



# **Citrix Workspace-App 2402 LTSR für Windows**

## Contents

<b>Info zur Citrix Workspace-App 2402 LTSR für Windows</b>	<b>4</b>
<b>Citrix Workspace-App 2402 LTSR für Windows</b>	<b>6</b>
<b>Behobene Probleme</b>	<b>70</b>
<b>Bekannte Probleme</b>	<b>72</b>
<b>Systemanforderungen und Kompatibilität</b>	<b>73</b>
<b>Installation und Deinstallation</b>	<b>79</b>
<b>Bereitstellen</b>	<b>102</b>
<b>Storekonfiguration</b>	<b>110</b>
<b>Updates und Plug-Ins verwalten</b>	<b>123</b>
<b>Aktualisieren</b>	<b>123</b>
<b>Plug-Ins verwalten</b>	<b>136</b>
<b>App-Erfahrung</b>	<b>146</b>
<b>Anwendungsbereitstellung</b>	<b>146</b>
<b>Verbesserter Start von Virtual Apps and Desktops</b>	<b>158</b>
<b>App-Einstellungen</b>	<b>159</b>
<b>SaaS-Apps</b>	<b>166</b>
<b>Datensammlung und Überwachung</b>	<b>167</b>
<b>Sicherheit und Authentifizierung</b>	<b>170</b>
<b>Sicherheit</b>	<b>171</b>
<b>Sichere Kommunikation</b>	<b>174</b>
<b>Authentifizierung</b>	<b>190</b>
<b>Domänen-Passthrough-Zugriffsmatrix</b>	<b>216</b>

<b>Domänen-Passthrough-Authentifizierung an Citrix Workspace mit On-Premises-Citrix Gateway als Identitätsanbieter</b>	<b>224</b>
<b>Domänen-Passthrough-Authentifizierung an Citrix Workspace mit Azure Active Directory als Identitätsanbieter</b>	<b>242</b>
<b>Domänen-Passthrough-Authentifizierung an Citrix Workspace mit Okta als Identitätsanbieter</b>	<b>246</b>
<b>HDX</b>	<b>248</b>
<b>Grafik und Display</b>	<b>249</b>
<b>Optimierung für Microsoft Teams</b>	<b>260</b>
<b>HDX-Transport</b>	<b>263</b>
<b>Browserinhaltsumleitung</b>	<b>264</b>
<b>Bidirektionale Inhaltsumleitung</b>	<b>267</b>
<b>Referenz für ICA-Einstellungen</b>	<b>273</b>
<b>Geräte</b>	<b>274</b>
<b>Maus</b>	<b>274</b>
<b>Tastatur</b>	<b>276</b>
<b>Drucken</b>	<b>295</b>
<b>USB</b>	<b>297</b>
<b>Clientlaufwerkzuordnung</b>	<b>317</b>
<b>Mikrofon</b>	<b>320</b>
<b>Gruppenrichtlinie</b>	<b>320</b>
<b>Sitzungserfahrung</b>	<b>323</b>
<b>Citrix Workspace-App Desktop Lock</b>	<b>334</b>
<b>Software Development Kit (SDK) und API</b>	<b>340</b>
<b>Storebrowse</b>	<b>342</b>

<b>Storebrowse für Workspace</b>	<b>352</b>
<b>Problembehandlung</b>	<b>355</b>
<b>Einstellung von Features und Plattformen</b>	<b>361</b>

## Info zur Citrix Workspace-App 2402 LTSR für Windows

April 22, 2024

In dieser Dokumentation werden die Funktionen und die Konfiguration der Citrix Workspace-App 2402 LTSR für Windows beschrieben. Diese Version ist das neueste Long Term Service Release (LTSR-Version) der Citrix Workspace-App für Windows und nur für LTSR-Kunden von Relevanz.

Die Dokumentation für das aktuelle Release (CR-Version) der Citrix Workspace-App für Windows ist verfügbar unter [Citrix Workspace-App für Windows](#). Weitere Informationen zu den Lebenszyklen der CR- und LTSR-Versionen finden Sie unter [Lifecycle Milestones for Citrix Workspace-App](#).

### Hinweis:

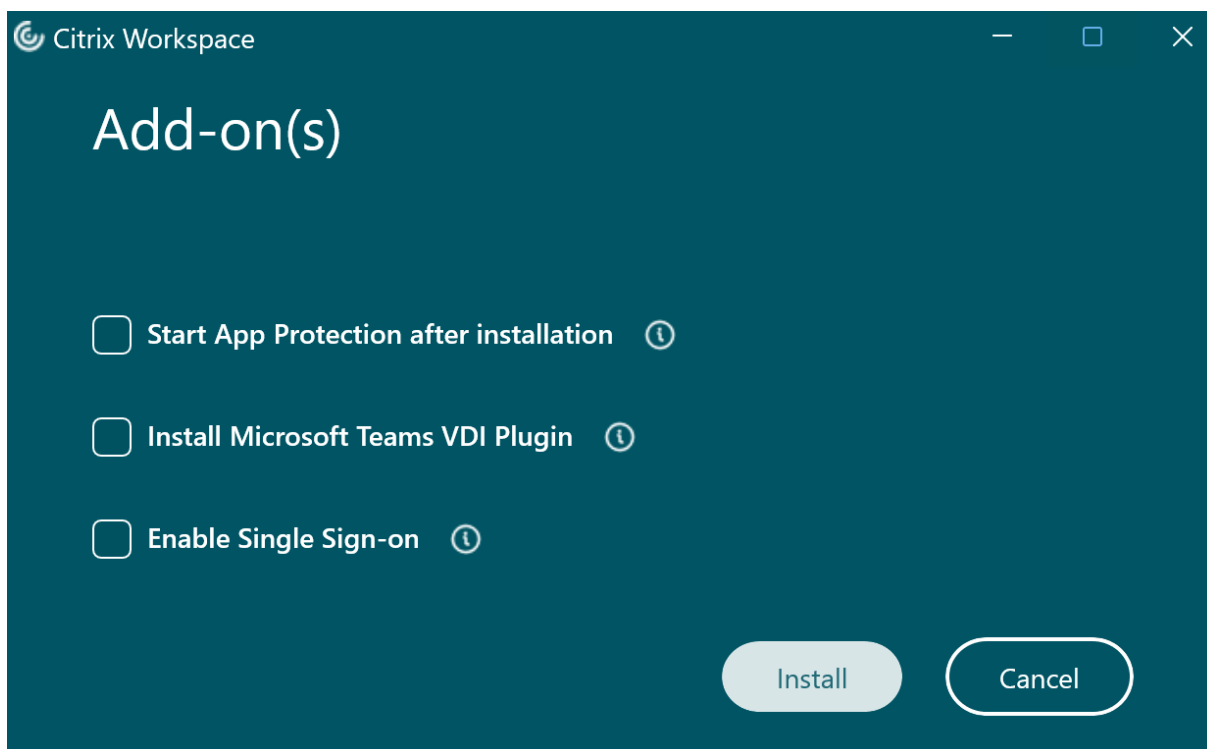
- Wenn Sie die automatische Aktualisierung in Ihrer Citrix Workspace-App aktiviert und sich für das LTSR-Programm entschieden haben, wird Citrix Workspace-App 2203.1 LTSR für Windows automatisch auf die Citrix Workspace-App 2402 LTSR für Windows aktualisiert.
- Wenn Sie die automatische Aktualisierung in Ihrer Citrix Workspace-App aktiviert und sich für das CR-Programm entschieden haben, wird die CR-Version der Citrix Workspace-App automatisch auf die Citrix Workspace-App 2311.1 für Windows aktualisiert.

