-Features für die Citrix Workspace-App für Windows:

- **Keyloggingschutz und Screenshotschutz:**
  - Informationen bezüglich Virtual Apps and Desktops finden Sie unter Keyloggingschutz und Screenshotschutz für Virtual Appsand Desktops konfigurieren.
  - Informationen bezüglich Web- oder SaaS-Apps finden Sie unter Keyloggingschutz und Screenshotschutz für Web- oder SaaS-Apps konfigurieren.
  - Für Authentifizierung und Self-Service-Plug-In:
    - Wenn Sie die Benutzeroberfläche der Global App Configuration Service verwenden, finden Sie weitere Informationen unter Keyloggingschutz und Screenshotschutz für Authentifizierung und Self-Service-Plug-In konfigurieren –Benutzeroberfläche des Global App Configuration Service verwenden
    - Wenn Sie das Gruppenrichtlinienobjekt verwenden, finden Sie weitere Informationen unter Keyloggingschutz und Screenshotschutz für Authentifizierung und Self-Service-Plug-In konfigurieren –Gruppenrichtlinienobjekt verwenden
    - Wenn Sie die API verwenden, finden Sie weitere Informationen unter Keyloggingschutz und Screenshotschutz für Authentifizierung und Self-Service-Plug-In konfigurieren –Global App Configuration Service-API verwenden
- Informationen zum Konfigurieren des DLL-Einschleusungsschutzfeatures finden Sie unter DLL-Einschleusungsschutz konfigurieren.
- Informationen zum Konfigurieren der App Protection-Richtlinienmanipulation finden Sie unter App Protection Richtlinienmanipulation konfigurieren.
- Informationen zum Konfigurieren des App Protection Posture Check finden Sie unter App Protection Posture Check konfigurieren.
- Informationen zum Aktivieren der Einstellung zum Blockieren des DoubleHop-Starts finden Sie unter DoubleHop-Start blockieren.

Einschränkungen

- Dieses Feature wird nur unter Desktop-Betriebssystemen wie Windows 11 und Windows 10 unterstützt.
- Die Citrix Workspace-App wird ab Version 2006.1 unter Windows 7 nicht unterstützt. Daher funktioniert auch App Protection unter Windows 7 nicht. Weitere Informationen finden Sie unter Einstellung von Features und Plattformen.
- Das Feature wird nicht über RDP (Remote Desktop Protocol) unterstützt.

Befehlszeilenoberfläche

Sie können App Protection mit dem Befehlszeilenparameter /`startappprotection` starten. Der ältere Switch /`includeappprotection` ist veraltet.

Die folgende Tabelle enthält Informationen zu Bildschirmen, die je nach Bereitstellung geschützt sind:

App Protection bereitstellen	Geschützte Bildschirme	Nicht geschützte Bildschirme
In der Citrix Workspace-App enthalten	Self-Service-Plug-In und Authentifizierungsmanager / Dialogfeld "Benutzeranmeldeinformationen"	Connection Center, Geräte, Fehlermeldungen der Citrix Workspace-App, Automatische Wiederverbindung von Clients, Konto hinzufügen
Auf dem Controller konfiguriert	ICA-Sitzungsbildschirm (für Apps und Desktops)	Connection Center, Geräte, Fehlermeldungen der Citrix Workspace-App, Automatische Wiederverbindung von Clients, Konto hinzufügen

Wenn Sie einen Screenshot erstellen, wird nur das geschützte Fenster abgedunkelt. Sie können einen Screenshot des Bereichs außerhalb des geschützten Fensters erstellen. Wenn Sie jedoch die Taste **Druck S-Abf** verwenden, um einen Screenshot auf einem Windows 10-Gerät zu erfassen, müssen Sie das geschützte Fenster minimieren.

Bisher wurden der Screenshotschutz und der Keyloggingschutz für Citrix Authentifizierung und Citrix Workspace-App-Bildschirme standardmäßig erzwungen. Ab Release 2212 sind diese Funktionen standardmäßig deaktiviert und müssen über das Gruppenrichtlinienobjekt konfiguriert werden.

> **Hinweis:**
>
> Diese GPO-Richtlinie gilt nicht für ICA- und SaaS-Sitzungen. Die ICA- und SaaS-Sitzungen werden weiterhin mit dem Delivery Controller und dem Citrix Secure Private Access gesteuert.

Verbesserung App Protection:

Ab Citrix Workspace-App für Windows 2305 und höher ist Keyloggingschutz auf den Authentifizierungs- und Self-Service-Plug-In-Bildschirmen aktiviert, wenn eines der folgenden Kriterien erfüllt ist:

- Sie haben App Protection mit einer der folgenden Methoden aktiviert:
  - Aktivieren Sie das Kontrollkästchen **App Protection starten** während der Installation.
  - Starten von App Protection mit dem Befehlszeilenparameter **/startappprotection**.
- Wenn Sie das Kontrollkästchen **App Protection starten** nicht aktiviert oder während der Installation den Befehlszeilenparameter **/startappprotection** verwendet haben, wird der Keyloggingschutz nach dem Start der ersten geschützten Ressource aktiviert.

> **Hinweis:**
>
> Der Global App Configuration Service und die Einstellungen für Gruppenrichtlinienobjekte haben Vorrang vor dem vorherigen Verhalten. Wenn Sie beispielsweise die GACS- oder Gruppenrichtlinienobjekt-Richtlinie für diese Bildschirme deaktiviert haben, ist der Keyloggingschutz auf den Authentifizierungs- und SSP-Bildschirmen nicht aktiviert.

Citrix Workspace-App für Linux

Ab Version 2108 ist das App Protection-Feature voll funktionsfähig. Dieses Feature unterstützt Virtual Apps and Desktops und ist standardmäßig aktiviert. Sie müssen das App Protection-Feature jedoch in der Datei `AuthManConfig.xml` konfigurieren, um es für den Authentifizierungsmanager und das Self-Service-Plug-In zu aktivieren.

Voraussetzung

Das App Protection-Feature funktioniert am besten mit folgenden Betriebssystemen und dem Gnome-Anzeigemanager:

- 64-Bit Ubuntu 22.04, Ubuntu 20.04 und Ubuntu 18.04
- 64-Bit Debian 10 und Debian 9
- 64-Bit CentOS 7
- 64-Bit RHEL 7
- ARMHF 32-Bit-Raspberry Pi-OS (basierend auf Debian 10 (Buster))
- ARM64 Raspberry Pi OS (basierend auf Debian 11 (Bullseye))

> **Hinweis:**
>
> Bei Verwendung einer früheren Version der Citrix Workspace-App als 2204 werden Betriebssysteme, die `glibc` 2.34 oder höher verwenden, nicht von App Protection unterstützt.
>
> Wenn Sie die Citrix Workspace-App mit aktiviertem App Protection-Feature auf einem Betriebssystem mit `glibc` 2.34 oder höher installieren, kann der Betriebssystemstart beim Neustart des Systems fehlschlagen. Führen Sie einen der folgenden Schritte aus, um den Fehler beim Betriebssystemstart zu beheben:
>
> - Installieren Sie das Betriebssystem neu.
> - Aktivieren Sie den Wiederherstellungsmodus des Betriebssystems und deinstallieren Sie die Citrix Workspace-App am Terminal.
> - Starten Sie das Live-Betriebssystem und entfernen Sie die Datei `rm -rf /etc/ld.so.preload` aus dem vorhandenen Betriebssystem.

App Protection installieren

1. Wenn Sie die Citrix Workspace-App mit dem Tarball-Paket installieren, wird die folgende Meldung angezeigt**Möchten Sie App Protection installieren? Warnung: Sie können dieses Feature nicht deaktivieren. Zum Deaktivieren müssen Sie die Citrix Workspace-App deinstallieren. Weitere Informationen erhalten Sie von Ihrem Systemadministrator. [default $INSTALLER_N]:**
2. Geben Sie **Y** ein, um App Protection zu installieren. App Protection ist standardmäßig nicht installiert.
3. Starten Sie Ihre Maschine neu, damit die Änderungen übernommen werden. Damit App Protection wie erwartet funktioniert, müssen Sie Ihre Maschine neu starten.

Installieren von App Protection auf RPM-Paketen Ab Version 2104 wird App Protection von der RPM-Version der Citrix Workspace-App unterstützt.

Mit den folgenden Schritten installieren Sie App Protection:

1. Installieren Sie die Citrix Workspace-App.
2. Paket für App Protection `ctxappprotection<version>.rpm` aus dem Installer der Citrix Workspace-App.
3. Starten Sie das System neu, damit die Änderungen übernommen werden.

Installieren von App Protection auf Debian-Paketen Ab Version 2101 wird App Protection von der Debian-Version der Citrix Workspace-App unterstützt.

Führen Sie zur Installation von App Protection den folgenden Befehl vom Terminal aus, bevor Sie die Citrix Workspace-App installieren:

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

Die Citrix Workspace-App bietet ab Version 2106 eine Option, mit der Sie die Funktionen zum Keylogging- und Screenshotschutz für den Authentifizierungsmanager und das Self-Service-Plug-In separat konfigurieren können.

Konfigurieren

Konfigurieren Sie die folgenden App Protection-Features für die Citrix Workspace-App für Linux:

- Informationen zum Konfigurieren von Keyloggingschutz und Screenshotschutz für den Authentifizierungsbildschirm finden Sie unter AuthManConfig.xml für den Authentifizierungsmanager verwenden.
- Informationen zum Konfigurieren von Keyloggingschutz und Screenshotschutz für den Self-Service-Plug-In-Bildschirm finden Sie unter AuthManConfig.xml für die Self-Service-Plug-In-Schnittstelle verwenden.
- Informationen zum Konfigurieren von Keyloggingschutz und Screenshotschutz für Virtual Apps and Desktops finden Sie unter Keyloggingschutz und Screenshotschutz für Virtual Apps and Desktops konfigurieren.
- Informationen zum Konfigurieren der App Protection-Richtlinienmanipulation finden Sie unter App Protection Richtlinienmanipulation konfigurieren.
- Informationen zum Konfigurieren des App Protection Posture Check finden Sie unter App Protection Posture Check konfigurieren.

Citrix Workspace-App für Mac

Konfigurieren Sie die folgenden App Protection-Features für die Citrix Workspace-App für Mac:

- Informationen zum Konfigurieren von Keyloggingschutz und Screenshotschutz für die Authentifizierung und das Self-Service Plug-In über die Benutzeroberfläche des Global App Configuration Service finden Sie unter Keyloggingschutz und Screenshotschutz für Authentifizierung und

Self-Service-Plug-In über die Benutzeroberfläche des Global App Configuration Service konfigurieren.

- Informationen zum Konfigurieren von Keyloggingschutz und Screenshotschutz für die Authentifizierung und das Self-Service-Plug-In über die API finden Sie unter Keyloggingschutz und Screenshotschutz für Authentifizierung und Self-Service-Plug-In über die API konfigurieren.
- Informationen zum Konfigurieren von Keyloggingschutz und Screenshotschutz für Virtual Apps and Desktops finden Sie unter Keyloggingschutz und Screenshotschutz für Virtual Apps and Desktops konfigurieren.
- Informationen zum Konfigurieren von Keyloggingschutz und Screenshotschutz für Web- und SaaS-Apps finden Sie unter Keyloggingschutz und Screenshotschutz für Web- und SaaS-Apps konfigurieren.
- Informationen zum Konfigurieren der App Protection-Richtlinienmanipulation finden Sie unter App Protection Richtlinienmanipulation konfigurieren.
- Informationen zum Konfigurieren des App Protection Posture Check finden Sie unter App Protection Posture Check konfigurieren.

Empfehlung

App Protection-Richtlinien konzentrieren sich in erster Linie auf die Verbesserung der Sicherheit und des Schutzes von Endpunkten. Überprüfen Sie alle anderen Sicherheitsempfehlungen und Richtlinien für Ihre Umgebung. Sie können eine **Sicherheit und Steuerung**-Richtlinienvorlage für eine empfohlene Konfiguration in Umgebungen mit geringer Risikotoleranz verwenden. Weitere Informationen finden Sie unter Richtlinienvorlagen.

Keyloggingschutz und Screenshotschutz konfigurieren

April 10, 2024

Keyloggingschutz und Screenshotschutz können für folgende Funktionen konfiguriert werden:

- Authentifizierung und Self-Service-Plug-In
- Virtual Apps and Desktops
- Web- und SaaS-Apps

Keyloggingschutz und Screenshotschutz für Authentifizierung und Self-Service-Plug-In konfigurieren

Mit den folgenden Methoden können Sie Keyloggingschutz und Screenshotschutz für Authentifizierung und Self-Service-Plug-In konfigurieren:

Konfigurationsmethode	Citrix Workspace-App für Linux	Citrix Workspace-App für Mac	Citrix Workspace-App für Windows
Gruppenrichtlinienobjekt verwenden	Nein	Nein	Ja
Konfiguration mit dem Global App Configuration Service	Nein	Ja	Ja
AuthManConfig.xml verwenden	Ja	Nein	Nein

Gruppenrichtlinienobjekt verwenden

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace**.
3. Führen Sie je nachdem, ob Sie App Protection für den Authentifizierungsmanager oder das Self-Service-Plug-In konfigurieren, einen der folgenden Schritte aus:

    - **Authentifizierungsmanager**

      Um den Keylogging- und Screenshotschutz für den Authentifizierungsmanager zu konfigurieren, wählen Sie **Benutzerauthentifizierung** > **App Protection verwalten**.

    - **Self-Service-Plug-In-Schnittstelle**

      Um den Keylogging- und Screenshotschutz für die Self-Service-Plug-In-Schnittstelle zu konfigurieren, wählen Sie **Self-Service** > **App Protection verwalten** aus.

4. Wählen Sie mindestens eine der folgenden Optionen aus:

    - **Keyloggingschutz:** Verhindert, dass Keylogger Tastenanschläge erfassen.
    - **Screenshotschutz:** Verhindert, dass Benutzer Screenshots erstellen und ihren Bildschirm teilen.

5. Klicken Sie auf **Anwenden** und auf **OK**.

Erwartetes Verhalten:

Das erwartete Verhalten hängt davon ab, wie der Zugriff auf den StoreFront-Store erfolgt, der die geschützten Ressourcen enthält.

Benutzeroberfläche des Global App Configuration Service verwenden

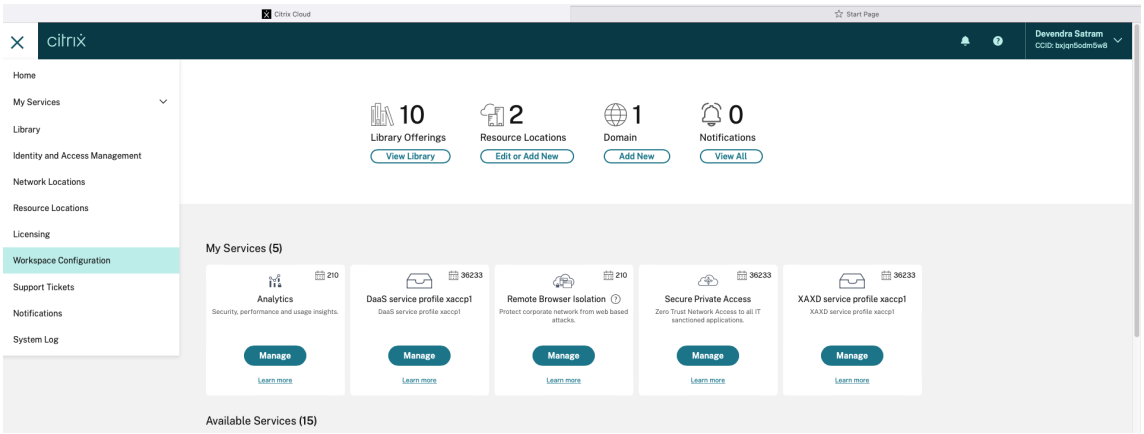
Ab Citrix Workspace-App für Windows 2302 oder Citrix Workspace-App für Windows 2301 können Sie mit der Citrix Workspace-App die App Protection für die Authentifizierungs- und Self-Service-Plug-In-Bildschirme mit dem Global App Configuration Service (GACS) konfigurieren.

Wenn Sie die Funktionen zum Keylogging- und Screenshotschutz mit dem GACS aktivieren, gelten sie sowohl für die Authentifizierung als auch für das Self-Service-Plug-In.

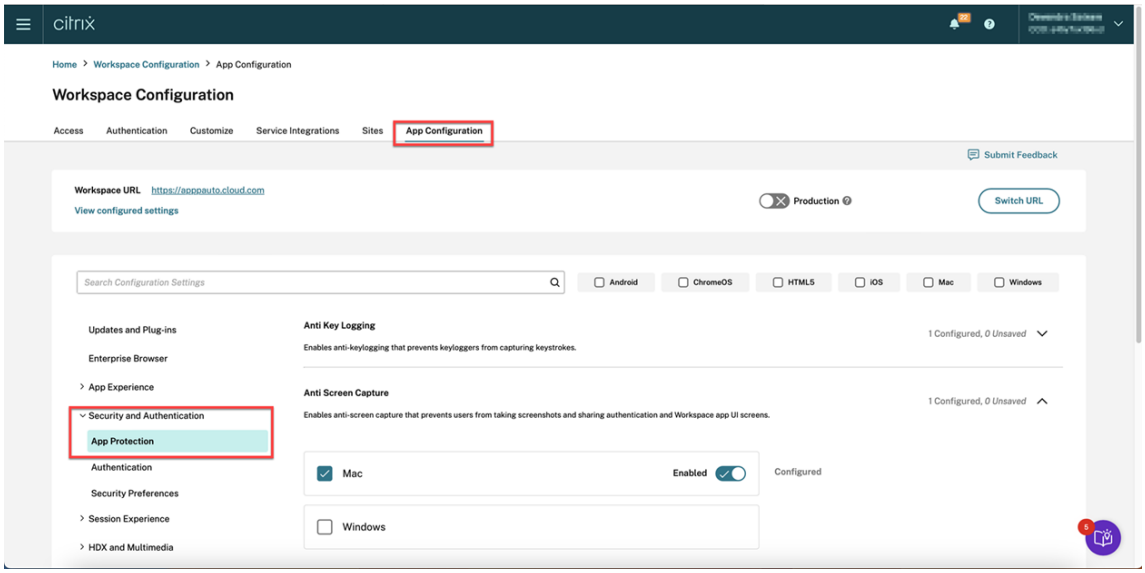
> **Hinweis:**
>
> - Die Konfiguration des Keyloggingschutzes und des Screenshotschutzes für die Authentifizierung und das Self-Service-Plug-In mit GACS gilt für die Citrix Workspace-App für Windows und die Citrix Workspace-App für Mac. Sie gilt nicht für die Citrix Workspace-App für Linux.
> - Die Konfigurationen über GACS gelten nicht für Virtual Apps and Desktops, Web-Apps und SaaS-Apps. Diese Ressourcen werden weiterhin über den Delivery Controller und Citrix Secure Private Access verwaltet.
> - Ab Version 2311 der Citrix Workspace-App für Mac können Sie App Protection für die Authentifizierung und das Self-Service-Plug-In mithilfe der Benutzeroberfläche des Global App Configuration Service sowohl für Cloudstores als auch on-premises konfigurieren. Wenn Sie jedoch die Citrix Workspace-App für Mac vor Version 2311 verwenden, können Sie sie nur für Cloudstores konfigurieren.

Administratoren können App Protection mit der Workspacekonfiguration-Benutzeroberfläche konfigurieren:

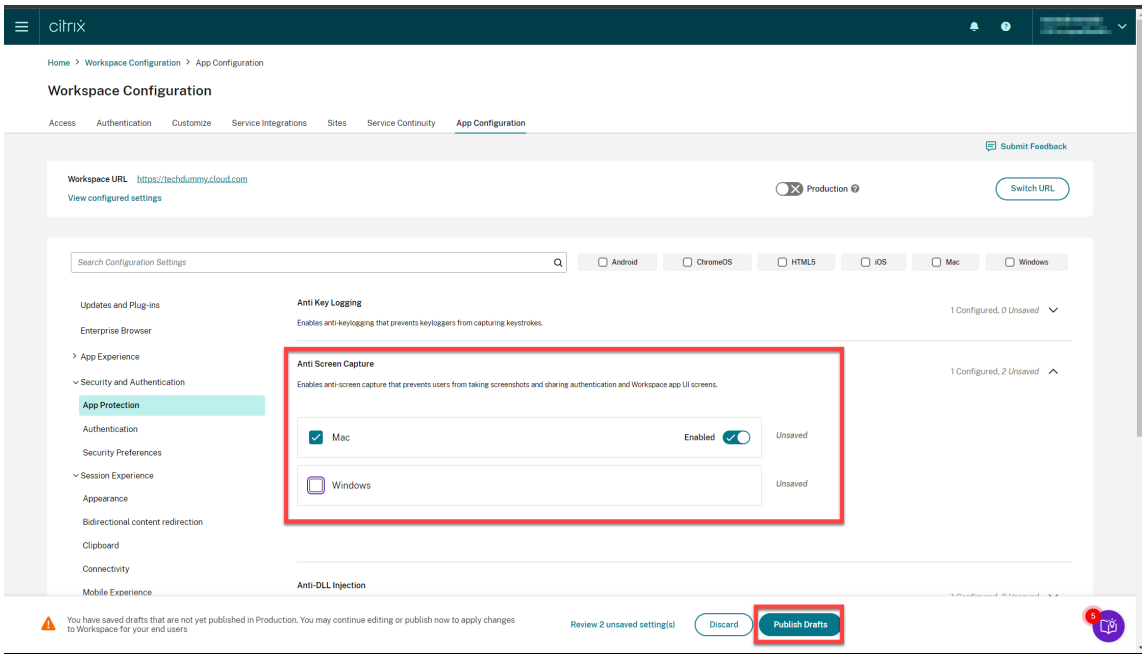
1. Melden Sie sich an Ihrem Citrix Cloud-Konto an und wählen Sie **Workspacekonfiguration**.



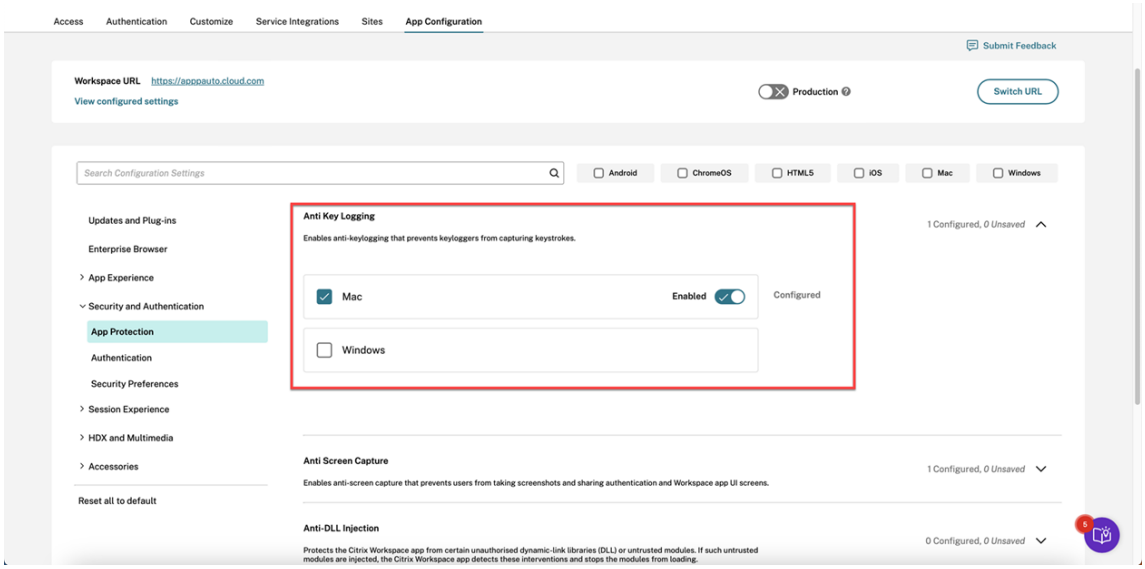
2. Wählen Sie **App-Konfiguration** > **Sicherheit und Authentifizierung** > **App Protection**.



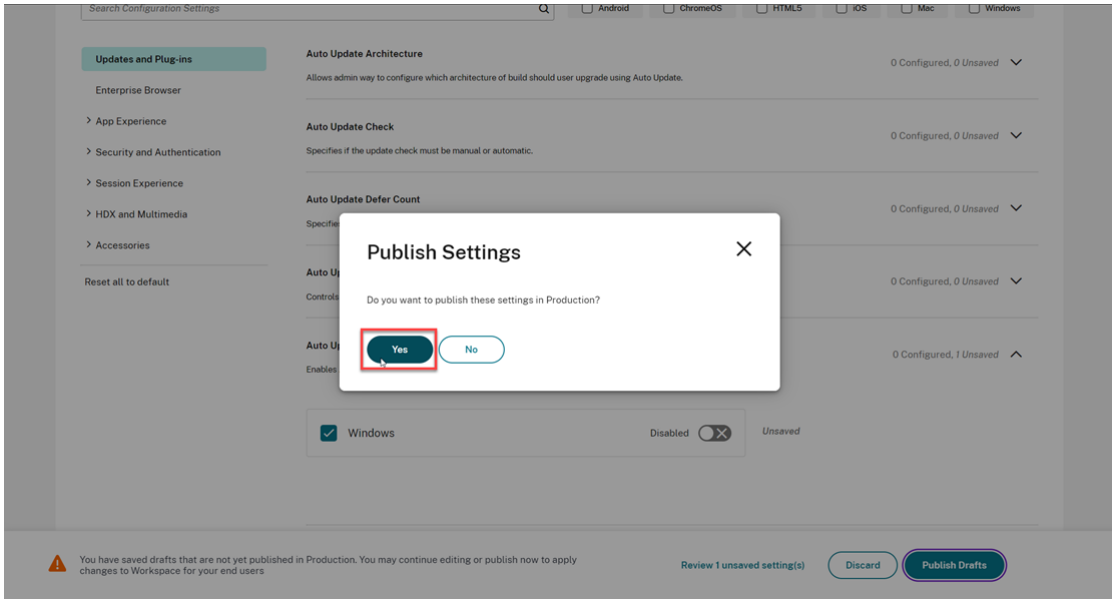
3. Klicken Sie auf **Screenshotschutz** und wählen Sie dann das entsprechende Betriebssystem (Windows oder Mac) aus.
4. Klicken Sie auf die Umschaltfläche **Aktiviert** und dann auf **Entwürfe veröffentlichen**.



5. Klicken Sie auf **Keyloggingschutz** und wählen Sie dann das entsprechende Betriebssystem (Windows oder Mac) aus.
6. Klicken Sie auf die Umschaltfläche **Aktiviert** und dann auf **Entwürfe veröffentlichen**.



7. Klicken Sie im Dialogfeld **Einstellungen veröffentlichen** auf **Ja**.



Global App Configuration Service-API verwenden

Administratoren können mit dieser API die folgenden App Protection-Funktionen konfigurieren. Die Einstellungen lauten wie folgt:

- **Einstellung zum Aktivieren oder Deaktivieren des Screenshotschutzes:**

  “Name”: “enable anti screen capture for auth and ssp”
  “Wert”:”true”oder “false”

- **Einstellung zum Aktivieren oder Deaktivieren des Keyloggingschutzes:**

“Name”: “enable anti key-logging for auth and ssp”
“Wert”: “true”oder “false”

Beispiel: für eine JSON-Datei zur Aktivierung von Screenshotschutz und Keyloggingschutz für die Citrix Workspace-App in GACS:

```
{


          "category": "App Protection",

          "userOverride": true,

          "assignedTo": [

            "AllUsersNoAuthentication"

          ],

          "settings": [

            {


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

              "value": true

             }
 ,

            {


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

              "value": true

             }


          ] }
```

AuthManConfig.xml für einen Authentifizierungsmanager verwenden

Navigieren Sie zu der Datei `$ICAROOT/config/AuthManConfig.xml` und bearbeiten Sie sie wie folgt:

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



```
    <value>true</value>
    <key>AuthManAntiKeyLoggingEnabled</key>
    <value>true </value>

<!--NeedCopy-->
```

AuthManConfig.xml für die Self-Service Plug-in-Schnittstelle verwenden

Navigieren Sie zu der Datei `$ICAROOT/config/AuthManConfig.xml` und bearbeiten Sie sie wie folgt:

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

<!--NeedCopy-->
```

Keyloggingschutz und Screenshotschutz für Virtual Apps and Desktops konfigurieren

Zwei Richtlinien bieten Keylogging- und Screenshotschutz in einer Sitzung. Sie können Keyloggingschutz und Screenshotschutz für Virtual Apps and Desktops wie folgt konfigurieren:

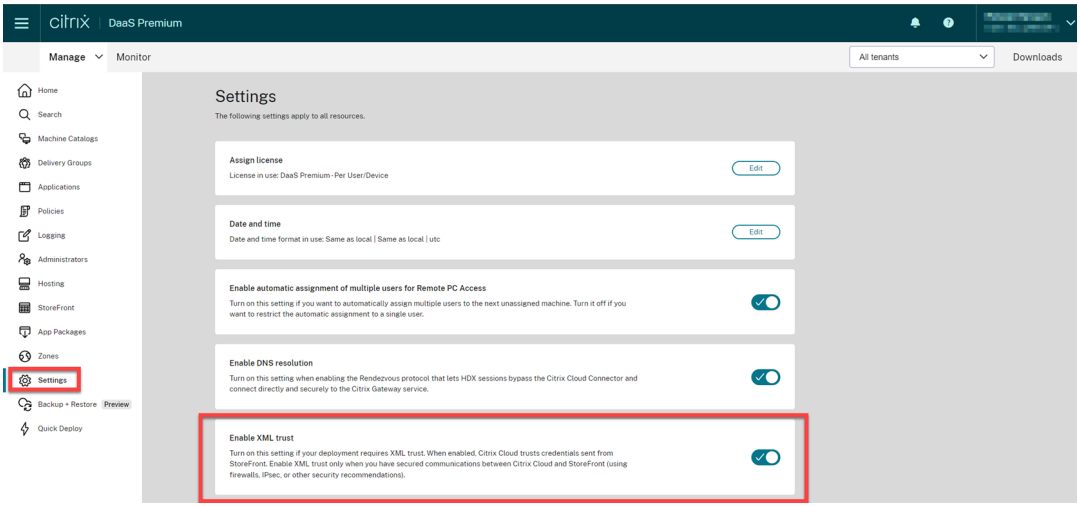
> **Hinweis:**
>
> Citrix DaaS unterstützt App Protection ab Version 2103 mit StoreFront und Workspace.

Web Studio verwenden

Gehen Sie wie folgt vor, um Keyloggingschutz und Screenshotschutz für Citrix Virtual Apps oder Desktops über Web Studio zu konfigurieren:

1. App Protection erfordert XML-Vertrauen. Gehen Sie wie folgt vor, um XML-Vertrauen zu aktivieren:

    a) Melden Sie sich bei Ihrem Citrix DaaS-Konto an und gehen Sie zu **Verwalten** > **Einstellungen** > **XML-Vertrauen aktivieren**.

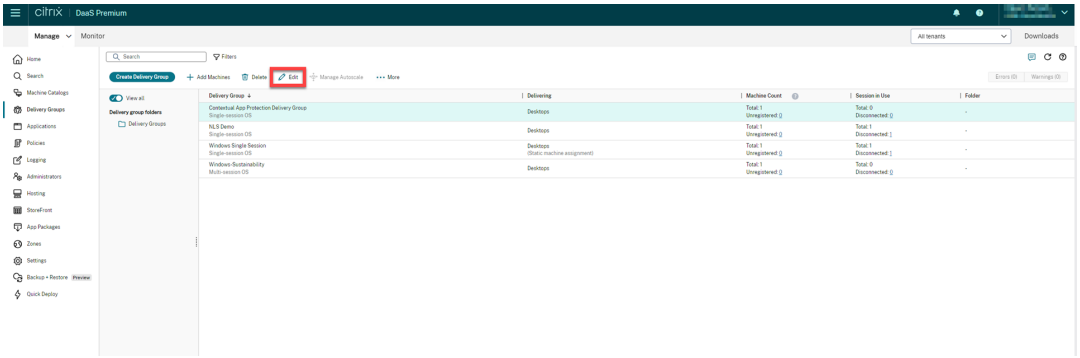


b) Aktivieren Sie den Schalter **XML-Vertrauen aktivieren**.

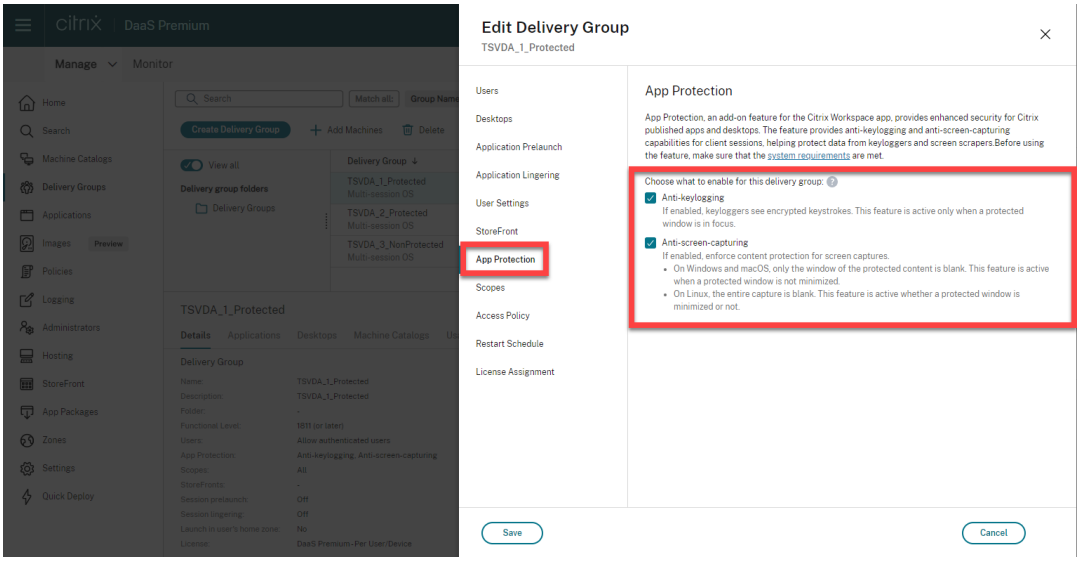
2. Gehen Sie wie folgt vor, um eine App Protection-Methode für eine Bereitstellungsgruppe auszuwählen:

   a) Gehen Sie in Citrix DaaS zu **Verwalten** > **Bereitstellungsgruppen**.

   b) Wählen Sie eine Bereitstellungsgruppe und klicken Sie in der Aktionsleiste auf **Bearbeiten**.



   c) Klicken Sie auf **App Protection** und aktivieren Sie dann die Kontrollkästchen **Keylogging-schutz** und **Screenshotschutz**.



d) Klicken Sie auf **Speichern**.

PowerShell verwenden

> **Hinweis:**
>
> Verwenden Sie in einer Citrix DaaS-Umgebung die Cmdlets im Citrix Virtual Apps and Desktops Remote PowerShell SDK auf einer beliebigen Maschine (Ausnahme: Citrix Cloud Connector-Maschinen) zum Eingeben der in diesem Abschnitt aufgeführten Befehle.

Aktivieren Sie die folgenden Eigenschaften für die App Protection-Bereitstellungsgruppe mit dem Citrix Virtual Apps and Desktops-SDK auf jeder Maschine mit installiertem Delivery Controller oder auf einer Maschine mit eigenständiger Studio-Instanz und installierten FMA PowerShell-Snap-Ins.

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

Sie können jede Richtlinie individuell pro Bereitstellungsgruppe aktivieren. Beispielsweise können Sie den Schutz vor Keylogging nur für DG1 und den Schutz vor Bildschirmerfassung nur für DG2 konfigurieren. Für DG3 können Sie beide Richtlinien aktivieren.

Beispiel:

Um beide Richtlinien für die Bereitstellungsgruppe **DG3** zu aktivieren, führen Sie folgenden Befehl auf einem beliebigen Delivery Controller in der Site aus:

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

Führen Sie folgendes Cmdlet aus, um die Einstellungen zu überprüfen:


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

Aktivieren Sie außerdem XML-Vertrauen:

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

Schützen Sie das Netzwerk zwischen StoreFront und Broker. Weitere Informationen finden Sie in den Knowledge Center-Artikeln CTX236929 und Schützen des XenApp und XenDesktop-XML-Diensts.

Keyloggingschutz und Screenshotschutz für Web- oder SaaS-Apps konfigurieren

Web- und SaaS-Apps werden im Citrix Enterprise Browser für Citrix Workspace-App für Windows und Citrix Workspace-App für Mac geöffnet. Wenn die Apps so konfiguriert sind, dass die App Protection-Richtlinien über Citrix Secure Private Access angewendet werden, wird App Protection pro Registerkarte angewendet.

Mit den folgenden Optionen konfigurieren Sie App Protection für Web- und SaaS-Apps:

- Informationen zum Konfigurieren von App Protection für Web- und SaaS-Apps für Workspace finden Sie unter Citrix Secure Private Access für Citrix Workspace.
- Informationen zum Konfigurieren von App Protection für Web- und SaaS-Apps für StoreFront finden Sie unter Citrix Secure Private Access-Unterstützung für StoreFront.

DLL-Einschleusungsschutz konfigurieren

March 11, 2024

Der DLL-Einschleusungsschutz ist standardmäßig deaktiviert. Sie können dieses Feature wie folgt aktivieren:

- Gruppenrichtlinienobjekt (GPO)
- Global App Configuration Service (GACS)

Über das Gruppenrichtlinienobjekt konfigurieren

Die folgenden Richtlinien wurden zum Konfigurieren des DLL-Einschleusungsschutzes hinzugefügt:

- DLL-Einschleusungsschutz
- Positivliste für DLL-Einschleusungsschutz

DLL-Einschleusungsschutz verwenden

Verwenden Sie diese Richtlinie, um den DLL-Einschleusungsschutz zu aktivieren oder zu deaktivieren. Wenn diese Richtlinie nicht konfiguriert ist, ist der DLL-Einschleusungsschutz deaktiviert. Zulässige Werte:

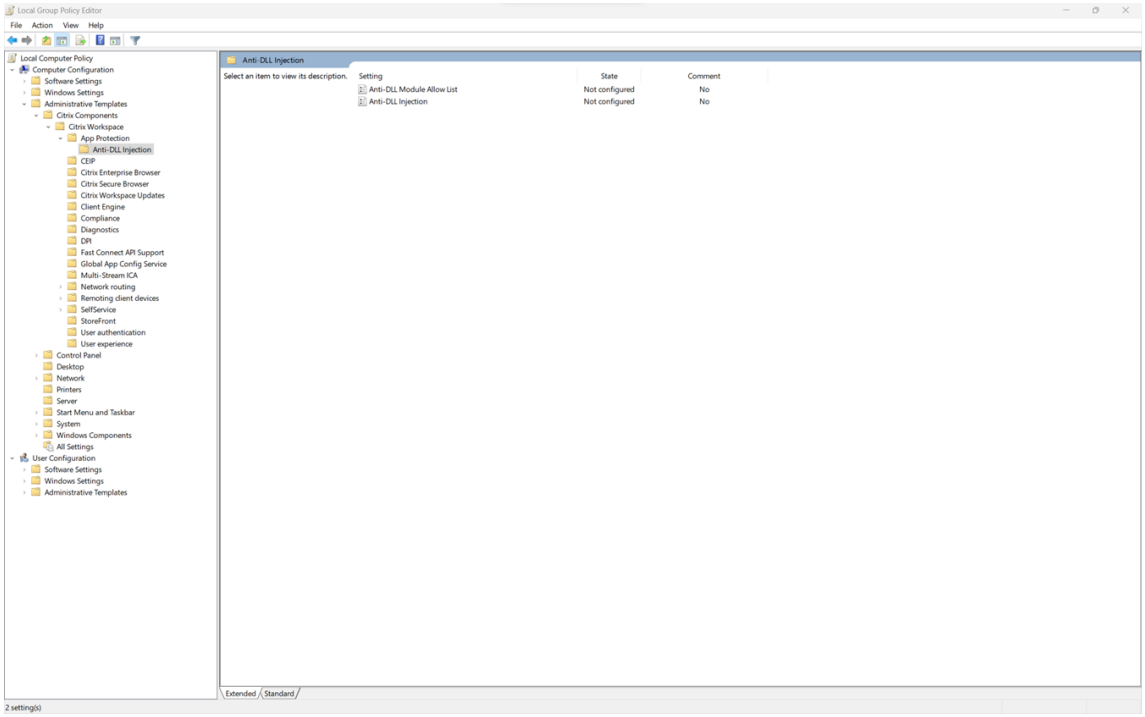
- **Aktiviert** –Der DLL-Einschleusungsschutz ist für Citrix Authentifizierungsmanager, die Citrix Workspace-App-Benutzeroberfläche und Citrix Virtual Apps and Desktops aktiviert. Administratoren können die erforderlichen Komponenten auswählen, um den DLL-Einschleusungsschutz zu aktivieren.
- **Deaktiviert** –Der DLL-Einschleusungsschutz ist für Citrix Authentifizierungsmanager, die Citrix Workspace-App-Benutzeroberfläche und Citrix Virtual Apps and Desktops deaktiviert.

Gehen Sie wie folgt vor, um die DLL-Einschleusungsschutz-Richtlinie zu aktivieren:

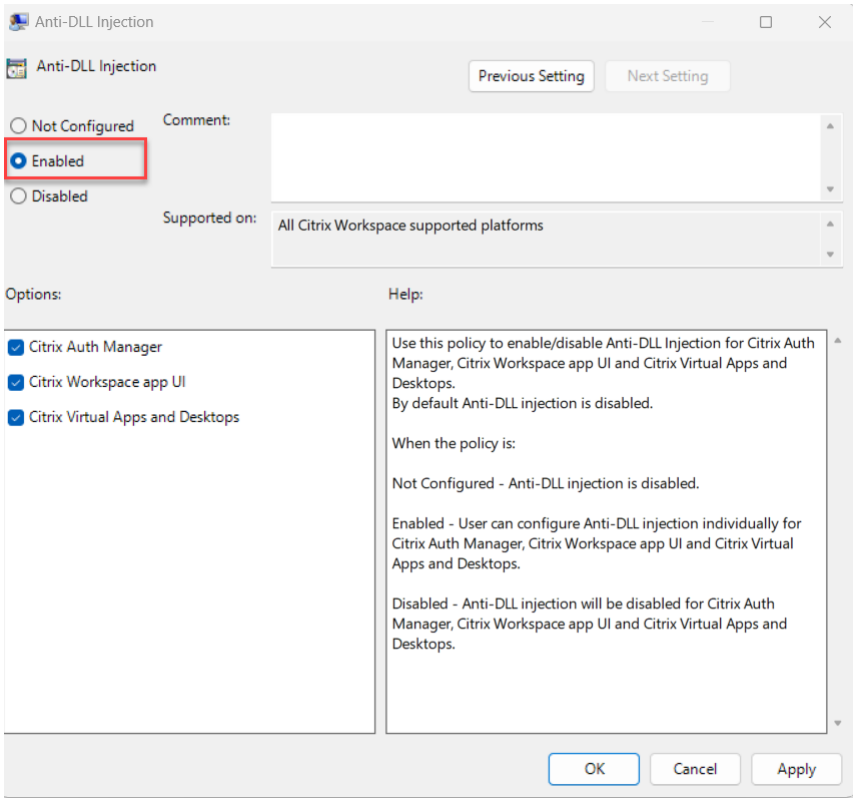
1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App mit dem folgenden Befehl:

   ```
   gpedit.msc
   ```

2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **App Protection** > **DLL-Einschleusungsschutz**.



3. Klicken Sie auf die Richtlinie **DLL-Einschleusungsschutz** und wählen Sie **Aktiviert** aus. Alle Komponenten sind ausgewählt. Sie können jedoch die Auswahl der Komponenten unter Optionen ändern.



4. Klicken Sie auf **OK**.

Richtlinie “Positivliste für DLL-Einschleusungsschutz”verwenden

Als Administrator können Sie diese Richtlinie verwenden, um beliebige DLLs vom DLL-Einschleusungsschutz auszuschließen. Citrix empfiehlt, diese Richtlinie nur für Ausnahmeszenarien zu verwenden. Wenn diese Richtlinie nicht konfiguriert ist, steht keine DLL auf der Positivliste. Alle DLLs werden in den DLL-Einschleusungsschutz einbezogen. Zulässige Werte:

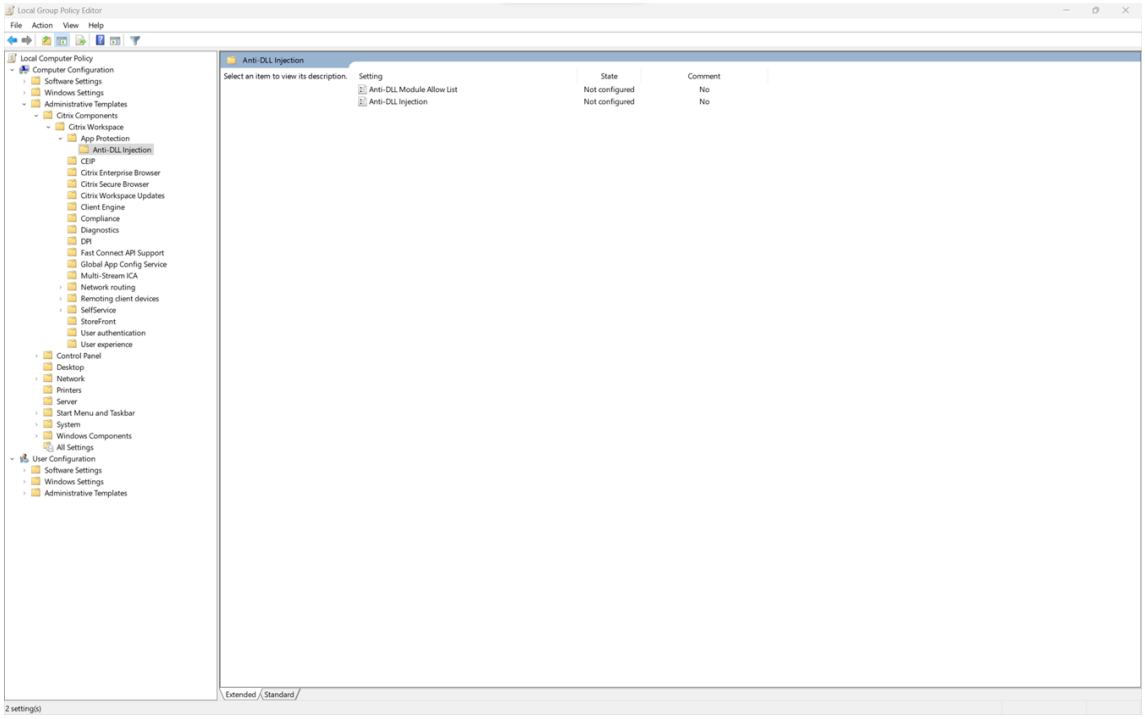
- **Aktiviert** – Schließt DLLs, die auf der Positivliste sind, vom DLL-Schutz aus.
- **Deaktiviert** – Löscht die DLLs von der Positivliste.

Gehen Sie wie folgt vor, um die Richtlinie “Positivliste für DLL-Einschleusungsschutz”zu aktivieren:

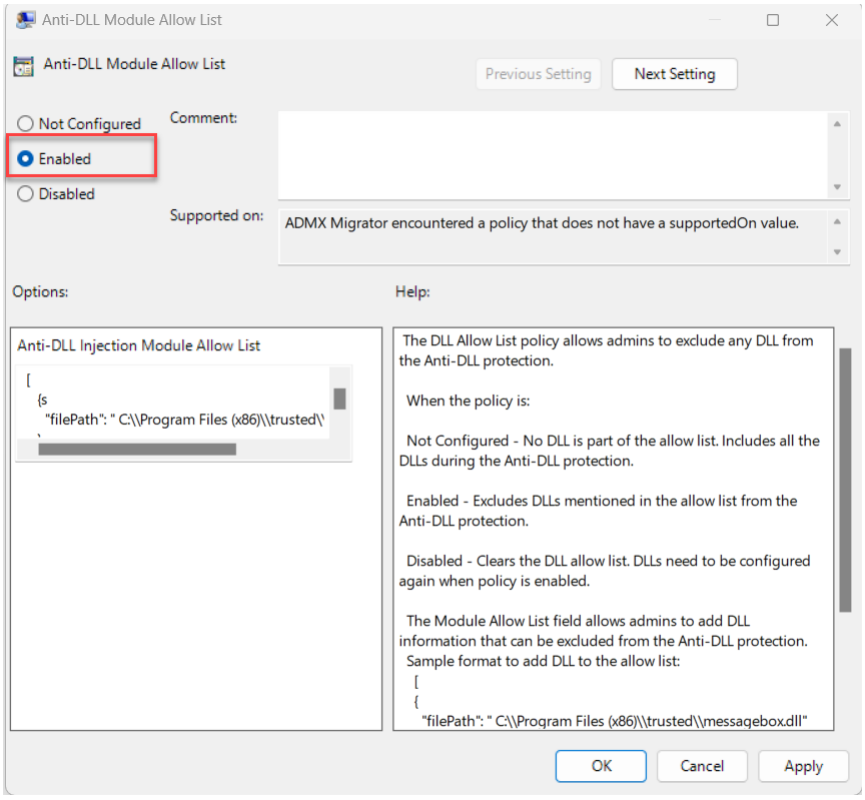
1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App mit dem folgenden Befehl:

   ```
   gpedit.msc
   ```

2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **App Protection** > **Positivliste für DLL-Schutz**.



3. Klicken Sie auf die Richtlinie **Positivliste für DLL-Schutz** und wählen Sie **Aktiviert** aus.



4. Fügen Sie die Module, die Sie vom DLL-Einschleusungsschutz ausschließen möchten, im Feld **Positivliste für DLL-Einschleusungsschutz** hinzu.
   Beispielformat zum Hinzufügen einer DLL zur Positivliste:


```
[
    {

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

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

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

5. Klicken Sie auf **OK**.

Über die Global App Configuration Service-Benutzeroberfläche konfigurieren

Mit dem GACS können Administratoren den DLL-Einschleusungsschutz konfigurieren. Die Einstellungen lauten wie folgt:

- DLL-Einschleusungsschutz: Fügen Sie die gewünschten Module hinzu.
- Positivliste für DLL-Schutz: Fügen Sie die DLLs hinzu, die Sie vom DLL-Einschleusungsschutz ausschließen möchten

Weitere Informationen finden Sie unter Global App Configuration Service.

Die nachstehende JSON-Datei zeigt, wie der **DLL-Einschleusungsschutz** und die **Positivliste für DLL-Schutz** der Citrix Workspace-App für Windows in GACS aktiviert werden:

```
{

  "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"
                   }
  ,
                  {

                    "filePath": "C:\Program Files (x86)\Citrix\ICA Client
                       \AuthManager\AuthManSvr.exe"
                   }

                ]
               }

            ]
           }

        ]
      }
  ,
     "name": "name",
     "description": "desc",
     "useForAppConfig": true
    }

  }

<!--NeedCopy-->
```

Erkennung von Richtlinienmanipulationen konfigurieren

March 11, 2024

Voraussetzungen

Um das Feature zur Erkennung von Richtlinienmanipulationen zu konfigurieren, bereiten Sie Folgendes vor:

- Für Cloud-Bereitstellungen —Cloud Desktop Delivery Controller Version 1.1.5 oder höher
- Für On-Premises-Bereitstellungen —Citrix Virtual Apps and Desktops Version 2308 oder höher
- Windows Virtual Delivery Agent-Installationsprogramm Version 2308 oder höher
- Windows: Citrix Workspace App für Windows 2309 oder höher
- Mac: Citrix Workspace App für Mac 2308 oder höher
- Linux: Citrix Workspace App für Linux 2308 oder höher

Um die Erkennung von Richtlinienmanipulationen zu aktivieren, muss der Administrator den **Citrix App Protection Service** auf den TS/WS-VDAs starten, die die mit App Protection konfigurierten virtuellen Apps und Desktops hosten.

Führen Sie einen der folgenden Schritte aus, um die Erkennung von Richtlinienmanipulationen zu aktivieren:

- Über die Befehlszeile:

  1. Klicken Sie ganz links in der Taskleiste auf das **Suchsymbol** . Geben Sie **cmd** ein und klicken Sie auf **Als Administrator ausführen**. Ein Fenster mit **Eingabeaufforderung** wird geöffnet.
  2. Führen Sie die folgenden Befehle aus:

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

     <!--NeedCopy-->
     ```

- Über die Benutzeroberfläche:

  1. Klicken Sie ganz links in der Taskleiste auf das **Suchsymbol** . Geben Sie **services.msc** ein, und drücken Sie die **Eingabetaste**. Der Bildschirm **Dienste** wird angezeigt.
  2. Wählen Sie **Citrix AppProtection Service** und klicken Sie auf **Start**.
  3. Klicken Sie mit der rechten Maustaste auf **Citrix AppProtection Service** und wählen Sie **Eigenschaften**.
  4. Wählen Sie **Allgemein** > **Starttyp** > **Automatisch** und klicken Sie auf **OK**, damit der Dienst beim Systemstart automatisch gestartet wird.

Das Feature zur Erkennung von Richtlinienmanipulationen ist damit aktiviert.

Mit App Protection Posture Check können Sie frühere Versionen der Citrix Workspace-App, die die Erkennung von Richtlinienmanipulationen nicht unterstützen, erkennen und blockieren. Weitere Informationen finden Sie unter App Protection Posture Check.

App Protection Posture Check konfigurieren

March 11, 2024

Um App Protection Posture Check zu aktivieren, konfigurieren Sie die neue VDA-Citrix-Richtlinie zu diesem Feature.

Voraussetzungen

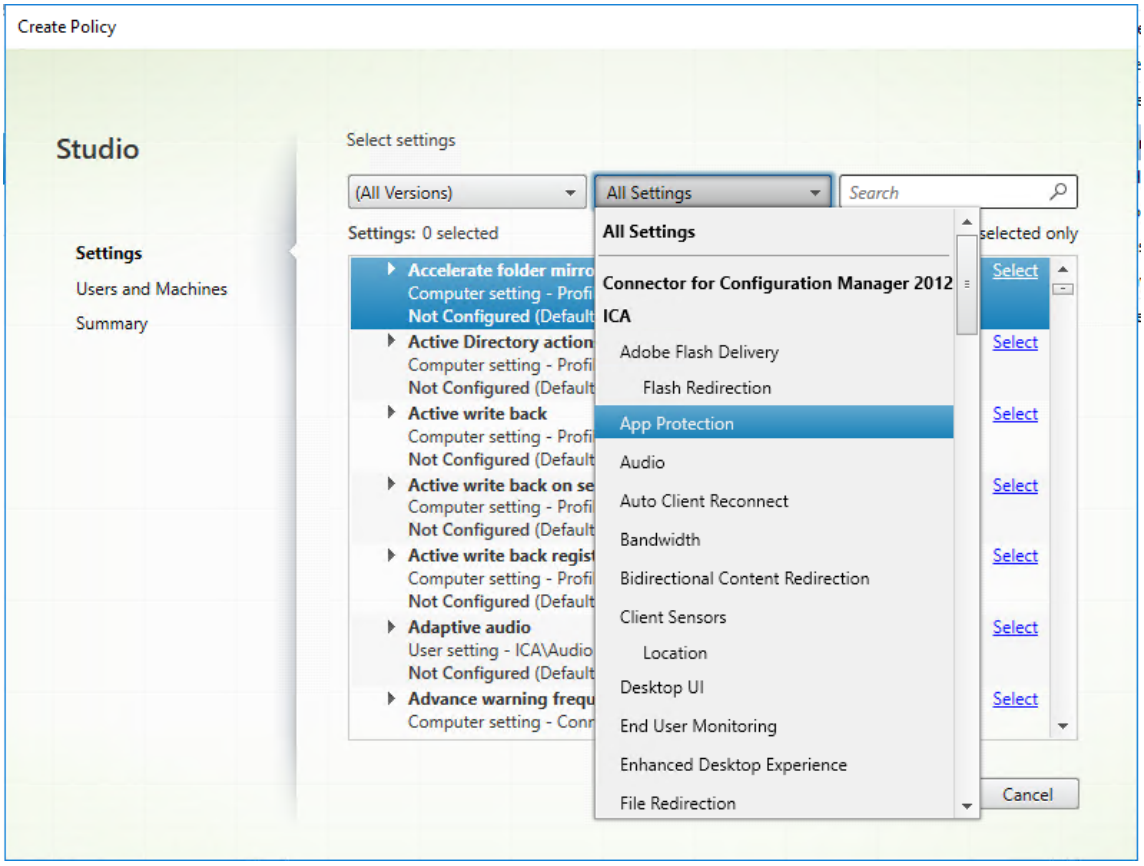
Bereiten Sie Folgendes vor:

- Für Cloud-Bereitstellungen —Cloud Desktop Delivery Controller Version 1.1.5 oder höher
- Für On-Premises-Bereitstellungen —Citrix Virtual Apps and Desktops Version 2308 oder höher
- Windows Virtual Delivery Agent-Installationsprogramm Version 2308 oder höher
- Windows: Citrix Workspace App für Windows 2309 oder höher
- Mac: Citrix Workspace App für Mac 2308 oder höher
- Linux: Citrix Workspace App für Linux 2308 oder höher

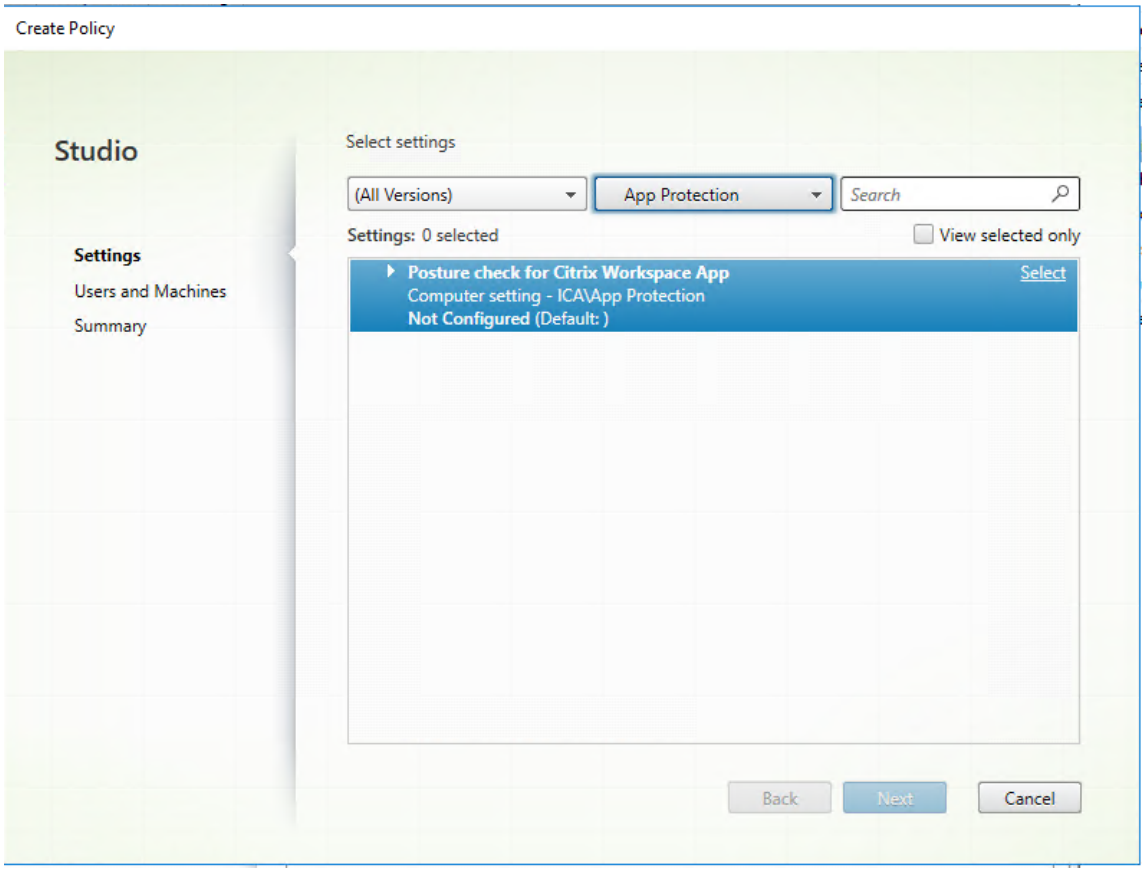
Konfigurieren Sie wie folgt die neue VDA-Citrix-Richtlinie für Posture Check:

> **Hinweis:**
>
> Diese neue VDA-Citrix-Richtlinie kann mit Citrix Studio und mit Web Studio bereitgestellt werden. Das folgende Verfahren wird über Citrix Studio bereitgestellt. Sie können es aber auch für Web Studio verwenden.

1. Öffnen Sie für On-Premises-Bereitstellungen die Citrix Studio-App auf dem Desktop Delivery Controller (DDC) oder für Cloudbereitstellungen Web Studio. Wählen Sie dann **Richtlinien**.
2. Wählen Sie unter **Aktionen** die Option **Richtlinien** > **Richtlinie erstellen**.
3. Klicken Sie auf das Dropdownmenü **Alle Einstellungen** und wählen Sie unter **ICA** die Option **App Protection**.



4. Wählen Sie **Statusprüfung für Citrix Workspace-App** und klicken Sie auf **Auswählen**.

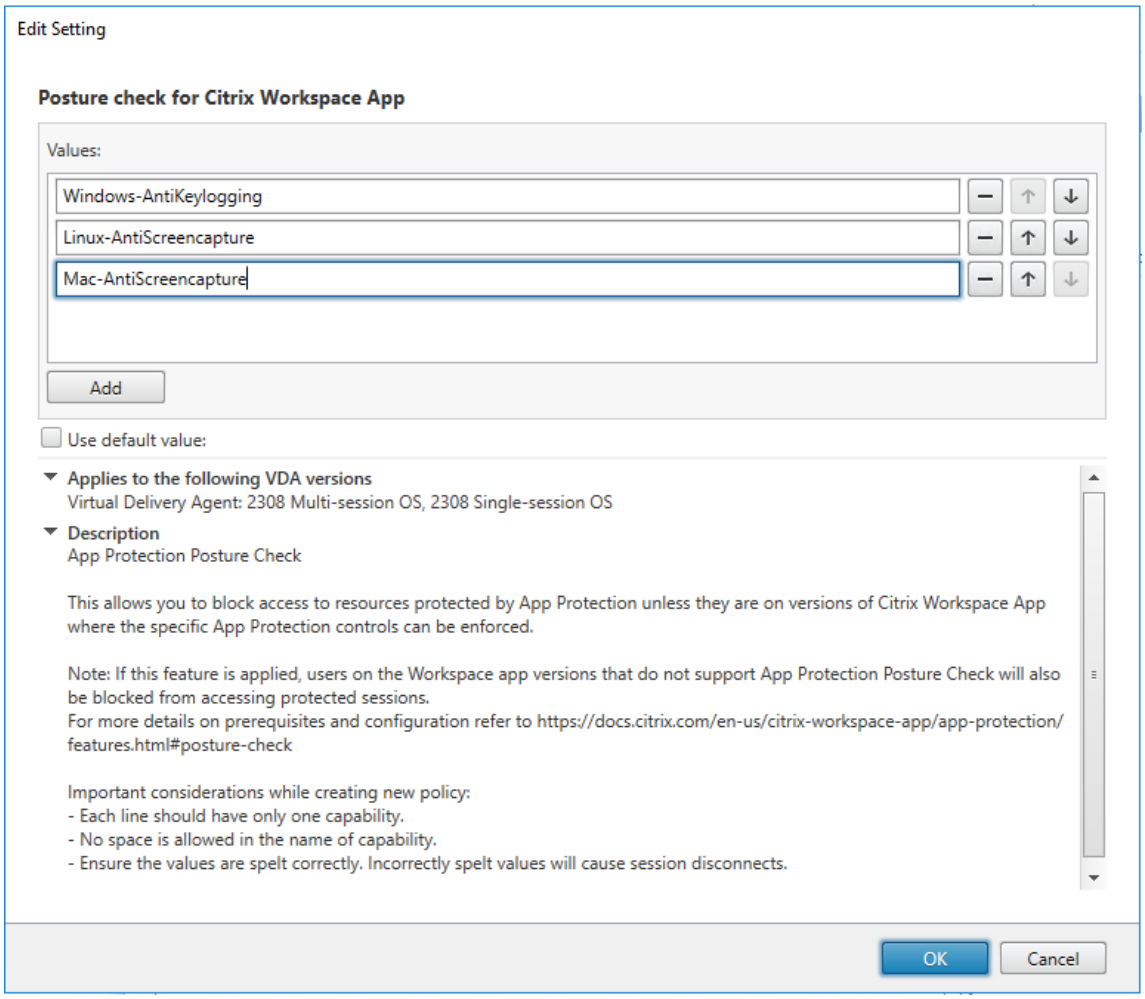


Das Fenster **Einstellung bearbeiten** wird angezeigt.

5. Deaktivieren Sie das Kontrollkästchen **Standardwert verwenden**.
6. Klicken Sie auf **Hinzufügen** und geben Sie die entsprechenden Werte aus Folgendem ein:

   - Windows-AntiScreencapture
   - Windows-AntiKeylogging
   - Linux-AntiScreencapture
   - Linux-AntiKeylogging
   - Mac-AntiScreencapture
   - Mac-AntiKeylogging

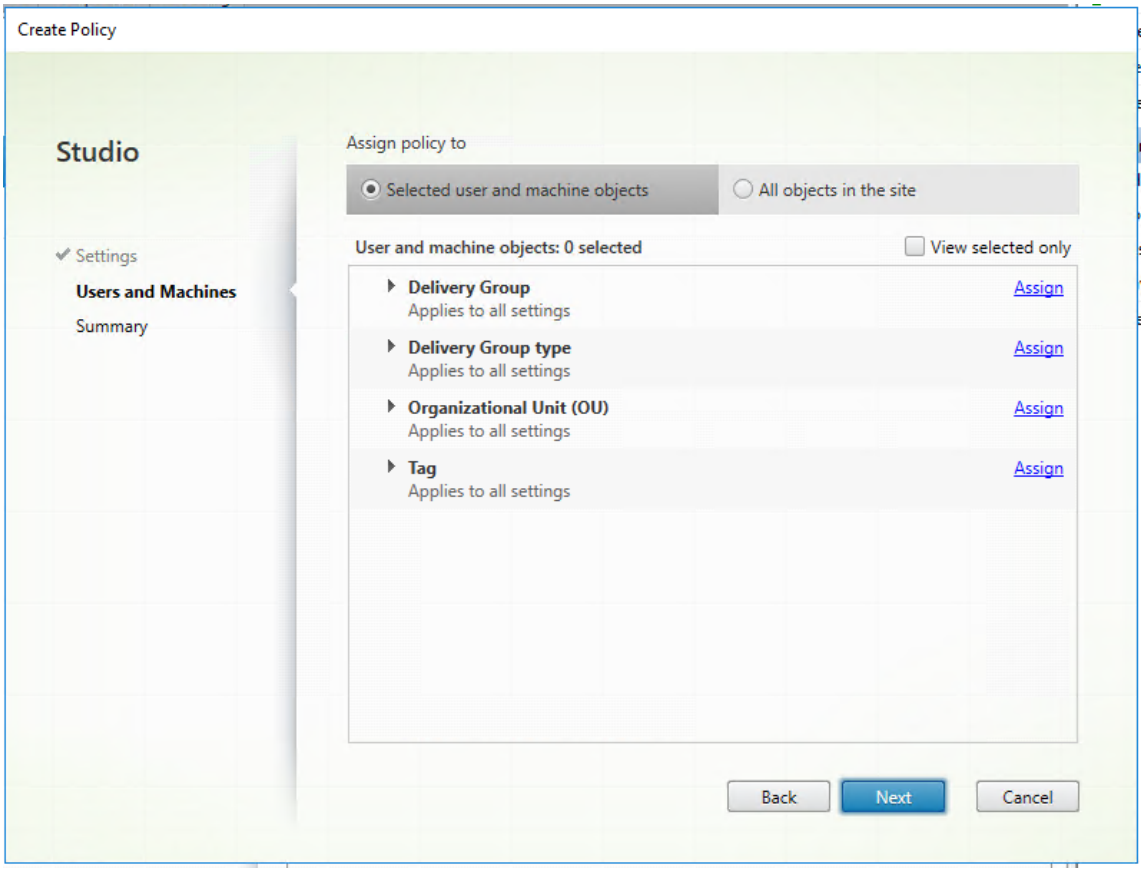
   Wenn Sie beispielsweise “Windows-AntiScreencapture”und “Windows-AntiKeylogging” hinzugefügt haben, darf die Citrix Workspace-App für Windows, die Posture Check unterstützt und über diese Funktionen verfügt, eine Verbindung zum VDA herstellen.



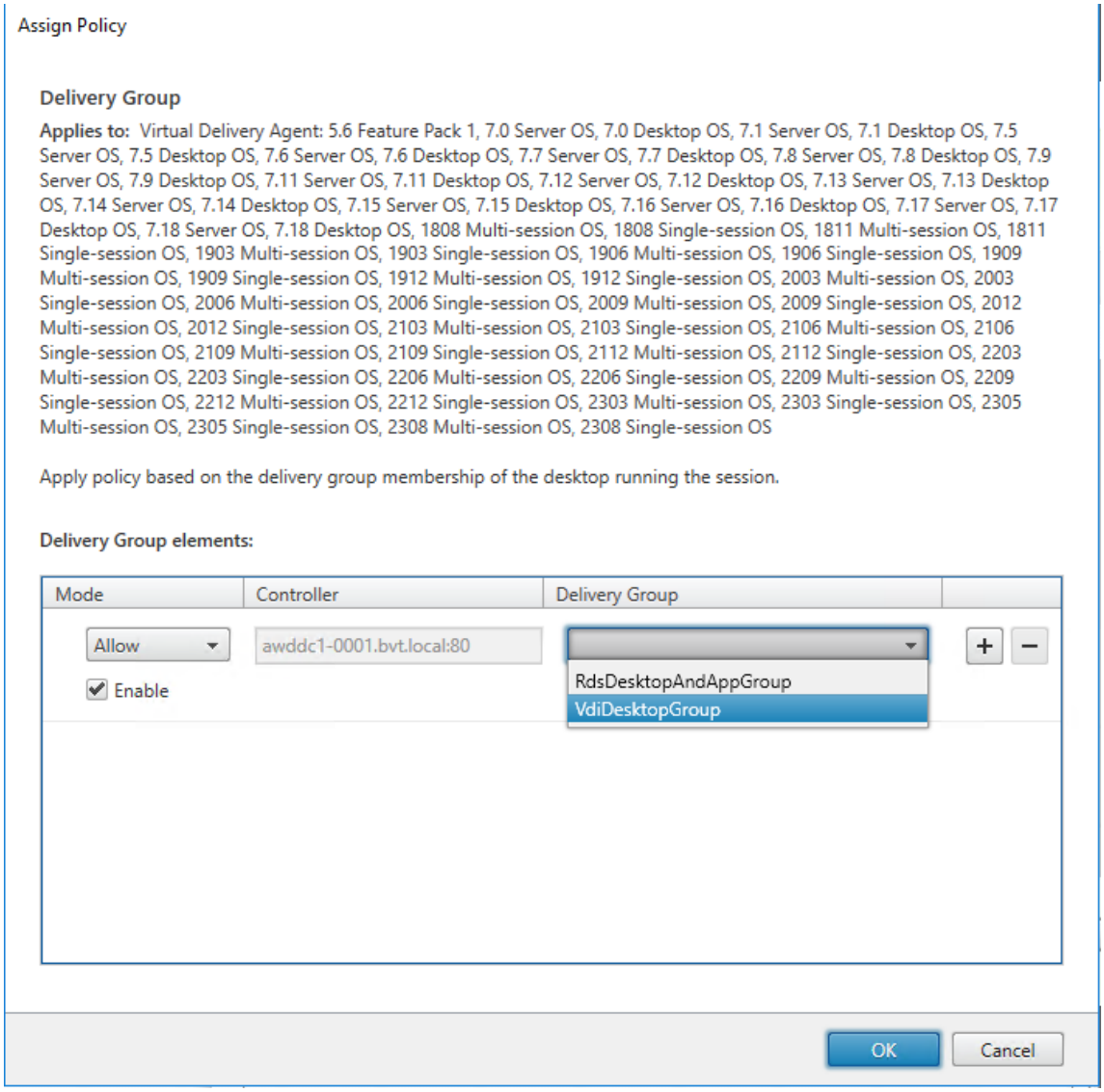
Hinweis:

- Jeder Eintrag darf nur eine Funktion enthalten.
- Der Name der Funktion darf kein Leerzeichen enthalten.
- Achten Sie auf eine richtige Schreibweise der Werte. Falsch geschriebene Werte führen dazu, dass die Sitzung beendet wird.
- Werte ohne das Präfix Windows-, Linux- oder Mac- werden ignoriert.

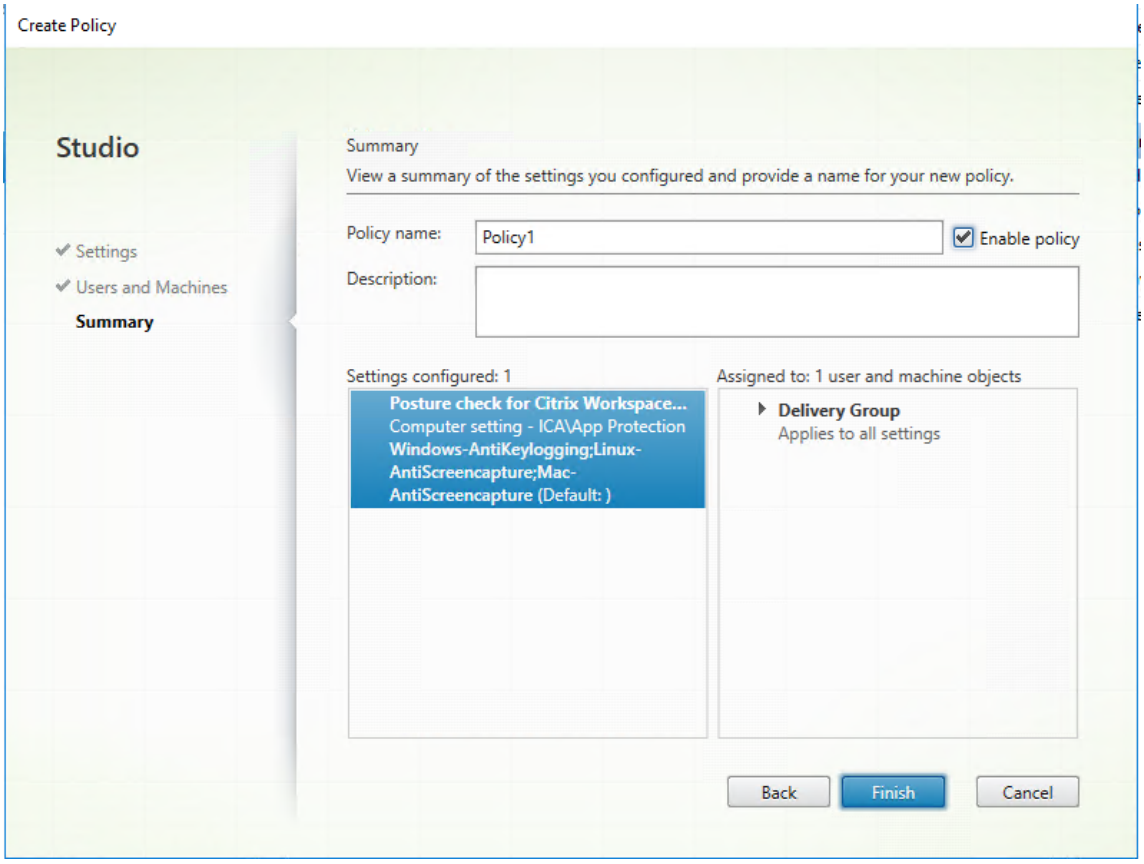
7. Nachdem Sie alle erforderlichen Werte hinzugefügt haben, klicken Sie auf **OK**.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie **Richtlinie zuweisen zu** > **Ausgewählte Benutzer- und Maschinenobjekte**.



10. Wählen Sie die erforderlichen Bereitstellungsgruppen, in denen diese Richtlinie bereitgestellt werden muss, und klicken Sie auf **OK**.



11. Klicken Sie auf **Weiter**.
12. Geben Sie den Richtliniennamen in das Feld **Richtlinienname** ein und aktivieren Sie das Kontrollkästchen **Richtlinie aktivieren**.

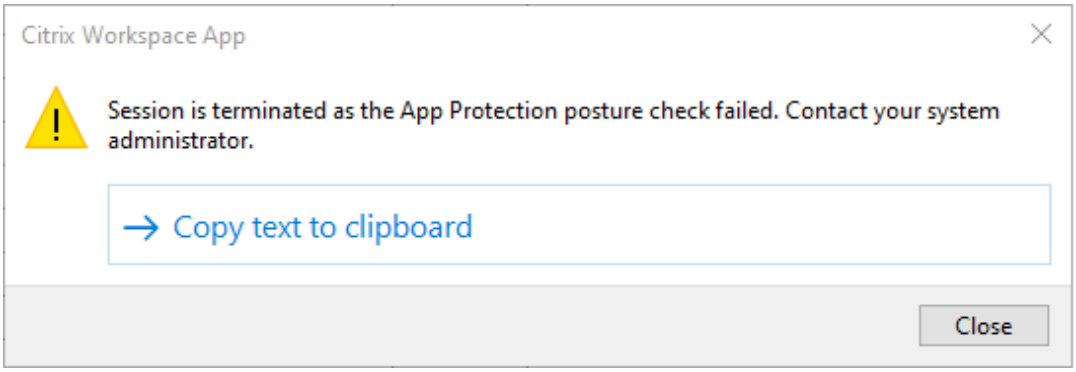


13. Klicken Sie auf **Fertig stellen**.

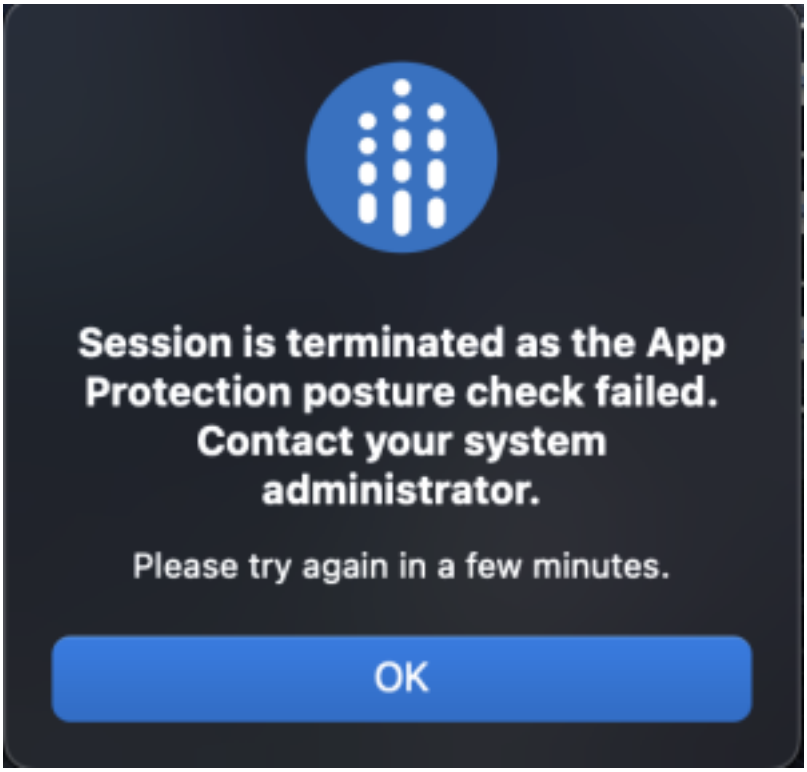
Eine Richtlinie für Posture Check wurde erstellt.

Erwartetes Verhalten beim Fehlschlagen der Statusprüfung für App Protection

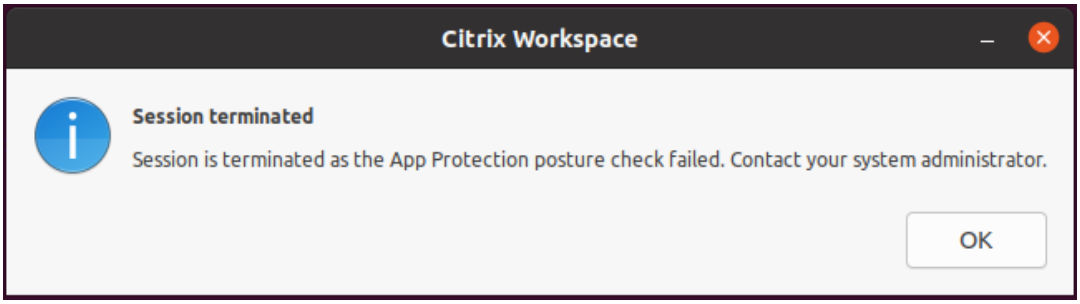
- Wenn Sie bei aktivierter VDA-Citrix-Richtlinie zur Statusprüfung eine Version der Citrix Workspace-App verwenden, die Posture Check nicht unterstützt, wird die Sitzung ohne Fehlermeldung beendet.
- Wenn Sie eine Version der Citrix Workspace-App verwenden, die Posture Check unterstützt, wird die Sitzung beendet, und es werden jeweils die folgenden Fehlermeldungen angezeigt:
  - Windows:



- Mac



- Linux



DoubleHop-Start blockieren

March 11, 2024

Um den Double-Hop-Start zu blockieren, führen Sie die Citrix Workspace-App für Windows 2309 oder höher am ersten Hop aus.

Stellen Sie im ersten Hop die folgenden Konfigurationen für alle VDAs bereit:

1. Aktualisieren Sie die neuesten GPO-Richtlinien. Weitere Informationen finden Sie unter Aktuelle GPO-Richtlinien aktualisieren.
2. Starten Sie den **Gruppenrichtlinien-Editor** und gehen Sie zu **Computerkonfiguration** > **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **App Protection** > **DoubleHop-Start blockieren**.
3. Wählen Sie **Aktiviert** und klicken Sie auf **OK**.

   Die Einstellung **DoubleHop-Start blockieren** ist aktiviert und die Ausführung von Double-Hop-Starts wird blockiert.

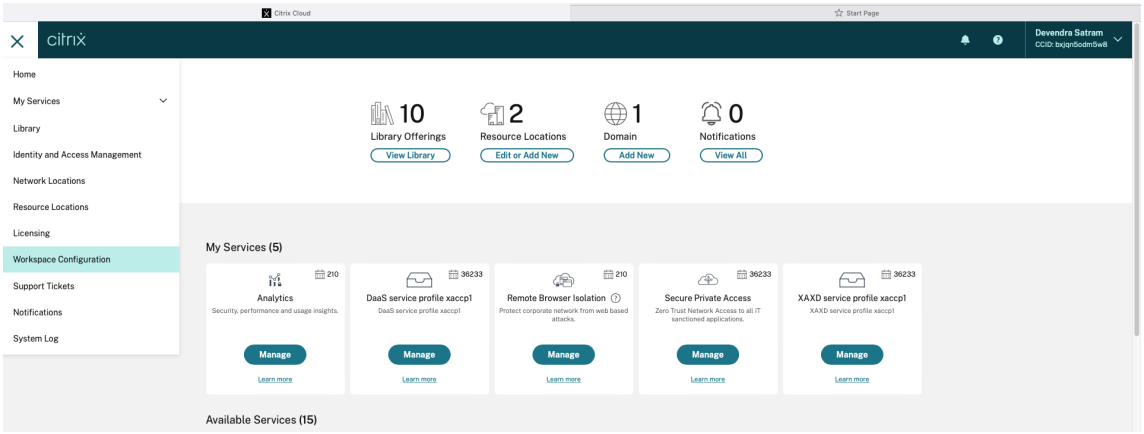
> **Hinweis:**
>
> Windows Server OS unterstützt App Protection nicht. Daher werden die Virtual Apps and Desktops, die mit App Protection aktiviert sind, nicht angezeigt, wenn Sie im ersten Hop ein Windows-Serverbetriebssystem ausführen.