## Downloads

[Citrix Workspace-App 2402 LTSR für Windows](#)

## Neue Add-Ons und Paketerstellung

Für die Citrix Workspace-App für 2402 LTSR können Sie das Microsoft Teams Optimization Plugin, den Citrix Enterprise Browser und App Protection während der Installation der Citrix Workspace-App von der “Add-ons”-Auswahl installieren. Sie können diese Add-Ons unabhängig von der Citrix Workspace-App verwalten. Sie können sie beispielsweise unabhängig von der Citrix Workspace-App aktualisieren oder deinstallieren.



### **.NET 6.0.25 Voraussetzung**

Die neueste Version der Citrix Workspace-App 2402 LTSR erfordert .NET 6.0.25 und ist auch mit höheren Versionen von .NET kompatibel.

### **Verhaltensänderung bei der Optimierung von Microsoft Teams**

Mit der Veröffentlichung der Citrix Workspace-App 2402 LTSR haben Benutzer jetzt die Möglichkeit, das neue Microsoft Teams VDI-Plug-In während der Installation der Citrix Workspace-App direkt vom Bildschirm "Add-on(s)" aus zu installieren.

Weitere Informationen finden Sie unter [Neue Features](#).

Sie können sich auch auf [Microsoft Teams 2.1 beziehen, das für VDI/DaaS unterstützt wird](#).

### **Neue Features und Verbesserungen**

Weitere Informationen zu neuen Features, behobenen Problemen und bekannten Problemen in dieser Version finden Sie in den folgenden Abschnitten.

- [Neue Features in 2402 LTSR](#)
- [Behobene Probleme in Release 2402 LTSR](#)
- [Bekannte Probleme in Release 2402 LTSR](#)

## Hilfreiche Links

- [Citrix Workspace-App – Featurematrix](#)
- [Lifecycle Milestones for Citrix Workspace-App](#)
- [Zusätzliche Lebenszyklusinformationen für Citrix Receiver für Windows](#)

## Änderungen an Citrix-Produktnamen und -Versionsnummern

Informationen über seit 2018 geänderte Produktnamen und Versionsnummern finden Sie unter [Neue Namen und Nummern](#).

## Basiskomponenten

---

2402 LTSR-Basiskomponenten	Version
Citrix Virtual Apps and Desktops 7 LTSR mit CUs	1912 LTSR
Citrix Virtual Apps and Desktops 7 LTSR mit CUs	2203.1 LTSR
Citrix Virtual Apps and Desktops 7 CR	2402 CR

---

## Kompatible Komponenten

Die folgenden Komponenten sind kompatibel mit LTSR-Umgebungen. Für sie können die LTSR-Vorteile (erweiterter Lebenszyklus und kumulative Updates mit Fixes) nicht beansprucht werden.

---

### Kompatible Komponenten und Features

---

Citrix Endpoint Analysis

Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)

Browserinhaltsumleitung

Citrix Enterprise Browser

---

## Citrix Workspace-App 2402 LTSR für Windows

April 23, 2024

Erfahren Sie mehr über die neuen Features und Verbesserungen, die für die Citrix Workspace-App 2402 LTSR für Windows verfügbar sind.

**Wichtig:**

Der Citrix Enterprise Browser kann mit der Citrix Workspace-App LTSR als kompatible Komponente verwendet werden. Er ist jedoch nicht standardmäßig installiert.

Um den Citrix Enterprise Browser zu installieren, fügen Sie die Installationsoption `InstallEmbeddedBrowser=Y` oder `AddLocal` mit Parameter `CitrixEnterpriseBrowser` als Teil der Befehlszeileninstallation hinzu.

## Neue Features in 2402 LTSR

Im Folgenden finden Sie eine Liste der Funktionen, die in der Citrix Workspace-App 2402 LTSR für Windows verfügbar sind.

**Hinweis:**

Informationen zu neuen Add-Ons und Änderungen der Paketerstellung finden Sie unter [Neue Add-Ons und Paketerstellung](#).

- 2402
  - Nachhaltigkeitsinitiative für die Einführung von Cloud-Hybridinstallationen
  - Verbesserter Domänen-Passthrough für Single Sign-On (Enhanced SSO)
  - Unterstützung für erweiterte NetScaler-Richtlinien für Storebrowse unter Windows
  - Versionsupgrade für Chromium Embedded Framework
  - Microsoft Teams VDI-Plug-In für Citrix installieren
  - Systemaudio in Besprechungen teilen (Technical Preview)
  - Option zur Problembehandlung für Endbenutzer ausblenden
  - App Protection
    - \* Positivliste für Screenshots
    - \* Ausschlussliste für Prozesse
    - \* Ausschlussliste für USB-Filtertreiber
  - Citrix Endpoint Analysis
  - Citrix Enterprise Browser
    - \* Sicherheitsindikator beim Besuch von Websites



- \* [Citrix Enterprise Browser führt zusätzliche Einstellungen im Global App Configuration Service ein] (#Citrix Enterprise Browser führt zusätzliche Einstellungen im Global App Configuration Service ein)
- 2311.1
  - Einführung des neuen Citrix Workspace-App-Installationsprogramms
  - Unterstützung für Aktivitätsmanager in Cloudstores
  - Automatische Auswahl des Videocodecs
  - Verlusttoleranzmodus für Audio
  - Synchronisierung mehrerer Tastaturen beim Sitzungsstart
  - Verbesserte Leistung bei der Browserinhaltsumleitung
  - Versionsupgrade für Chromium Embedded Framework
  - Wichtiges Update zu Datei- und Treibernamen von App Protection
  - Verbesserung der Hintergrundunschärfe und -effekte für Microsoft Teams-Optimierung mit HDX
  - Citrix Enterprise Browser
    - \* [Verbesserte Benutzererfahrung und Ladezeit der Sitzung](#)
    - \* [Verbessertes Wasserzeichendesign](#)
    - \* [Unterstützung für benutzerdefinierte Browsererweiterung](#)
    - \* Vereinfachtes SSO für Web- und SaaS-Apps über den Global App Configuration Service
    - \* [Passthrough-Authentifizierung im Citrix Enterprise Browser verwalten](#)
    - \* [Verbesserte Funktionen zur Überwachung der Endbenutzeraktivitäten](#)
- 2309
  - Zusätzliche .NET-Voraussetzungen
  - Verbesserter Start von Virtual Apps and Desktops
  - Option “Problembehandlung” zu Taskleiste der Citrix Workspace-App hinzugefügt
  - Nachhaltigkeitsinitiative der Citrix Workspace-App
  - Befehle zum Konfigurieren der Tastaturlayoutsynchronisierung über die Befehlszeilenschnittstelle
  - Befehl zum Bereinigen und Installieren der Citrix Workspace-App
  - Neues zu optimiertem Microsoft Teams
  - App Protection
    - \* Wichtiges Update zu Dateinamen
    - \* Richtlinienmanipulationen erkennen
    - \* App Protection und Double-Hop-Szenario
  - Citrix Enterprise Browser
    - \* [Authentifizierung über Citrix Enterprise Browser](#)
- 2307

- Unterstützung für die Wiedergabe kurzer Töne in optimiertem Microsoft Teams hinzugefügt
- Citrix Enterprise Browser
  - \* [Verknüpfung für Citrix Enterprise Browser](#)
- 2305.1
  - Verbesserter Start von Virtual Apps and Desktops
  - Status des Storebrowse-Befehls verfolgen
  - Unterstützung moderner Authentifizierungsmethoden für StoreFront-Stores
  - Unterstützung für mehr als 200 Gruppen in Azure AD
  - App Protection
    - \* Verbesserungen beim Keyloggingschutz
  - Citrix Enterprise Browser
    - \* Unterstützung für Browsererweiterungen
    - \* Änderung der Implementierung von SPA-Richtlinien für interne Web- und SaaS-Apps
    - \* Citrix Enterprise Browser mit dem Global App Config Service verwalten
- 2303
  - Speicherpfad für temporäre Daten für Browserinhaltsumleitungs-Overlay konfigurieren
  - Unterstützung moderner Authentifizierungsmethoden für StoreFront-Stores
  - Verbessertes Erlebnis bei optimierten Microsoft Teams-Videokonferenzen
  - Verbesserung von App Protection: DLL-Einschleusungsschutz
  - Citrix Enterprise Browser
    - \* Secure Private Access-Unterstützung für StoreFront
- 2302
  - Verbesserte Wiederverbindung für virtuelle Apps und Desktops
  - Client App Management für Zoom-Plug-In
  - Aktualisiertes Verhalten bei der Auswahl von Audiogeräten für optimiertes Microsoft Teams
  - Verbesserung von App Protection
  - Citrix Enterprise Browser
    - \* Alle Web- und SaaS-Anwendungen über Citrix Enterprise Browser öffnen
    - \* Option zum Starten des Citrix Enterprise Browser in der Citrix Workspace-App
- 2212
  - Client-App-Verwaltung
  - Versionssteuerung für automatische Updates

- Anmeldeaufforderung für Verbundidentitätsanbieter erzwingen
- Bessere Wiederverbindung nach Ablauf der Verbindungsleasedatei
- Unterstützung für die standardmäßige Installation von App Protection
- Verbesserung von App Protection: Screenshot-Erkennung und Benachrichtigung
- Desktop Viewer-Optimierung
- Citrix Enterprise Browser
  - \* [Citrix Enterprise Browser als Arbeitsbrowser festlegen](#)
- 2210.5
  - Verbesserung der automatischen Aktualisierung
- 2210
  - Hintergrundunschärfe für Webcamumleitung
  - Verbesserung von App Protection für Web- und SaaS-Apps unter Windows 11
  - Videoauflösungen einschränken
  - Neuer Name für Citrix Workspace Browser
  - Alle Web- und SaaS-Anwendungen über Citrix Enterprise Browser öffnen
  - Unterstützung der automatischen Aktualisierung der Citrix Workspace-App auf dem VDA
  - Citrix Enterprise Browser (zuvor “Citrix Workspace Browser”)
- 2207
  - Hintergrundunschärfe und -effekte für Microsoft Teams-Optimierung mit HDX
  - Verbesserung der automatischen Updates
  - Hinweis zum Update der Citrix Workspace-App
- 2206
  - Verbesserte Grafikleistung
  - Aktivieren der DPI-Anpassung
- 2205
  - Wechsel bei Citrix Casting
  - Schneller Zugriff auf Ressourcen
  - Abmeldung von benutzerdefinierten Webstores beim Beenden der Citrix Workspace-App
  - Unterstützung für das Öffnen der Citrix Workspace-App im maximierten Modus
  - Storebrowse-Unterstützung für Workspace
- 2204.1
  - Verbesserung der Audioumleitung
  - Microsoft Teams-Optimierung

## 2402 LTSR (Erstveröffentlichung)

### Nachhaltigkeitsinitiative für die Einführung von Cloud-Hybridinstallationen

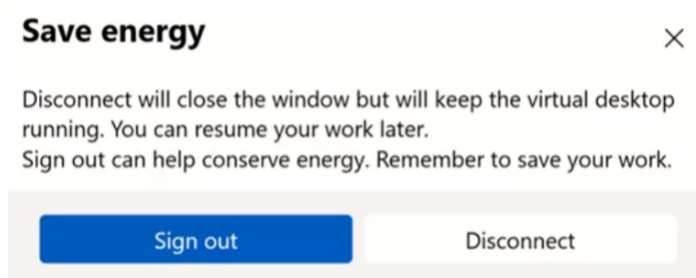
#### Hinweis:

Diese Funktion war zuvor für native Starts (Cloud und on-premises) ab Version 2309 der Citrix Workspace-App verfügbar.

Ab Version 2402 der Citrix Workspace-App ist diese Funktion für hybride Starts in der Cloud verfügbar. Nachdem dieses Feature aktiviert ist, wird eine Aufforderung zum Abmelden von der Desktopsitzung angezeigt, sobald ein Benutzer einen virtuellen Desktop schließt. Das Feature trägt zur Energieeinsparung bei, sofern Windows-Betriebssystemrichtlinien verwendet werden, die VMs herunterfahren, wenn keine Benutzer angemeldet sind.

Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Gehen Sie zu Citrix Studio.
2. Klicken Sie im linken Navigationsbereich auf **Bereitstellungsgruppen**.
3. Wählen Sie im Abschnitt **Bereitstellungsgruppe** den erforderlichen VDA aus.
4. Klicken Sie auf das Symbol **Bearbeiten**. Die Seite **Bereitstellungsgruppe bearbeiten** wird angezeigt.
5. Klicken Sie im linken Navigationsbereich auf **Desktops**.
6. Wählen Sie den VDA aus, zu dem Sie die Schlüsselwörter hinzufügen müssen.
7. Klicken Sie auf **Bearbeiten**. Die Seite **Desktop bearbeiten** wird angezeigt.
8. Legen Sie das Schlüsselwort `ICA-LogOffOnClose` im Feld **Beschreibung** auf **true** fest.
9. Klicken Sie auf **OK**. Das folgende Dialogfeld wird angezeigt, wenn Sie den virtuellen Desktop schließen:



**Text der Bildschirmanzeige “Energie sparen” ändern** Sie können den Text ändern, der auf dem Bildschirm **Energie sparen** erscheint.

1. Folgen Sie den Schritten 1–8 im vorherigen Abschnitt.
2. Legen Sie das Schlüsselwort `ICA-PromptMessage` im Feld **Beschreibung** auf den gewünschten Text fest.

**Hinweis:**

Im Feld "Beschreibung" sind maximal 200 Zeichen zulässig.

**Beispiel:**

```
1 KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to  
   Log off?"  
2 <!--NeedCopy-->
```

## Edit Desktop

Display name:

Description:

The name and description are shown in Citrix Workspace app.