Positivliste für Screenshots konfigurieren

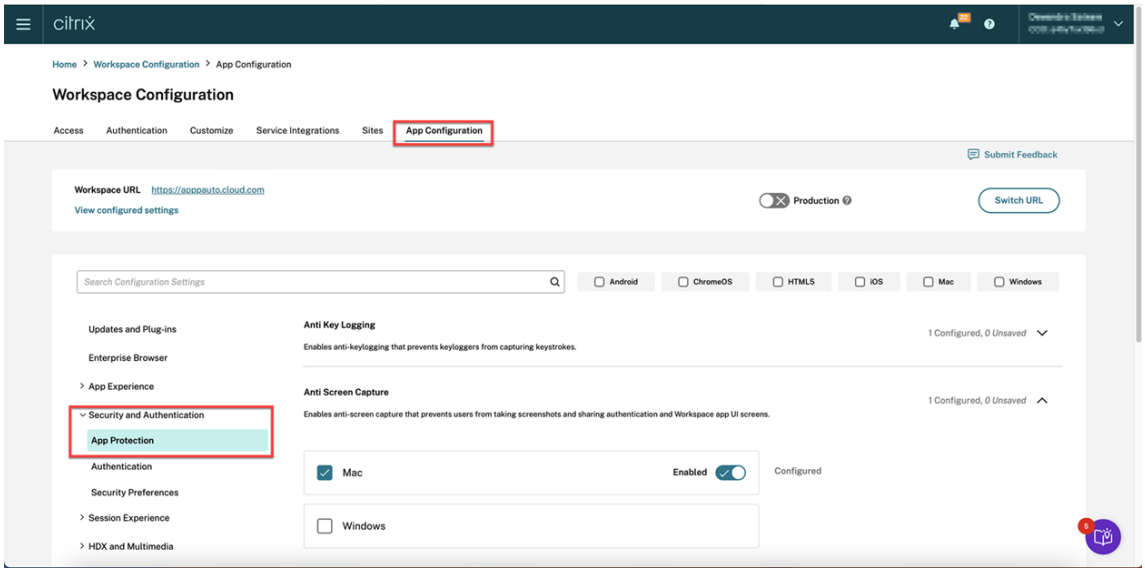
April 25, 2024

Gehen Sie wie folgt vor, um eine App zur Positivliste für Screenshots hinzuzufügen:

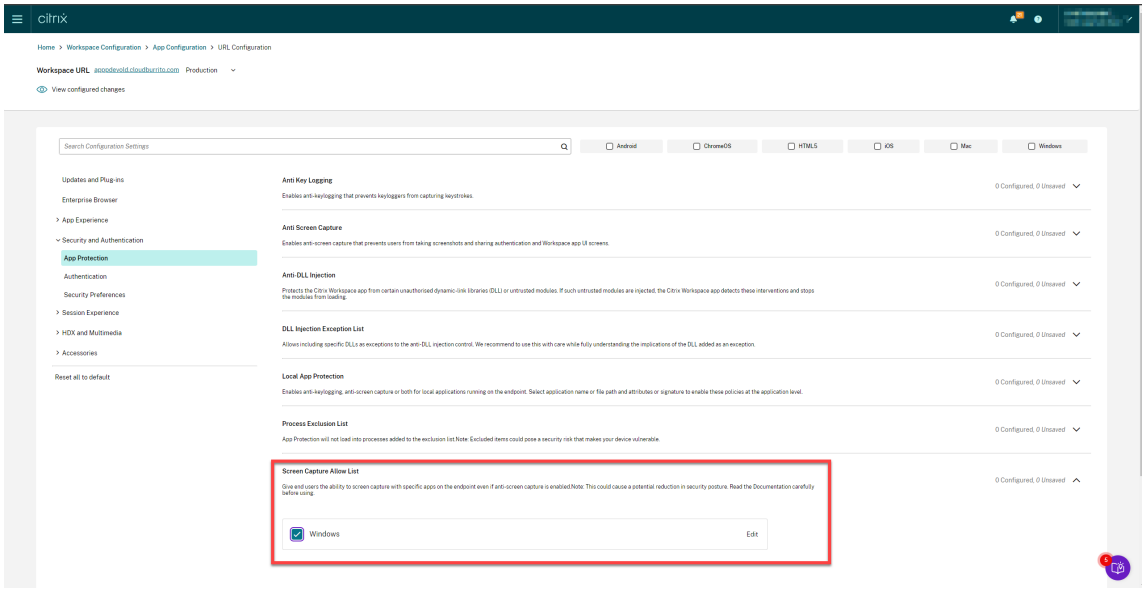
1. Melden Sie sich an Ihrem Citrix Cloud-Konto an und wählen Sie **Workspacekonfiguration**.



2. Wählen Sie **App-Konfiguration** > **Sicherheit und Authentifizierung** > **Konfigurieren** > **App Protection**.



3. Klicken Sie auf **Positivliste für Screenshots** und aktivieren Sie das Kontrollkästchen **Windows**.



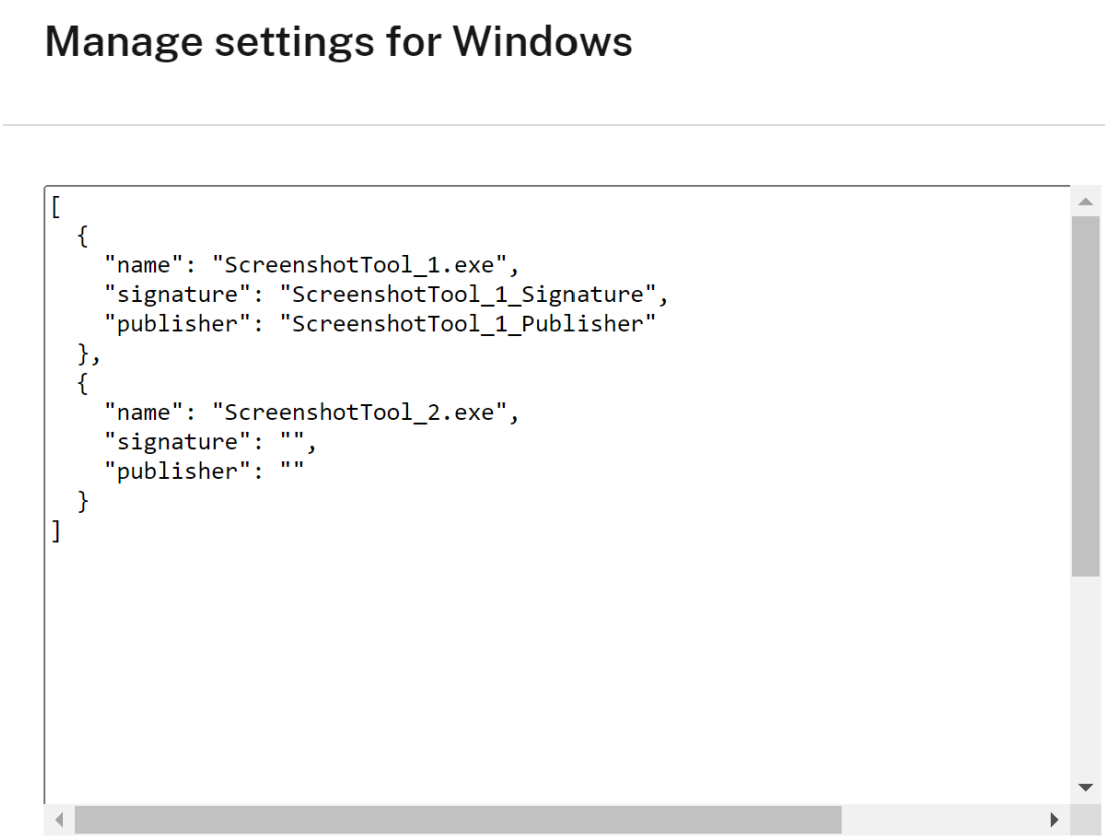
4. Klicken Sie auf die Option **Bearbeiten**.

   Der Bildschirm **Einstellungen für Windows verwalten** wird angezeigt.

5. Fügen Sie die Informationen zu der App hinzu, die Sie zur Positivliste für Screenshots hinzufügen möchten.

   Zum Beispiel:

```
[
 {

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

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

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

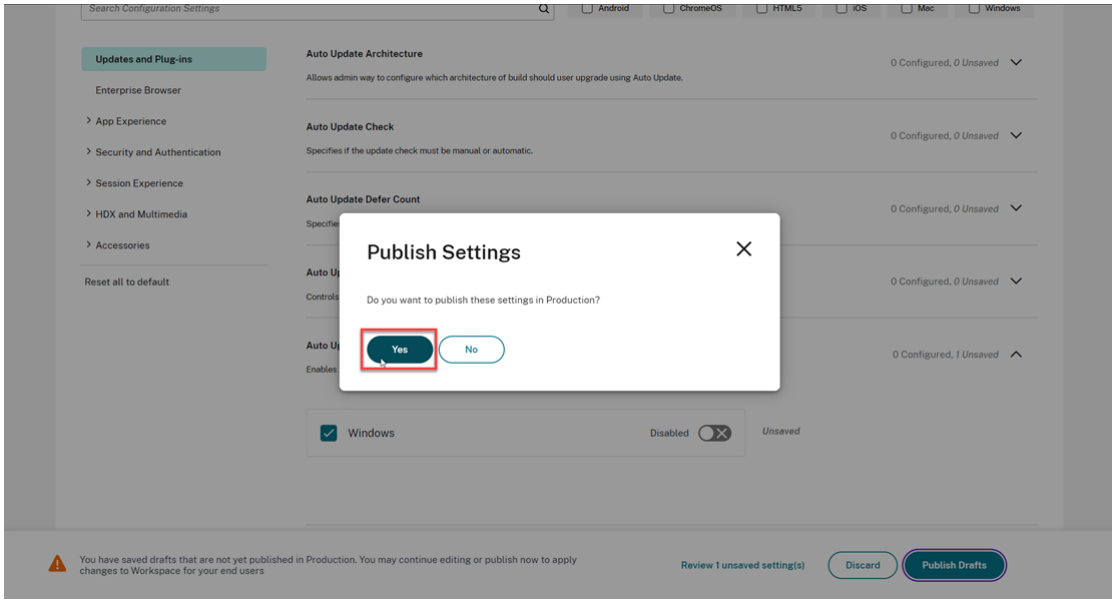



Hinweis:

- Das `name` muss zwingend ausgefüllt werden. Andererseits sind `publisher` und `signature` nicht erforderlich. Es wird jedoch empfohlen, die entsprechenden Werte für `publisher` und `signature` hinzuzufügen, um sicherzustellen, dass nur die App auf der Positivliste die Screenshots aufnehmen kann.
- Ohne Werte für `publisher` und `signature` kann eine schädliche Anwendung mit demselben Namen Screenshots aufnehmen.
- Sie können auch mehrere Apps zur Positivliste für Screenshots hinzufügen, indem Sie diesem Block mehrere Einträge hinzufügen.

Informationen zum Abrufen der Informationen für `publisher` und `signature` finden Sie im Abschnitt Informationen für `publisher` und `signature` abrufen.

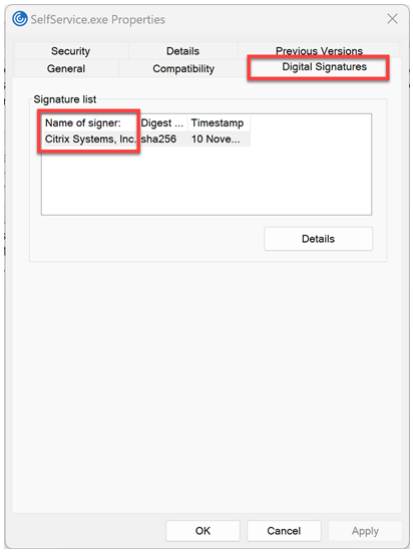
6. Klicken Sie auf **Entwurf speichern** und dann auf **Entwürfe veröffentlichen**.
7. Klicken Sie im Dialogfeld **Einstellungen veröffentlichen** auf **Ja**.



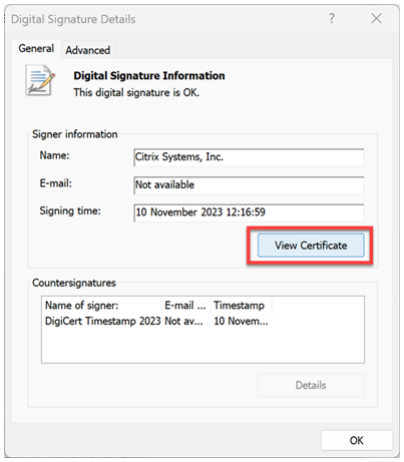
Informationen für `publisher` und `signature` abrufen

Gehen Sie wie folgt vor, um die Informationen für `publisher` und `signature` abzurufen:

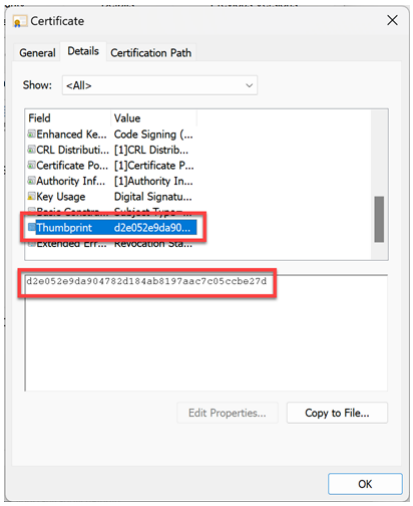
1. Öffnen Sie den Dateispeicherort, an dem die entsprechende `.exe`-Datei der App abgelegt ist.
2. Klicken Sie mit der rechten Maustaste auf die `.exe`-Datei und dann auf **Eigenschaften**. Ein Popup-Fenster mit den Eigenschaften wird angezeigt.
3. Klicken Sie auf **Digitale Signaturen**. Der **Name des Unterzeichners** ist der Wert für `publisher`.



4. Klicken Sie auf den ersten Eintrag in **Namen des Unterzeichners** und dann auf **Details** > **Zertifikat anzeigen**.



5. Klicken Sie auf **Details** > **Fingerabdruck**. Der Inhalt, der im Textfeld angezeigt wird, ist die `signature`.

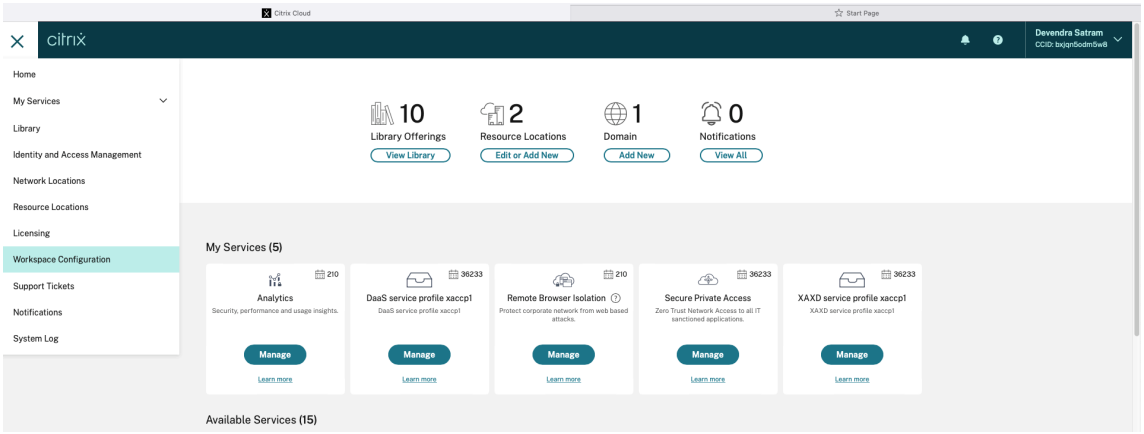


Prozessausschlussliste konfigurieren

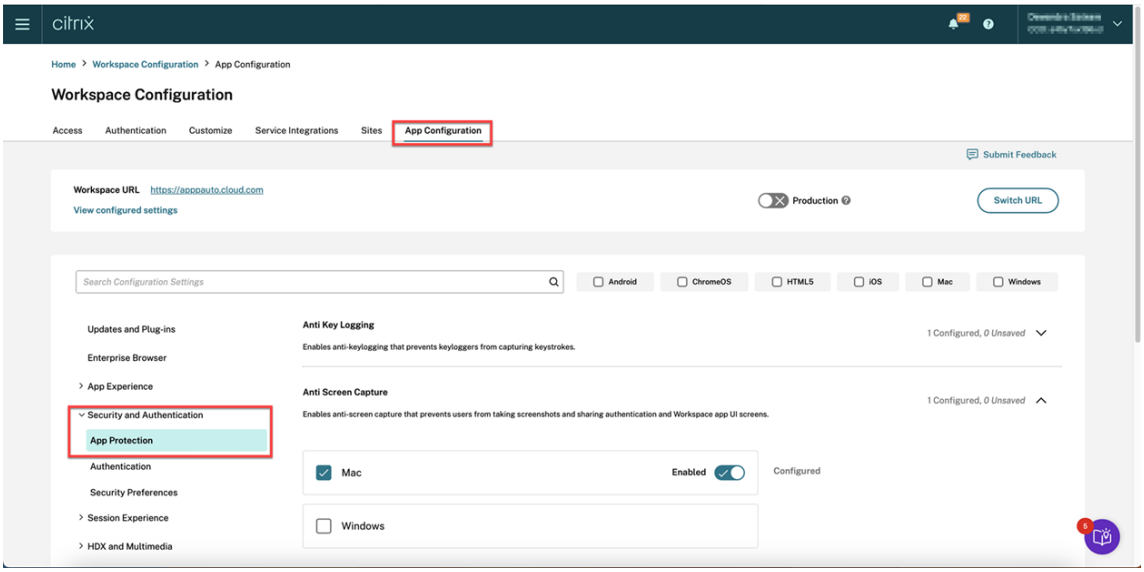
April 29, 2024

Gehen Sie wie folgt vor, um einen Prozess zur Prozessausschlussliste hinzuzufügen:

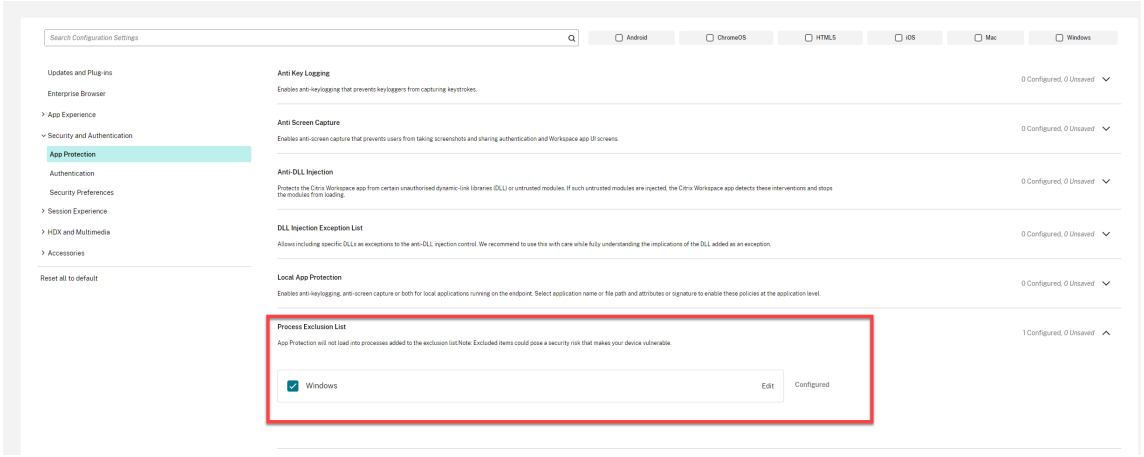
1. Melden Sie sich an Ihrem Citrix Cloud-Konto an und wählen Sie **Workspacekonfiguration**.



2. Wählen Sie **App-Konfiguration** > **Sicherheit und Authentifizierung** > **Konfigurieren** > **App Protection**.



3. Klicken Sie auf **Prozessausschlussliste** und aktivieren Sie dann das Kontrollkästchen **Windows**.



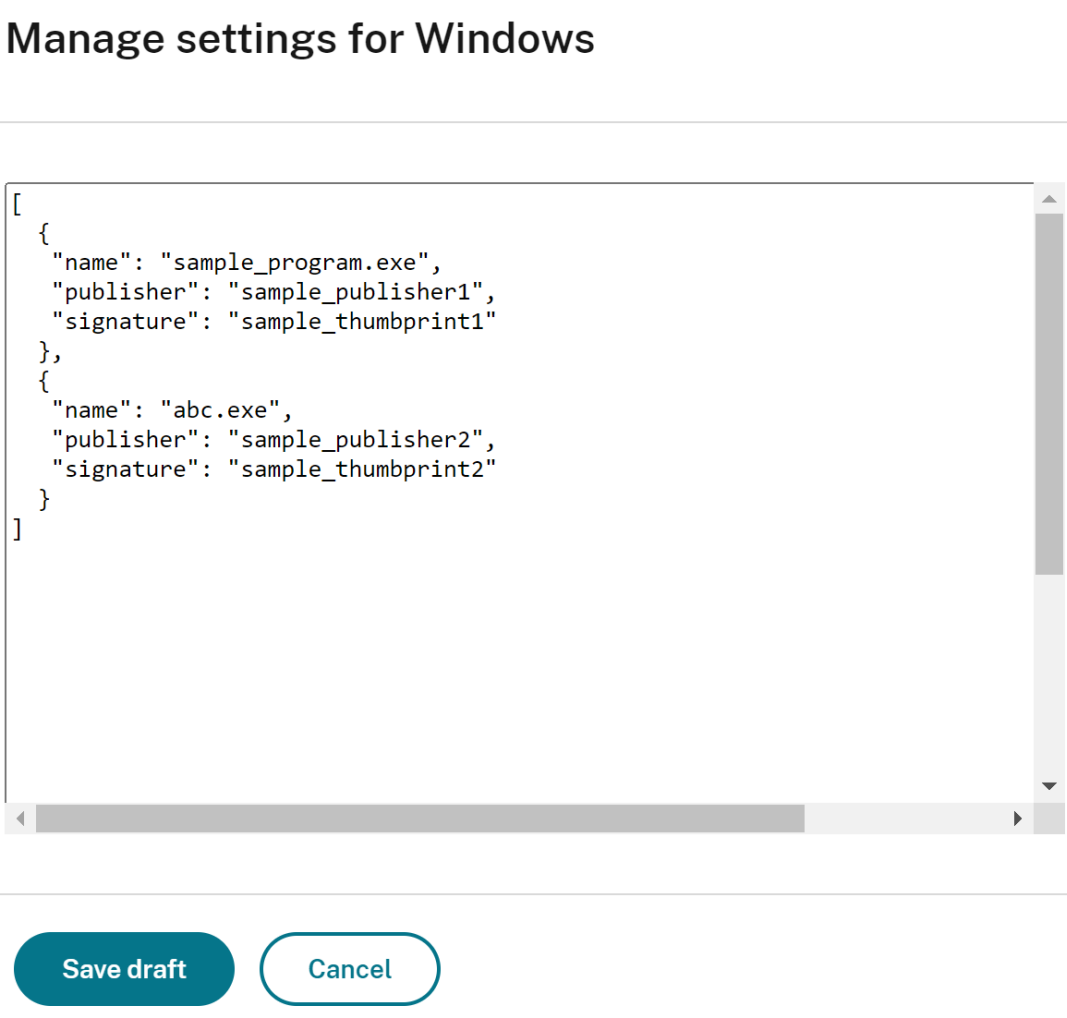
4. Klicken Sie auf die Option **Bearbeiten**.

   Der Bildschirm **Einstellungen für Windows verwalten** wird angezeigt.

5. Fügen Sie die Informationen über den Prozess hinzu, den Sie zur Prozessausschlussliste hinzufügen möchten.

   Zum Beispiel:

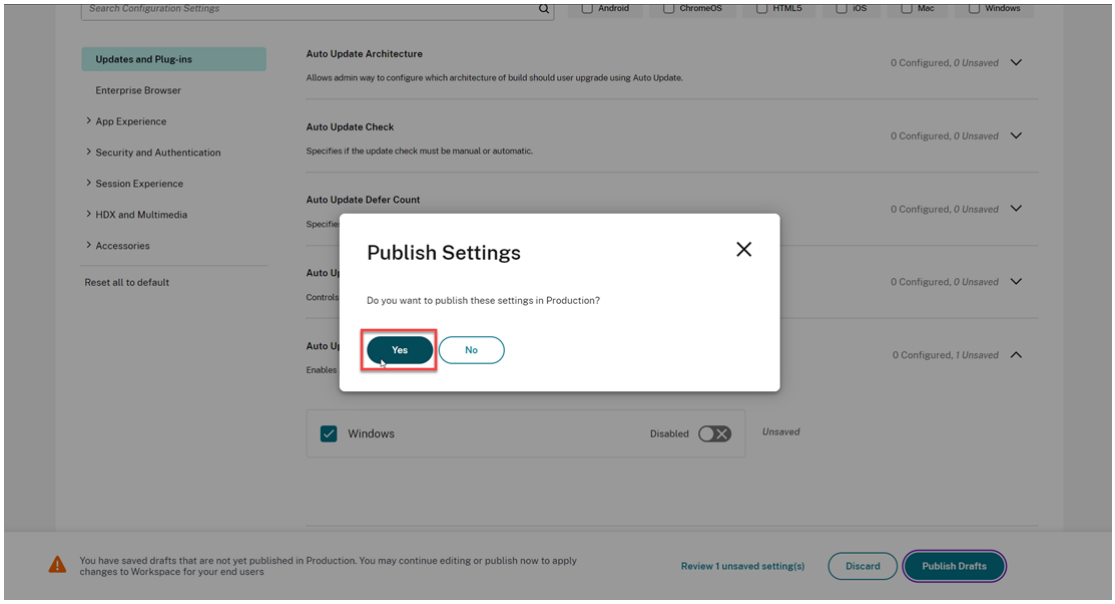
```
[
 {

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

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



> **Hinweis:**
>
> - Das `name` muss zwingend ausgefüllt werden. Andererseits sind `publisher` und `signature` nicht erforderlich. Es wird jedoch empfohlen, `signature` und `publisher` hinzuzufügen, um sicherzustellen, dass der richtige Prozess zur Liste hinzugefügt wird.
> - Sie können der Prozessausschlussliste auch mehrere Prozesse hinzufügen, indem Sie diesem Block mehrere Einträge hinzufügen.

Informationen zum Abrufen der Informationen für `publisher` und `signature` finden Sie im Abschnitt Informationen für `publisher` und `signature` abrufen.

6. Klicken Sie auf **Entwurf speichern** und dann auf **Entwürfe veröffentlichen**.
7. Klicken Sie im Dialogfeld **Einstellungen veröffentlichen** auf **Ja**.



8. Starten Sie die Citrix Workspace-App neu.

Ausschlussliste für USB-Filtertreiber konfigurieren

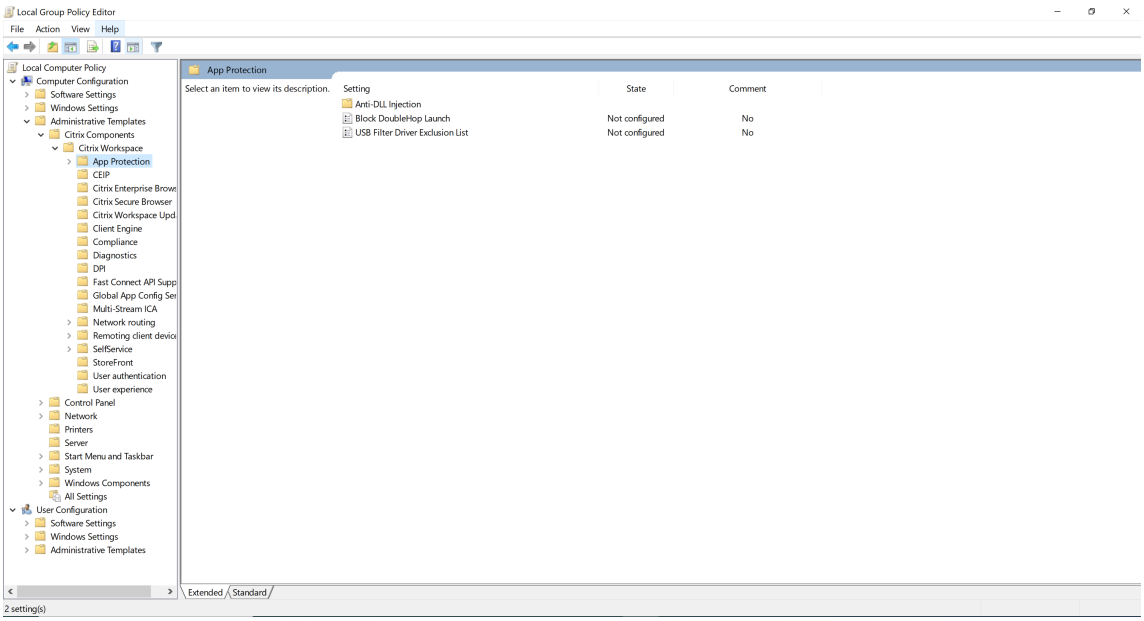
April 29, 2024

Sie können ein USB-Gerät mit einer der folgenden Methoden zur Ausschlussliste für USB-Filtertreiber hinzufügen:

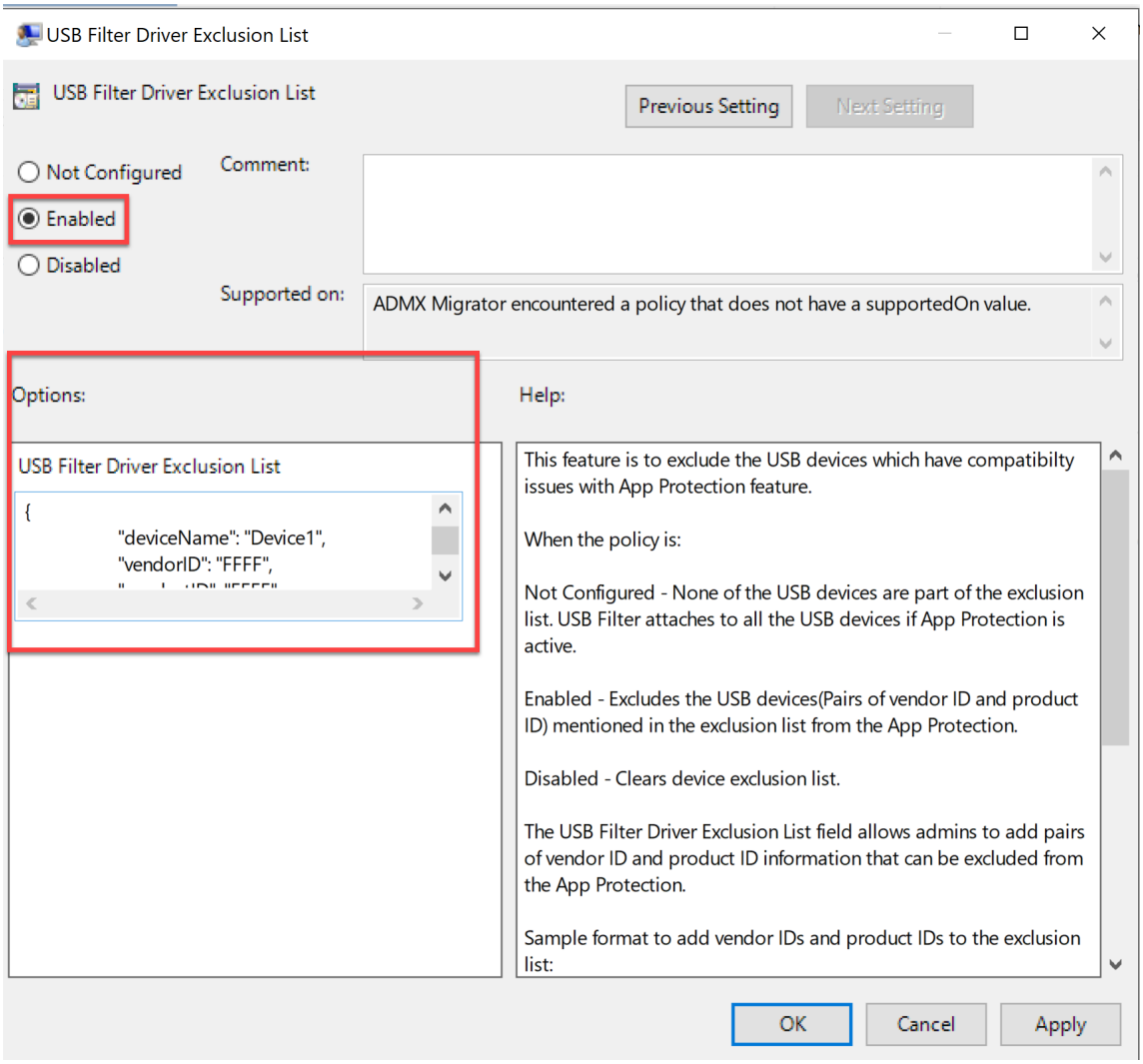
- Gruppenrichtlinienobjekt verwenden
- Benutzeroberfläche des Global App Configuration Service verwenden

Gruppenrichtlinienobjekt verwenden

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen. Weitere Informationen finden Sie unter Gruppenrichtlinienobjekt.
2. Gehen Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **App Protection** > **Ausschlussliste für USB-Filtertreiber**.



3. Wählen Sie **Aktiviert** aus und geben Sie die **Anbieter-ID** und die **Produkt-ID** des USB-Geräts, das Sie ausschließen möchten, in das Textfeld **Optionen** ein.



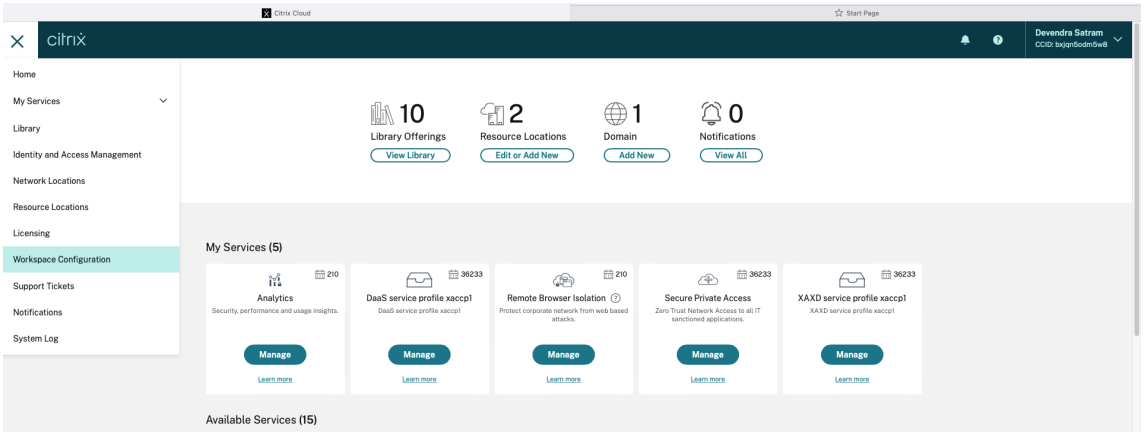
> **Hinweis:**
>
> - Die Felder `productID` und `vendorID` sind erforderlich und müssen ausgefüllt werden. Andererseits ist `deviceName` nicht erforderlich.
> - Sie können der Ausschlussliste auch mehrere USB-Geräte hinzufügen, indem Sie diesem Block mehrere Einträge hinzufügen.

Informationen zum Abrufen von `productID` und `vendorID` finden Sie unter `productID` und abrufen`vendorID`.

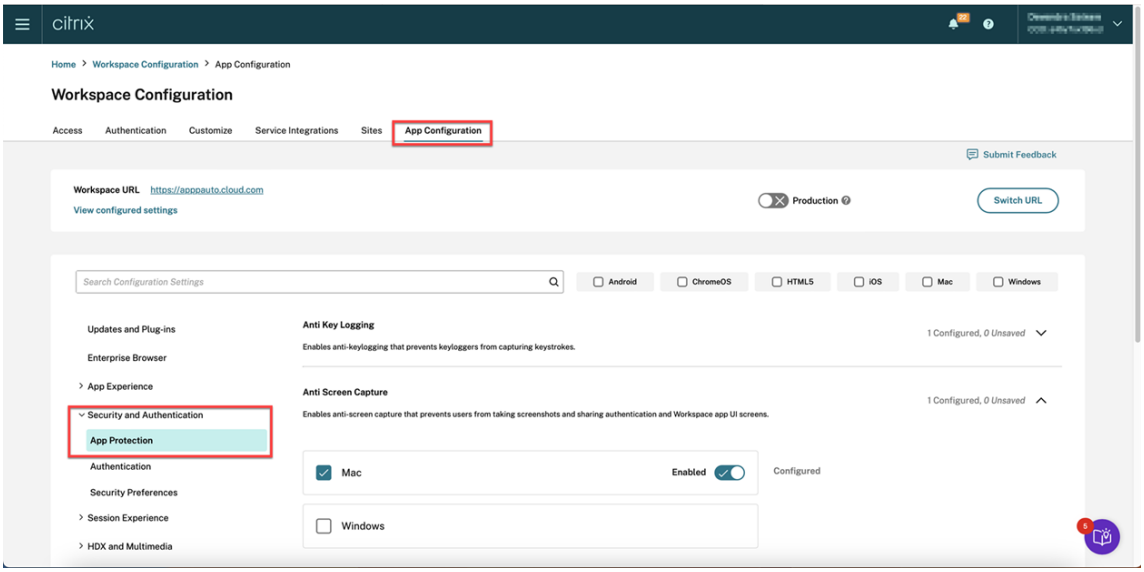
4. Klicken Sie auf **OK**.

Benutzeroberfläche des Global App Configuration Service verwenden

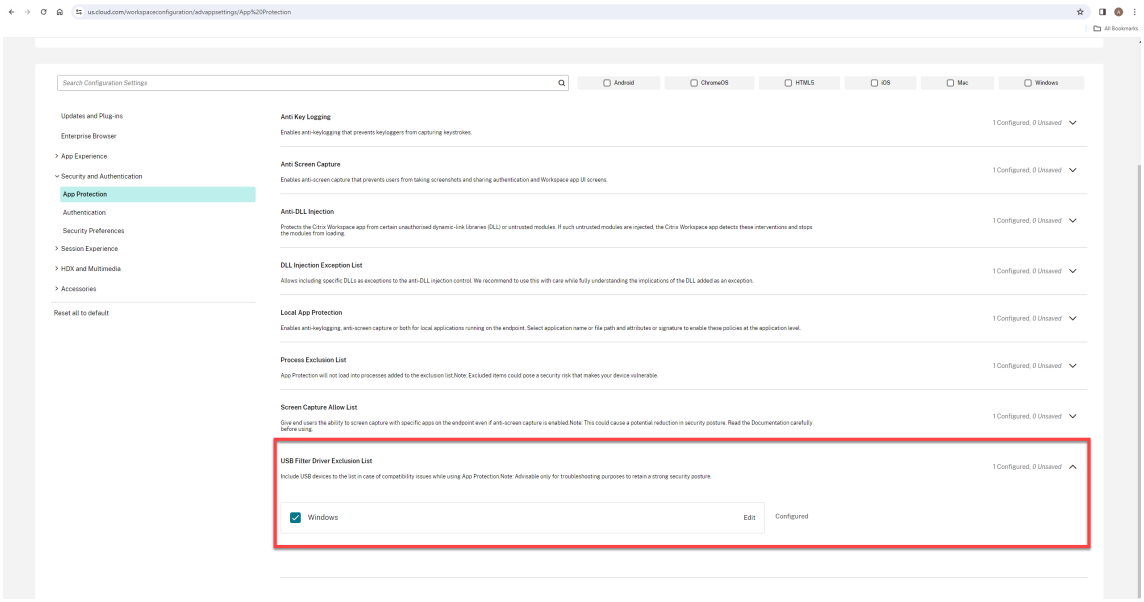
1. Melden Sie sich an Ihrem Citrix Cloud-Konto an und wählen Sie **Workspacekonfiguration**.



2. Wählen Sie **App-Konfiguration** > **Sicherheit und Authentifizierung** > **Konfigurieren** > **App Protection**.



3. Klicken Sie auf **Ausschlussliste für USB-Filtertreiber** und aktivieren Sie dann das Kontrollkästchen **Windows**.



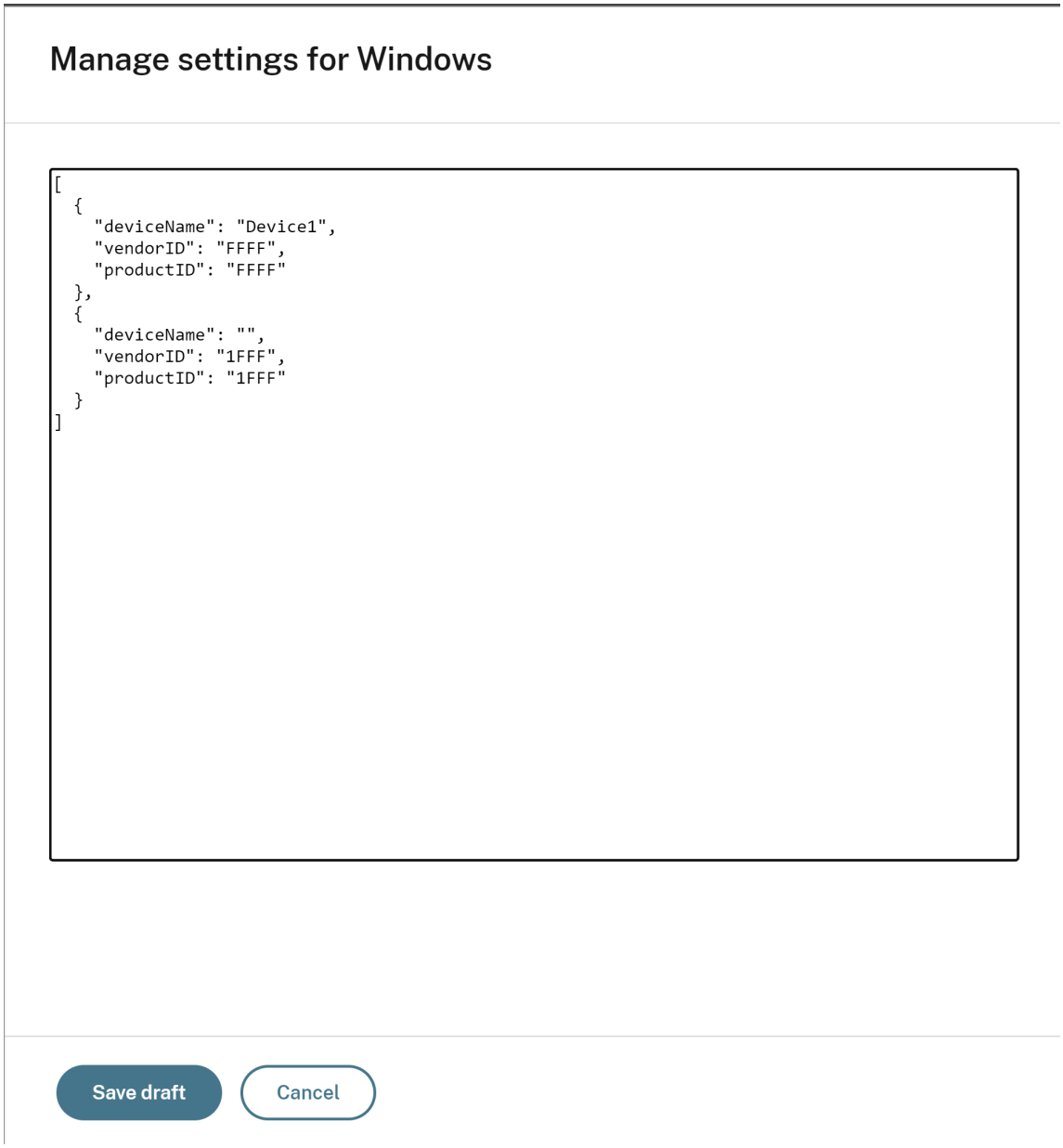
4. Klicken Sie auf die Option **Bearbeiten**.

   Der Bildschirm **Einstellungen für Windows verwalten** wird angezeigt.

5. Fügen Sie die Informationen über den Prozess oder die App hinzu, die Sie zur Ausschlussliste für USB-Filtertreiber hinzufügen möchten.

   Zum Beispiel:

```
[
 {

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

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

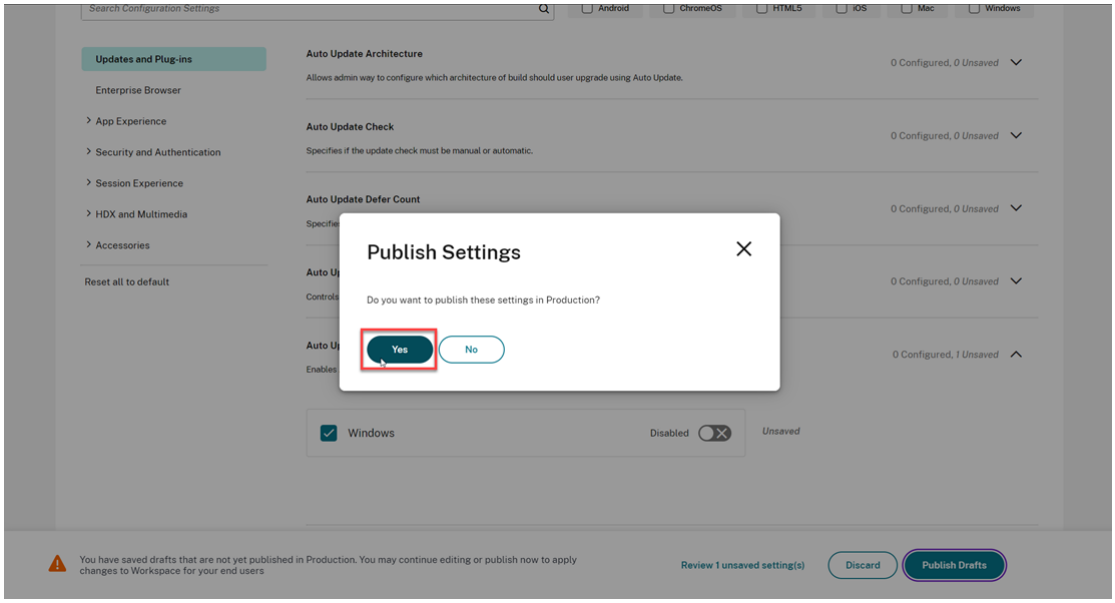



Hinweis:

- Die Felder `productID` und `vendorID` sind erforderlich und müssen ausgefüllt werden. Andererseits ist `deviceName` nicht erforderlich.
- Sie können der Ausschlussliste auch mehrere USB-Geräte hinzufügen, indem Sie diesem Block mehrere Einträge hinzufügen.

Informationen zum Abrufen von `productID` und `vendorID` finden Sie unter `productID` und abrufen`vendorID`.

6. Klicken Sie auf **Entwurf speichern** und dann auf **Entwürfe veröffentlichen**.
7. Klicken Sie im Dialogfeld **Einstellungen veröffentlichen** auf **Ja**.

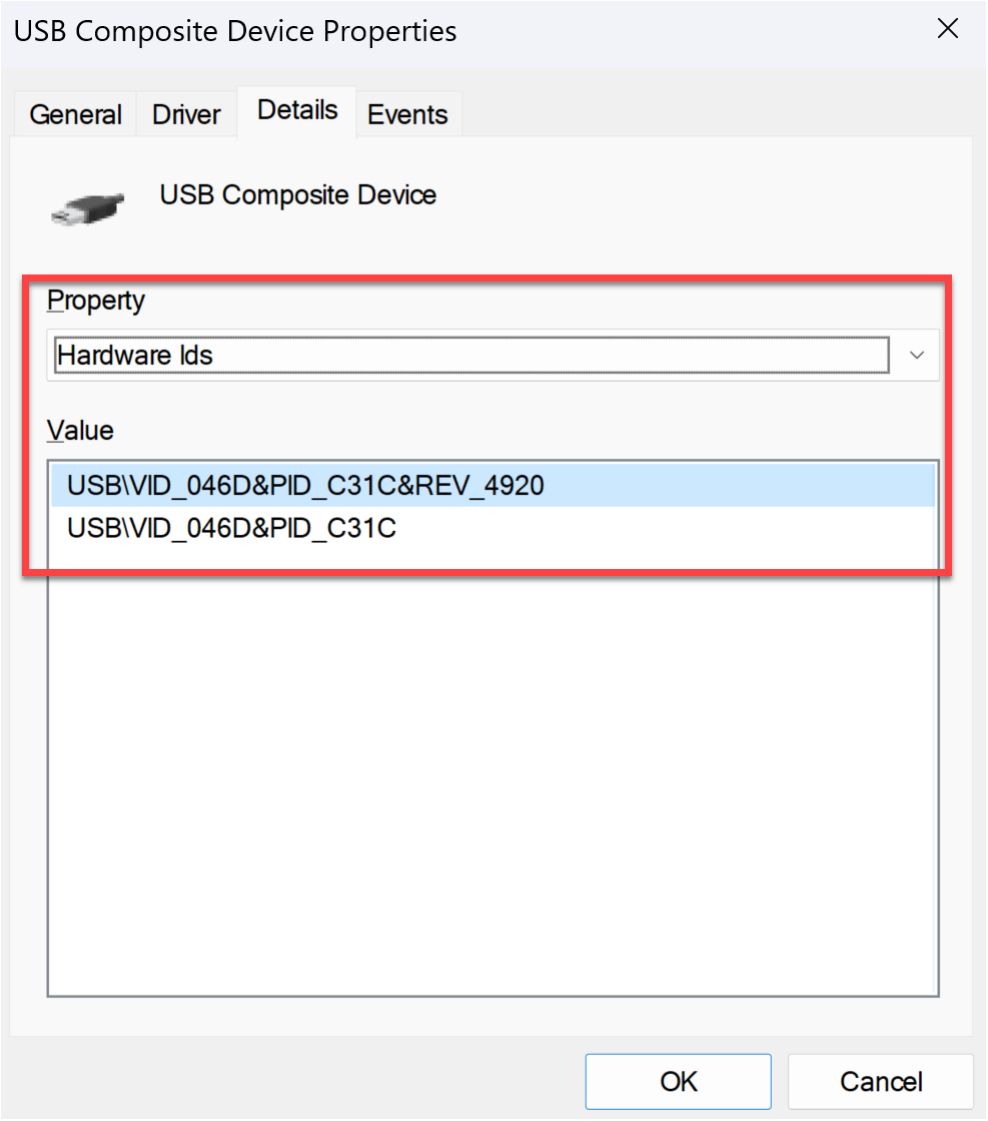


8. Starten Sie die Citrix Workspace-App neu.

`productID` und `vendorID` abrufen

Gehen Sie wie folgt vor, um `productID` und `vendorID` abzurufen:

1. Öffnen Sie den **Geräte-Manager** und suchen Sie das Gerät, das Sie zur Ausschlussliste hinzufügen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Gerätenamen und klicken Sie dann auf **Eigenschaften**. Ein Popup-Fenster mit den Eigenschaften wird angezeigt.
3. Klicken Sie auf **Details** und wählen Sie dann die Option **Hardware-IDs** aus der Liste **Eigenschaft** aus.
4. Im Feld **Wert** ist der Wert mit dem Präfix `VID_` die `vendorID` und der Wert mit dem Präfix `PID_` die `productID`



Problembehandlung

March 11, 2024

In diesem Artikel wird erläutert, wie Sie Probleme mit App Protection auf verschiedenen Plattformen für die Citrix Workspace-App beheben.

Problembehandlungsszenarien finden Sie in den folgenden Abschnitten:

- Allgemeine Problembehandlungsszenarien
- Erkennung von Richtlinienmanipulationen
- App Protection Posture Check

Citrix Workspace-App für Windows

1. Sammeln Sie Protokolle wie unter Protokollsammlung beschrieben.
2. Drücken Sie **Win + R**, um das Feld "Ausführen"zu öffnen, geben Sie `cmd` ein und drücken Sie die **Eingabetaste**.
3. Führen Sie die folgenden Befehle aus:
   - Wenn Sie die Citrix Workspace-App für Windows vor Version 2311 verwenden, führen Sie die folgenden Befehle aus:
     - `sc query appprotectionsvc`
     - `sc query entryprotectdrv`
     - `sc query epinject6`
     - `sc query epusbfilter`
   - Wenn Sie die Citrix Workspace-App für Windows Version 2311 oder später verwenden, führen Sie die folgenden Befehle aus:
     - `sc query appprotectionsvc`
     - `sc query ctxapdriver`
     - `sc query ctxapinject`
     - `sc query ctxapusbfilter`

Stellen Sie die Ergebnisse und die mit dem Protokollsammlungstool gesammelten Tracingberichte zur Verfügung.

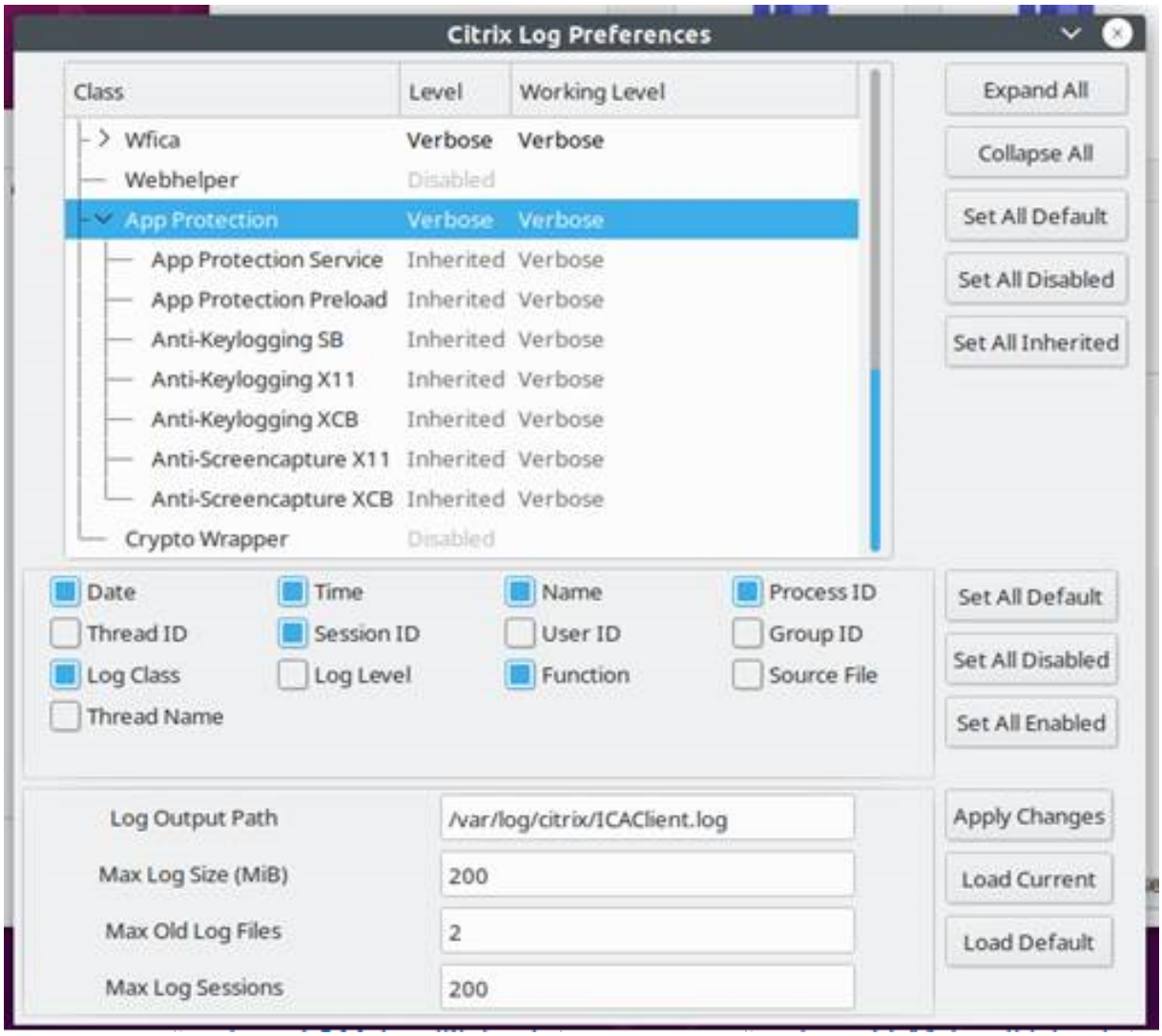
Citrix Workspace-App für Mac

Sammeln Sie die Protokolle wie unter Protokollsammlung beschrieben und stellen Sie sie zur Verfügung.

Citrix Workspace-App für Linux

1. Führen Sie die ausführbare Datei set log aus, die sich im Ordner *util* der Installation befindet. Beispiel: `/opt/Citrix/ICAClient/util/setlog`.
2. Klicken Sie auf **Alle deaktivieren** (Dieser Schritt ist optional und stellt sicher, dass nur die erforderlichen Protokolle erfasst werden).
3. Gehen Sie in App Protection zu Protokollierung.
4. Stellen Sie die Protokollebene in App Protection auf "Ausführlich"ein, indem Sie mit der rechten Maustaste klicken und "Ausführlich"auswählen (nur Warnungen und Fehler werden protokolliert).

5. Erweitern Sie die Klasse “App Protection”und klicken Sie mit der rechten Maustaste auf das untergeordnete Element. Wählen Sie **Gruppe > Geerbt** aus.
6. Aktivieren Sie Protokolle für **wfica**. Klicken Sie mit der rechten Maustaste auf **wfica** und wählen Sie **Ausführlich** aus. Wenn App Protection nicht installiert ist oder von **wfica** nicht erkannt werden kann, erhalten Sie das Protokoll als **[NCS] < P3563 > citrix-wfica: App Protection is not installed**.
7. Wenn Sie die Sitzung starten, werden die Protokolle in der Datei aufgezeichnet, die im *Protokollausgabepfad* des eingestellten Protokolls angegeben ist.



Allgemeine Problembehandlung

March 11, 2024

Ressourcen, für die App Protection-Richtlinien aktiviert wurden, werden in nativen Apps nicht angezeigt

Wenn die mit App Protection-Richtlinien aktivierten Ressourcen in den nativen Apps nicht angezeigt werden, gehen Sie wie folgt vor:

1. Aktualisieren Sie Ihre Citrix Workspace-App auf eine höhere Version, wenn sie älter als die folgende ist:
    - Citrix Workspace-App 2108 für Linux
    - Citrix Workspace-App 2203.1 LTSR für Windows
    - Citrix Workspace-App 2002 für Windows
    - Citrix Workspace-App 2305.1 für Windows (Store)
    - Citrix Workspace-App 2001 für Mac
2. Achten Sie darauf, dass die Citrix Workspace-App nicht in einem Windows-Multisitzungsbetriebssystem wie Windows 2K16 oder Windows 2K22 installiert ist.
3. Wenn die oben genannten Bedingungen erfüllt sind, die Ressourcen jedoch immer noch nicht angezeigt werden, sammeln Sie die Protokolle und wenden Sie sich an den technischen Support von Citrix. Weitere Informationen zum Sammeln von Protokollen finden Sie unter Protokollsammlung.

Ressourcen, für die App Protection-Richtlinien aktiviert sind, werden im Browser nicht angezeigt, wenn Sie den On-Premises-Store verwenden

Wenn die mit App Protection-Richtlinien aktivierten Ressourcen nicht im Browser angezeigt werden, während Sie den On-Premises-Store verwenden, gehen Sie wie folgt vor:

1. Achten Sie darauf, dass Ihre Delivery Controller-Version nicht niedriger als 1912 ist.

    > **Hinweis:**
    >
    > App Protection wird nicht unterstützt, wenn Sie einen Delivery Controller vor Version 1912 verwenden.

2. Wenn Sie StoreFront-Versionen zwischen 1912 und 2203 verwenden, überprüfen Sie, ob Sie die StoreFront-Anpassung aktiviert haben. Weitere Informationen zum Aktivieren der StoreFront-Anpassung finden Sie unter StoreFront-Anpassung aktivieren.
3. Wenn Sie StoreFront Version 2308 oder höher verwenden, müssen Sie die StoreFront-Anpassung nicht aktivieren. Überprüfen Sie anhand von Hybrider Start über StoreFront Version 2308 oder höher, ob Sie App Protection für den Hybridstart auf StoreFront korrekt aktiviert haben.

4. Überprüfen Sie, ob Sie die App Protection-Features für die Bereitstellungsgruppe korrekt aktiviert haben.
5. Wenn die oben genannten Bedingungen erfüllt sind, die Ressourcen jedoch immer noch nicht angezeigt werden, sammeln Sie die Protokolle und wenden Sie sich an den technischen Support von Citrix. Weitere Informationen zum Sammeln von Protokollen finden Sie unter Protokolle für die Citrix Workspace-App sammeln und Protokolle für StoreFront sammeln.

Beim Starten von App Protection-fähigen Ressourcen kann keine sichere Umgebung eingerichtet werden

Für die Citrix Workspace-App für Windows muss das Kontrollkästchen **App Protection nach der Installation starten** während der Installation aktiviert werden, um sicherzustellen, dass die App Protection-Dienste gestartet werden und die sichere Umgebung eingerichtet wird. Wenn Sie während der Installation das Kontrollkästchen **App Protection nach der Installation starten** nicht aktiviert haben, wird der App Protection-Dienst automatisch gestartet, sobald Sie eine Ressource starten, für die App Protection-Richtlinien aktiviert sind. Je nach Systemlast kann es einige Zeit dauern, bis App Protection gestartet wird. Wenn der Start nicht erfolgt, kann es zu einem Timeout kommen. Daher wird empfohlen, während der Installation das Kontrollkästchen **App Protection nach der Installation starten** zu aktivieren. In der Regel starten Sie die mit App Protection aktivierte Ressource erneut, und die sichere Verbindung muss hergestellt werden. Wenn Sie die mit App Protection aktivierte Ressource jedoch immer noch nicht starten können, gehen Sie wie folgt vor:

1. Öffnen Sie die Eingabeaufforderung als Administrator, führen Sie den folgenden Befehl aus und überprüfen Sie, ob der App Protection-Dienst ausgeführt wird:

```
sc query AppProtectionSvc
<!--NeedCopy-->
```

2. Wenn der App Protection-Dienst nicht ausgeführt wird, starten Sie ihn mit dem folgenden Befehl:

```
sc start AppProtectionSvc
<!--NeedCopy-->
```

3. Wenn der Fehler weiterhin auftritt, sammeln Sie die Protokolle und wenden Sie sich an den technischen Support von Citrix. Weitere Informationen zum Sammeln von Protokollen finden Sie unter Protokollsammlung.

App Protection kann nicht aktiviert oder deaktiviert werden

Wenn Sie App Protection für eine Bereitstellungsgruppe für On-Premise oder Cloud mit Web Studio oder PowerShell nicht aktivieren oder deaktivieren können, gehen Sie wie folgt vor:

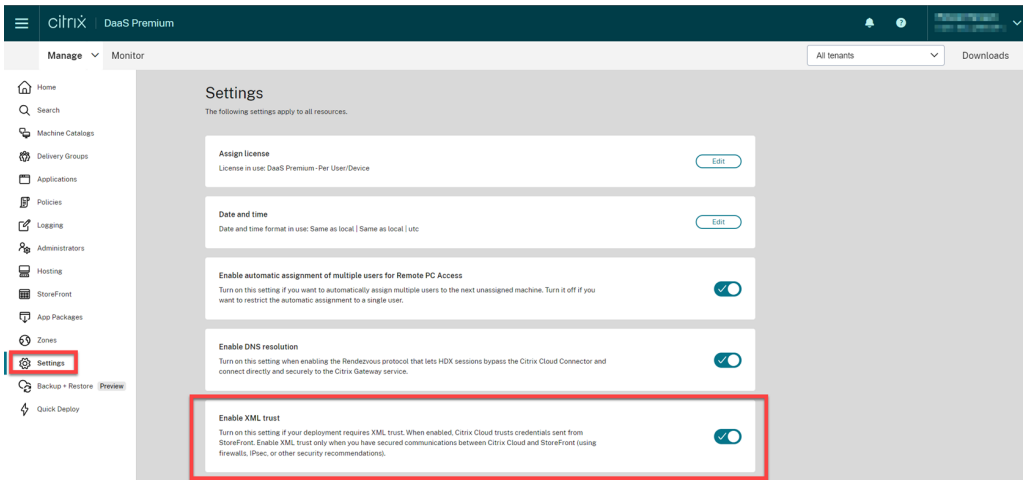
1. Prüfen Sie, ob Sie über die erforderliche Lizenz verfügen. Wenn die erforderlichen Lizenzen nicht verfügbar sind, können Sie App Protection nicht aktivieren.
2. Wenn die erforderlichen Lizenzen nicht verfügbar sind, rufen Sie die erforderlichen Lizenzen ab und fügen Sie sie hinzu.
3. Starten Sie nach dem Hinzufügen der Lizenzen den Lizenzserver neu und versuchen Sie erneut, App Protection zu aktivieren.
4. Wenn gültige Lizenzen verfügbar sind, Sie App Protection jedoch immer noch nicht aktivieren oder deaktivieren können, überprüfen Sie, ob `TrustRequestsSentToTheXmlServicePort` aktiviert ist, indem Sie den folgenden Befehl ausführen:

```
Get-BrokerSite | Select-Object
    TrustRequestsSentToTheXmlServicePort
<!--NeedCopy-->
```

5. Wenn `TrustRequestsSentToTheXmlServicePort` nicht aktiviert ist, aktivieren Sie XML-Vertrauen mit einer der folgenden Methoden:

   - **Web Studio:**

     a) Melden Sie sich bei Ihrem Citrix DaaS-Konto an und gehen Sie zu **Verwalten** > **Einstellungen** > **XML-Vertrauen aktivieren**.

     b) Aktivieren Sie den Schalter **XML-Vertrauen aktivieren**.

   - **PowerShell:** Führen Sie den folgenden Befehl aus, um XML-Vertrauen zu aktivieren:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
<!--NeedCopy-->
```

6. Nach dem Aktivieren von `TrustRequestsSentToTheXmlServicePort` aktivieren Sie App Protection erneut.

7. Wenn die oben genannten Bedingungen erfüllt sind, Sie App Protection aber immer noch nicht aktivieren oder deaktivieren können, wenden Sie sich an den technischen Support von Citrix.

App Protection-Richtlinien werden nicht ordnungsgemäß angewendet

1. Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:
   - Sie verwenden eine unterstützte Version der Citrix Workspace-App.
   - Für die Bereitstellungsgruppe sind die richtigen Features aktiviert.
   - Das Feature ist auf dem Endpunkt installiert.
   - Die Citrix Workspace-App wurde mit aktiviertem Switch `/includeappprotection` installiert.
2. Wenn die oben genannten Bedingungen erfüllt sind, die App Protection-Richtlinien jedoch immer noch nicht richtig angewendet werden, sammeln Sie die Protokolle und wenden Sie sich an den technischen Support von Citrix. Weitere Informationen zum Sammeln von Protokollen finden Sie unter Protokolle für die Citrix Workspace-App sammeln.

Keine Bildschirmerfassung in Citrix-fremden Fenstern:

- Minimieren oder schließen Sie die geschützten Citrix Fenster, einschließlich der Citrix Workspace-App.

Problembehandlung bei der Erkennung von Richtlinienmanipulationen

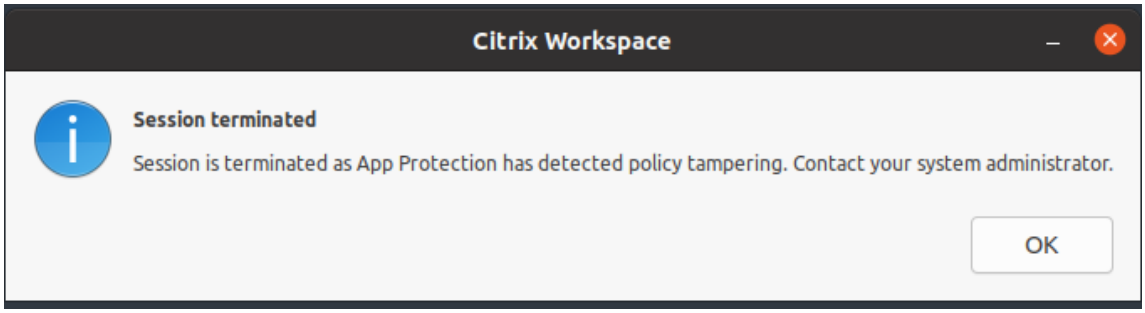
March 11, 2024

Im folgenden Abschnitt werden eventuell auftretende Probleme und Maßnahmen zu ihrer Behebung beschrieben:

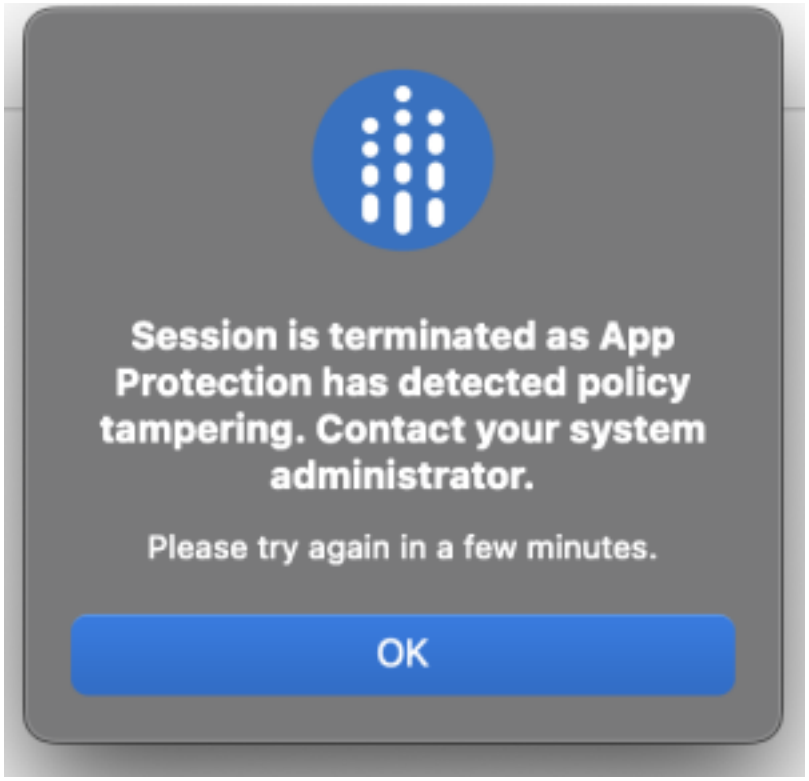
Die ICA-Datei ist manipuliert und die Sitzung wird noch ausgeführt

Bei einer Manipulation der ICA-Datei einer virtuellen App- oder Desktopsitzung, für die das App Protection-Feature zur Erkennung von Richtlinienmanipulationen aktiviert ist, muss die Sitzung mit einer der folgenden Fehlermeldungen beendet werden:

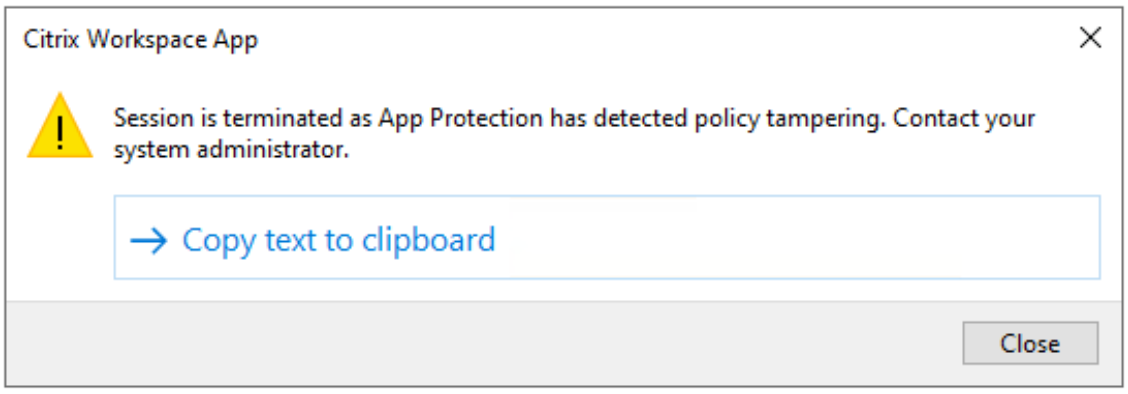
- Citrix Workspace-App für Linux



- Citrix Workspace-App für Mac



- Citrix Workspace-App für Windows



Wenn die Sitzung trotz der Manipulation einer ICA-Datei ausgeführt wird und die Erkennung von

Richtlinienmanipulationen aktiviert ist, führen Sie folgende Schritte durch:

1. Gehen Sie in Virtual Delivery Agent wie folgt vor:

   a) Führen Sie den folgenden Befehl aus und überprüfen Sie, ob der Dienst `ctxappprotectionsv` ausgeführt wird:

   ```
   sc query ctxappprotectionsvc
   ```

   b) Wenn der Dienst `ctxappprotectionsvc` nicht ausgeführt wird, starten Sie ihn wie folgt:

      i. Ändern Sie mit dem folgenden Befehl den Starttyp des Diensts `ctxappprotectionsvc` in "automatisch":

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

      ii. Starten Sie den Dienst mit dem folgenden Befehl:

      ```
      sc start ctxappprotectionsvc
      ```

2. Gehen Sie im Client wie folgt vor:

   a) Überprüfen Sie, ob sich die Datei *vdappp.dll* im Installationsverzeichnis der Citrix Workspace-App befindet. Der Standardinstallationsort der Citrix Workspace-App lautet wie folgt:

   - Windows − C:\Programme (x86)\Citrix\ICA Client
   - Linux − /opt/Citrix/ICAClient
   - Mac − Nicht zutreffend

   b) Überprüfen Sie für die Citrix Workspace-App für Windows mit *procexp.exe*, ob die Datei *vdappp.dll* in *wfica32.exe* geladen ist.

   c) Überprüfen Sie für die Citrix Workspace-App für Linux, ob die Datei *vdappp.dll* in *wfica.exe* geladen ist.

3. Wenn die Sitzung noch ausgeführt wird, sammeln Sie die Protokolle und wenden Sie sich an den technischen Support von Citrix. Weitere Informationen zum Sammeln von Protokollen finden Sie unter Protokollsammlung.

Die Erkennung von Richtlinienmanipulationen funktioniert nach dem Neustart von Virtual Delivery Agent nicht mehr

Wenn Sie Virtual Delivery Agent neu starten und das Feature zur Erkennung von Richtlinienmanipulationen nicht mehr funktioniert, kann dies daran liegen, dass der App Protection-Dienst nach dem Neustart nicht ausgeführt wird. Führen Sie die folgenden Schritte auf Virtual Delivery Agent aus:

1. Führen Sie den folgenden Befehl aus und überprüfen Sie, ob der Dienst `ctxappprotectionsvc` ausgeführt wird und auf **automatisch** eingestellt ist:

   ```
   sc query ctxappprotectionsvc
   ```

2. Wenn der Dienst `ctxappprotectionsvc` nicht ausgeführt wird, starten Sie ihn wie folgt:

   a) Ändern Sie mit dem folgenden Befehl den Starttyp des Diensts `ctxappprotectionsvc` in **automatisch**:

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

   b) Starten Sie den Dienst mit dem folgenden Befehl:

   ```
   sc start ctxappprotectionsvc
   ```

3. Wenn das Feature zur Erkennung von Richtlinienmanipulationen immer noch nicht funktioniert, sammeln Sie die Protokolle und wenden Sie sich an den technischen Support von Citrix. Weitere Informationen zum Sammeln von Protokollen finden Sie unter Protokollsammlung.

Problembehandlung beim App Protection Stature Check

March 11, 2024

Im folgenden Abschnitt werden eventuell auftretende Probleme und Maßnahmen zu ihrer Behebung beschrieben:

Sitzung wurde ohne Fehlermeldung beendet

Wenn Ihre virtuellen App- oder Desktop-Sitzungen abrupt beendet werden, ohne dass eine Fehlermeldung angezeigt wird, gehen Sie wie folgt vor:

1. Überprüfen Sie, ob Ihre Citrix Workspace-App-Version älter als eine der folgenden Versionen ist:

   - Citrix Workspace-App für Windows 2309
   - Citrix Workspace-App für Mac 2308
   - Citrix Workspace-App für Linux 2308

   > **Hinweis:**
   >
   > Wenn die Citrix Workspace-App-Version älter als die in Schritt 1 angeführten Versionen ist und das App Protection Posture Check-Feature aktiviert ist, wird die virtuelle App- oder Desktopsitzung beendet, ohne dass eine Fehlermeldung angezeigt wird. Wenn die Citrix Workspace-App-Version jedoch größer oder gleich den in Schritt 1 angeführten Versionen

> ist und das App Protection Posture Check-Feature aktiviert ist, wird die virtuelle App- oder Desktopsitzung mit einer Fehlermeldung beendet.

2. Prüfen Sie, ob das App Protection Posture Check-Feature aktiviert ist.
3. Wenn die Citrix Workspace-App-Version größer oder gleich den angegebenen Versionen ist und das Posture Check-Feature ebenfalls aktiv ist, sammeln Sie die Protokolle und wenden Sie sich an den technischen Support von Citrix. Weitere Informationen zum Sammeln von Protokollen finden Sie unter Protokollsammlung.

App Protection Posture Check ist aktiviert, aber die Sitzung wird bei älteren Versionen nicht beendet

Wenn das App Protection Posture Check-Feature aktiviert ist und Sie eine Verbindung über eine ältere Version der Citrix Workspace-App herstellen, muss die Sitzung beendet werden.

Wenn die Sitzung jedoch nicht beendet wird, gehen Sie wie folgt vor:

1. Gehen Sie in Virtual Delivery Agent wie folgt vor:
   a) Führen Sie den folgenden Befehl aus und überprüfen Sie, ob der Dienst `ctxappprotectionsvc` ausgeführt wird:

      ```
      sc query ctxappprotectionsvc
      ```

   b) Wenn der Dienst `ctxappprotectionsvc` nicht ausgeführt wird, starten Sie ihn wie folgt:
      i. Ändern Sie den Starttyp von `ctxappprotectionsvc service` auf **automatisch**, indem Sie den folgenden Befehl ausführen:

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

      ii. Starten Sie den Dienst mit dem folgenden Befehl:

         ```
         sc start ctxappprotectionsvc
         ```

2. Prüfen Sie, ob die von Ihnen eingegebenen Posture Check-Werte eines der folgenden Präfixe haben:
   - Citrix Workspace-App für Windows: `windows-`
   - Citrix Workspace-App für Linux: `linux-`
   - Citrix Workspace-App für Mac: `mac-`
3. Prüfen Sie, ob die Posture Check-Werte für die jeweilige Plattform korrekt hinzugefügt wurden, da sie plattformspezifisch sind.

4. Überprüfen Sie den `reg`-Speicherort (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) in der Registrierung, um zu ermitteln, ob Posture Check mit Virtual Delivery Agent synchronisiert ist.
5. Wenn alle oben genannten Bedingungen erfüllt sind und die Sitzung immer noch über eine ältere Version der Citrix Workspace-App verbunden ist, sammeln Sie die Protokolle und wenden Sie sich an den technischen Support von Citrix. Weitere Informationen zum Sammeln von Protokollen finden Sie unter Protokollsammlung.

App Protection Posture Check funktioniert auf einer Plattform, auf einer anderen jedoch nicht

Manchmal funktioniert das App Protection Posture Check-Feature auf einer Plattform und nicht auf einer anderen. Beispielsweise funktioniert das App Protection Posture Check-Feature in der Citrix Workspace-App für Windows, aber nicht in der Citrix Workspace-App für Linux.

Gehen Sie in solchen Szenarien wie folgt vor:

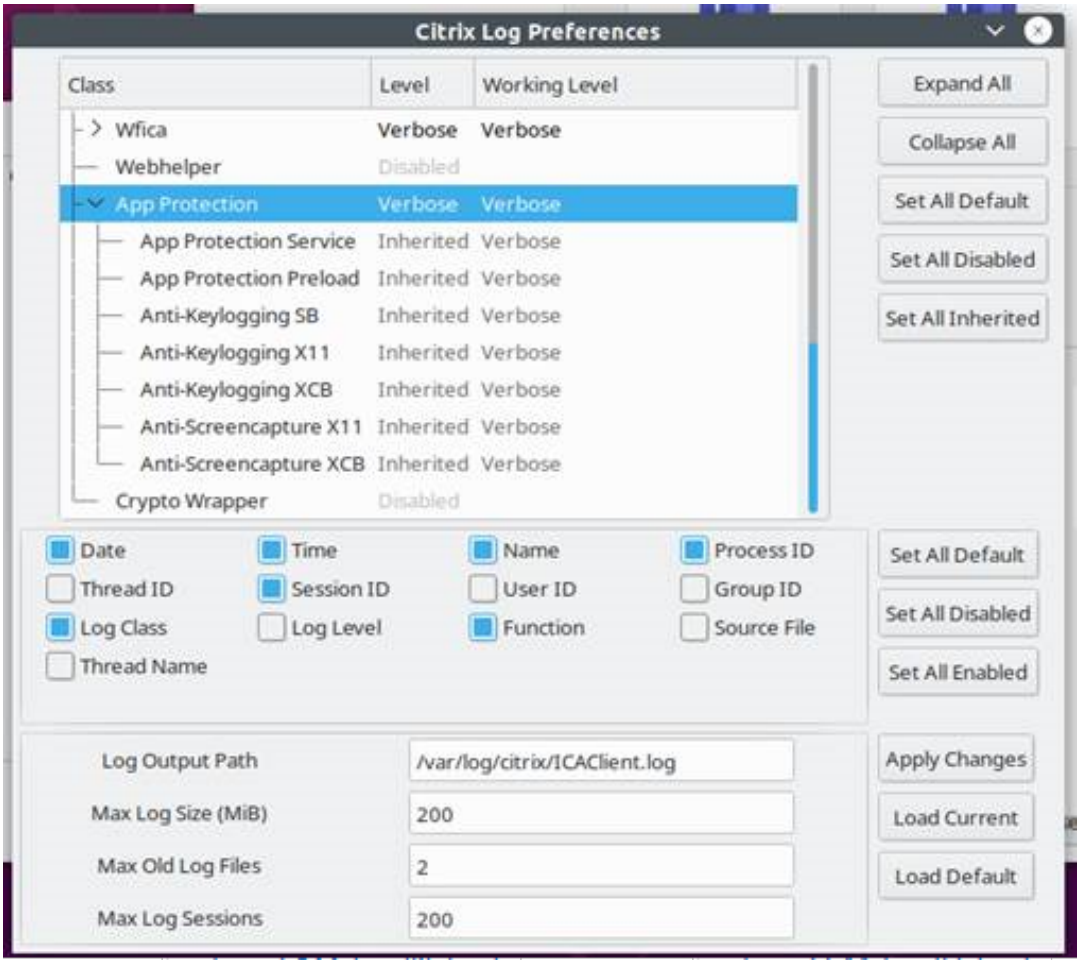
1. Prüfen Sie, ob die von Ihnen eingegebenen Posture Check-Werte eines der folgenden Präfixe haben:
   - Citrix Workspace-App für Windows: `windows-`
   - Citrix Workspace-App für Linux: `linux-`
   - Citrix Workspace-App für Mac: `mac-`
2. Prüfen Sie, ob die Posture Check-Werte für die jeweilige Plattform korrekt hinzugefügt wurden, da sie plattformspezifisch sind.
3. Überprüfen Sie den `reg`-Speicherort (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) in der Registrierung auf Virtual Delivery Agent, um zu ermitteln, ob Posture Check mit Virtual Delivery Agent synchronisiert ist. Dies muss mit dem übereinstimmen, was in Studio konfiguriert wurde.
4. Wenn alle oben genannten Bedingungen erfüllt sind und die Sitzung immer noch über eine ältere Version der Citrix Workspace-App verbunden ist, sammeln Sie die Protokolle und wenden Sie sich an den technischen Support von Citrix. Weitere Informationen zum Sammeln von Protokollen finden Sie unter Protokollsammlung.