Restrict launches to machines with tag:

Allow everyone with access to this delivery group to use a desktop

Restrict desktop use:

Allow list <span>?</span> ↓
CWAWINAD\Domain Users
TestVeda(CWAWINAD\TestVeda)

**Enable desktop**  
Clear this check box to disable delivery of this desktop.

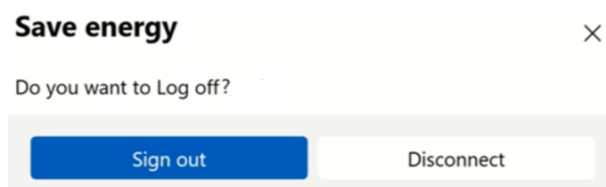
**Session roaming**  
When enabled, if the user launches this desktop and then moves to another device, the same session is used, and applications are available on both devices. When disabled, the session no longer roams between devices.

Die Schlüsselwörter werden standardmäßig für neue Desktopmaschinen zugewiesen, die der Gruppe zugewiesen sind. Für vorhandene Desktopmaschinen müssen Sie die folgenden PowerShell-Befehle ausführen, damit die Änderungen wirksam werden:

```
1 $dg = Get-BrokerDesktopGroup -Name '<group name>' -Property 'Name'  
    , 'Uid'  
2  
3 $apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid  
    -Property 'Description' )  
4  
5 Get-BrokerMachine -DesktopGroupUid $dg.Uid -IsAssigned $true | Set  
    -BrokerMachine -Description $apr[0].Description  
6 <!--NeedCopy-->
```

Mit diesem PowerShell-Skript ist es möglich, mehrere Zuweisungsrichtlinienregeln für eine einzelne Bereitstellungsgruppe zu verwenden. Mit Citrix Studio können Sie auch mehrere Zuweisungsrichtlinienregeln konfigurieren, jede mit einem eindeutigen Beschreibungswert und einem möglichen Satz unterschiedlicher Schlüsselwörter.

3. Klicken Sie auf **OK**. Das folgende Dialogfeld wird angezeigt, wenn Sie den virtuellen Desktop schließen.



### Verbesserter Domänen-Passthrough für Single Sign-On (Enhanced SSO)

Bisher unterstützte die Citrix Workspace-App für Windows nur die SSON-Authentifizierung oder Authentifizierung mit Domänen-Passthrough für Single Sign-On in Citrix Virtual Apps and Desktops-Umgebungen mit Benutzeranmeldeinformationen. Diese Authentifizierung ermöglicht die Authentifizierung bei der Domäne auf dem Gerät und die Verwendung virtueller Apps und Desktops ohne erneute Authentifizierung.

Beim Domänen-Passthrough mit Benutzeranmeldedaten gelten folgende Einschränkungen:

- Die Authentifizierungsmethode unterstützt keine kennwortlose Authentifizierung wie Windows Hello oder FIDO2. Für SSO ist zusätzlich der Verbundauthentifizierungsdienst (FAS) erforderlich.
- Für die Installation oder das Upgrade der Citrix Workspace-App mit aktiviertem SSON ist ein Neustart des Geräts erforderlich.
- Erfordert die Aktivierung von Multi Provider Router-Benachrichtigungen auf Windows 11-Maschinen.
- Muss ganz oben auf der Liste der Netzanbieter stehen.

**Hinweis:**

Das Feature wird für 32-Bit-Windows 10- und Windows Server 2016-Maschinen nicht unterstützt.

**Systemanforderungen:**

- Citrix Workspace-App 2309 oder höher
- Citrix Virtual Apps and Desktops 2308 oder höher

**Unterstützte VDA-Betriebssystemversionen:**

- Multisitzungs-OS:
  - Windows Server 2019
  - Windows Server 2022
- Einzelsitzungs-OS:
  - Windows 10 Version 22H2
  - Windows 11 Version 22H2

**Voraussetzungen:**

- Der Client bzw. Endpunkt muss mit der Domäne verbunden sein.
- Erfordert eine direkte Verbindung zu Active Directory.

**StoreFront- und DDC-Einstellungen** Richten Sie die Domänen-Passthrough-Umgebung mit den folgenden Einstellungen ein:

**Hinweis:**

Sie können diesen Schritt überspringen, wenn Sie in Ihrer Umgebung bereits Domänen-Passthrough konfiguriert haben.

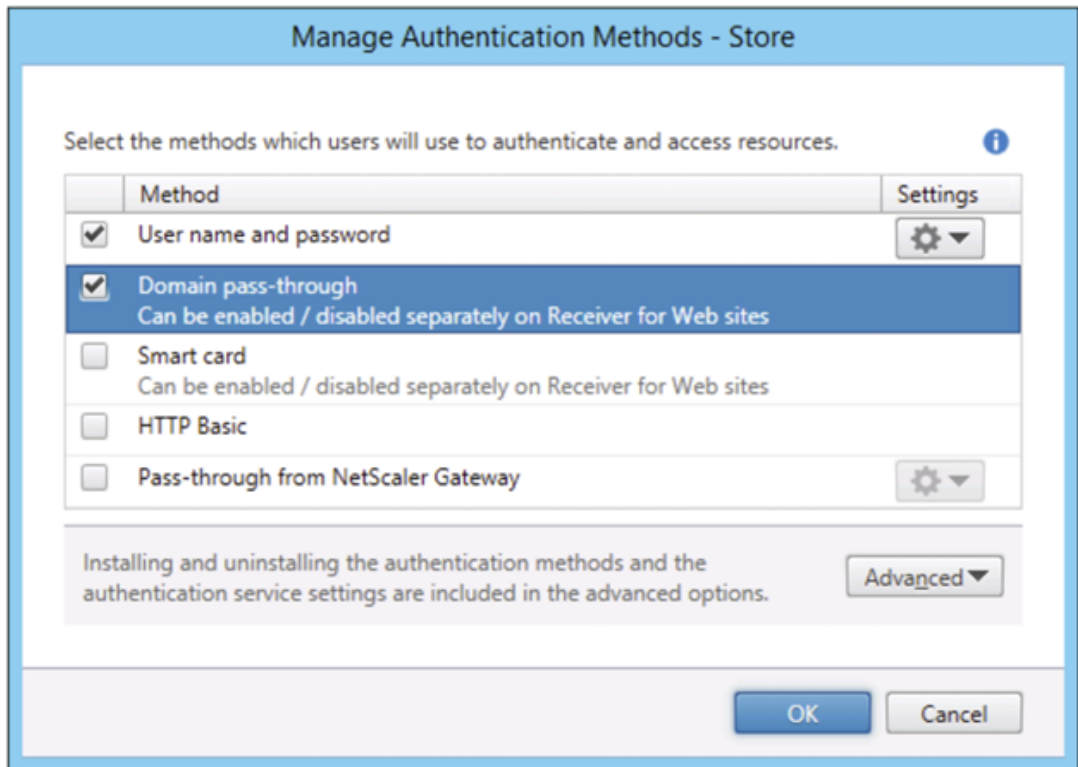
1. Wenn die Citrix Workspace-App in StoreFront konfiguriert ist:
  - a) Öffnen Sie **StoreFront Studio**.
  - b) Gehen Sie zu **Store > Authentifizierungsmethoden verwalten**.
  - c) Aktivieren Sie **Domänen-Passthrough**.

Oder

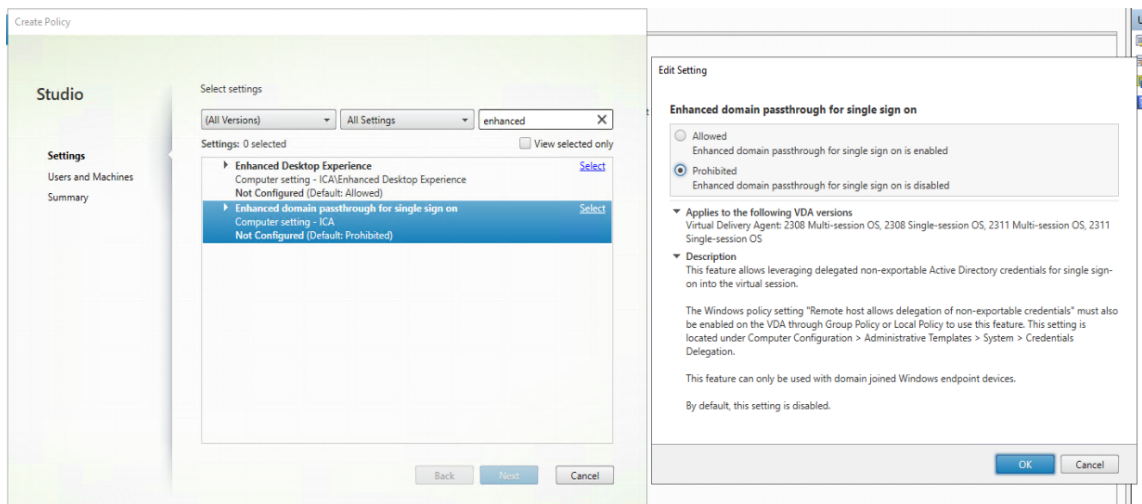
1. Wenn Sie die Citrix Workspace-App über den Browser verwenden:
  - a) Öffnen Sie StoreFront.
  - b) Gehen Sie zu **Stores > Receiver für Websites > Authentifizierungsmethoden verwalten**.



c) Aktivieren Sie **Domänen-Passthrough**.



2. Aktivieren Sie das **erweiterte Domain-Passthrough für die Single-Sign-On-Richtlinie** auf DDC.

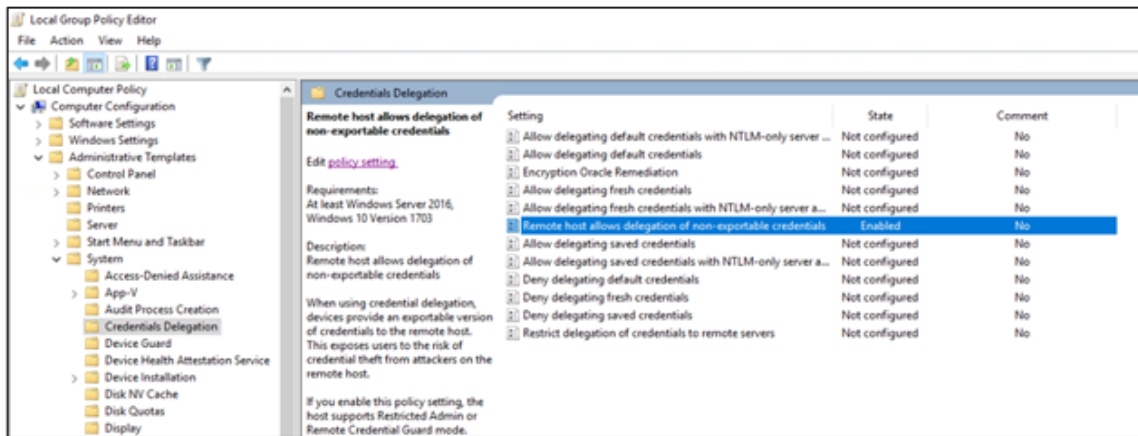


3. Klicken Sie auf **OK**.

## VDA-Einstellungen

1. Gehen Sie auf dem VDA zu **Computerkonfiguration\Administrative Vorlagen\System\Anmeldeinformationen**

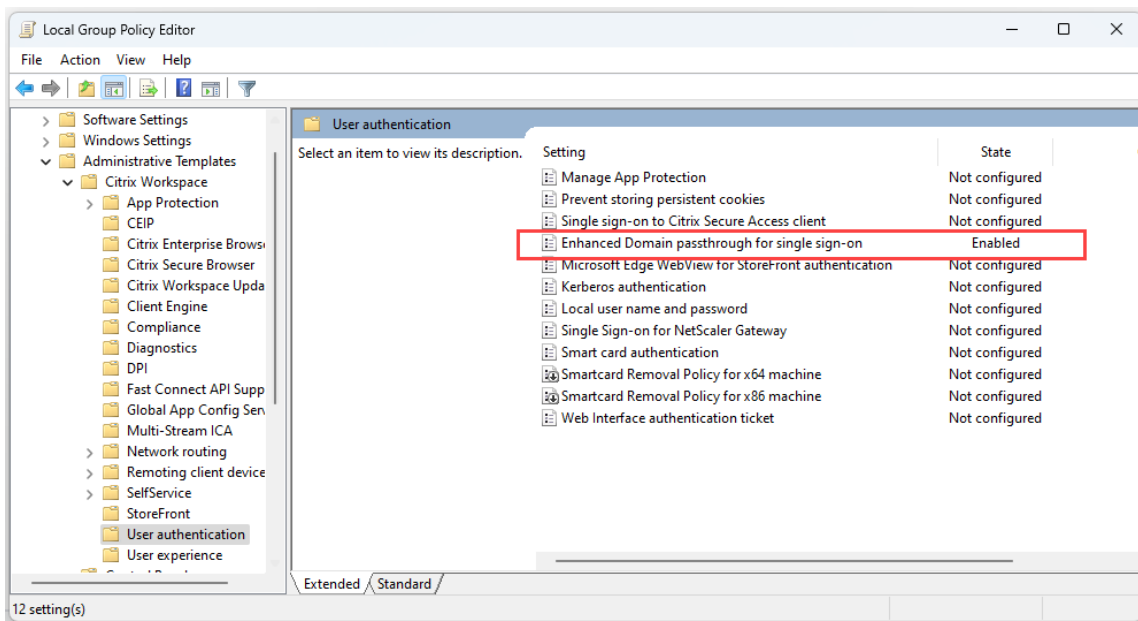
2. Aktivieren Sie die Windows-Richtlinie **Remotehost ermöglicht die Delegation nicht exportierbarer Anmeldeinformationen** auf dem VDA.