Protokollsammlung

March 11, 2024

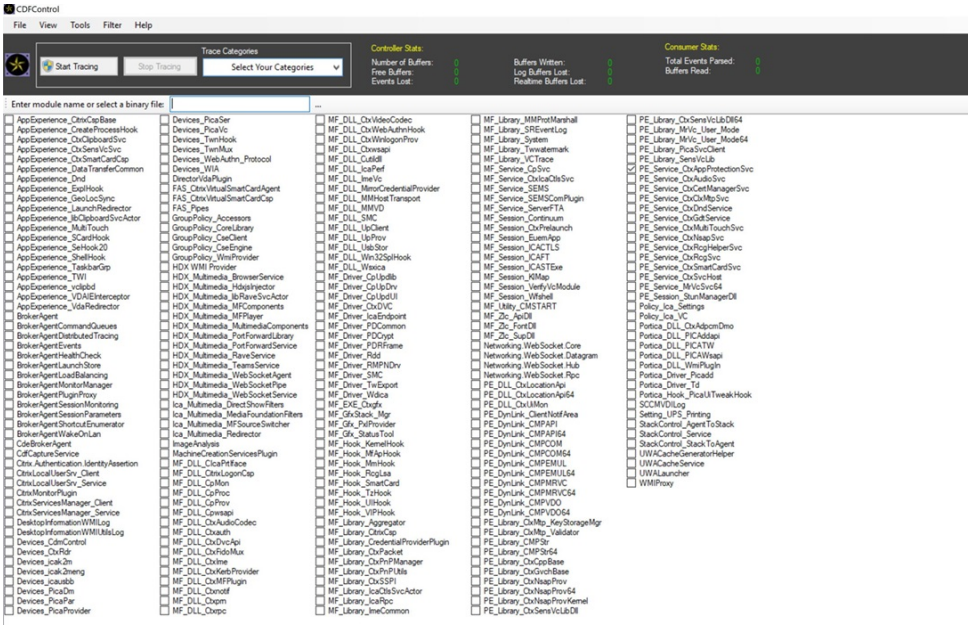
- Informationen zum Sammeln von Protokollen für die Citrix Workspace-App für Windows finden Sie unter Protokollsammlung für Windows.
- Informationen zum Sammeln von Protokollen für die Citrix Workspace-App für Mac finden Sie unter Protokollsammlung für Mac.
- Gehen Sie wie folgt vor, um Protokolle für die Citrix Workspace-App für Linux zu sammeln:

  1. Führen Sie die ausführbare Datei "set log"aus, die sich im Verzeichnis *util* der Installation befindet. Beispiel: */opt/Citrix/ICAClient/util/setlog*.
  2. (Optional) Klicken Sie auf **Alle auf 'Deaktiviert'setzen** und stellen Sie sicher, dass nur die erforderlichen Protokolle erfasst werden.
  3. Gehen Sie in App Protection zu Protokollierung.
  4. Stellen Sie die Protokollebene in App Protection auf "Ausführlich"ein, indem Sie mit der rechten Maustaste klicken und **Ausführlich** auswählen (nur Warnungen und Fehler werden protokolliert).
  5. Erweitern Sie die Klasse "App Protection"und klicken Sie mit der rechten Maustaste auf das untergeordnete Element. Wählen Sie **Gruppe** > **Geerbt** aus.
  6. Verwenden Sie das Linux-Hilfsprogramm zur Protokollerfassung (aus dem *Installationsverzeichnis* starten Sie *util/setlog*) und ändern Sie die Protokollierungsstufe für den virtuellen Kanal auf "Ausführlich".
  7. Aktivieren Sie Protokolle für **wfica**. Klicken Sie mit der rechten Maustaste auf **wfica** und wählen Sie **Ausführlich** aus. Wenn App Protection nicht installiert ist oder von **wfica** nicht erkannt werden kann, erhalten Sie das Protokoll als **[NCS] < P3563 > citrix-wfica: App Protection is not installed**.
  8. Klicken Sie auf **wfica** und ändern Sie die Protokollierungsstufe für den **WinStation-Treiber** in **Ausführlich**.
  9. Wenn Sie die Sitzung starten, werden die Protokolle in der Datei aufgezeichnet, die im Protokollausgabepfad des eingestellten Protokolls angegeben ist.



- So sammeln Sie Protokolle für Virtual Delivery Agent:

    1. Um Tracingberichte vom App Protection-Dienst über die CDF-Steuerung abzurufen, wählen Sie alle Module aus.



2. In bestimmten Fällen müssen CDF-Tracingberichte von einer anderen Maschine erfasst werden. Informationen zum Sammeln von CDF-Tracingberichten finden Sie unter CTX237216.

Kontextbezogenes App Protection für Workspace

March 11, 2024

Kontextbezogenes App Protection ermöglicht es, App Protection-Richtlinien flexibel und granular nur auf bestimmte Benutzergruppen anzuwenden –basierend auf Benutzern, ihrem Gerät und der Netzwerkstruktur.

App Protection kontextbezogen implementieren

Sie können kontextbezogenes App Protection mit den Verbindungsfiltern implementieren, die in der Brokerzugriffsrichtlinienregel definiert sind. Die Brokerzugriffsrichtlinien definieren die Regeln, die den Zugriff eines Benutzers auf Bereitstellungsgruppen steuern. Die Richtlinie umfasst mehrere Regeln. Jede Regel bezieht sich auf eine einzelne Bereitstellungsgruppe und hat eine Reihe von Verbindungsfiltern und Steuerelementen für Zugriffsrechte.

Benutzer erhalten Zugriff auf eine Bereitstellungsgruppe, wenn ihre Verbindungsdetails mit den Verbindungsfiltern einer oder mehrerer Regeln in der Brokerzugriffsrichtlinie übereinstimmen. Benutzer können standardmäßig auf keine Bereitstellungsgruppe in einer Site zugreifen. Je nach Bedarf

können Sie weitere Brokerzugriffsrichtlinien erstellen. Es können mehrere Regeln für dieselbe Bereitstellungsgruppe gelten. Weitere Informationen finden Sie unter New-BrokerAccessPolicyRule.

Die folgenden Parameter in der Brokerzugriffsrichtlinienregel bieten die Möglichkeit, App Protection flexibel und kontextbezogen zu aktivieren, wenn die Verbindung des Benutzers mit den Verbindungsfiltern übereinstimmt, die in der Zugriffsrichtlinienregel definiert sind:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Verwenden Sie die Smart Access-Richtlinien, auf die in den Brokerzugriffsrichtlinien verwiesen wird, um die Verbindungsrichtlinien weiter anzupassen. Die in diesem Artikel erläuterten Szenarien verdeutlichen, wie Sie die Smart Access-Richtlinien zum Einrichten von kontextbezogenem App Protection verwenden.

Kontextbezogenes App Protection - Szenarien

Im Folgenden finden Sie Szenarien, in denen beschrieben wird, wie Sie kontextbezogenes App Protection aktivieren können:

- App Protection für externe Benutzer mit Zugriff über Access Gateway aktivieren
- App Protection für nicht vertrauenswürdige Geräte aktivieren
- App Protection basierend auf Gerätestatusergebnissen aktivieren
- App Protection für spezifische Benutzergruppen aktivieren

Voraussetzungen

March 11, 2024

Bereiten Sie Folgendes vor:

- Netzwerkpositionsdienst (NLS) für Szenarios basierend auf dem Netzwerkstandort des Benutzers
- Lizenzanforderungen -
  - App Protection für DaaS
  - Anspruch auf adaptive Authentifizierung für Szenarios mit Smart Access-Richtlinien.

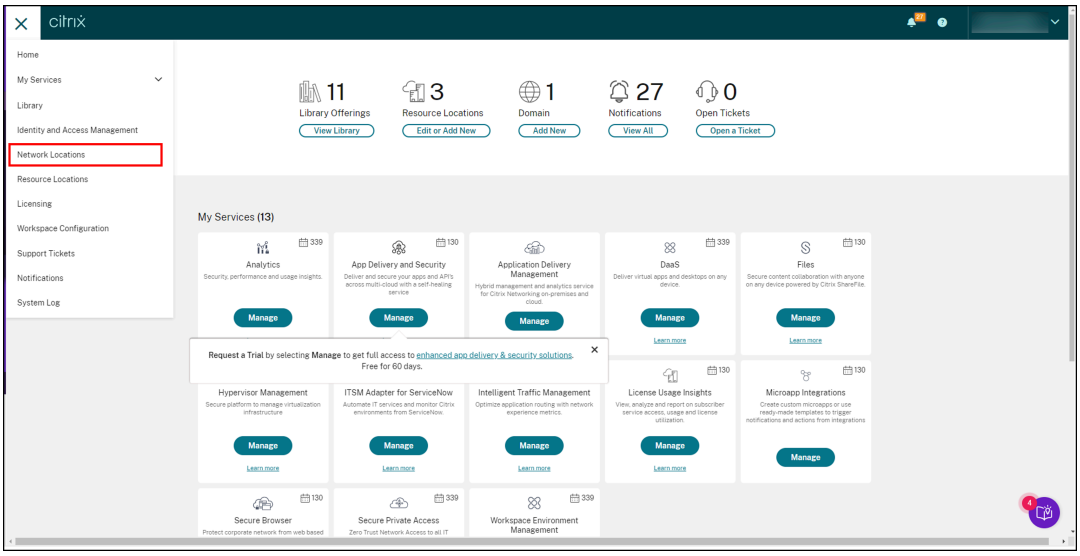
Szenario 1

April 10, 2024

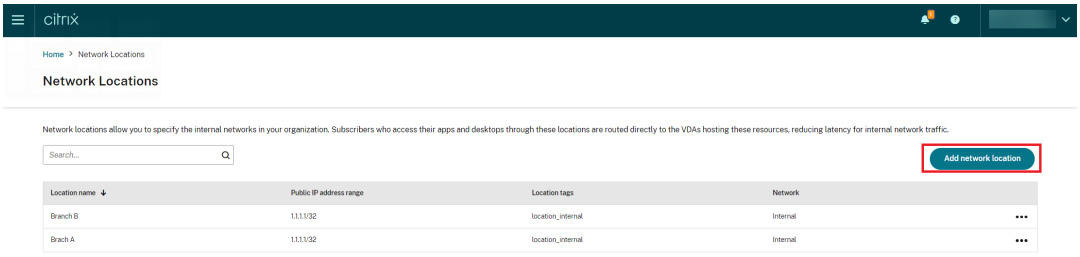
Dieses Szenario umfasst das Aktivieren von App Protection für externe Benutzer mit Zugriff über Access Gateway.

1. Adaptive Authentifizierung konfigurieren
2. Adaptiven Zugriff basierend auf dem Netzwerkstandort konfigurieren

   a) Melden Sie sich bei Citrix Cloud an und gehen Sie zu **Netzwerkstandorte**.



   b) Klicken Sie auf **Netzwerkspeicherort hinzufügen**.



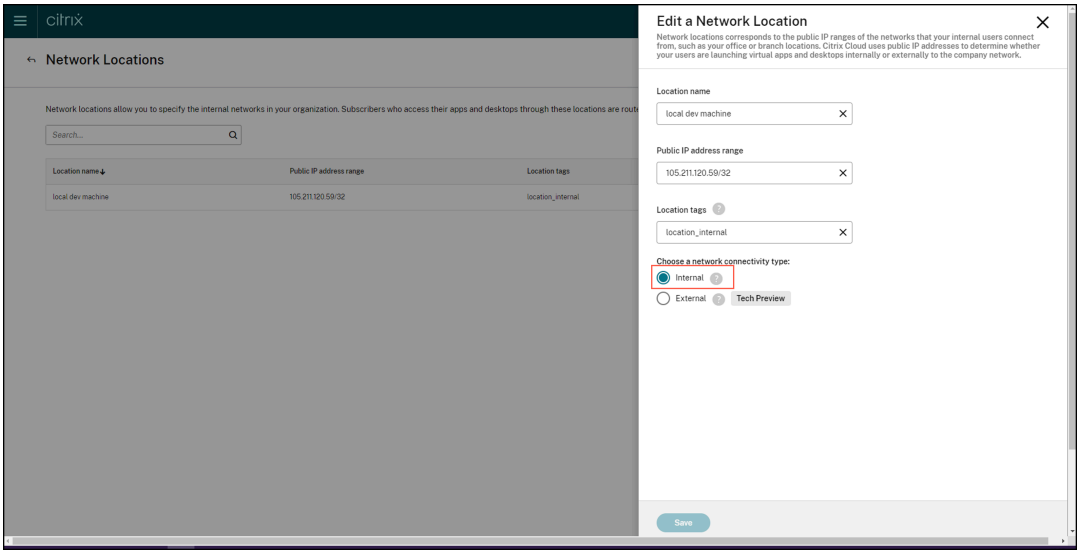
   Die Seite **Netzwerkstandort hinzufügen** wird angezeigt.

   c) Geben Sie im Feld **Standortname** den entsprechenden Standortnamen ein.

   d) Geben Sie im Feld **Öffentlicher IP-Adressbereich** die Netzwerk-IP-Adresse oder das Subnetz ein, das als internes Netzwerk gelten soll.

   e) Geben Sie im Feld **Tags für den Ort** die Zeichenfolge **location_internal** ein. Weitere Informationen zu diesem Tag finden Sie unter Tags für den Ort.

f) Wählen Sie unter **Wählen Sie einen Netzwerkverbindungstyp:** die Option *Intern*.



Wenn Sie sich beim Cloudstore von einem Gerät aus anmelden, dessen IP-Adresse unter **Wählen Sie einen Netzwerkverbindungstyp** als *Intern* konfiguriert ist, gilt die Verbindung als interne Verbindung.

3. Richtlinienregeln für den Brokerzugriff konfigurieren

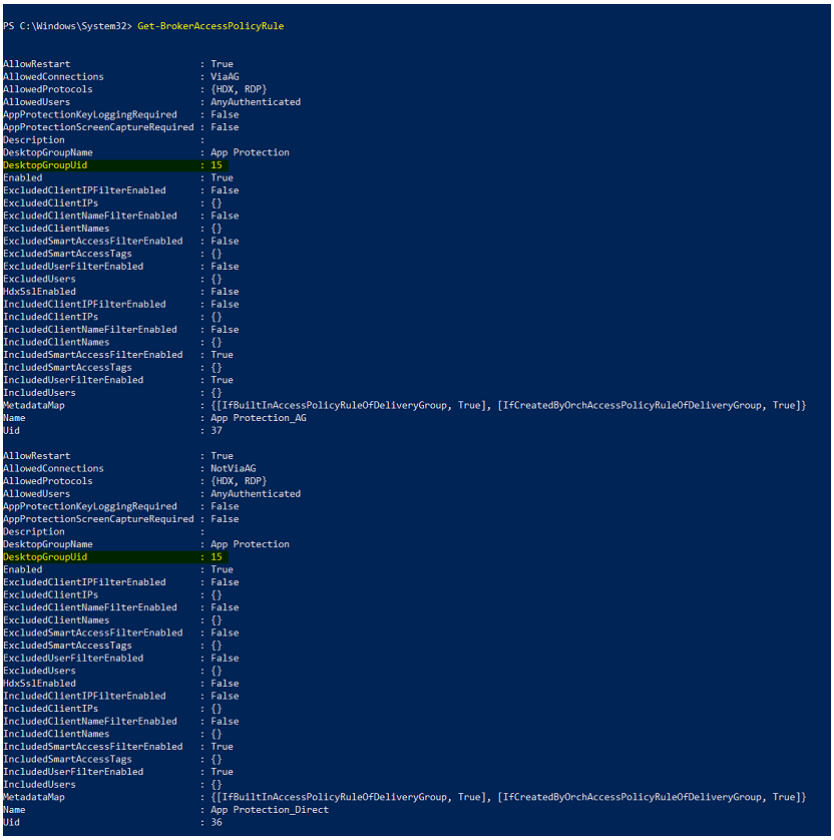
   Für jede Bereitstellungsgruppe werden standardmäßig zwei Brokerzugriffsrichtlinien erstellt, eine für über Access Gateway eingehende Verbindungen, die zweite für direkte Verbindungen. Sie können App Protection nur für Verbindungen über Access Gateway aktivieren (externe Verbindungen). Gehen Sie wie folgt vor, um Richtlinienregeln für den Brokerzugriff zu konfigurieren:

   a) Installieren Sie das Citrix PowerShell-SDK und stellen Sie eine Verbindung mit der Cloud-API her (Anweisungen siehe Citrix Blogbeitrag Getting started with PowerShell automation for Citrix Cloud).

   b) Führen Sie den Befehl `Get-BrokerAccessPolicyRule` aus.

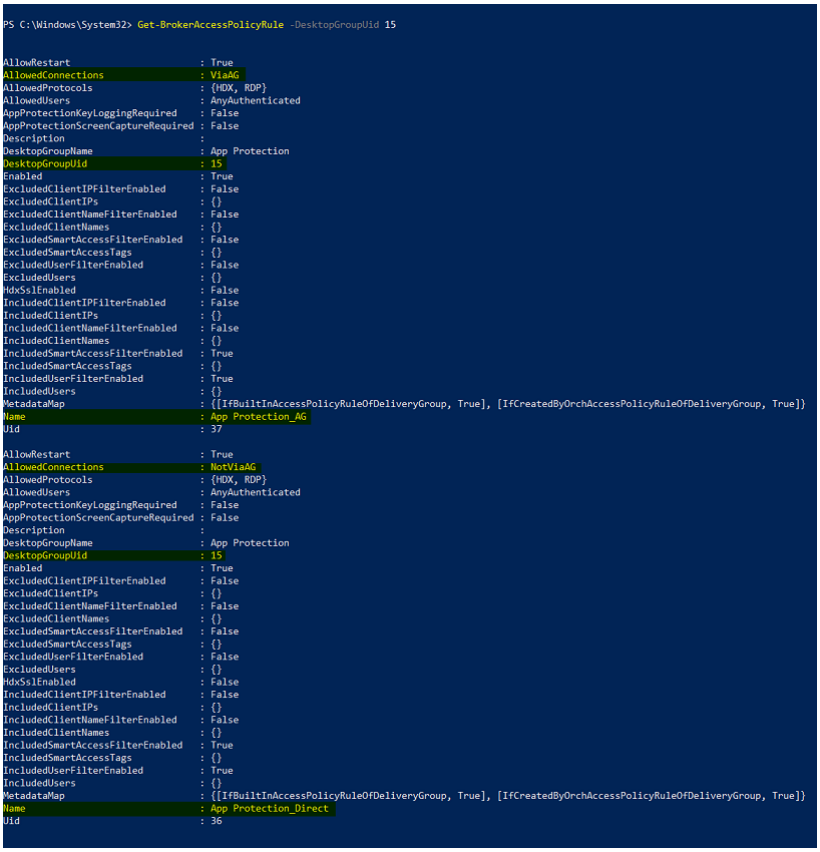
      Eine Liste aller Brokerzugriffsrichtlinien für alle Bereitstellungsgruppen wird angezeigt.

   c) Suchen Sie die **DesktopGroupUid** der Bereitstellungsgruppe, die Sie ändern möchten.



d) Führen Sie den folgenden Befehl mit der **DesktopGroupUid** aus, um für die jeweilige Bereitstellungsgruppe geltende Richtlinien abzurufen. Es gibt mindestens zwei Richtlinien, eine mit der Einstellung *ViaAG* für *AllowedConnections* und eine zweite mit der Einstellung *NotViaAG*.

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 15
```

Der Screenshot zeigt zwei Richtlinien:

- App Protection_AG – *AllowedConnections* mit *ViaAG*: Richtlinie für Verbindungen über das Access Gateway
- App Protection_Direct – *AllowedConnections* mit *NotViaAG*: Richtlinie für Verbindungen, die nicht über das Access Gateway hergestellt wurden

4. Aktivieren Sie mit den folgenden Befehlen App Protection-Richtlinien nur für externe Verbindungen und deaktivieren Sie sie für interne Verbindungen:

   - `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”`

5. Verifizierung:

   Melden Sie sich bei der Citrix Workspace-App ab und wieder an. Starten Sie die geschützte Ressource über eine externe Verbindung. Die App Protection-Richtlinien werden angewendet. Starten Sie dieselbe Ressource über eine interne Verbindung (Gerät innerhalb des im ersten Schritt konfigurierten IP-Adressbereichs). Die App Protection-Richtlinien sind deaktiviert.

Szenario 2

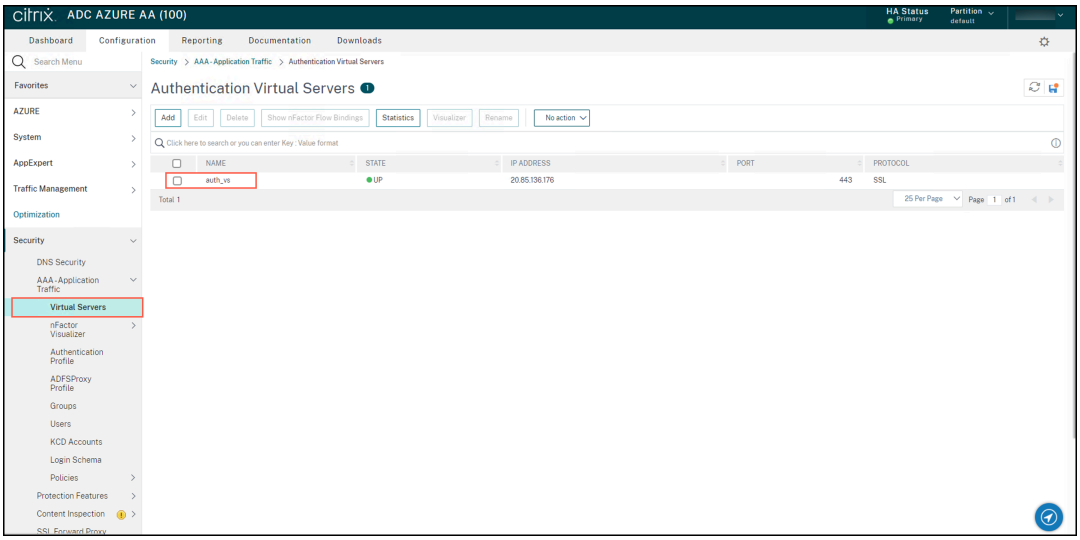
April 10, 2024

Dieses Szenario umfasst das Aktivieren von App Protection für nicht vertrauenswürdige Geräte.

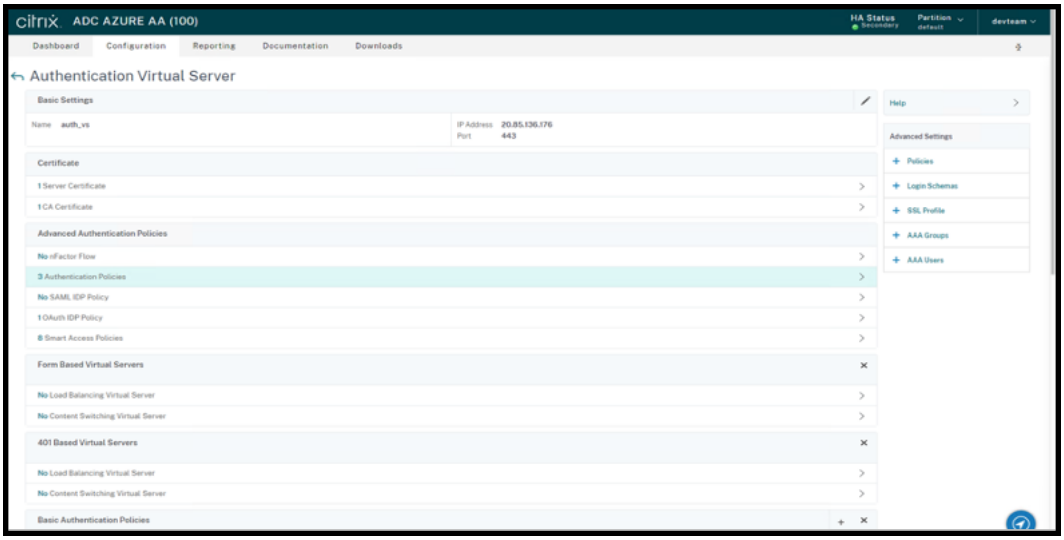
Es gibt mehrere Definitionen vertrauenswürdiger und nicht vertrauenswürdiger Geräte. In diesem Beispiel gilt ein Gerät als vertrauenswürdig, wenn die Endpunktanalyse (EPA) erfolgreich ist. Alle anderen Geräte gelten als nicht vertrauenswürdige Geräte.

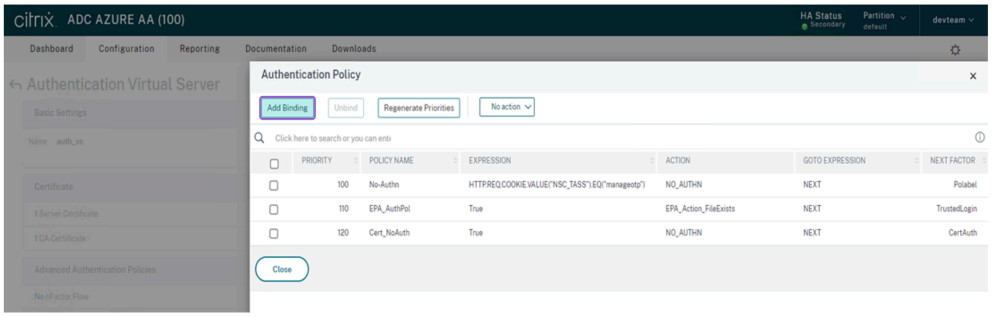
1. Adaptive Authentifizierung konfigurieren.
2. Erstellen Sie die Authentifizierungsrichtlinie mit EPA:

   a) Melden Sie sich an der Verwaltungsoberfläche von Citrix ADC an. Gehen Sie auf der Registerkarte **Configuration** zu **Security > AAA-Application Traffic -> Virtual Servers**. Klicken Sie auf den gewünschten virtuellen Server (in diesem Beispiel *auth_vs*).

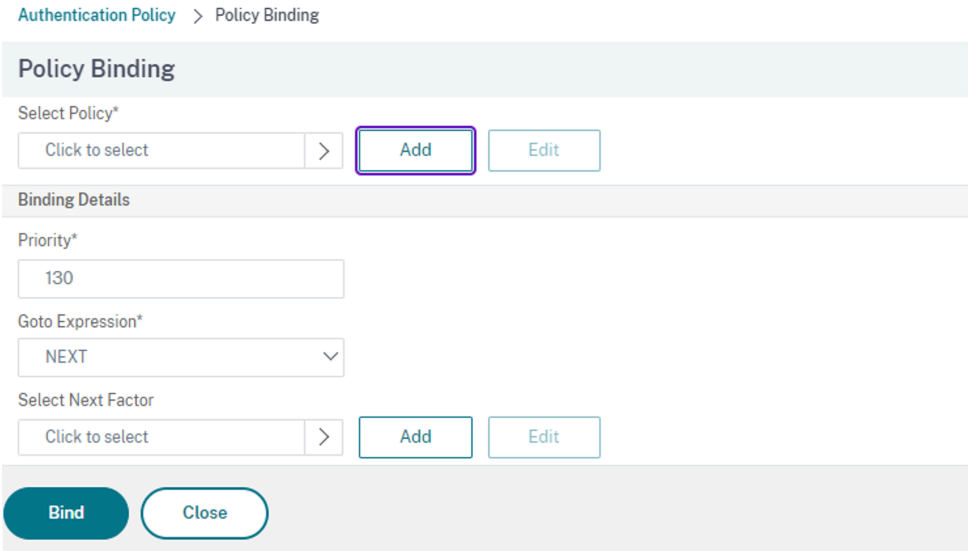


   b) Gehen Sie zu **Authentication Policies > Add Binding**.

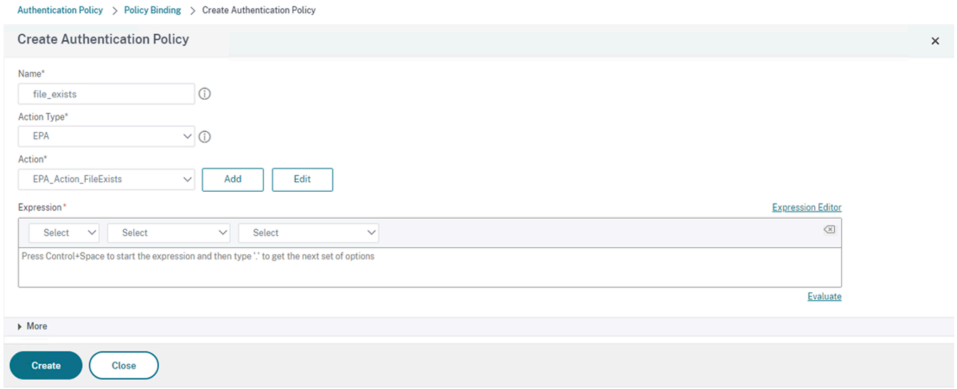




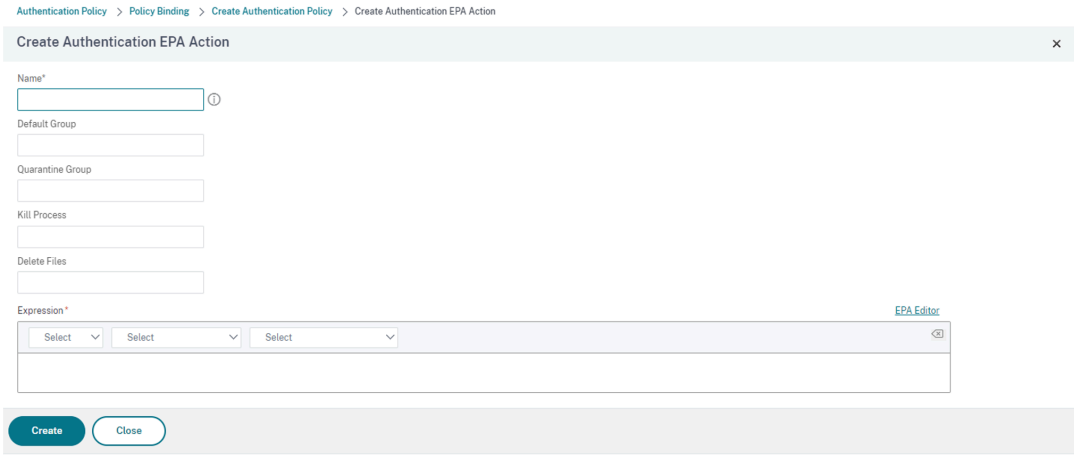
c) Klicken Sie auf **Hinzufügen**, um eine Richtlinie zu erstellen.



d) Erstellen Sie eine auf der EPA basierende Authentifizierungsrichtlinie. Geben Sie einen Namen für die Richtlinie ein. Wählen Sie für **Action Type** die Option *EPA*. Klicken Sie auf **Add**, um die Aktion zu erstellen.



Die Seite **Create Authentication EPA Action** wird angezeigt.

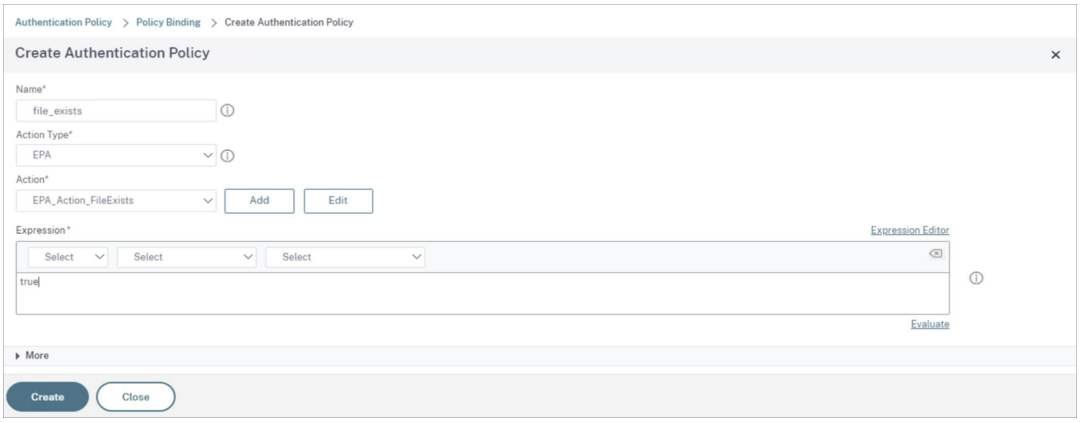


e) Geben Sie auf der Seite **Create Authentication EPA Action** die folgenden Details ein und klicken Sie auf **Create**, um die Aktion zu erstellen:

- **Name:** Namen der EPA-Aktion. In diesem Beispiel *EPA_Action_FileExists*.
- **Standardgruppe:** Geben Sie den Namen der Standardgruppe ein. Wenn der EPA-Ausdruck auf *True* festgelegt ist, werden Benutzer der Standardgruppe hinzugefügt. Die **Standardgruppe** ist in diesem Beispiel *FileExists*.
- **Quarantänegruppe**: Geben Sie den Namen der Quarantänegruppe ein. Wenn der EPA-Ausdruck auf *True* festgelegt ist, werden Benutzer der Quarantänegruppe hinzugefügt.
- **Ausdruck:** Fügen Sie den zu analysierenden EPA-Ausdruck hinzu. In diesem Beispiel gilt die EPA als erfolgreich, wenn die Datei `sys.client_expr("file_0_C:\\\\\epa\\\\\avinstalled.txt")` vorhanden ist.

Die Seite **Create Authentication Policy** wird wieder angezeigt.

f) Geben Sie im Ausdruckseditor **true** ein und klicken Sie auf **Create**.



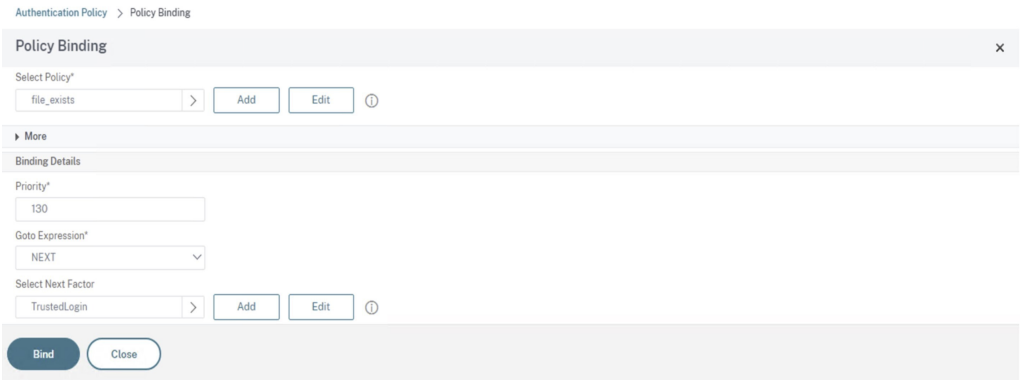
Die Seite **Policy Binding** wird wieder angezeigt.

g) Gehen Sie auf der Seite **Policy Binding** wie folgt vor:

i. Wählen Sie **NEXT** für **Goto Expression**.

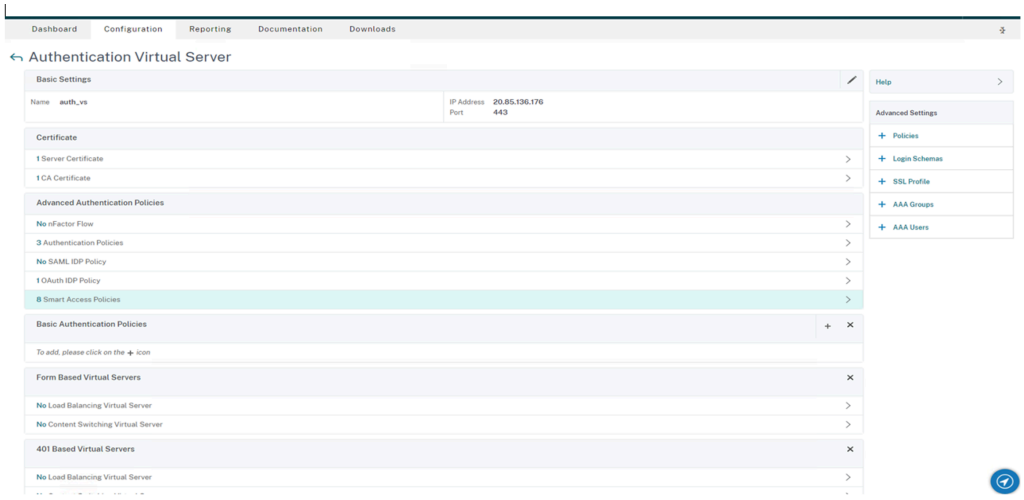
ii. Wählen Sie im Bereich **Next Factor** die LDAP-Richtlinie aus, die Sie für die Authentifizierung in Application Delivery Controller (ADC) konfiguriert haben.

iii. Klicken Sie auf **Bind**.

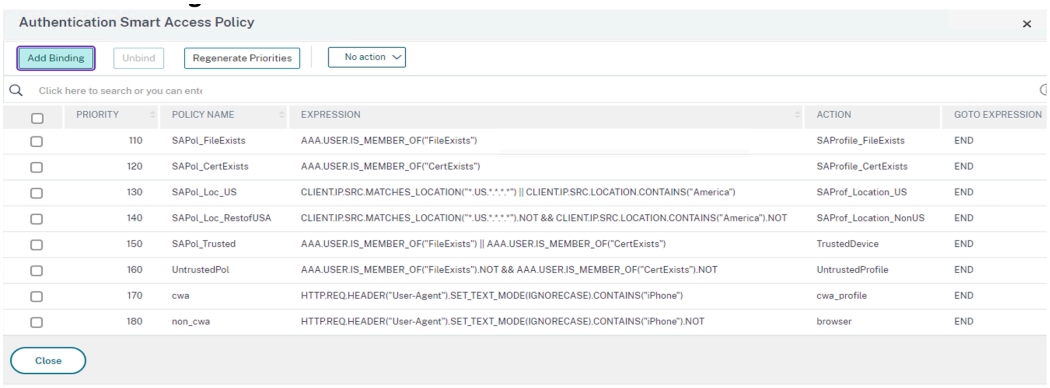


3. Erstellen Sie eine Smart Access-Richtlinie für vertrauenswürdige Geräte:

a) Wählen Sie auf der Seite **Authentication Virtual Server** des Servers *auth_vs* die Option **Smart Access Policies**.

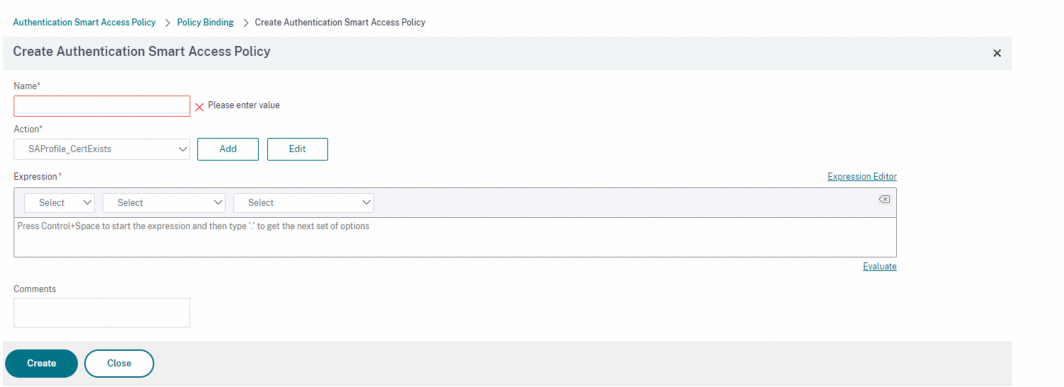


b) Klicken Sie auf **Add binding**.



c) Klicken Sie auf der Seite **Policy Binding** im Bereich **Select Policy** auf **Add**.

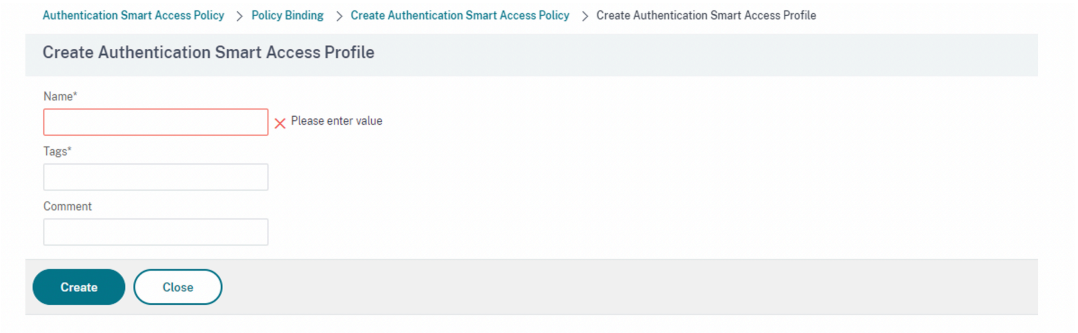
Die Seite **Create Authentication Smart Access Policy** wird angezeigt.



d) Geben Sie auf der Seite **Create Authentication Smart Access Policy** einen **Namen** für die Smart Access-Richtlinie ein und klicken Sie auf **Add**, um ein Smart Access-Profil zu erstellen.

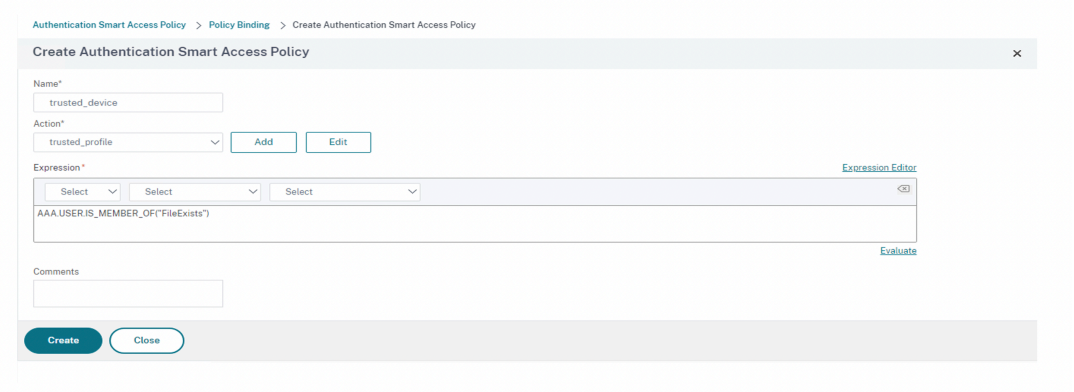
   Die Seite **Create Authentication Smart Access Profile** wird angezeigt.

e) Fügen Sie einen **Namen** für die Aktion hinzu. Geben Sie *trusted* für **Tags** ein. Das Tag wird später in der Brokerzugriffsrichtlinienregel zur Konfiguration referenziert. Klicken Sie auf **Erstellen**.



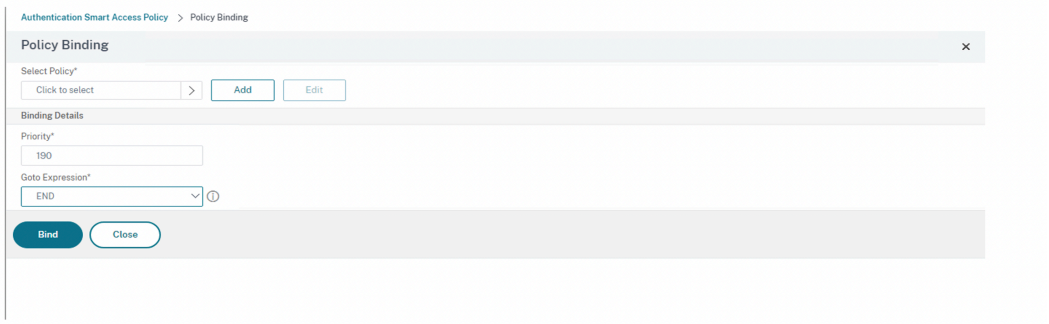
   Die Seite **Create Authentication Smart Access Policy** wird wieder angezeigt.

f) Geben Sie im Abschnitt **Expression** den Ausdruck ein, für den Sie das Tag bereitstellen möchten. Da das Tag in diesem Beispiel für vertrauenswürdige Geräte bereitgestellt wird, geben Sie `AAA.USER.IS_MEMBER_OF("FileExists")` ein. Klicken Sie auf **Erstellen**.



Die Seite **Policy Binding** wird wieder angezeigt.

g) Wählen Sie für **Goto Expression** die Option **End** und klicken Sie auf *Bind*.



4. Erstellen Sie eine Smart Access-Richtlinie für nicht vertrauenswürdige Geräte:

   a) Folgen Sie den Anweisungen des vorherigen Verfahrens mit Ausnahme der Schritte **v** und **vi**.

   b) Fügen Sie für Schritt **v** auf der Seite **Create Authentication Smart Access Profile** für die Aktion **Name** hinzu. Geben Sie *untrusted* für **Tags** ein. Das Tag wird später in der Brokerzugriffsrichtlinienregel zur Konfiguration referenziert. Klicken Sie auf **Erstellen**.

   c) Geben Sie für Schritt **vi** im Bereich **Expression** der Seite **Create Authentication Smart Access Policy** den Ausdruck ein, für den Sie das Tag bereitstellen möchten. Da das Tag in diesem Beispiel für nicht vertrauenswürdige Geräte bereitgestellt wird, geben Sie `AAA.USER.IS_MEMBER_OF("FileExists").NOT` ein.

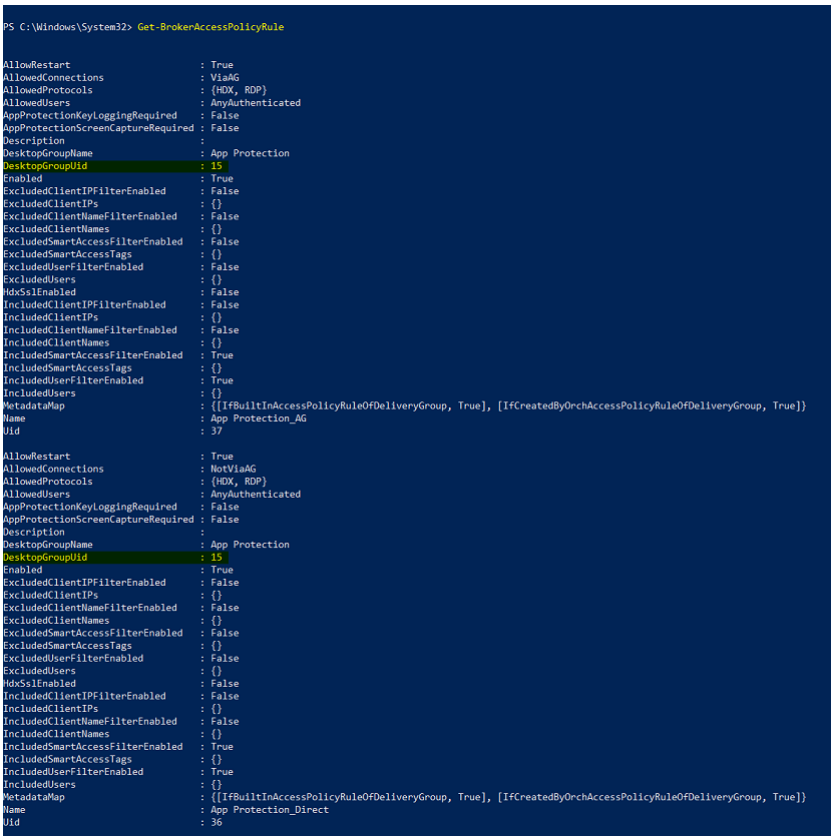
5. Richtlinienregeln für den Brokerzugriff konfigurieren:

   a) Installieren Sie das Citrix PowerShell-SDK und stellen Sie eine Verbindung mit der Cloud-API her (Anweisungen siehe Citrix Blogbeitrag Getting started with PowerShell automation for Citrix Cloud).

   b) Führen Sie den Befehl `Get-BrokerAccessPolicyRule` aus.

Eine Liste aller Brokerzugriffsrichtlinien für alle Bereitstellungsgruppen wird angezeigt.

c) Suchen Sie die **DesktopGroupUid** der Bereitstellungsgruppe, die Sie ändern möchten.



d) Rufen Sie die Richtlinien, die nur auf eine bestimmte Bereitstellungsgruppe angewendet werden, mit dem folgenden Befehl ab:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) Zum Filtern von Benutzern mit vertrauenswürdigen Geräten erstellen Sie eine weitere Brokerzugriffsrichtlinie mit folgendem Befehl:

```
New-BrokerAccessPolicyRule -Name CAP_Desktops_AG_Trusted-
DesktopGroupUid 7 - AllowedConnections ViaAG -AllowedProtocols
 HDX, RDP -AllowedUsers AnyAuthenticated - AllowRestart $true
 -Enabled $true-IncludedSmartAccessFilterEnabled $true
```

f) Verwenden Sie den folgenden Befehl, um App Protection für vertrauenswürdige Geräte zu deaktivieren und für nicht vertrauenswürdige Geräte zu aktivieren:

```
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. Verifizierung:

   Melden Sie sich bei der Citrix Workspace-App ab und wieder an. Starten Sie die geschützte Ressource von einem vertrauenswürdigen Gerät, das die EPA-Bedingung erfüllt. Die App Protection-Richtlinien werden nicht angewendet. Starten derselben Ressource von einem nicht vertrauenswürdigen Gerät. Die App Protection-Richtlinien werden angewendet.

Szenario 3

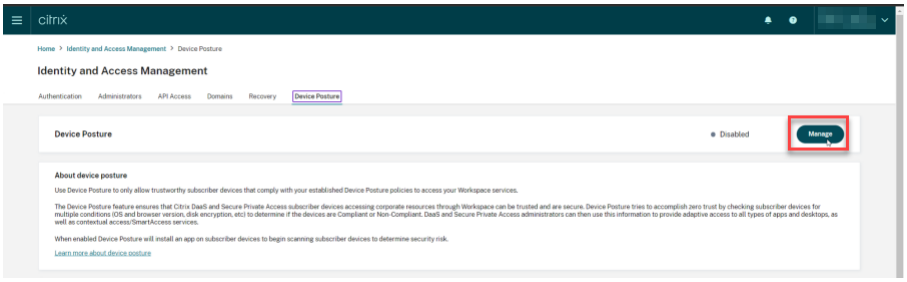
March 11, 2024

In diesem Szenario wird beschrieben, wie Sie App Protection basierend auf den Gerätestatus-Ergebnissen aktivieren.

1. Gerätestatudienst konfigurieren:

   a) Melden Sie sich bei Citrix Cloud an.

   b) Gehen Sie zu **Identitäts- und Zugriffsverwaltung** > **Gerätestatus** und klicken Sie auf **Verwalten**.

   c) Klicken Sie auf **Geräterichtlinie erstellen**.

      Die Seite **Geräterichtlinie erstellen** wird angezeigt.

   d) Klicken Sie unter **Richtlinienregeln** auf das Dropdownmenü **Regel auswählen** und wählen Sie *Citrix Workspace-App-Version*.

   e) Klicken Sie auf das Dropdownmenü **Regel auswählen** und wählen Sie *Größer oder gleich* >=.

   f) Geben Sie die Version der Citrix Workspace-App ein, die Sie als Bedingung festlegen möchten. In diesem Beispiel ist es *23.7.0.19*.

   g) Wählen Sie unter **Richtlinienergebnis** die Option **Richtlinientreu**.

h) Geben Sie im Feld **Name** einen Namen für die Richtlinie ein.

i) Geben Sie im Feld **Priorität** die Priorität der Richtlinie ein.

j) Aktivieren Sie das Kontrollkästchen **Bei der Erstellung aktivieren**, um die Richtlinie bei deren Erstellung zu aktivieren.

k) Klicken Sie auf **Erstellen**.

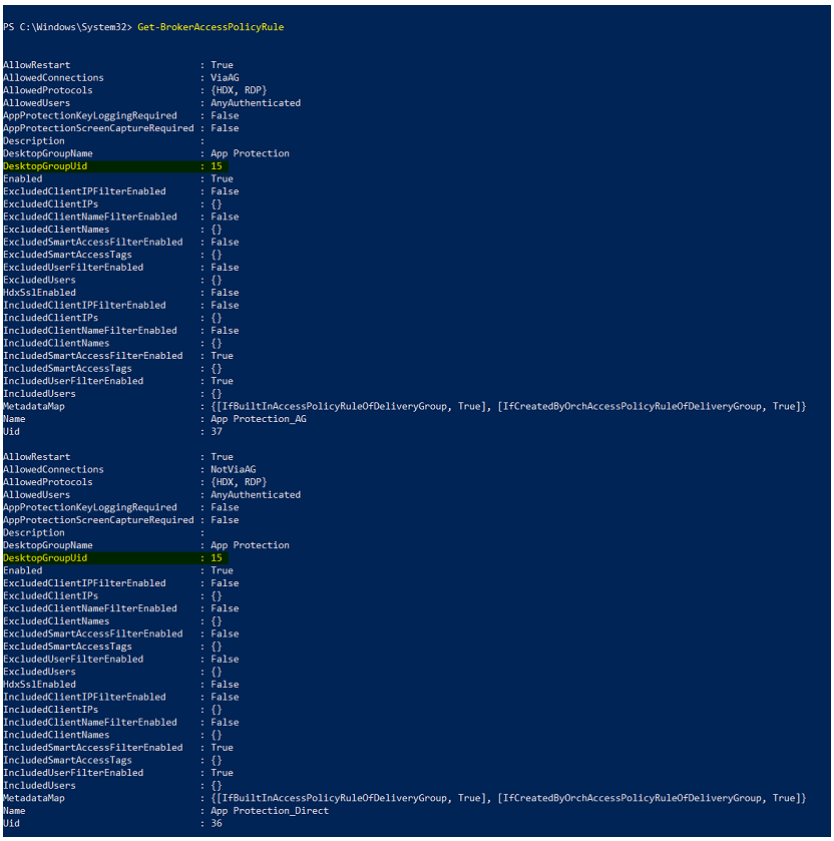
2. Richtlinienregeln für den Brokerzugriff konfigurieren:

a) Installieren Sie das Citrix PowerShell-SDK und stellen Sie eine Verbindung mit der Cloud-API her (Anweisungen siehe Citrix Blogbeitrag Getting started with PowerShell automation for Citrix Cloud).

b) Führen Sie den Befehl `Get-BrokerAccessPolicyRule` aus.

Eine Liste aller Brokerzugriffsrichtlinien für alle Bereitstellungsgruppen wird angezeigt.

c) Suchen Sie die **DesktopGroupUid** der Bereitstellungsgruppe, die Sie ändern möchten.



d) Rufen Sie die Richtlinien, die nur auf eine bestimmte Bereitstellungsgruppe angewendet werden, mit dem folgenden Befehl ab:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```


e) Führen Sie den folgenden Befehl aus, um App Protection auf die richtlinientreuen Geräte anzuwenden:

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG"-IncludedSmartAccessFilterEnabled $true -IncludedSmartAccess
 Workspace:COMPLIANT
```

f) Führen Sie den folgenden Befehl aus, um App Protection auf die nicht richtlinientreuen Geräte anzuwenden:

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG_NonCompliant"-DesktopGroupUid 7 -AllowedConnections
 ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
 $true -ExcludedSmartAccessFilterEnabled $true -ExcludedSmartAccessTag
 Workspace:COMPLIANT-IncludedSmartAccessFilterEnabled $true
```

3. Verifizierung:

   Melden Sie sich von der Citrix Workspace-App ab. Melden Sie sich mit einer Version der Citrix Workspace-App an, die der Geräterichtlinie entspricht. Die App Protection-Richtlinien werden nicht angewendet. Melden Sie sich erneut von der Citrix Workspace-App ab und melden Sie sich mit einer Version der Citrix Workspace-App an, die nicht der Geräterichtlinie entspricht. Die App Protection-Richtlinien werden angewendet.

Szenario 4

October 27, 2023

In diesem Szenario wird beschrieben, wie App Protection für spezifische Benutzergruppen aktiviert wird.

Mit den folgenden Schritten können Sie App Protection für Benutzer einer spezifischen Gruppe aktivieren:

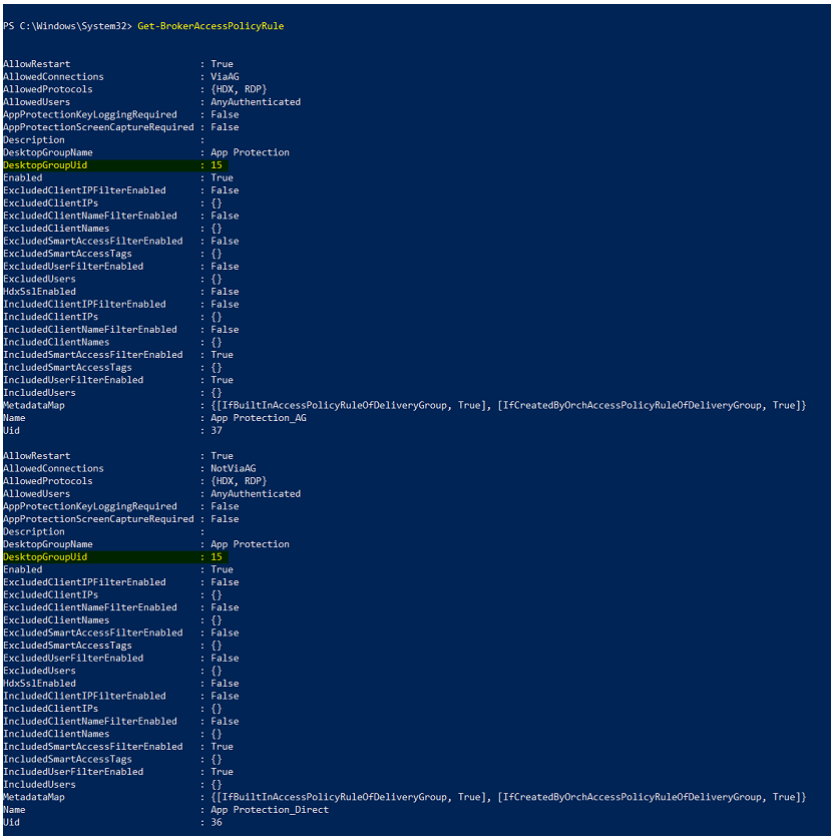
1. Wählen Sie die Active Directory-Benutzergruppe aus, für deren Mitglieder Sie die App Protection-Richtlinien aktivieren möchten. In diesem Beispiel ist dies **ProductManagers**.
2. Richtlinienregeln für den Brokerzugriff konfigurieren:

   a) Installieren Sie das Citrix PowerShell-SDK und stellen Sie eine Verbindung mit der Cloud-API her (Anweisungen siehe Citrix Blogbeitrag Getting started with PowerShell automation for Citrix Cloud).

b) Führen Sie den Befehl `Get-BrokerAccessPolicyRule` aus.

Eine Liste aller Brokerzugriffsrichtlinien für alle Bereitstellungsgruppen wird angezeigt.

c) Suchen Sie die **DesktopGroupUid** der Bereitstellungsgruppe, die Sie ändern möchten.



d) Rufen Sie die Richtlinien, die nur auf eine bestimmte Bereitstellungsgruppe angewendet werden, mit dem folgenden Befehl ab:

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) Führen Sie die folgenden Befehle aus, um die App Protection-Richtlinien für Benutzer der **ProductManagers**-Benutzergruppe zu aktivieren:

```
New-BrokerAccessPolicyRule "Example Rule Name_1"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $true -IncludedUserFilte
 $true -IncludedUsers domain.com\ProductManagers
```

f) Führen Sie die folgenden Befehle aus, um die App Protection-Richtlinien für Benutzer zu deaktivieren, die nicht zur **ProductManagers**-Benutzergruppe gehören:

```
New-BrokerAccessPolicyRule "Example Rule Name_2"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
```



```
Filtered -AppProtectionScreenCaptureRequired $false-ExcludedUserFilte
$true -ExcludedUsers domain.com\ProductManagers
```

3. Verifizierung:

   Melden Sie sich von der Citrix Workspace-App ab, falls sie bereits geöffnet ist. Melden Sie sich bei der Citrix Workspace-App als Benutzer an, der Mitglied der Active Directory-Benutzergruppe **ProductManagers** ist. Starten Sie die geschützte Ressource. Sie sehen dann, dass App Protection deaktiviert ist. Melden Sie sich bei der Citrix Workspace-App ab und melden Sie sich dann als Benutzer wieder an, der kein Mitglied der Active Directory-Benutzergruppe **ProductManagers** ist. Starten Sie die geschützte Ressource. Sie sehen dann, dass App Protection aktiviert ist.

Kontextbezogenes App Protection für StoreFront

March 11, 2024

Kontextbezogenes App Protection ermöglicht es, App Protection-Richtlinien flexibel und granular nur auf bestimmte Benutzergruppen anzuwenden –basierend auf Benutzern, ihrem Gerät und der Netzwerkstruktur.

App Protection kontextbezogen implementieren

Sie können kontextbezogenes App Protection mit den Verbindungsfiltern implementieren, die in der Brokerzugriffsrichtlinienregel definiert sind. Die Brokerzugriffsrichtlinien definieren die Regeln, die den Zugriff eines Benutzers auf Bereitstellungsgruppen steuern. Die Richtlinie umfasst mehrere Regeln. Jede Regel bezieht sich auf eine einzelne Bereitstellungsgruppe und hat eine Reihe von Verbindungsfiltern und Steuerelementen für Zugriffsrechte.

Benutzer erhalten Zugriff auf eine Bereitstellungsgruppe, wenn ihre Verbindungsdetails mit den Verbindungsfiltern einer oder mehrerer Regeln in der Brokerzugriffsrichtlinie übereinstimmen. Benutzer können standardmäßig auf keine Desktopgruppe in einer Site zugreifen. Je nach Bedarf können Sie weitere Brokerzugriffsrichtlinien erstellen. Es können mehrere Regeln für dieselbe Bereitstellungsgruppe gelten. Weitere Informationen finden Sie unter New-BrokerAccessPolicyRule.

Die folgenden Parameter in der Brokerzugriffsrichtlinienregel bieten die Möglichkeit, App Protection flexibel und kontextbezogen zu aktivieren, wenn die Verbindung des Benutzers mit den Verbindungsfiltern übereinstimmt, die in der Zugriffsrichtlinienregel definiert sind:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Verwenden Sie die Smart Access-Filter, auf die in den Brokerzugriffsrichtlinien verwiesen wird, um die Verbindungsfilter weiter anzupassen. Informationen zum Konfigurieren von Smart Access-Filtern finden Sie unter CTX227055. Die folgenden Szenarien verdeutlichen, wie Sie die Smart Access-Richtlinien zum Einrichten von kontextbezogenem App Protection verwenden.

> **Hinweis:**
>
> Wenn App Protection für die Bereitstellungsgruppe aktiviert ist, kann kontextbezogenes App Protection nicht standardmäßig angewendet werden. Deaktivieren Sie App Protection für die Bereitstellungsgruppe mit dem folgenden Befehl:

```
Set-BrokerDesktopGroup -Name "Admin Desktop" -
   AppProtectionKeyLoggingRequired $false -
   AppProtectionScreenCaptureRequired $false
<!--NeedCopy-->
```

Voraussetzungen

Um kontextbezogenes App Protection für StoreFront zu aktivieren, stellen Sie sicher, dass die im Abschnitt Voraussetzungen aufgeführten Anforderungen erfüllt sind.

Kontextbezogenes App Protection aktivieren

1. Laden Sie die Richtlinien für kontextbezogenes App Protection (Feature-Tabelle) für Ihre Version von Citrix Virtual Apps and Desktops von der Citrix-Downloadseite herunter.
2. Führen Sie den folgenden PowerShell-Befehl auf dem Delivery Controller aus:

   ```
   asnp Citrix*
   Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
   <!--NeedCopy-->
   ```

3. Führen Sie den folgenden Befehl aus, um kontextbezogenes App Protection im Delivery Controller zu aktivieren:

   ```
   Import-ConfigFeatureTable <path to the downloaded feature table>
   <!--NeedCopy-->
   ```

   Beispiel:

   ```
   Import-ConfigFeatureTable\Downloads\FeatureTable.OnPrem.
      AppProtContextualAccess.xml
   <!--NeedCopy-->
   ```


Kontextbezogenes App Protection - Szenarien

Im Folgenden finden Sie Szenarien, in denen beschrieben wird, wie Sie kontextbezogenes App Protection aktivieren bzw. deaktivieren können:

- App Protection für bestimmte Gerätetypen deaktivieren
- App Protection für Verbindungen, die über einen browserbasierten Zugriff gestartet wurden deaktivieren, und App Protection für Verbindungen, die über die Citrix Workspace-App gestartet wurden, aktivieren
- App Protection für Benutzer in einer bestimmten Active Directory-Gruppe deaktivieren
- App Protection für Geräte auf der Grundlage der EPA-Scanergebnisse aktivieren
- App Protection für spezifische Benutzergruppen aktivieren

Voraussetzungen

March 11, 2024

Bereiten Sie Folgendes vor:

- Citrix Virtual Apps and Desktops Version 2109 oder höher
- Delivery Controller Version 2109 oder höher
- StoreFront Version 1912 LTSR oder höher
- Konfigurationen mit virtuellem VPN-Server oder mit Gateway und virtuellem Authentifizierungsserver
- Erfolgreiche Verbindung zwischen NetScaler und StoreFront. Weitere Informationen finden Sie unter NetScaler Gateway in StoreFront integrieren
- XML-Tabellenimport bis Version 2006 von Citrix Virtual Apps and Desktops erforderlich
- Der Import der Tabelle für kontextbezogene App Protection ist bis zur Version 2209 von Citrix Virtual Apps and Desktops erforderlich
- Aktivieren von Smart Access auf NetScaler Gateway für Szenarien, die Smart Access-Tags erfordern. Weitere Informationen bietet dieser Supportartikel.
- Lizenzanforderungen -
  - App Protection: On-Premises-Lizenz
  - Citrix Gateway: Universallizenz für Szenarien mit Smart Access-Tags

Szenario 1

March 11, 2024

Dieses Szenario umfasst das Deaktivieren von App Protection für bestimmte Gerätetypen.

Mit der folgenden Schrittfolge deaktivieren Sie App Protection für iPhone-Benutzer in der Bereitstellungsgruppe `Win10Desktop`:

1. Erstellen Sie eine Smart Access-Richtlinie:

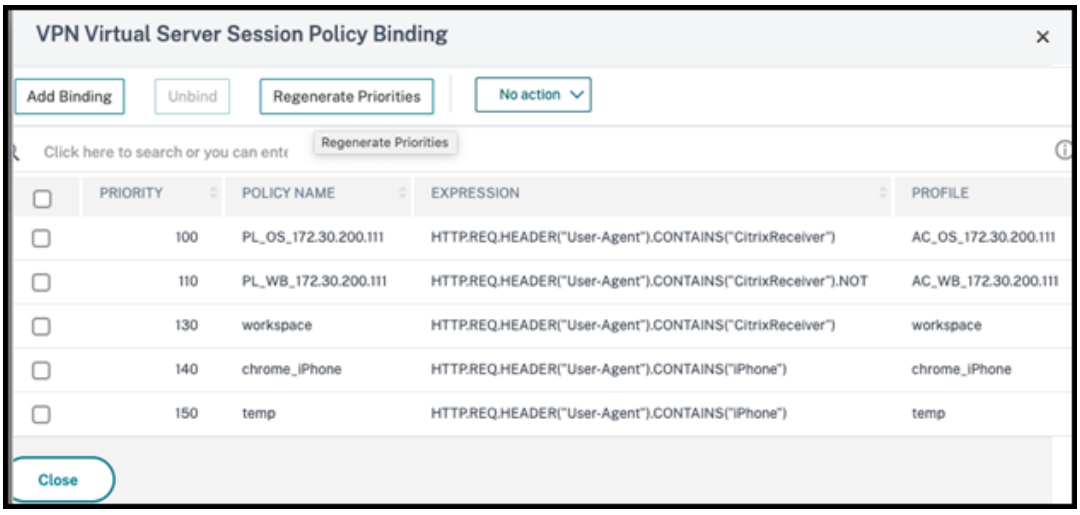
   a) Melden Sie sich bei der Verwaltungsoberfläche von Citrix ADC an.

   b) Gehen Sie im linken Navigationsmenü zu **Citrix Gateway** > **Virtual Servers**.

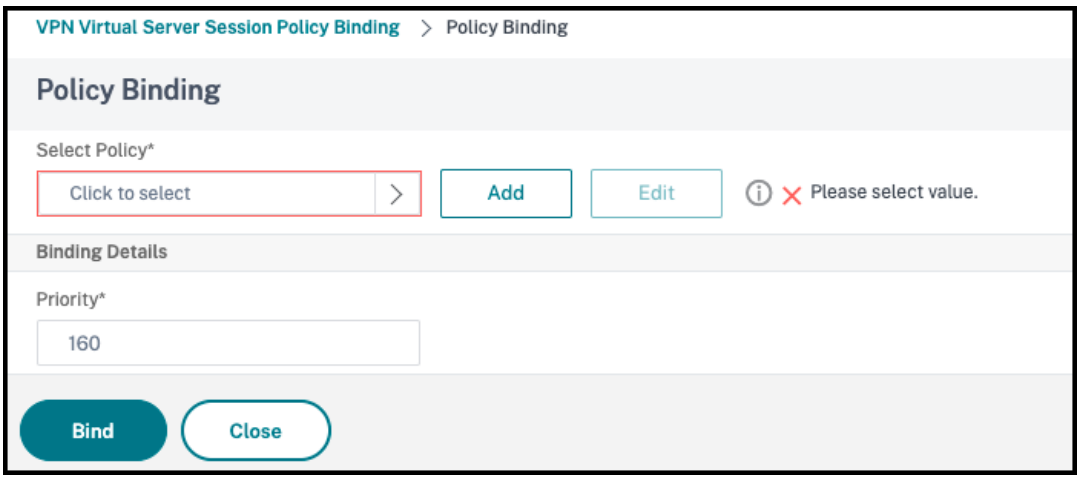
   Notieren Sie sich den Namen des virtuellen VPN-Servers. Sie benötigen ihn später für die Konfiguration der Brokerzugriffsrichtlinie.

   c) Klicken Sie auf **VPN Virtual Server**. Scrollen Sie zum Ende der Seite und klicken Sie auf **Session policies**. Eine Liste der Sitzungsrichtlinien wird angezeigt.

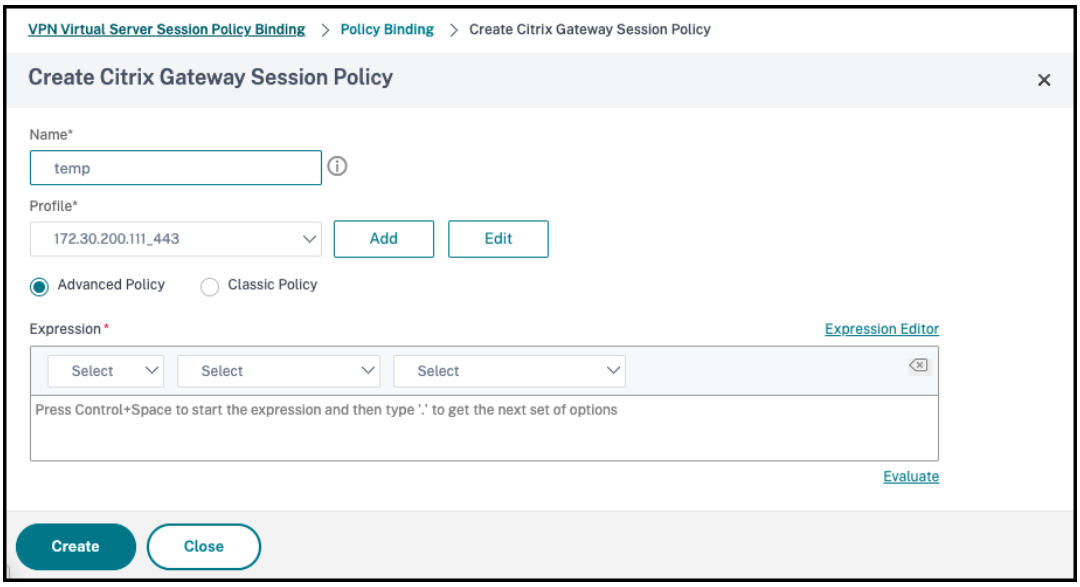
   d) Klicken Sie auf **Add binding**.



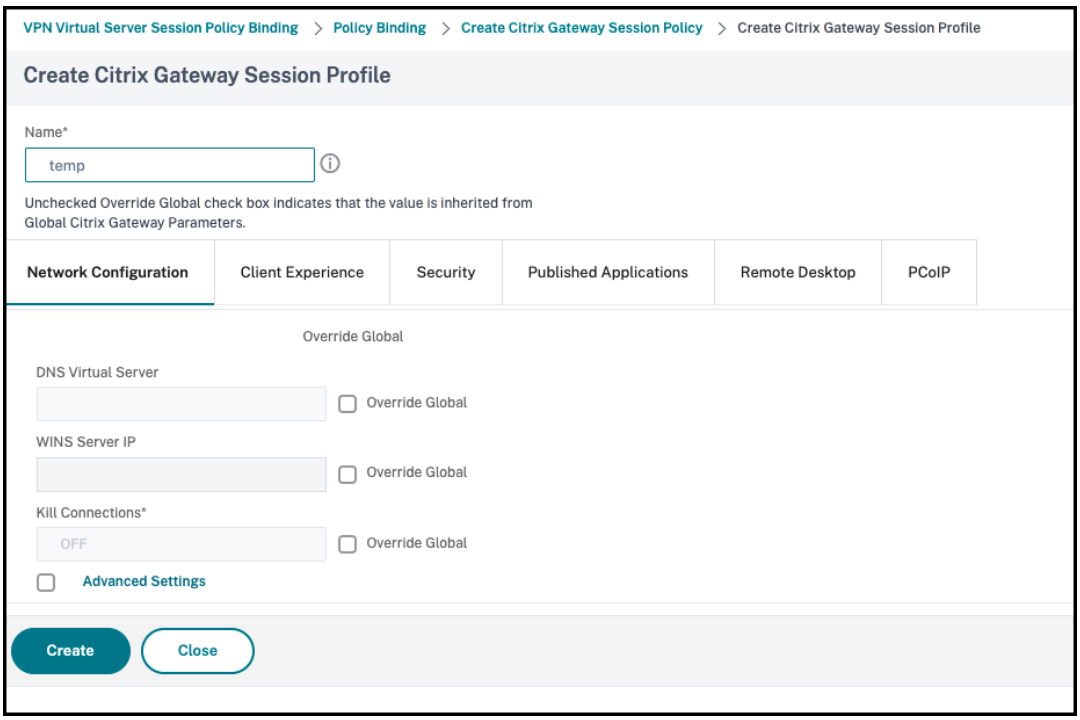
   e) Klicken Sie auf **Add to create a session policy**.



f) Geben Sie einen Namen für die Sitzungsrichtlinie ein. In diesem Szenario ist dies *temp*.



g) Klicken Sie neben “Profile”auf **Add**, um einen Profilnamen anzugeben. Klicken Sie auf **Erstellen**.



h) Klicken Sie im Fenster der Sitzungsrichtlinie auf **Expression Editor**.

i) Erstellen Sie den folgenden Ausdruck, um in der Zeichenfolge **User Agent** nach *iPhone* zu suchen:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
<!--NeedCopy-->
```

j) Klicken Sie auf **Bind**, um die Sitzungsrichtlinie zu erstellen.

2. Brokerzugriffsrichtlinienregeln erstellen:

   Mit der folgenden Schrittfolge wenden Sie die Richtlinie auf iPhone-Benutzer an, die über das Access Gateway auf `Win10Desktop` zugreifen:

   a) Führen Sie den folgenden Befehl im Desktop Delivery Controller (DDC) aus:

```
Get-BrokerAccessPolicyRule
<!--NeedCopy-->
```


Damit werden alle im DDC definierten Brokerzugriffsrichtlinien aufgeführt. In diesem Szenario sind `Win10Desktop_AG` und `Win10Desktop_Direct` die Brokerzugriffsrichtlinien für die Bereitstellungsgruppe `Win10Desktop`. Notieren Sie sich die Desktopgruppen-UID der Bereitstellungsgruppe für den nächsten Schritt.

b) Erstellen Sie mit dem folgenden Befehl eine Brokerzugriffsrichtlinienregel für `Win10Desktop` um nach iPhone-Benutzern zu filtern, die über Access Gateway geleitet werden:

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

Uid_of_desktopGroup ist die DesktopGroupUID der Bereitstellungsgruppe, die durch Ausführen der Regel "GetBrokerAccessPolicy"in Schritt 1 ermittelt wurde.

c) Um App Protection für iPhone-Benutzer zu deaktivieren, die über Access Gateway auf `Win10Desktop` zugreifen, verweisen Sie auf das Smart Access-Tag *temp*, das in Schritt 1 erstellt wurde. Erstellen Sie mit dem folgenden Befehl eine Smart Access-Richtlinie:

```
1 Set-BrokerAccessPolicyRule Win10Desktop_AG_iPhone -
      IncludedSmartAccessTags Primary_HDX_Proxy:temp -
      AppProtectionScreenCaptureRequired $false -
      AppProtectionKeyLoggingRequired $false
2 <!--NeedCopy-->
```

Primary_HDX_Proxy ist der Name des virtuellen VPN-Servers aus Schritt 1: Erstellen einer Smart Access-Richtlinie.

d) Verwenden Sie den folgenden Befehl, um App Protection-Richtlinien für die übrigen `Win10desktop`-Benutzer zu aktivieren:

```
1 Set-BrokerAccessPolicyRule Win10Desktop_AG -
      AppProtectionScreenCaptureRequired $true -
      AppProtectionKeyLoggingRequired $true
2 <!--NeedCopy-->
```

3. **Verifizierung**

Für iPhone: Melden Sie sich von der Citrix Workspace-App ab, falls sie auf dem iPhone bereits geöffnet ist. Melden Sie sich extern über eine Access Gateway-Verbindung bei der Citrix Workspace-App an. Sie können die erforderlichen Ressourcen in StoreFront sehen und App Protection muss deaktiviert sein.

Andere Geräte als iPhones: Melden Sie sich von der Citrix Workspace-App ab, falls sie auf dem Gerät bereits geöffnet ist. Melden Sie sich extern über eine Access Gateway-Verbindung bei der

Citrix Workspace-App an. Sie können die erforderlichen Ressourcen in StoreFront sehen und App Protection muss deaktiviert sein.

Szenario 2

March 11, 2024

Dieses Szenario umfasst das Deaktivieren von App Protection für Verbindungen, die über einen browserbasierten Zugriff gestartet wurden, und zum Aktivieren von App Protection für Verbindungen, die über die Citrix Workspace-App gestartet wurden.

Mit der folgenden Schrittfolge deaktivieren Sie App Protection für die Bereitstellungsgruppe `Win10Desktop`, wenn Verbindungen über einen Browser gestartet werden, und aktivieren App Protection für Verbindungen über die Citrix Workspace-App:

1. Smart Access-Richtlinien erstellen:

   a) Erstellen Sie eine Smart Access-Richtlinie, um nach den von der Citrix Workspace-App gestarteten Verbindungen zu filtern (siehe obiges Szenario **App Protection für bestimmte Gerätetypen deaktivieren**). Erstellen Sie den folgenden Ausdruck, um in der Zeichenfolge **User Agent** nach **CitrixReceiver** zu suchen:

   ```
   1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
   2 <!--NeedCopy-->
   ```

   In diesem Szenario lautet die Smart Access-Richtlinie `cwa`.

   b) Erstellen Sie eine weitere Smart Access-Richtlinie, um nach Verbindungen zu filtern, die nicht über die Citrix Workspace-App gestartet werden: `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT`. In diesem Fall lautet die Smart Access-Richtlinie *browser*.

2. Brokerzugriffsrichtlinienregeln erstellen:

   a) Führen Sie `GetBrokerAccessPolicyRule` aus, um die beiden Brokerzugriffsrichtlinien für `Win10Desktop` anzuzeigen. Für die Bereitstellungsgruppe `Win10Desktop` lauten die Broker-Zugriffsrichtlinien `Win10Desktop_AG` und `Win10Desktop_Direct`. Notieren Sie sich die Desktop-Gruppen-UID von `Win10Desktop`.

   b) Erstellen Sie mithilfe des folgenden Befehls eine Brokerzugriffsrichtlinie für `Win10Desktop`, um nach Verbindungen zu filtern, die über die Citrix Workspace-App gestartet wurden:

```
1 New-BrokerAccessPolicyRule -Name Win10Desktop_AG_CWA -
      DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
      ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
      AnyAuthenticated -AllowRestart $true -Enabled $true -
      IncludedSmartAccessFilterEnabled $true
2 <!--NeedCopy-->
```

   Uid_of_desktopGroup ist die DesktopGroupUID der Bereitstellungsgruppe, die durch Ausführen der Regel "GetBrokerAccessPolicy"in Schritt 1 ermittelt wurde.

   c) Verwenden Sie den folgenden Befehl, um App Protection-Richtlinien nur für Verbindungen zu aktivieren, die über CWA kommen, indem Sie auf das Smart Access-Tag `cwa` verweisen:

```
1 Set-BrokerAccessPolicyRule Win10Desktop_AG_CWA -
      IncludedSmartAccessTags Primary_HDX_Proxy:cwa -
      AppProtectionScreenCaptureRequired $true -
      AppProtectionKeyLoggingRequired $true
2 <!--NeedCopy-->
```

   Primary_HDX_Proxy ist der Name des virtuellen VPN-Servers, den Sie in Schritt 1: Erstellen einer Smart Access-Richtlinie notiert haben.

   d) Verwenden Sie den folgenden Befehl, um App Protection-Richtlinien für die übrigen Verbindungen zu deaktivieren, die über den Browser eingehen:

```
1 Set-BrokerAccessPolicyRule Win10Desktop_AG -
      IncludedSmartAccessTags Primary_HDX_Proxy:browser -
      AppProtectionScreenCaptureRequired $false -
      AppProtectionKeyLoggingRequired $false
2 <!--NeedCopy-->
```

3. **Verifizierung**

Melden Sie sich von der Citrix Workspace-App ab, falls sie bereits geöffnet ist. Melden Sie sich erneut an der Citrix Workspace-App an, und starten Sie die erforderliche Ressource von einer externen Verbindung über Access Gateway. Sie sehen, dass die App Protection-Richtlinien für die Ressource aktiviert sind. Starten Sie dieselbe Ressource vom Browser aus über eine externe Verbindung. Sie sehen dann, dass die App Protection-Richtlinien deaktiviert sind.

Szenario 3

March 11, 2024

Dieses Szenario umfasst das Deaktivieren von App Protection für Benutzer in einer bestimmten Active Directory-Gruppe.

Mit der folgenden Schrittfolge deaktivieren Sie App Protection für `Win10Desktop`-Benutzer, die zur Active Directory-Gruppe **xd.local\sales** gehören:

1. Führen Sie `Get-BrokerAccessPolicyRule` aus, um die beiden Brokerzugriffsrichtlinien für `Win10Desktop` anzuzeigen. Für eine Bereitstellungsgruppe `Win10Desktop` gibt es zwei Broker-Zugriffsrichtlinien, `Win10Desktop_AG` und `Win10Desktop_Direct`. Notieren Sie sich die Desktopgruppen-UID von `Win10Desktop`.
2. Erstellen Sie eine Brokerzugriffsrichtlinienregel für `Win10Desktop`, um nach Verbindungen von Benutzern in der Active Directory-Gruppe `xd.local\sales` zu filtern.