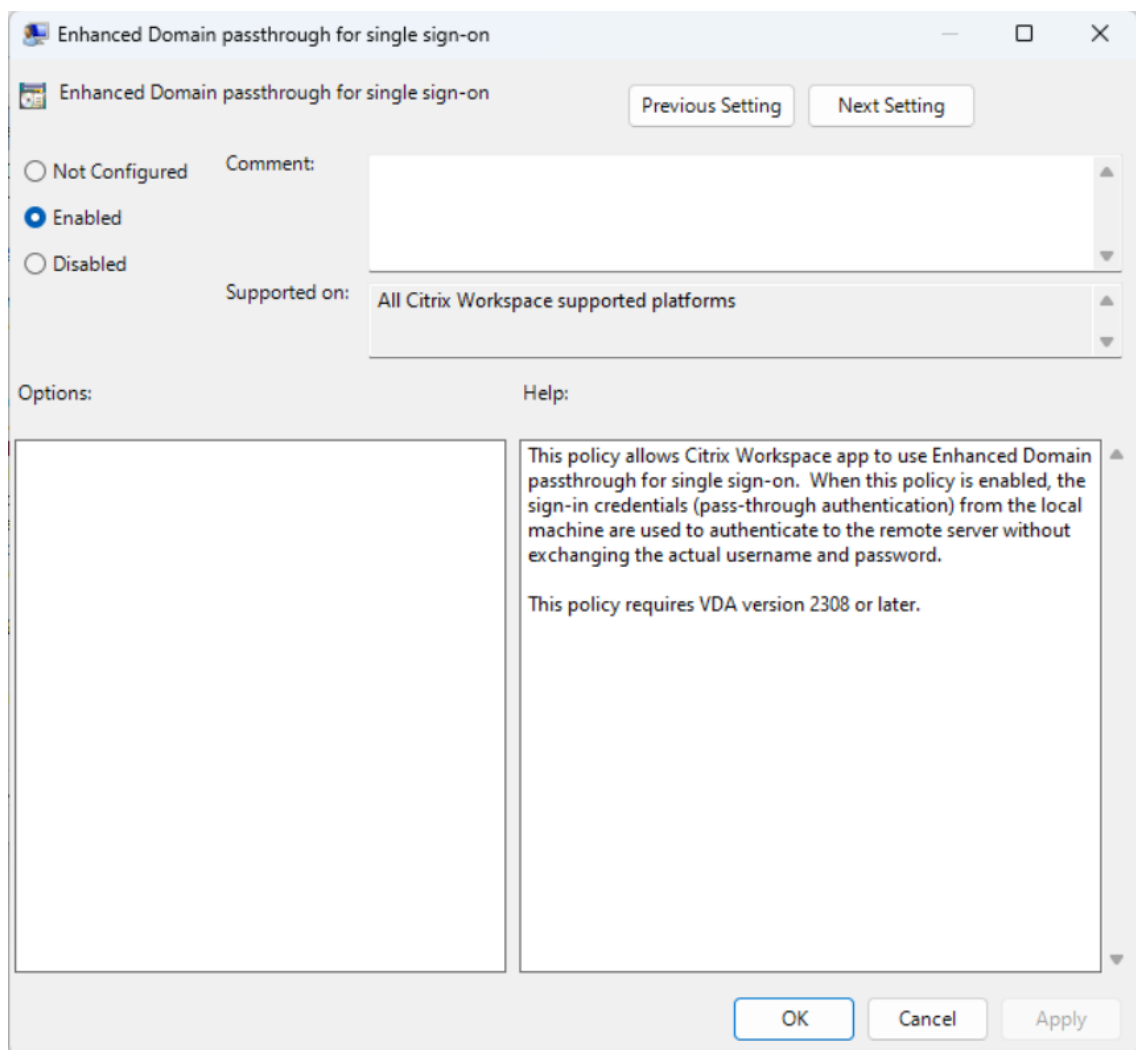


3. Starten Sie die VDA-Maschine neu.

## Clienteneinstellungen

1. Stellen Sie sicher, dass die Clientmaschine mit der Domäne verbunden ist.
2. Stellen Sie sicher, dass die Clientmaschine ein 64-Bit-Gerät ist.
3. Öffnen Sie den **Gruppenrichtlinien-Editor**.
4. Gehen Sie zu **Computerkonfiguration\Administrative Vorlagen\Citrix Components\Citrix Workspace\Benutzerauthentifizierung**.
5. Konfigurieren Sie die Gruppenrichtlinie **Erweitertes Domänen-Passthrough für Single Sign-On**.





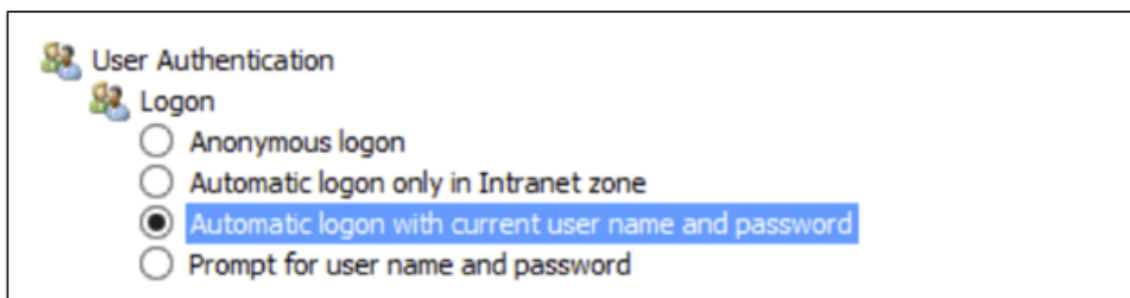
6. Ändern Sie die Einstellungen für **Internetoptionen** auf dem Client.

**Hinweis:**

Sie können diesen Schritt überspringen, wenn Sie in Ihrer Umgebung bereits Domänen-Passthrough konfiguriert haben.

1. Fügen Sie den StoreFront-Server der Liste der vertrauenswürdigen Sites über **Internetoptionen** hinzu. Schrittfolge zum Hinzufügen:
  - a) Öffnen Sie **Internetoptionen** über **Systemsteuerung > Netzwerk und Internet**.
  - b) Klicken Sie auf **Sicherheit > Lokales Intranet** und dann auf **Sites**. Das Fenster **Lokales Intranet** wird angezeigt.
  - c) Klicken Sie auf die Registerkarte **Erweitert**.
  - d) Fügen Sie die URL des StoreFront-FQDN mit den entsprechenden HTTP- oder HTTPS-Protokollen hinzu.
  - e) Klicken Sie auf **Schließen** und **OK**.

2. Ändern Sie im Internet Explorer die Einstellungen unter Benutzerauthentifizierung. Schrittfolge zum Modifizieren:
  - a) Öffnen Sie **Internetoptionen** über die **Systemsteuerung > Netzwerk und Internet**.
  - b) Klicken Sie auf die Registerkarte **Sicherheit > Lokales Intranet**.
  - c) Klicken Sie auf **Stufe anpassen**. Das Fenster **Sicherheitseinstellungen –lokale Intranetzone** wird angezeigt.
  - d) Wählen Sie im Bereich **Benutzerauthentifizierung** die Option **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort**.



3. Klicken Sie auf **OK**.

### **Unterstützung für erweiterte NetScaler-Richtlinien für Storebrowse unter Windows**

Die Citrix Workspace-App für Windows unterstützt jetzt erweiterte Richtlinien auf NetScaler Gateway mit Storebrowse. Das unterstützte Authentifizierungsprotokoll ist die LDAP-Authentifizierung. Storebrowse ist ein Befehlszeilenhilfsprogramm zur Interaktion zwischen Client und Server. Es wird zur Authentifizierung aller Operationen innerhalb von StoreFront und mit Citrix Gateway verwendet. Weitere Informationen finden Sie auf der Seite [Storebrowse](#).