```
1 New-BrokerAccessPolicyRule -Name Win10Desktop_AG_Sales_Group -
     DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections ViaAG
      -AllowedProtocols HDX, RDP -AllowedUsers Filtered -
     AllowRestart $true -Enabled $true
2 <!--NeedCopy-->
```

   Uid_of_desktopGroup ist die DesktopGroupUID der Bereitstellungsgruppe, die durch Ausführen der Regel "GetBrokerAccessPolicy"in Schritt 1 ermittelt wurde.
3. Verwenden Sie den folgenden Befehl, um App Protection-Richtlinien für die Windows 10 Desktop-Benutzer zu deaktivieren, die zur AD-Gruppe **xd.local\sales** gehören:

```
1 Set-BrokerAccessPolicyRule Win10Desktop_AG_Sales_Group -
     AllowedUsers Filtered -IncludedUsers xd.local\sales -
     IncludedUserFilterEnabled $true -
     AppProtectionScreenCaptureRequired $false -
     AppProtectionKeyLoggingRequired $false
2 <!--NeedCopy-->
```

4. Verwenden Sie den folgenden Befehl, um App Protection-Richtlinien für die übrigen Gateway-Verbindungen mit Ausnahme der Benutzer aus **xd.local\sales** zu aktivieren:


```
Set-BrokerAccessPolicyRule Win10Desktop_AG -AllowedUsers
    Anyauthenticated -ExcludedUserFilterEnabled $true -
    ExcludedUsers xd.local\sales -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

5. **Verifizierung**

   Melden Sie sich von der Citrix Workspace-App ab, falls sie bereits geöffnet ist. Melden Sie sich bei der Citrix Workspace-App als Benutzer in der Active Directory-Gruppe **xd.local\sales** an. Starten Sie die geschützte Ressource. Sie sehen dann, dass App Protection deaktiviert ist.

   Melden Sie sich von der Citrix Workspace-App ab und melden Sie sich erneut als Benutzer an, der nicht zu **xd.local\sales** gehört. Starten Sie die geschützte Ressource. Sie sehen dann, dass App Protection aktiviert ist.

Szenario 4

March 11, 2024

In diesem Szenario wird beschrieben, wie Sie App Protection für Geräte auf der Grundlage der EPA-Scanergebnisse aktivieren.

Im Folgenden finden Sie die Schritte, um App Protection für die Geräte zu aktivieren, die die EPA-Scans bestehen:

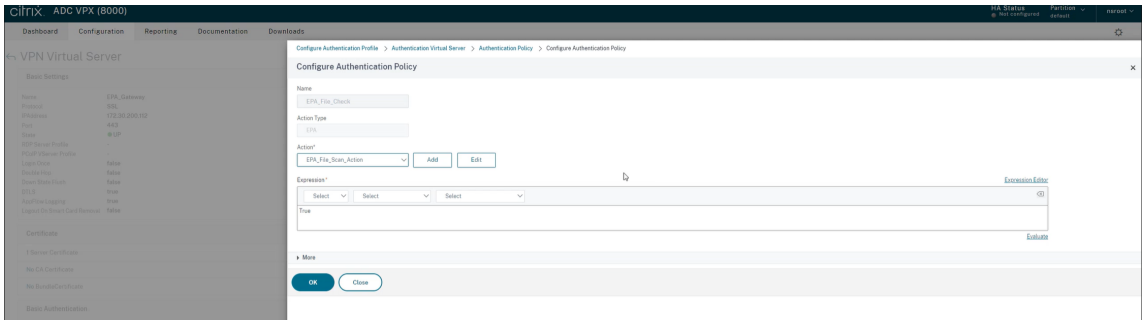
Voraussetzungen:

Bereiten Sie Folgendes vor:

- Benutzergruppen für Authentifizierung, Autorisierung und Überwachung (für standardmäßige Benutzergruppen und solche in Quarantäne) und zugehörige Richtlinien
- LDAP-Serverkonfigurationen und zugehörige Richtlinien

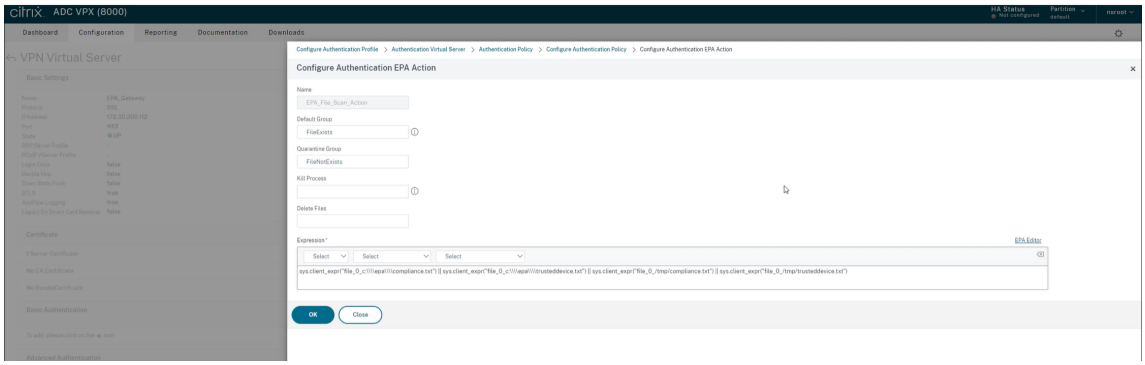
1. Melden Sie sich bei Citrix ADC an und gehen Sie zu **Configuration** > **Citrix Gateway** > **Virtual Servers**.
2. Wählen Sie den relevanten virtuellen Server aus und klicken Sie auf **Edit**.
3. Bearbeiten Sie das bestehende Authentifizierungsprofil.
4. Wählen Sie den relevanten virtuellen Server aus und klicken Sie auf **Edit**.
5. Klicken Sie auf **Authentication Policies** > **Add Binding**.
6. Klicken Sie unter **Select Policy** auf **Add**.

7. Geben Sie im Feld **Name** den Namen der Authentifizierungsrichtlinie ein.
8. Wählen Sie in der Dropdownliste **Action Type** die Option **EPA**.
9. Geben Sie im Feld **Expression** den Wert `True` ein.



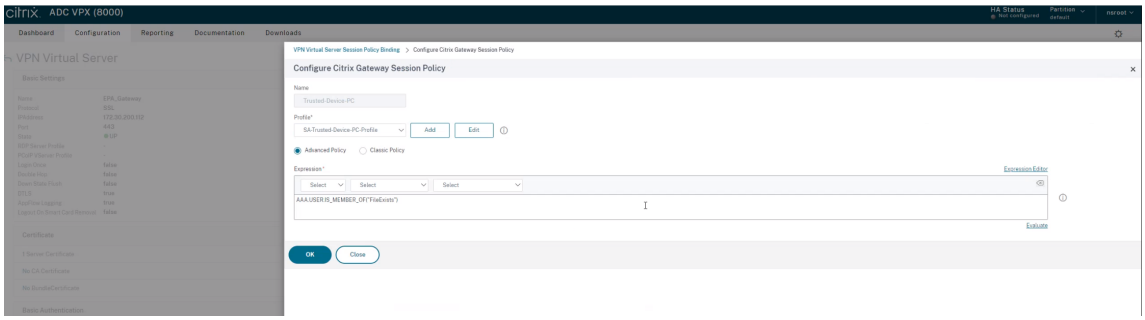
10. Klicken Sie unter **Action** auf **Add**.
11. Geben Sie im Feld **Name** den Namen der EPA-Aktion ein.
12. Geben Sie Namen für **Default Group** und **Quarantine Group** ein. In diesem Szenario lautet der Name der **Standardgruppe** auf **FileExists** und der Name der **Quarantänegruppe** auf **FileNotExists**.
13. Geben Sie im Feld **Expression** den folgenden Wert ein:

```
1 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")
2 <!--NeedCopy-->
```



14. Klicken Sie auf **Create** und dann auf **Bind**.
15. Klicken Sie auf **Session Policies** > **Add Binding**.
16. Klicken Sie unter **Select Policy** auf **Add**.
17. Geben Sie im Feld **Name** den Namen der Sitzungsrichtlinie ein.
18. Geben Sie im Feld **Expression** den folgenden Wert ein:


```
AAA.USER.IS_MEMBER_OF("FileExists")
<!--NeedCopy-->
```



19. Klicken Sie auf **Create** und dann auf **Bind**.
20. Klicken Sie ganz links in der Taskleiste auf das **Suchsymbol** .
21. Geben Sie **Powershell** ein und öffnen Sie **Windows Powershell**.
22. Verwenden Sie den folgenden Befehl, um App Protection-Richtlinien für Geräte zu deaktivieren, die die EPA-Scans bestanden haben, indem Sie auf das Smart Access-Tag **EPA_GW:Trusted-Device-PC** verweisen:

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG" -IncludedSmartAccessFilterEnabled $true -
    IncludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    AppProtectionScreenCaptureRequired $false
<!--NeedCopy-->
```

wobei *EPA_GW* der Name des virtuellen VPN-Servers ist.

23. Verwenden Sie den folgenden Befehl, um App Protection-Richtlinien für Geräte zu aktivieren, die die EPA-Scans nicht bestanden haben, indem Sie auf das Smart Access-Tag **EPA_GW:Trusted-Device-PC** verweisen:

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

24. **Verifizierung**

    Melden Sie sich von der Citrix Workspace-App ab, falls sie bereits geöffnet ist. Melden Sie sich mit einem vertrauenswürdigen Gerät bei der Citrix Workspace-App an. Starten Sie die geschützte Ressource. Sie sehen dann, dass App Protection deaktiviert ist.

Melden Sie sich von der Citrix Workspace-App ab und melden Sie sich mit einem nicht vertrauenswürdigen Gerät wieder an. Starten Sie die geschützte Ressource. Sie sehen dann, dass App Protection aktiviert ist.

Szenario 5

November 22, 2023

In diesem Szenario wird beschrieben, wie App Protection für spezifische Benutzergruppen aktiviert wird.

Informationen zum Aktivieren von App Protection für Benutzer einer bestimmten Gruppe finden Sie unter App Protection für spezifische Benutzergruppen aktivieren.

App Protection-Unterstützung für den Hybridstart über Workspace

March 11, 2024

Beim Hybridstart von Citrix Virtual Apps and Desktops melden Sie sich bei Citrix Workspace für Web durch Eingabe der Store-URL im nativen Browser an und starten dann virtuelle Apps und Desktops über die native Citrix Workspace-App und ihre HDX-Engine. Der Begriff "hybrid"verweist darauf, dass Citrix Workspace-App für Web und native Citrix Workspace-App kombiniert werden, um eine Verbindung herzustellen und die Ressourcen zu verwenden.

> **Hinweis:**
>
> Wenn auf dem Endpunkt keine Komponenten der nativen Citrix Workspace-App installiert sind, handelt es sich um eine Zero-Install-Konfiguration, wobei sich Citrix Workspace-Store und HDX Engine im Browser befinden. Dieses Szenario ist als Citrix Workspace-App für HTML5 bekannt und wird in Citrix Workspace oder in Citrix StoreFront gehostet. Dieses Dokument beschreibt dieses Szenario nicht.

Voraussetzungen

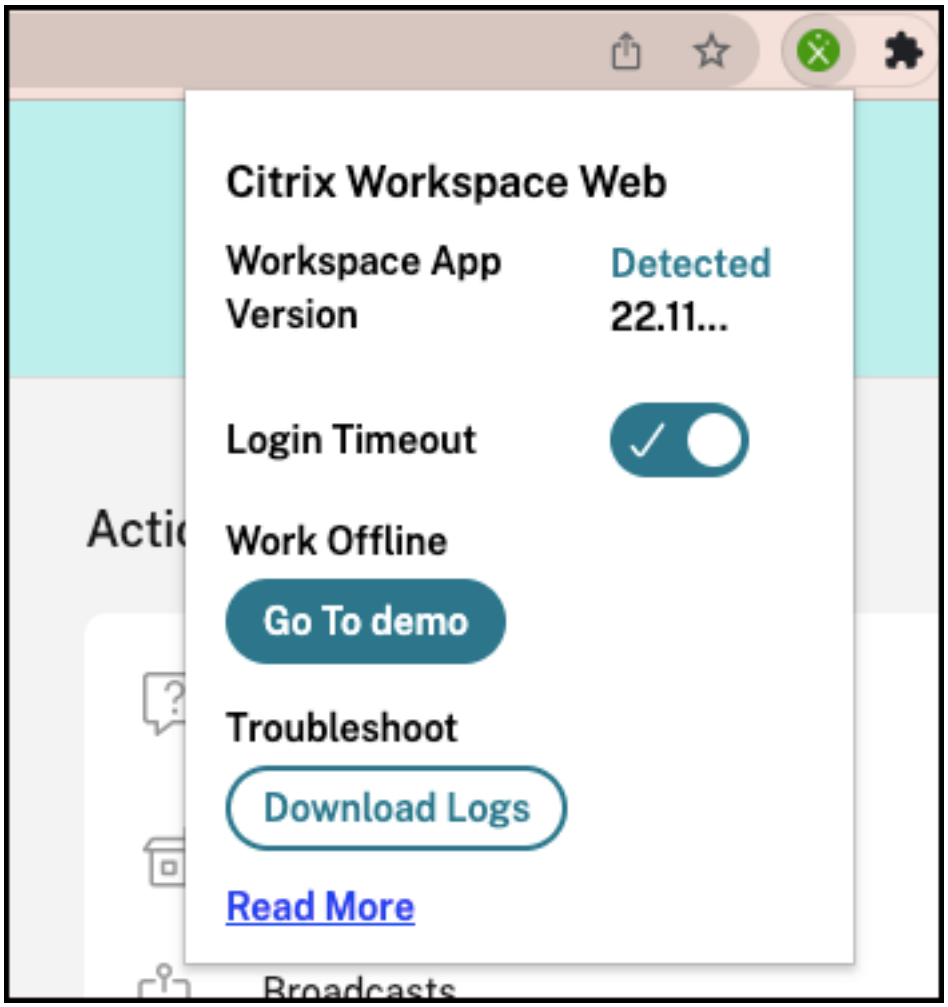
- Achten Sie darauf, einen Browser zu verwenden, der die Citrix Workspace Weberweiterung unterstützt.
- Achten Sie darauf, cloud.com als DNS-Suffix Ihrer Workspace-URL zu verwenden. Benutzerdefinierte Domänen werden derzeit nicht unterstützt.

- Achten Sie darauf, eine der folgenden Versionen der Citrix Workspace-App zu verwenden:
  - Citrix Workspace-App für Windows 2106 oder höher
  - Citrix Workspace-App für macOS 2106 oder höher

App Protection für Hybridstart aktivieren

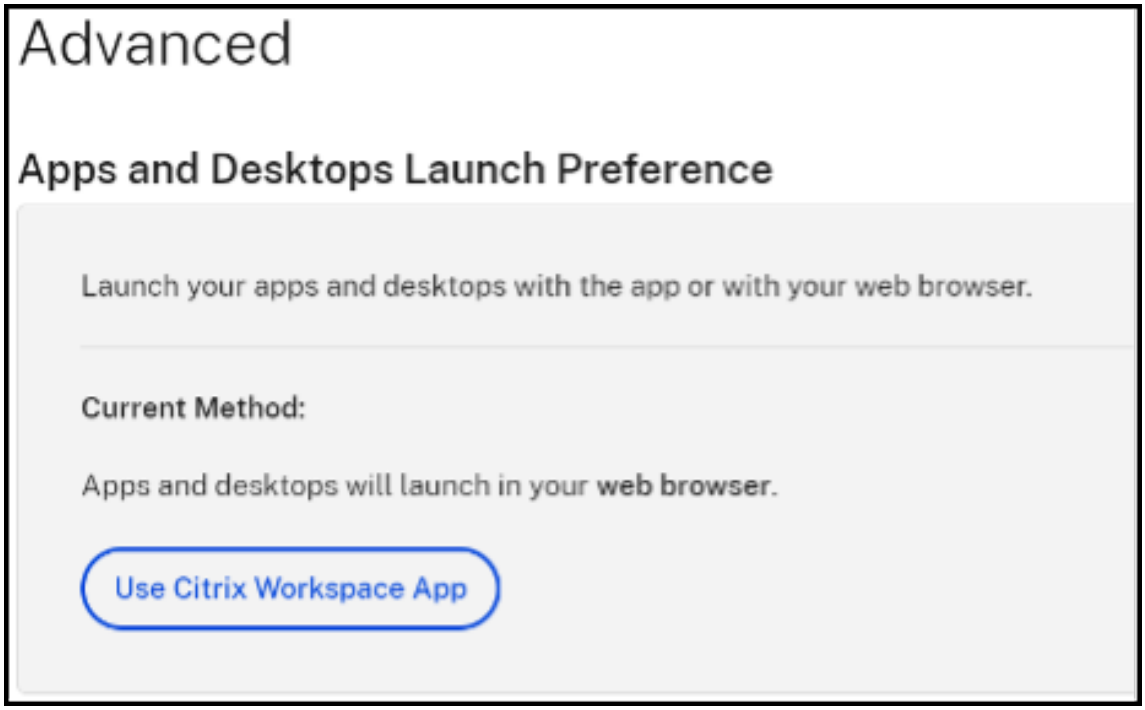
1. Installieren Sie die Citrix Workspace Web-Erweiterung für Ihren Browser, bevor Sie den Store hinzufügen. Verwenden Sie je nach vorhandenem Browser einen der folgenden Links:
   - Chrome
   - Edge Chromium

   Die Erweiterung wird nach der Installation im Browser-Abschnitt für Erweiterungen angezeigt.

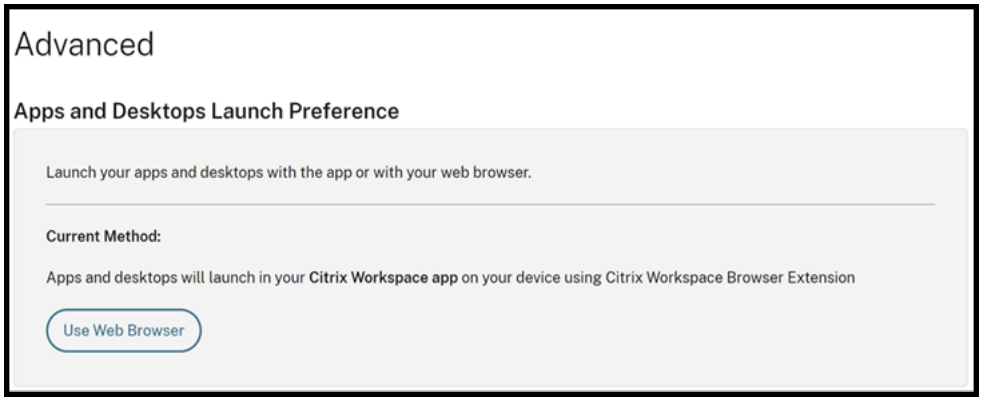


2. Melden Sie sich über Ihren nativen Browser am Store an.
3. Navigieren Sie zu **Profil > Kontoeinstellungen > Erweitert**.

Im Abschnitt **Startpräferenz für Apps und Desktops** sehen Sie, welches Verfahren aktuell zum Starten von Apps und Desktops im Webbrowser genutzt wird. Klicken Sie auf **Citrix Workspace-App verwenden**.



Wenn Sie die Citrix Workspace-App zum Start der Ressourcen verwenden, wird die folgende Option angezeigt. In diesem Fall sind keine Änderungen erforderlich.



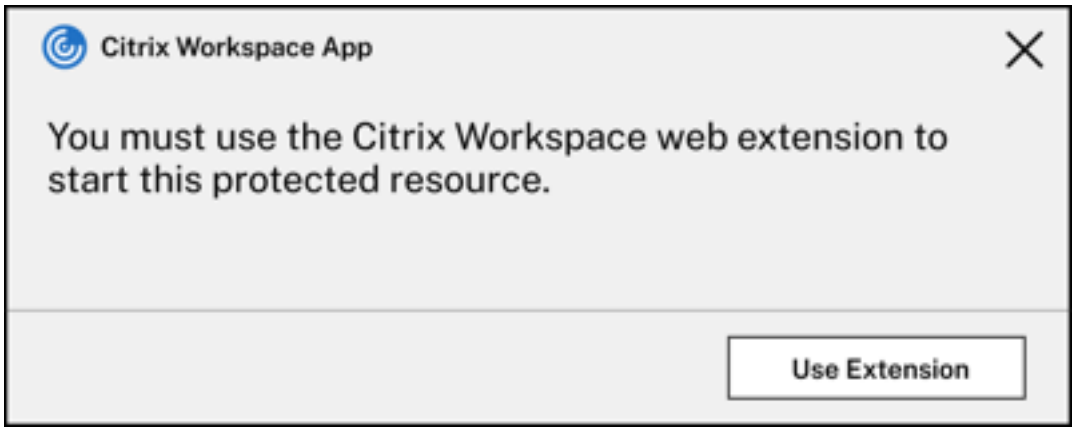
4. Sie können jetzt Ihre geschützte virtuelle App oder den geschützten Desktop starten.

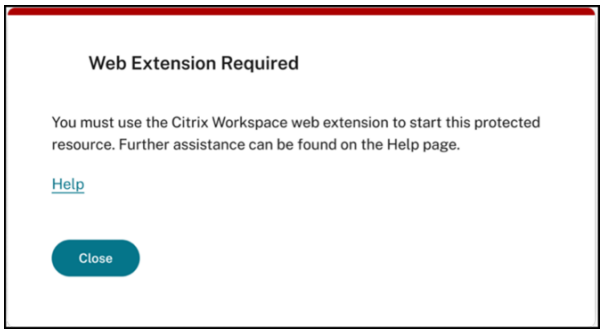
Häufig auftretende Fehler

Die folgenden Szenarien zeigen, welche Fehler beim Start möglich sind und wie sie behoben werden können.

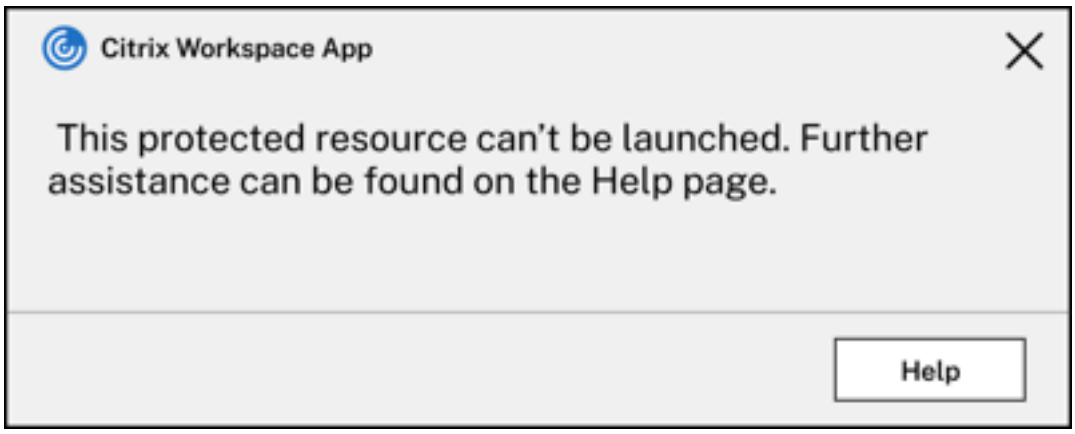
- Einer der folgenden Fehler wird angezeigt, wenn Sie die Citrix Workspace Web-Erweiterung

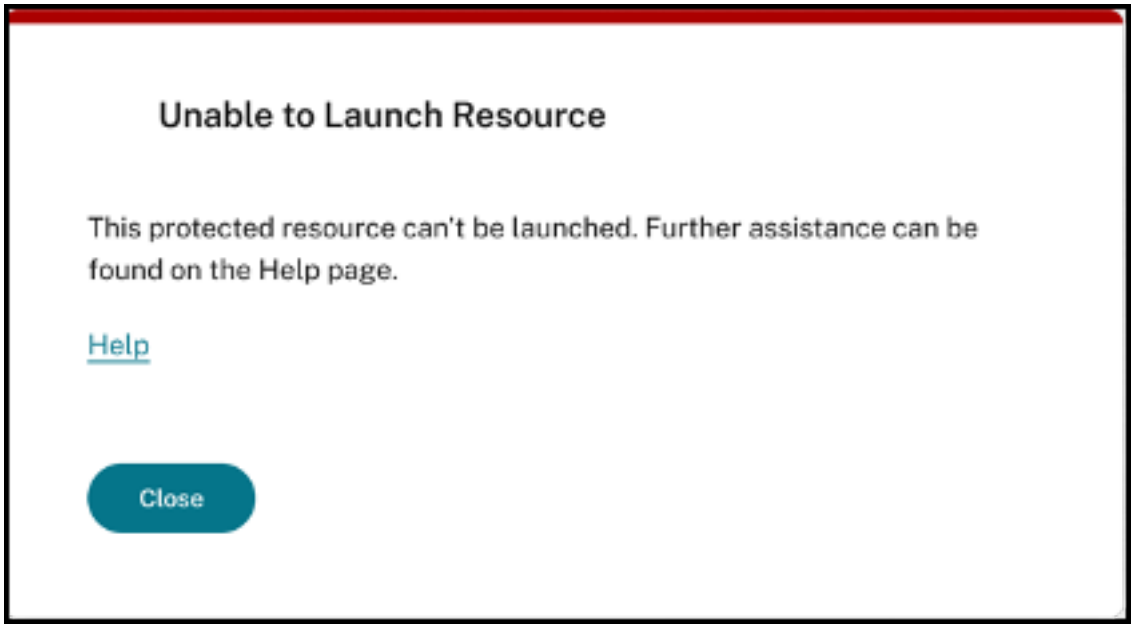
deaktivieren oder deinstallieren, bevor Sie die geschützte Anwendung starten. Installieren Sie die Erweiterung, bevor Sie sich bei Citrix Workspace für Web anmelden, um dies zu vermeiden.





- Sie erhalten einen der folgenden Fehler, wenn die Startpräferenz auf **Webbrowser** festgelegt ist. Ändern Sie die Startpräferenz in **Citrix Workspace-App verwenden**, um diesen Fehler zu beheben. Weitere Informationen bietet dieser Supportartikel.





App Protection-Unterstützung für den Hybridstart über StoreFront

March 11, 2024

Beim Hybridstart von Citrix Virtual Apps and Desktops melden Sie sich bei StoreFront für Web durch Eingabe der Store-URL im nativen Browser an und starten dann virtuelle Apps und Desktops über die native Citrix Workspace-App und ihre HDX-Engine. Der Begriff "Hybrid"verweist darauf, dass StoreFront für Web und die native Citrix Workspace-App kombiniert werden, um eine Verbindung herzustellen und die Ressourcen zu verwenden.

> **Hinweis:**
>
> Wenn auf dem Endpunkt keine Komponenten der nativen Citrix Workspace-App installiert sind, handelt es sich um eine Zero-Install-Konfiguration, wobei sich Citrix Workspace-Store und HDX Engine im Browser befinden. Dieses Szenario ist als Citrix Workspace-App für HTML5 bekannt und wird in Citrix Workspace oder in Citrix StoreFront gehostet. Dieses Dokument beschreibt dieses Szenario nicht.

App Protection-Unterstützung für Hybridstart über StoreFront ermöglicht es Ihnen, Ressourcen mit aktiviertem Anwendungsschutz anzuzeigen und von Browsern aus zu starten.

> **Hinweis:**
>
> Bei Auswahl der Optionen **Lightversion verwenden** (die den HTML5-Client verwendet) bzw. **Bereits installiert** werden Sitzungen mit aktiviertem App Protection blockiert, da die Citrix

> Workspace-App im Browser nicht erkannt wird.

Wenn Sie StoreFront 2308 oder höher verwenden, können Sie mit einem Webbrowser auf die Apps und Desktops zugreifen, für die App Protection-Richtlinien aktiviert sind, sofern StoreFront entsprechend konfiguriert ist und der Browser die native Citrix Workspace-App erfolgreich erkennt. Wenn Sie Versionen zwischen StoreFront 1912 und 2203 verwenden, müssen Sie die Anpassung anwenden, wie unter Bereitstellen beschrieben.

> **Einschränkung:**
>
> StoreFront ermittelt die Version der Citrix Workspace-App, wenn Sie sich zum ersten Mal bei der Website anmelden. Wenn Sie später eine andere Version der Citrix Workspace-App installieren, erkennt StoreFront die Änderung nicht. Daher kann es das Starten virtueller Apps und Desktops, für die App Protection-Richtlinien aktiviert sind, falsch zulassen bzw. verbieten. Citrix empfiehlt, App Protection Posture Check zu konfigurieren, um den Start von Virtual Apps and Desktops aus früheren Versionen der Citrix Workspace-App, die App Protection nicht unterstützen, zu unterbinden. Weitere Informationen zur Statusprüfung finden Sie unter App Protection Posture Check.

Hybrider Start über StoreFront Version 2308 oder höher

StoreFront unterstützt ab Version 2308 automatisch den hybriden Start von Virtual Apps and Desktops mit aktivierten App Protection-Richtlinien. Weitere Informationen zur Aktivierung von App Protection für den hybriden Start unter StoreFront 2308 oder höher finden Sie unter App Protection für Hybridstart mit StoreFront.

Hybrider Start über StoreFront-Versionen zwischen 1912 und 2203

StoreFront-Versionen zwischen 1912 und 2203 unterstützen die Aktivierung des Hybridstarts virtueller Apps und Desktops mit aktivierten App Protection-Richtlinien unter Verwendung einer Anpassung wie folgt:

Citrix empfiehlt das Entfernen der Anpassung, wenn Sie ein Upgrade auf StoreFront 2308 oder höher durchführen.

Voraussetzungen

Informationen zu den für App Protection benötigten Versionen der Citrix-Komponenten finden Sie unter Systemanforderungen.

Bereitstellung

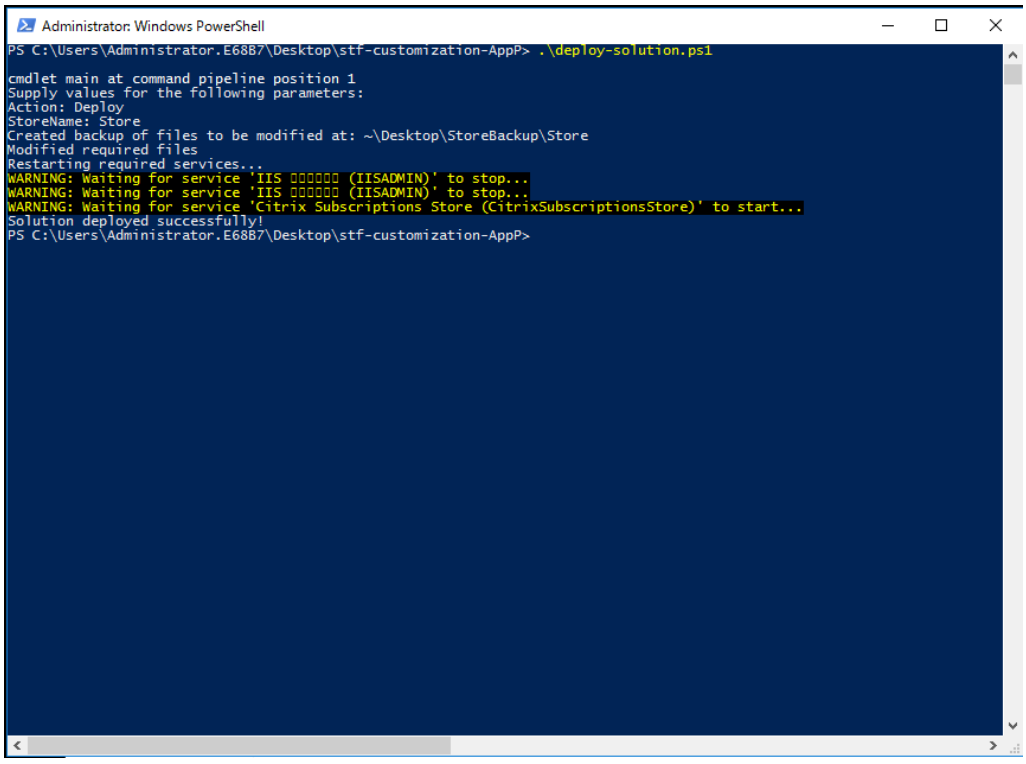
1. Laden Sie die Zip-Datei *stf-customization-AppP.zip* herunter. Sie enthält alle Dateien, die Sie auf dem StoreFront-Server bereitstellen müssen. Laden Sie die Datei von der Citrix Downloadseite herunter. In der Zip-Datei ist Folgendes enthalten:

   - DLL-Dateien, die Sie in den Ordner "bin"des Stores kopieren müssen
   - JavaScript-Dateien und andere Dateien, die zum Ausführen der Lösung erforderlich sind
   - das PowerShell-Skript *deploy-solution.ps1*, das der StoreFront-Administrator zum Bereitstellen der Lösung verwendet

2. Entpacken Sie die Datei *stf-customization-AppP.zip* und öffnen Sie eine neue Administrator-PowerShell, wo die Dateien extrahiert wurden. Führen Sie den Befehl `deploy-solution.ps1` aus, der folgende Argumente akzeptiert:

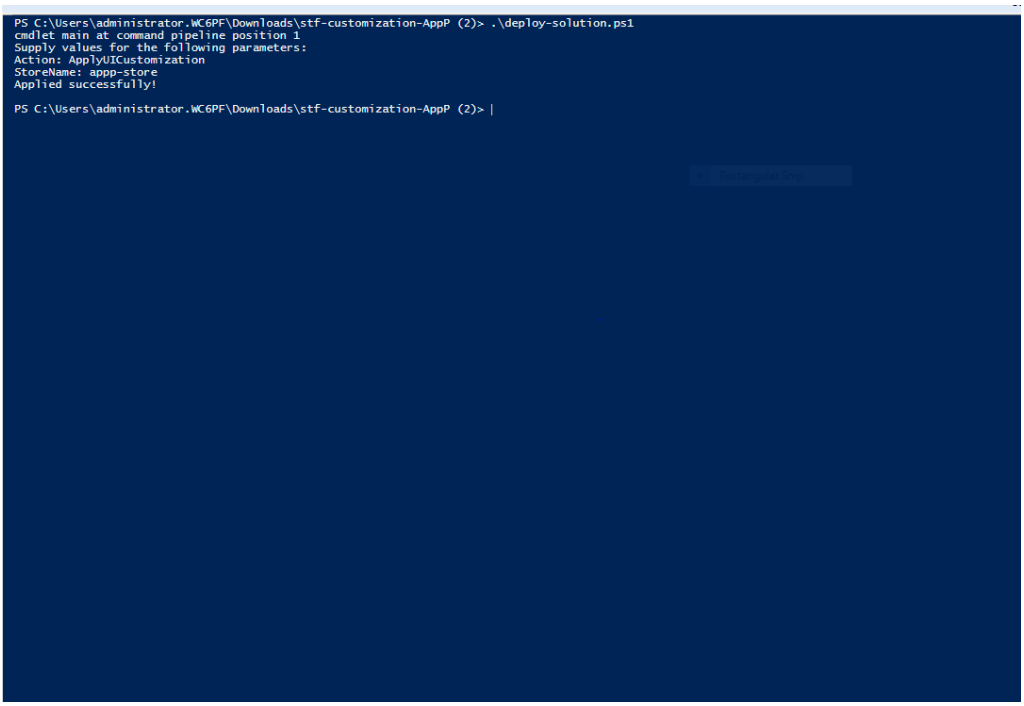
   - `-Action`: Die vom Skript ausgeführte Aktion. Folgende Werte sind zulässig:

     - Mit der Aktion `Deploy` wird die Lösung nahtlos bereitgestellt. Nach einem Backup aller Dateien, die von der Lösung geändert werden, werden die Dateien der Lösung kopiert und die Dienste neu gestartet. Der folgende Screenshot zeigt den Befehl zum Bereitstellen der Lösung auf dem StoreFront-Server:



     - Die Aktion `ApplyUICustomization` passt die Store-Benutzeroberfläche an, sodass die Optionen **Bereits installiert** und **Lightversion verwenden** nicht angezeigt werden. Diese Aktion erzwingt das Erkennen der nativen Citrix Workspace-App im

Browser und stellt sicher, dass Sie die blockierten oder nicht unterstützten Szenarien umgehen.



  - Die Aktion `RemoveUICustomization` macht die Aktion `ApplyUICustomization` rückgängig. Die Optionen **Bereits installiert** und **Lightversion verwenden** werden erneut angezeigt.

- `-StoreName`: Name des Stores, für den die Aktion ausgeführt werden muss. Dieser Parameter ist obligatorisch und muss mit der Aktion `Deploy` angegeben werden.
- `-BackupDir`: Parameter, der mit der Aktion `Deploy` angegeben werden kann, um ein Backup im erforderlichen Verzeichnis zu erstellen. Wenn kein Parameter angegeben wird, wird das Backup auf dem Desktop erstellt. Dieser Parameter ist optional.

> **Hinweis:**
>
> Wenn Anpassungen in den Dateien *StoreCustomization_Input.dll* oder *StoreCustomization_Launch.dll* vorliegen, werden sie durch das Bereitstellen dieser Lösung überschrieben.

Die Apps und Desktops mit aktiviertem App Protection werden erst angezeigt, nachdem die Anpassungen bereitgestellt wurden. Ohne die Bereitstellung werden die Apps und Desktops nicht angezeigt.

So machen Sie die StoreFront-Anpassung rückgängig

Gehen Sie wie folgt vor, um die vorherige StoreFront-Anpassung rückgängig zu machen:

1. Gehen Sie zum Verzeichnis *\Desktop\StoreBackup<store name>* und kopieren Sie die folgenden Dateien in die entsprechenden Verzeichnisse:

   - Die Dateien *StoreCustomization_Input.dll* und *StoreCustomization_Launch.dll* in das Verzeichnis *IISINETPub\Citrix<store name>\bin*
   - Die Datei *web.config* in das Verzeichnis *IISINETPub\Citrix\StoreWeb*
   - Die Dateien **.js* und *style.css* in das Verzeichnis *IISINETPub\Citrix\StoreWeb\Custom*

   > **Hinweis:**
   >
   > Wenn im Verzeichnis \Desktop\StoreBackup<store name> andere Anpassungsdateien enthalten sind als die vorgenannten, kopieren Sie nach Bedarf diese Dateien und Verzeichnisse in die entsprechenden Verzeichnisse.

2. Öffnen Sie PowerShell.
3. Beenden Sie die Dienste **IISADMIN** und **CitrixSubscriptionsStore**, indem Sie die folgenden Befehle ausführen:

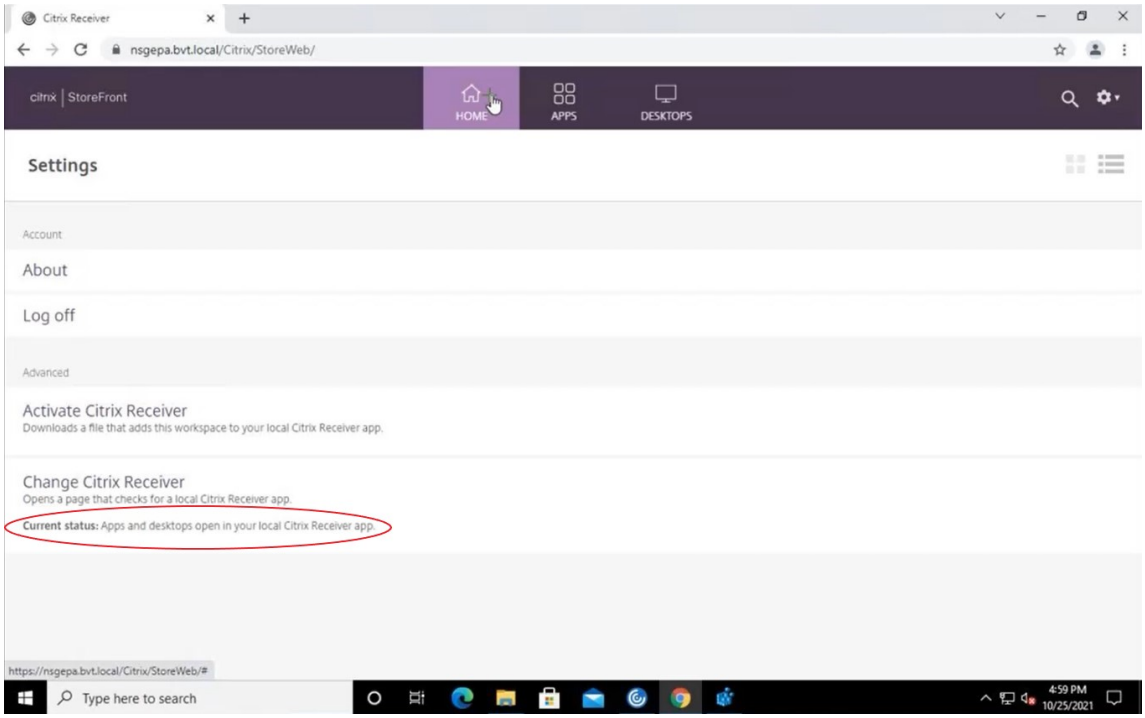
```
sc stop IISADMIN
sc stop CitrixSubscriptionsStore
<!--NeedCopy-->
```

4. Starten Sie die Dienste **IISADMIN** und **CitrixSubscriptionsStore** erneut, indem Sie die folgenden Befehle ausführen:

```
sc start IISADMIN
sc start CitrixSubscriptionsStore
<!--NeedCopy-->
```

Endbenutzererlebnis beim Hybridstart für geschützte Ressourcen

1. Nachdem die Lösung vom Administrator auf dem StoreFront-Server bereitgestellt wurde, melden Sie sich auf der Clientseite am Store an und greifen Sie über die URL in einem Webbrowser auf StoreFront zu.
2. Überprüfen Sie in den **Kontoeinstellungen** unter **Aktueller Status**, ob die Citrix Workspace-App im Browser erkannt wird.



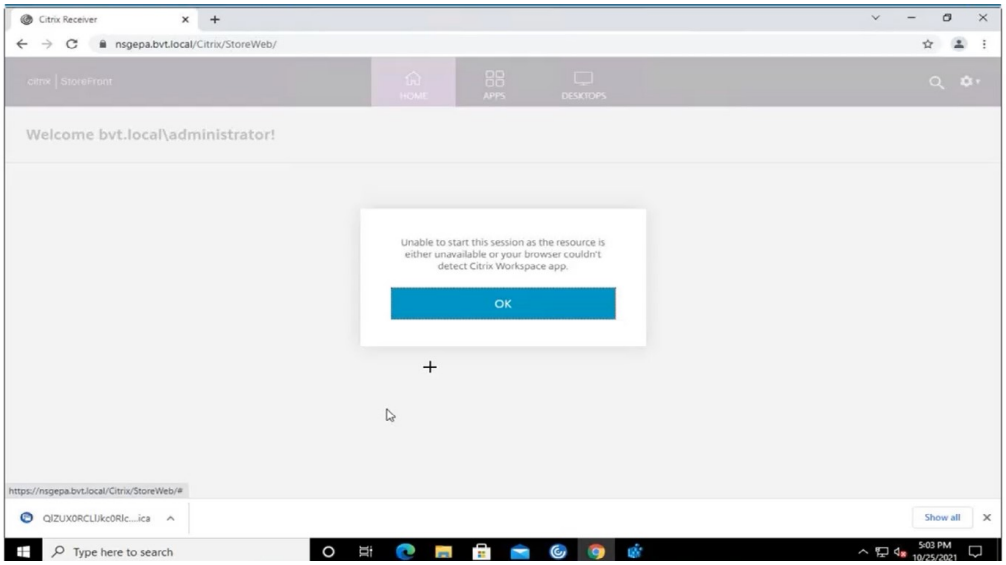
Nachdem die Citrix Workspace-App erkannt wurde, können Sie alle virtuellen Apps und Desktops sehen und starten, für die App Protection aktiviert ist.

Ablaufverfolgung in StoreFront aktivieren

Informationen zum Aktivieren der Ablaufverfolgung in StoreFront finden Sie in der StoreFront-Dokumentation. Damit kann überprüft werden, ob die konfigurierten NetScaler Gateway-Sitzungsrichtlinienbezeichnungen ordnungsgemäß an den Store weitergegeben werden.

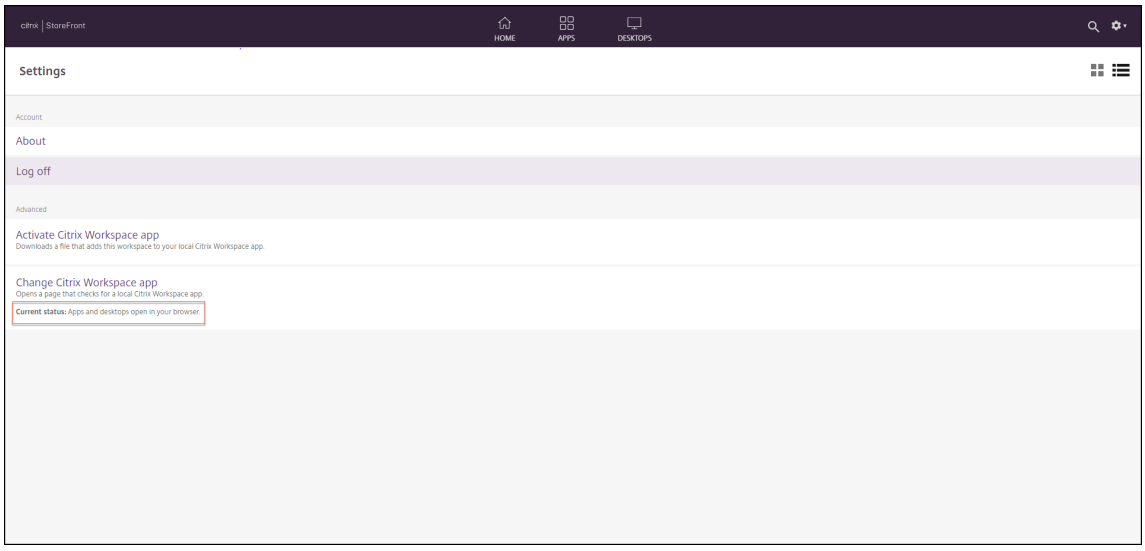
Problembehandlung

Wenn Sie die Sitzungen mit aktiviertem App Protection starten, wird manchmal der folgende Fehler angezeigt:

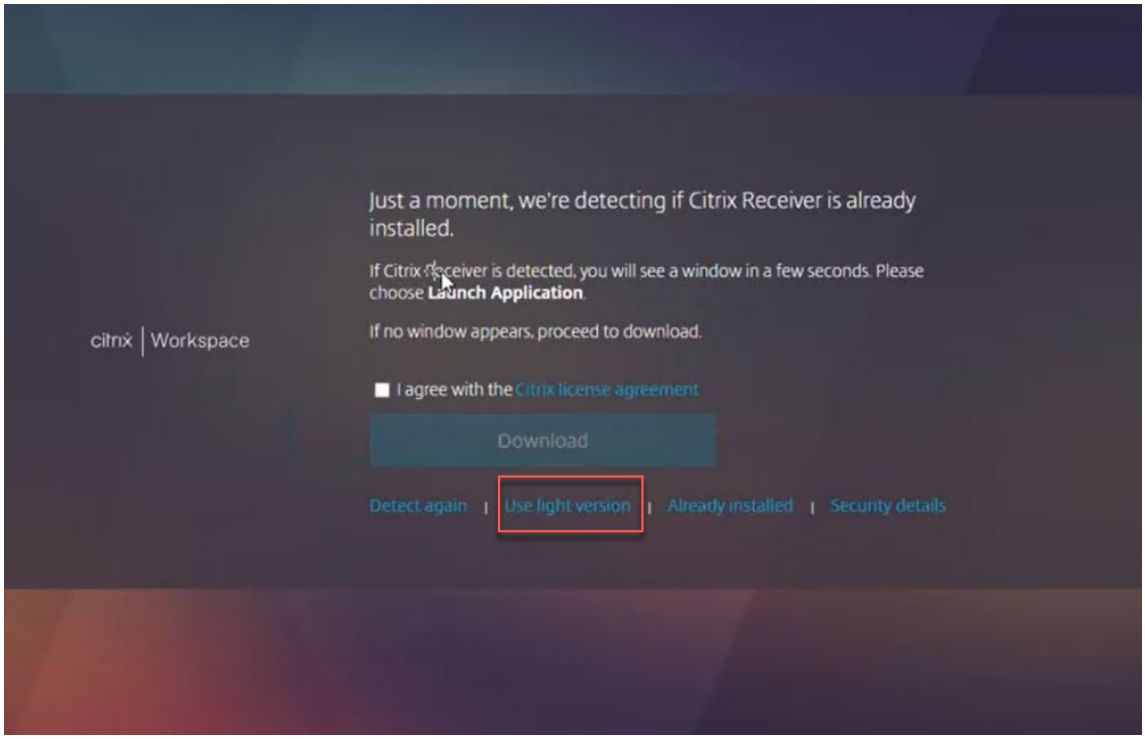


Mögliche Gründe für diesen Fehler sind:

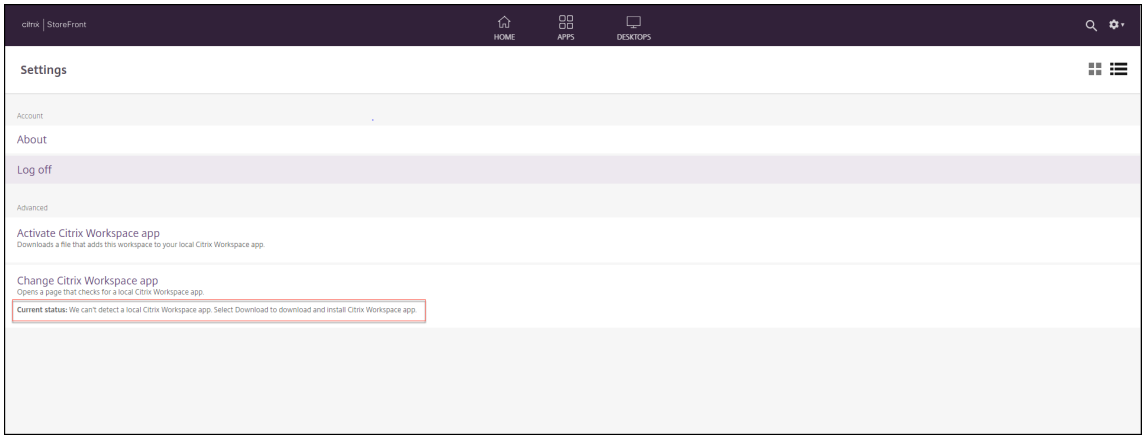
- Die Apps und Desktops sind für das Öffnen in einem Browser konfiguriert.



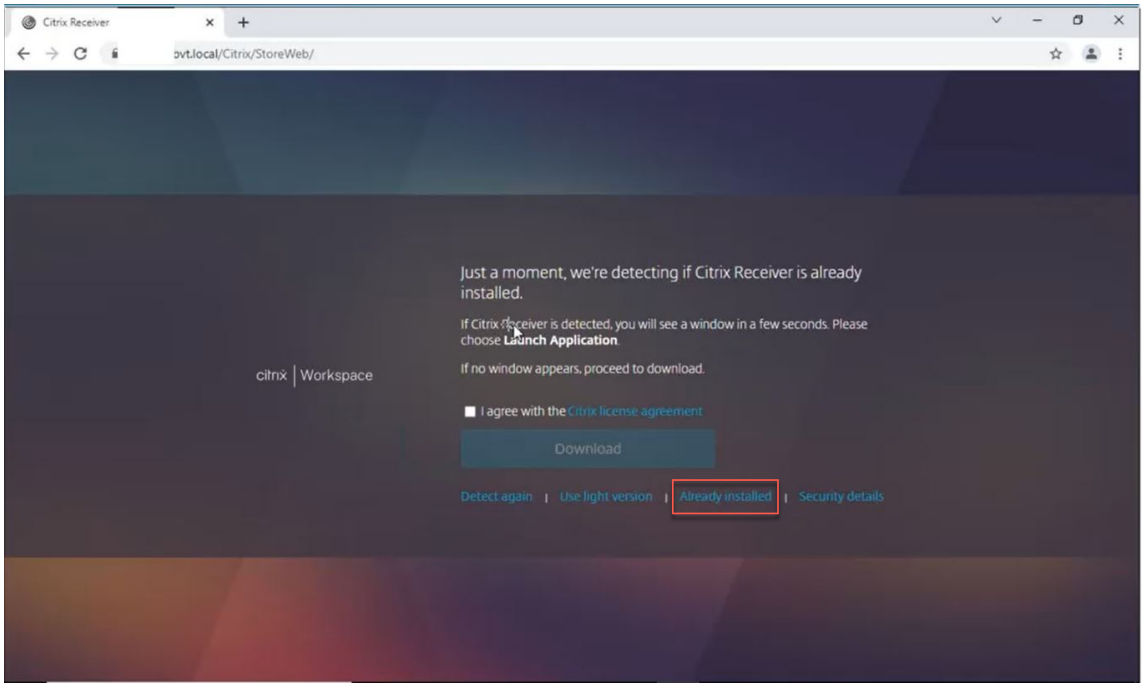
  Dieses Szenario tritt auf, wenn Sie beim Erkennen der Citrix Workspace-App auf **Lightversion verwenden** geklickt haben, wie im folgenden Bildschirm angezeigt:



- Die Citrix Workspace-App wird nicht vom Browser erkannt.



Dieses Szenario tritt auf, wenn Sie beim Erkennen der Citrix Workspace-App auf **Bereits installiert** geklickt haben, wie im folgenden Bildschirm angezeigt:



Lösung: Um die vorherigen Szenarien zu korrigieren und die Sitzungen mit aktiviertem App Protection zu starten, klicken Sie in den **Kontoeinstellungen** auf **Citrix Workspace-App ändern** und warten Sie, bis die Citrix Workspace-App erkannt wird.

Optimierung

Die Citrix Workspace-App muss erkannt werden, um Sitzungen mit aktiviertem App Protection zu starten. Um Fehler bei Hybridstarts geschützter Sitzungen zu vermeiden, können StoreFront-Administratoren die Aktion `ApplyUICustomization` des Befehls `deploy-solution.ps1` verwenden und die Optionen **Lightversion verwenden** und **Bereits installiert** ausblenden.

Citrix Workspace-App - Releasezeitplan

May 31, 2024

Der Releasezeitplan zeigt den Takt und die Veröffentlichungsdaten für die geplanten Citrix Workspace-App-Releases. Die genauen Daten können sich zwar ändern, aber wir hoffen, dass der Releasezeitplan trotzdem für Ihre Planung hilfreich ist. Außerdem möchten wir Ihnen die Verwaltung von Citrix Workspace-App-Bereitstellungen erleichtern.

Sie können neue Releases der Citrix Workspace-App von der Seite Downloads herunterladen. Citrix Workspace-App für Android, Citrix Workspace App für iOS und Citrix Workspace App für

Windows (Store) sind auch zum Download in den jeweiligen App-Stores verfügbar. Wenn Sie Citrix Workspace-Updates für die Citrix Workspace-App für Mac oder Windows aktiviert haben, werden Sie benachrichtigt, wenn ein Update zum Download und zur Installation verfügbar ist. Abonnieren Sie den RSS-Feed, um Benachrichtigungen über neue verfügbare Releases zu erhalten.

Informationen zu den Features in den jeweiligen Citrix Workspace-Apps finden Sie unter Citrix Workspace-App - Featurematrix.

Informationen zu den Lebenszyklen finden Sie unter Lifecycle Milestones for Citrix Workspace app.

Releasezeitplan

Die Releases der folgenden Citrix Workspace-App-Plattformen folgen einem Vierteljahrestakt:

- Linux
- Mac
- Windows

Die Releases der folgenden Citrix Workspace-App-Plattformen folgen einem Sechswochentakt:

- ChromeOS
- HTML5

Die Releases der folgenden Citrix Workspace-App-Plattformen folgen einem monatlichen Takt:

- Android
- iOS

> **Hinweis:**
>
> Die Citrix Workspace-App für Windows, die Citrix Workspace-App für Mac, die Citrix Workspace-App für Android und die Citrix Workspace-App für iOS werden künftig in einem Quartal in Haupt- und Nebenversionen veröffentlicht. Nebenversionen werden als '.10'bezeichnet und diese Versionen werden kleinere Verbesserungen in Bezug auf Qualitäts- und Leistungsverbesserungen enthalten. Die Nebenversion '.10'wird voraussichtlich keine wichtigen Features enthalten.

Zielveröffentlichungstermine für Desktop-Apps

Citrix Workspace App	Februar 2024	März 2024	April 2024	Mai 2024	Juni 2024	Juli 2024	August 2024	September 2024	Oktober 2024	November 2024	Dezember 2024
Windows		-	☑	☑	☒	-	☑	☒	-	☑	-

Citrix Workspace App	Februar 2024	März 2024	April 2024	Mai 2024	Juni 2024	Juli 2024	August 2024	September 2024	Oktober 2024	November 2024	Dezember 2024
Windows LTSR	☒	-	☑	-	☒	-	-	☒	-	-	☒
Mac	-	-	☑	☒	☑	-	☑	☒	-	☑	-
ChromeOS und HTML5	☒	-	☑	☑	☑	-	☑	☑	☑	-	☑
Linux	-	☑	-	☑	-	-	☑	-	-	☑	-

Citrix Workspace App	Februar 2024	März 2024	April 2024	Mai 2024	Juni 2024	Juli 2024	August 2024	September 2024	Oktober 2024	November 2024	Dezember 2024
Hinweis: Das Symbol ☑ steht für Hauptversionen und das Symbol ☒ für Nebenversionen. Das Symbol ☒ steht für kumulative Updates (CUs).											

Zieltermine für die Veröffentlichung von Apps für Mobilgeräte und Tablets

Die Citrix Workspace-App für Android und die Citrix Workspace-App für iOS folgen einem monatlichen Veröffentlichungsrhythmus.

Citrix Workspace App	März 2024	April 2024	Mai 2024	Juni 2024	Juli 2024	August 2024	September 2024	Oktober 2024	November 2024	Dezember 2024
Android und iOS	☑	☒	☑	☒	☑	☒	☑	☒	☑	☒

Citrix Workspace App	März 2024	April 2024	Mai 2024	Juni 2024	Juli 2024	August 2024	September 2024	Oktober 2024	November 2024	Dezember 2024

Hinweis: Das Symbol ☑ steht für Hauptversionen und das Symbol ☒ für Nebenversionen. Nebenversionen sind optionale Versionen, die auf bestimmte Anforderungen oder Verbesserungen zugeschnitten sind.

> **Haftungsausschluss:**
>
> Die Angaben zu Entwicklung, Release und Zeitplänen für unsere Produkte unterliegen unserem alleinigen Ermessen und können ohne vorherige Ankündigung geändert werden. Die zur Verfügung gestellten Daten dienen lediglich Informationszwecken und sind kein Versprechen, keine Zusage oder gesetzliche Verpflichtung zur Bereitstellung von Gütern, Code oder Funktionalitäten und sollten daher nicht als Grundlage für Kaufentscheidungen genommen oder in Verträge aufgenommen werden.

Citrix Workspace-App – Featurematrix

June 19, 2024

Die Citrix Workspace-App bietet vielfältige Features für verschiedene Plattformen bzw. Betriebssysteme. Dieser Featurematrix können Sie die Verfügbarkeit der Features auf verschiedenen Plattformen entnehmen. In jedem Abschnitt finden Sie neben der Featurematrix eine Definitionstabelle, in der jedes Feature kurz beschrieben wird.

Citrix Workspace

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Citrix Virtual Apps	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Citrix Virtual Desktops	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Citrix Secure Private Access	Ja	Ja	Nein	Ja	Ja	Ja	Nein	Nein

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Citrix Enterprise Browser (zuvor “Citrix Workspace Browser”)	Ja	Nein	Ja	Ja	Nein	Nein	Nein	Nein
Web-/SaaS-Apps mit SSO	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Mobile Apps von Citrix	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein
App-Personalisierungsdienst	Ja	Nein	Nein	Ja	Ja	Ja	Nein	Nein

Feature	Definition
Citrix Virtual Apps	Zugriff auf Citrix Virtual Apps über Citrix DaaS oder Citrix Virtual Apps and Desktops-Anspruch.
Citrix Virtual Desktops	Zugriff auf Citrix Virtual Desktops über Citrix DaaS oder Citrix Virtual Apps and Desktops-Anspruch.

Feature	Definition
Citrix Secure Private Access	Mit Citrix Secure Private Access können IT-Administratoren den Zugriff auf genehmigte SaaS-Apps steuern. Zudem können Administratoren dank der vereinfachten Single Sign-On-Erfahrung das Netzwerk und die Endbenutzergeräte vor Malware und Datenlecks schützen, indem sie den Zugriff auf bestimmte Websites und Websitekategorien filtern.
Citrix Enterprise Browser	Mit der Citrix Workspace-App gelieferter Browser für den sicheren Zugriff auf SaaS- und Web-Apps.
Web-/SaaS-Apps mit SSO	Zugreifen auf SaaS-/Web-Apps, die mit Secure Workspace Access mit SSO konfiguriert sind.
Mobile Apps von Citrix	Zugriff auf von Citrix Endpoint Management (zuvor "XenMobile") aggregierte mobile Citrix Apps.
Upgrades mobiler Apps von Citrix	Zugriff auf von Citrix Endpoint Management (zuvor "XenMobile") aggregierte mobile Citrix Apps.
App-Personalisierungsdienst	Ermöglicht eine nach Bedarf des Unternehmens personalisierte Erfahrung. Im gesamten App-Workflow können ein benutzerdefinierter App-Name und ein Symbol mit Co-Branding für die Citrix Workspace-App verwendet werden.

Workspace Management

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Automatische Konfiguration mit DNS für E-Mail-Discovery	Ja	Ja	Nein	Ja	Ja	Ja	Nein	Nein
Zentralisierte Verwaltungseinstellungen	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Ja
Global App Config Service (Workspace)	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja
Global App Config Service (StoreFront)	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja
App Store-Updates	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein
Automatische Citrix-Updates	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein

Client-App-Verwaltung	Ja	Nein	Nein	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Feature	Definition
Automatische Konfiguration mit DNS für E-Mail-Discovery	Ermöglicht die Konfiguration der Citrix Workspace-App über automatisch erkannte Einstellungen.
Zentralisierte Verwaltungseinstellungen	App-Einstellung über einem zentralen Dienst, z. B. Google Chrome-Verwaltung oder GPOs.
Global App Config Service (Workspace)	Der Global App Configuration Service für Citrix Workspace ermöglicht Citrix Administratoren, Workspace-Dienst-URLs und Citrix Workspace-App-Einstellungen über einen zentral verwalteten Dienst bereitzustellen.
Global App Config Service (StoreFront)	Der Global App Configuration Service für Citrix StoreFront ermöglicht Citrix Administratoren, Citrix Workspace-App-Einstellungen über einen zentral verwalteten Dienst bereitzustellen.
App Store-Updates	Updates aus dem App-Store des Anbieters
Automatische Citrix-Updates	Updates für Windows und Mac über das automatische Upgrade-Feature von Citrix
Client-App-Verwaltung	Hiermit wird die Citrix Workspace-App zur einzigen Client-App, die auf dem Endpunkt erforderlich ist, um Agents wie Secure Access Agent und das EPA-Plug-In zu installieren und zu verwalten. Mit diesem Feature können Administratoren erforderliche Agents über eine einzige Verwaltungskonsole mühelos bereitstellen und verwalten.

Benutzeroberfläche

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Desktop Viewer/Symbolleiste	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Multitasking	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Follow Me-Sitzungen (Workspace Control)	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Feature	Definition
Desktop Viewer/Symbolleiste	Ermöglicht die sitzungsinterne Steuerung von Sitzungsfunktionen wie das Senden von Strg+Alt+Entf über eine Symbolleiste.
Multitasking	Ermöglicht die gleichzeitige Verwendung mehrerer Apps und Desktops.
Follow Me-Sitzungen (Workspace Control)	Ermöglicht den Benutzern, Geräte zu wechseln und automatisch eine Verbindung zu all ihren Sitzungen herzustellen.

HDX Host Core

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Adaptiver Transport	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
Adaptiver HDX-Durchsatz	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
SDWAN-Unterstützung	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja
Sitzungszuverlässigkeit	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Automatische Wiederverbindung von Clients	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein
Sitzungsfreigabe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Multi-Port-ICA	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Feature	Definition
Adaptiver Transport	Ermöglicht den EDT-Transport für HDX für einen verbesserten Durchsatz unabhängig von Netzwerkbedingungen.
SDWAN-Unterstützung	Ermöglicht die SDWAN-Beschleunigung für QoS, TCP, Komprimierung und Deduplizierung.
Sitzungszuverlässigkeit	Hält Sitzungen aktiv und auf dem Bildschirm des Benutzers, wenn die Netzwerkkonnektivität unterbrochen wird.
Automatische Wiederverbindung von Clients	Verbindet Sitzungen bei Verbindungsunterbrechung erneut.

Feature	Definition
Sitzungsfreigabe	Ermöglicht die Ausführung der veröffentlichten App über dieselbe Verbindung wie andere veröffentlichte Anwendungen, deren Ausführung bereits auf demselben Server erfolgt.
Multi-Port-ICA	Unterstützt mehrere TCP-Ports für HDX-Datenverkehr zur Verbesserung der Servicequalität.

HDX E/A / Geräte / Drucken

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Lokaler Druck	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
Generische USB-Umleitung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Clientlaufwerkzuordnung / Dateiübertragung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
TWAIN 2.0	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein

Feature	Definition
Lokaler Druck	Ermöglicht Benutzern das Drucken von Dokumenten auf freigegebenen oder lokalen Druckern.

Feature	Definition
Generische USB-Umleitung	Ermöglicht die Verwendung von USB-Geräten innerhalb der Sitzung. Zum Beispiel Tastatur, Maus, externe Webcam und so weiter.
Clientlaufwerkzuordnung / Dateiübertragung	Ermöglicht die Verwendung integrierter oder angeschlossener Clientlaufwerke für die Datenspeicherung.
TWAIN	Ermöglicht das Zuordnen von TWAIN-Geräten, zum Beispiel Digitalkameras oder Scanner.

HDX-Integration

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Lokaler App-Zugriff	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Multitouch	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja
Mobility Pack	Ja	Ja	Nein	Nein	Ja	Ja	Ja	Ja
HDX Insight	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja
HDX Insight mit NSAP VC	Ja	Ja	Ja	Ja	Ja *(3)*	Ja *(3)*	Nein	Nein
EUEM Experience Matrix	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Bidirektionale Inhaltsumleitung	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
URL-Umleitung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Browserinhaltsumleitung	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Ja
Dateiöffnung in Citrix Workspace-App	Ja	Ja	Ja	Nein	Ja	Ja	Nein	Ja
Standortbasierte Dienste (Standort über API-Beschreibung verfügbar)	Ja	Ja	Nein	Nein	Ja	Ja	Nein	Nein

Feature	Definition
Lokaler App-Zugriff	Zugreifen innerhalb der Sitzung auf die lokale Anwendung auf einem Clientgerät.
Multitouch	Ermöglicht 10-Finger-Multitouch-Steuerung von Windows-/Linux-Desktops und -Apps.
Mobility Pack	Ermöglicht native Gerätefunktionen (z. B. automatische Popup-Tastatur und UI-Steuerelemente für lokale Geräte) sowie für Tablets optimierte Desktops.

Feature	Definition
HDX Insight	Bietet Einblick in die Start- und Endzeiten von Sitzungen anhand von ICA-Netzwerkleistungsmetriken.
HDX Insight mit NSAP VC	Bietet Einblick in die Start- und Endzeiten von Sitzungen unter Einsatz von NetScaler App Experience oder NSAP Virtual Channel zum Abrufen von HDX Insight-Daten.
EUEM Experience Matrix	Bietet Citrix Administratoren Einblick in Anmeldedauerdaten über den virtuellen Citrix Desktop, der früher "XenDesktop 7 Director" hieß.
Bidirektionale Inhaltsumleitung	Ermöglicht die Inhaltsumleitung zwischen den URLs von Client und Host sowie Host und Client.
URL-Umleitung	Ermöglicht die lokale Ausführung von Anwendungen auf dem Client.
Browserinhaltsumleitung	Ermöglicht die Umleitung einer gesamten Webseite (= Browserviewport) vom Server zum Endpunkt für lokales Rendern.
Dateiöffnung in Citrix Workspace-App	Ermöglicht das Öffnen einer lokalen Datei in der Citrix Workspace-App mit einer gehosteten Anwendung (Client-zu-Server-Inhaltsumleitung).
Standortbasierte Dienste (Standort über API-Beschreibung verfügbar)	Ermöglicht die Verwendung von Standortinformationen durch von Citrix Virtual Desktop (zuvor "XenDesktop") bereitgestellte Anwendungen.

HDX-Multimedia

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Audiowiedergabe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Bidirektionales Audio (VoIP)	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Webcamumleitung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Videowiedergabe	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Optimierung für Microsoft Teams	Ja	Ja	Ja (nur x64)	Ja	Nein	Nein	Ja	Ja
Skype for Business Optimization Pack	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
Cisco Jabber Unified Communications-Optimierung	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
Windows-Multimediaumleitung	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
UDP-Audio	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein

Feature	Definition
Audiowiedergabe	Ermöglicht Audiowiedergabe mit Serverrendering

Feature	Definition
Bidirektionales Audio (VoIP)	Ermöglicht die Verwendung gehosteter Softphone-/Voice-Chat-Anwendungen für die Zusammenarbeit.
Webcamumleitung	Ermöglicht die Verwendung von Videochat-Anwendungen mit einer lokalen Webcam.
Videowiedergabe	Ermöglicht das Ansehen aufgezeichneter Videos.
Optimierung für Microsoft Teams	Verlagert die Microsoft Teams-Medienverarbeitung vom Citrix Server auf das Benutzergerät.
Optimierung für Skype for Business	Verlagert die Skype for Business-Medienverarbeitung vom Citrix Server auf das Benutzergerät. Dies wird für die Citrix Workspace-App für Android nur auf Chrome-Geräten unterstützt.
Cisco Jabber Unified Communications-Optimierung	Verlagert die Jabber-Medienverarbeitung vom Citrix Server auf das Benutzergerät.
Windows-Multimediaumleitung	Ermöglicht das Rendern von Windows-Multimedia auf Benutzergeräten, wodurch der Server entlastet wird.
UDP-Audio	Unterstützung für Audioeingang und -ausgang über UDP.

Sicherheit

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
TLS 1.2	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
TLS 1.0/1.1	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
DTLS 1.0	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
DTLS 1.2	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
SHA2 Cert	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Smart Access	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Remotezugriff über Citrix Gateway	Ja *(1)*	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Workspace für Web-Zugriff	Ja	Ja	Ja	Ja	Über ICA-Datei	Ja	Ja	Ja
IPV6	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
App Protection	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein

Feature	Definition
TLS 1.2	Nachfolger von SSL, starke Sicherheit für Kommunikationskanäle.
TLS 1.0/1.1	Nachfolger von SSL, starke Sicherheit für Kommunikationskanäle.
DTLS 1.0	DTLS ist eine Ableitung des SSL-Protokolls. Es bietet dieselben Sicherheitsdienste (Integrität, Authentifizierung und Vertraulichkeit), jedoch unter dem UDP-Protokoll.
DTLS 1.2	DTLS ist eine Ableitung des SSL-Protokolls. Es bietet dieselben Sicherheitsdienste (Integrität, Authentifizierung und Vertraulichkeit), jedoch unter dem UDP-Protokoll.
SHA2 Cert	Ermöglicht die Verwendung von SHA2-Zertifikaten.

Feature	Definition
Smart Access	Steuert den Zugriff auf verfügbare Apps mithilfe von Gateway-Richtlinien und -Filtern.
Remotezugriff über Gateway	Bietet Benutzern ortsunabhängig sicheren Zugriff auf Unternehmensapps, virtuelle Desktops und Daten ohne VPN-Client.
Workspace für Web-Zugriff	Zugriff auf gehostete Anwendungen oder virtuelle Desktops über einen Browser.
IPV6	Ermöglicht die Verwendung in IPv6-Netzwerken.

HDX-Grafik

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
H.264-erweiterter Super-Codec	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Clienthardwarebeschleunigung	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein
3DPro-Grafiken	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Unterstützung für externe Bildschirme	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Desktopgestaltungsumleitung	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
True Multi-Monitor	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja

Feature	Definition
H.264-erweiterter SuperCodec	Ermöglicht die optimierte Bereitstellung von Anwendungen mit XenApp/Desktop 7.X H264-erweitertem Supercodec.
Clienthardwarebeschleunigung	Ermöglicht Hardwarebeschleunigung für HDX-Features (z. B. Grafik und Webcam). Die Verwendung der Hardwarefunktionen variiert je nach Citrix Workspace-App.
3DPro-Grafiken	Ermöglicht die Verwendung von professionellen im Datencenter gehosteten 3D-Grafikanwendungen.
Unterstützung für externe Bildschirme	Ermöglicht die Verwendung eines externen Bildschirms.
Desktopgestaltungsumleitung	Ermöglicht Rendering-Grafikbefehle remote vom Client zur Gewährleistung der Serverskalierbarkeit. In der Version 12.9 von Receiver für Mac veraltet.
True Multi-Monitor	XenApp oder XenDesktop erstellt dieselbe Anzahl von Bildschirmen gemäß Unterstützung des Clients.

Authentifizierung

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Verbundauthentifizierung (SAML/Azure AD)	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
ADC Voll-VPN	Ja	Ja	Ja	Ja	Nein	Nein	Nein	Nein
RSA-Softwaretoken	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Challenge-Response-SMS (Radius)	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
Authentifizierung von Benutzerzertifikaten über Gateway (über die native Workspace-App)	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Ja
Authentifizierung von Benutzerzertifikaten über Gateway (über den Browser)	Ja *(4)*	Ja *(4)*	Nein	Ja	Nein	Nein	Ja	Ja
Smartcard (CAC, PIV usw.)	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja
Proximity-/kontaktlose Karte	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Ja

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Einfügen von Anmeldeinformationen (z. B. Fast Connect, Storebrowse)	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Ja
Passthrough-Authentifizierung	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Anmeldeinformationen speichern	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein
*On-Premises und nur StoreFront								
ADC nFactor-Authentifizierung	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
ADC-natives OTP	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Biometrische Authentifizierung (Touch ID, Face ID)	Nein	Nein	Nein	Nein	Ja	Nein	Nein	Nein

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Single Sign-On bei mobilen Citrix Apps	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Nein
Anonymer Store-Zugriff	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

Feature	Definition
Verbundauthentifizierung (SAML/Azure AD)	Aktiviert den FAS-Server für die Benutzerauthentifizierung, wobei der Microsoft AD FS-Server (oder ein anderer SAML-fähiger IdP) von Azure AD oder SAML delegiert wird.
ADC (NetScaler), vollständiges VPN	Erstellt einen vollständigen VPN-Tunnel für Gateway.
RSA-Softwaretoken	Ermöglicht eine vereinfachte Authentifizierung bei der Verwendung von RSA-Softwaretoken.
Challenge-Response-SMS (Radius)	Ermöglicht die Verwendung der Challenge-Response-Authentifizierung, z. B. die Verwendung von SMS-Passcodes.
Authentifizierung von Benutzerzertifikaten über Gateway (nur über den Browser)	Ermöglicht die Verwendung von Benutzerzertifikaten als Authentifizierungsfaktor mit Gateway (für die browserbasierte Authentifizierung unter Windows).
Smartcard (CAC, PIV usw.)	Ermöglicht die Verwendung einer standardmäßigen PCSC-kompatiblen kryptografischen Smartcard zur Authentifizierung und Signatur.

Feature	Definition
Proximity-/kontaktlose Karte	Ermöglicht Benutzern die Verwendung von Citrix Apps oder Desktops unter Authentifizierung mit einer Proximity- oder kontaktlosen Smartcard.
Einfügen von Anmeldeinformationen (z. B. Fast Connect, Storebrowse)	Ermöglicht Benutzern die Verwendung von Citrix Apps oder Desktops unter Authentifizierung mit einer Proximity- oder kontaktlosen Smartcard. Storebrowse ist ein mit der Citrix Workspace-App für Windows verfügbares Befehlszeilenhilfsprogramm. Mit Storebrowse und Skripts können Sie die Citrix Workspace-App anpassen.
Passthrough-Authentifizierung	Übergibt Benutzeranmeldeinformationen an eine Webinterface-Site und von dort an die Citrix Virtual Apps and Desktops-Server. Dadurch wird verhindert, dass sich Benutzer beim Citrix App-Start zu einem beliebigen Zeitpunkt explizit authentifizieren.
Anmeldeinformationen speichern *On-Premises und nur StoreFront	Ermöglicht das Speichern von Anmeldeinformationen on-premises und nur unter Verwendung von Citrix StoreFront.
Gateway-natives OTP	Gateway unterstützt Einmalkennwörter (OTP) ohne Erfordernis des Servers eines Drittanbieters, da die gesamte Konfiguration auf der NetScaler-Appliance verbleibt.
NetScaler nFactor-Authentifizierung	nFactor-Authentifizierung ermöglicht dynamische Authentifizierungsflüsse basierend auf dem Benutzerprofil. Diese können einfach und für den Benutzer intuitiv sein. Die erforderliche Mindestversion von NetScaler ist 12.1.49.x.
Biometrische Authentifizierung (Touch ID, Face ID)	Ermöglicht die biometrische Authentifizierung, etwa per Touch ID oder Face ID.
Single Sign-On bei mobilen Citrix Apps	Aktiviert Single Sign-On bei mobilen Citrix Apps.
Anonymer Store-Zugriff	Unterstützung des Zugriffs durch nicht authentifizierte (anonyme) Benutzer

Eingabe

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Tastaturlayoutsynchronisierung - Client zu VDA (Windows VDA)	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
Tastaturlayoutsynchronisierung - Client zu VDA (Linux VDA)	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
Tastaturlayoutsynchronisierung - VDA zu Client (Windows VDA)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Tastaturlayoutsynchronisierung - VDA zu Client (Linux VDA)	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Unicode-Tastaturlayoutzuordnung	Nein	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Tastatureingabemodus - Unicode	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Tastatureingabemodus - Scancode	Ja	Ja	Ja	Ja	Nein	Nein	Ja	Ja

Feature	Windows 2403.1 und Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Server-IME	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Generischer Client-IME (CTXIME) für CJK-IMEs	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja
Befehlszeilenschnittstelle	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
Benutzeroberfläche und Konfigurationen für die Tastatursynchronisierung	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Nein
Benutzeroberfläche und Konfigurationen für den Eingabemodus	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein
Benutzeroberfläche und Konfigurationen für die Sprachenleiste	Ja	Ja	Nein	Ja	Nein	Nein	Nein	Nein

Feature	Definition
Tastaturlayoutsynchronisierung - Client zu VDA (Windows VDA)	Ermöglicht Benutzern, aktive Tastaturlayouts zu synchronisieren oder zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Das Tastaturlayout auf dem Clientgerät wird automatisch auf dem Windows VDA festgelegt.
Tastaturlayoutsynchronisierung - Client zu VDA (Linux VDA)	Ermöglicht Benutzern, aktive Tastaturlayouts zu synchronisieren oder zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Das Tastaturlayout auf dem Clientgerät wird automatisch auf dem Linux VDA festgelegt.
Tastaturlayoutsynchronisierung - VDA zu Client (Windows VDA)	Ermöglicht Benutzern, aktive Tastaturlayouts zu synchronisieren oder zwischen bevorzugten Tastaturlayouts auf dem Windows VDA zu wechseln. Das Tastaturlayout auf dem Windows VDA wird automatisch auf dem Clientgerät festgelegt.
Tastaturlayoutsynchronisierung - VDA zu Client (Linux VDA)	Ermöglicht Benutzern, aktive Tastaturlayouts zu synchronisieren oder zwischen bevorzugten Tastaturlayouts auf dem Linux VDA zu wechseln. Das Tastaturlayout auf dem Linux VDA wird automatisch auf dem Clientgerät festgelegt.
Unicode-Tastaturlayoutzuordnung	Unterstützt die Unicode-Tastaturlayoutzuordnung für Windows VDAs mit einer Citrix Workspace-App für andere Plattformen (nicht Windows).
Tastatureingabemodus - Unicode	Der Unicode-Eingabemodus sendet die Tasteneingabe von der clientseitigen Tastatur an den VDA, der das gleiche Zeichen auf dem VDA generiert. Wendet clientseitiges Tastaturlayout an.
Tastatureingabemodus - Scancode	Der Scancode-Eingabemodus sendet die Tastenposition von der clientseitigen Tastatur an den VDA, der das entsprechende Zeichen generiert. Wendet serverseitiges Tastaturlayout an.

Feature	Definition
Server-IME	Bietet die Benutzerfreundlichkeit und -erfahrung des Eingabemethoden-Editors (IME) auf der Seite des Dienstes (oder VDA).
Generischer Client-IME (CTXIME) für CJK-IMEs	Bietet eine höhere Benutzerfreundlichkeit für den Client-IME und ein besseres nahtloses Erlebnis für ostasiatische Sprachen (Chinesisch, Japanisch, Koreanisch).
Befehlszeilenschnittstelle	Benutzer können den Client-IME mit den Befehlszeilenschnittstellen aktivieren oder deaktivieren.
Benutzeroberfläche und Konfigurationen für die Tastatursynchronisierung	Benutzer können mit der grafischen Benutzeroberfläche verschiedene Synchronisierungsoptionen für das Tastaturlayout auswählen.
Benutzeroberfläche und Konfigurationen für den Eingabemodus	Benutzer können mit der grafischen Benutzeroberfläche verschiedene Optionen für den Tastatureingabemodus auswählen.
Benutzeroberfläche und Konfigurationen für die Sprachenleiste	Die Benutzer können die Anzeige der Remotesprachenleiste in einer VDA-App-Sitzung über die grafische Benutzeroberfläche ein- und ausblenden. Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Sitzungen angezeigt.
Administrative Gruppenrichtlinienobjektvorlage für die Synchronisierung des Tastaturlayouts	Administratoren können die Synchronisierungskonfigurationen für das Tastaturlayout überschreiben, indem sie die entsprechenden Richtlinien mit der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App bereitstellen.

Bedeutung der Kennzahlen in den Tabellen

Kennzahl	Beschreibung
1	Nur StoreFront

Kennzahl	Beschreibung
2	HDX 3D Pro wechselt für diese Citrix Workspace-Apps zu JPEG. 3 Mbit/s empfohlen, im Gegensatz zu 1,5 Mbit/s bei H.264-Tiefenkomprimierung.
3	Unterstützung für NSAP VC durch die Workspace-App für iOS/Android, für ADC/ADM Unterstützung noch ausstehend.
4	Die Authentifizierungsmethode Authentifizierung von Benutzerzertifikaten über Gateway (nur über den Browser) unterstützt die Erkennung von Citrix Workspace-App-Clients nicht. Sie können eine virtuelle App oder einen virtuellen Desktop mit der Citrix Workspace-App nur öffnen, wenn die ICA-Datei heruntergeladen wurde.

> **Hinweis:**
>
> Die Entwicklung, Veröffentlichung und Zeitpläne der für unsere Produkte beschriebenen Features oder Funktionen liegen in unserem alleinigen Ermessen. Die hier zur Verfügung gestellten Informationen dienen lediglich Informationszwecken und sind kein Versprechen, keine Zusage oder gesetzliche Verpflichtung zur Bereitstellung von Gütern, Code oder Funktionalitäten und sollten daher nicht als Grundlage für Kaufentscheidungen genommen oder in Verträge aufgenommen werden. Die Angaben zu Entwicklung, Release und Zeitplänen der für unsere Produkte beschriebenen Features oder Funktionen unterliegen unserem alleinigen Ermessen und können ohne vorherige Ankündigung geändert werden.