#### **Hinweis:**

Das nFactor-Authentifizierungsprotokoll wird mit Storebrowse unter Windows nicht unterstützt.

### **Microsoft Teams VDI-Plug-In für Citrix installieren**

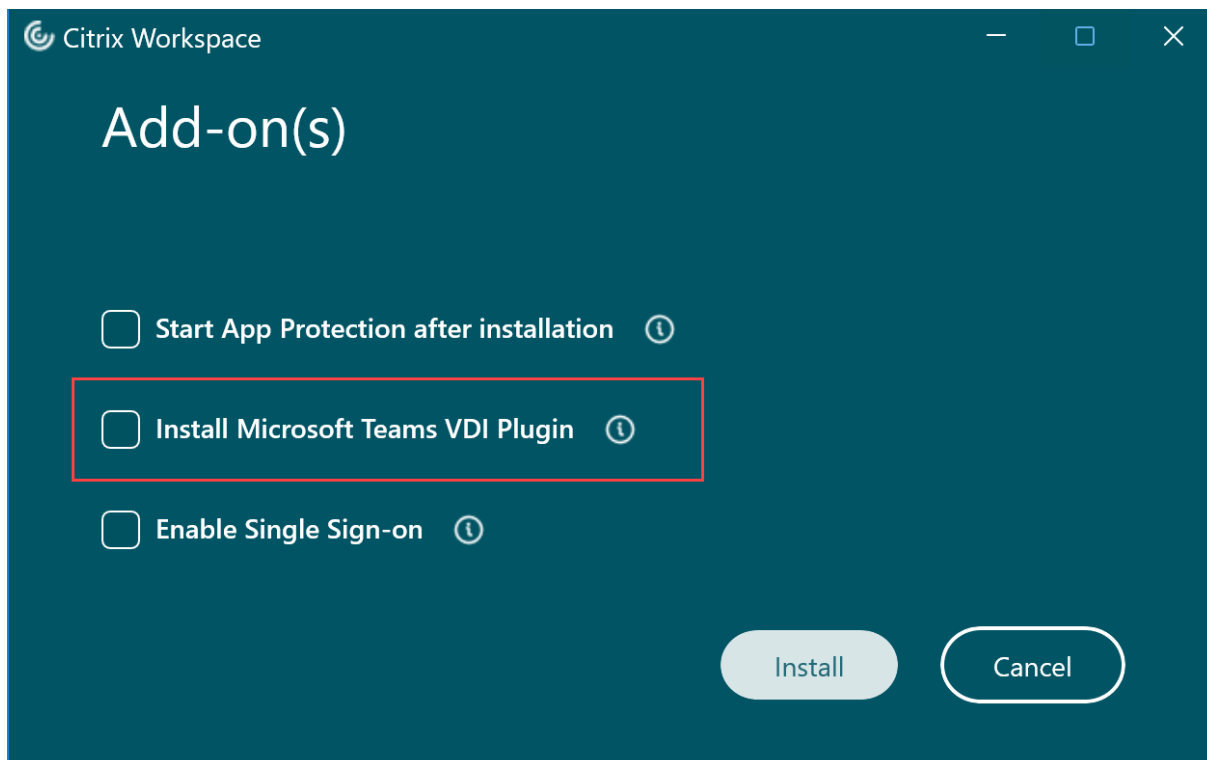
Sie können jetzt das Microsoft Teams VDI-Plug-In während der Installation der Citrix Workspace-App mit einer der folgenden Optionen installieren.

#### **Hinweis:**

Informationen zur Versionskompatibilität mit VDI und Konfigurationsdetails finden Sie unter [Microsoft Teams 2.1 unterstützt für VDI/DaaS und New Teams VDI-Anforderungen](#).

### Benutzeroberfläche verwenden

1. Markieren Sie auf der Seite **Add-on(s)** das Kontrollkästchen **Microsoft Teams VDI-Plug-In installieren**, und klicken Sie dann auf **Installieren**.
2. Stimmen Sie der Benutzervereinbarung zu, die angezeigt wird, und fahren Sie mit der Installation der Citrix Workspace-App fort.



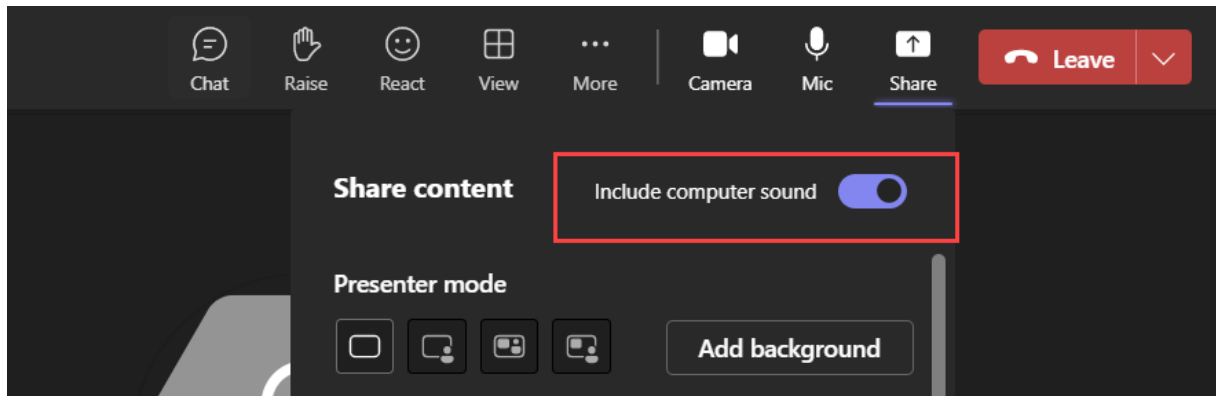
**Befehlszeile verwenden** Verwenden Sie die Befehlszeilenoption `/installMSTeamsPlugin`.

Beispiel: `CitrixWorkspaceApp.exe /installMSTeamsPlugin`

### Systemaudio teilen [Technical Preview]

Sie können jetzt die Audiowiedergabe auf Ihrem VDA mit Teilnehmern einer Besprechung teilen. Wählen Sie die Option **Computersound einbeziehen**, um Ihre Besprechungen ansprechender zu gestalten. Sie müssen diese Funktion über die Registrierung aktivieren, indem Sie `HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\EnableSystemAudio (DWORD)` auf 1 einstellen.

Für Endbenutzer ist diese Option standardmäßig nicht aktiviert. Sie müssen sie aktivieren, bevor sie ihren Bildschirm teilen können.



### Einschränkungen

- Audio kann mit diesem Feature nicht geteilt werden, wenn der Bildschirm mit RAVE- und BCR-umgeleiteten Apps oder Tabs geteilt wird.
- Die Echokompensation ist deaktiviert, wenn die Share-System-Audiofunktion aktiviert ist.
- Diese Funktion wird nur auf veröffentlichten Desktops unterstützt.

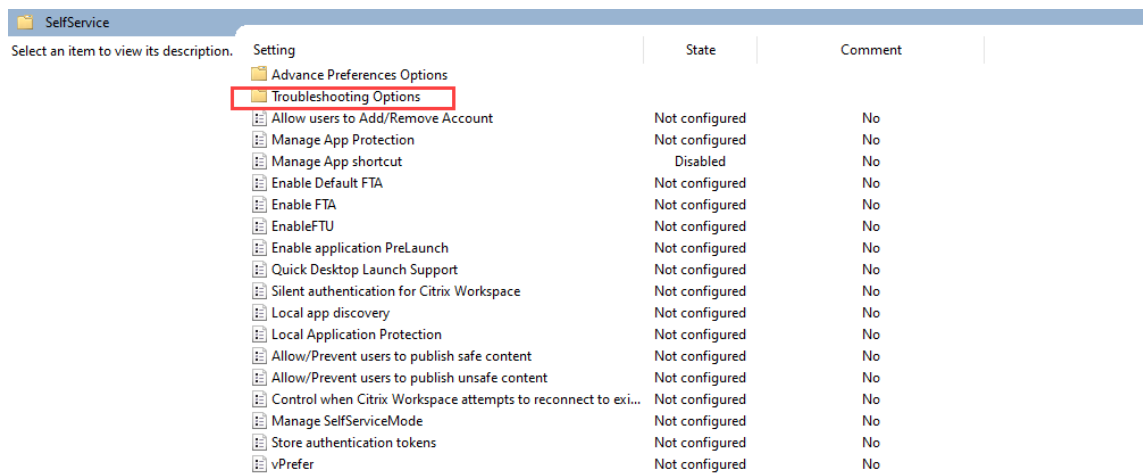
#### Hinweis:

Dieses Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfügbar.

### Option zur Problembehandlung für Endbenutzer ausblenden

Administratoren können jetzt die Fehlerbehebungsoptionen für ihre Endbenutzer mit dem GPO-Editor ausblenden. Sobald diese Einstellung aktiviert ist, wird die Option zur Fehlerbehebung, die zuvor für die Endbenutzer in der Taskleiste sichtbar war, ausgeblendet.

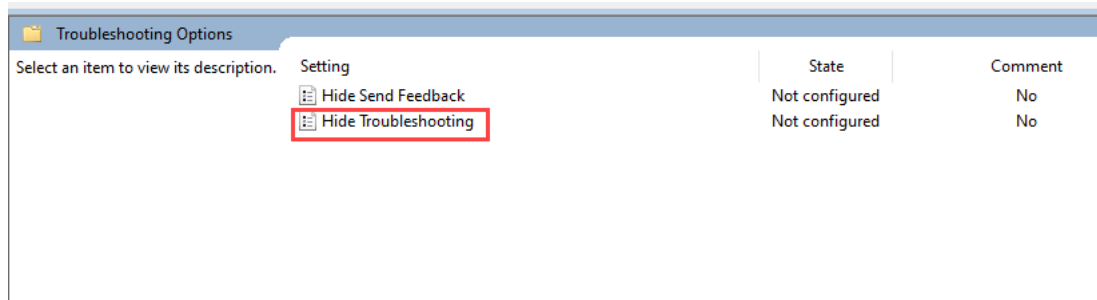
1. Navigieren Sie im GPO-Editor zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Self-Service**.
2. Wählen Sie den Ordner **Optionen zur Problembehandlung** aus.



The screenshot shows the 'SelfService' settings window. The 'Troubleshooting Options' folder is highlighted with a red box. Below it, a list of settings is displayed in a table format.

Setting	State	Comment
Advance Preferences Options		
<b>Troubleshooting Options</b>		
Allow users to Add/Remove Account	Not configured	No
Manage App Protection	Not configured	No
Manage App shortcut	Disabled	No
Enable Default FTA	Not configured	No
Enable FTA	Not configured	No
EnableFTU	Not configured	No
Enable application PreLaunch	Not configured	No
Quick Desktop Launch Support	Not configured	No
Silent authentication for Citrix Workspace	Not configured	No
Local app discovery	Not configured	No
Local Application Protection	Not configured	No
Allow/Prevent users to publish safe content	Not configured	No
Allow/Prevent users to publish unsafe content	Not configured	No
Control when Citrix Workspace attempts to reconnect to exi...	Not configured	No
Manage SelfServiceMode	Not configured	No
Store authentication tokens	Not configured	No
vPrefer	Not configured	No

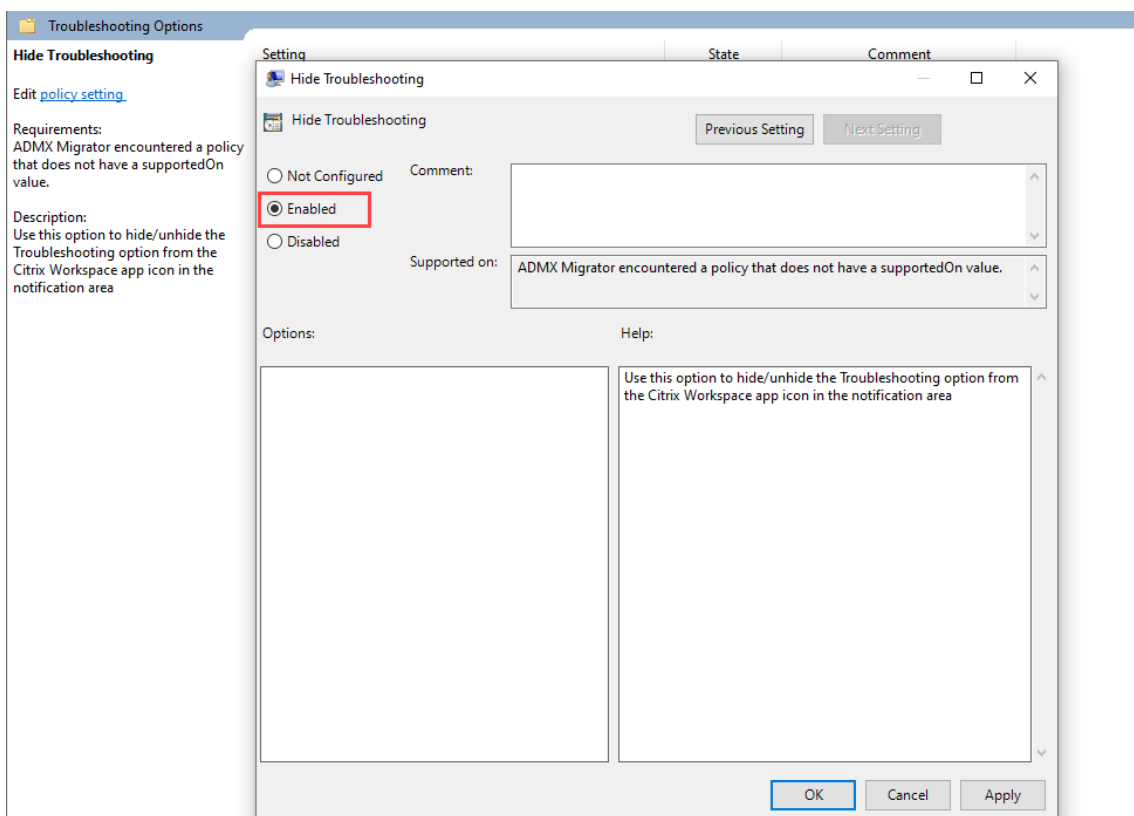
3. Wählen Sie die Einstellung **Problembehandlung ausblenden**.



The screenshot shows the 'Troubleshooting Options' settings window. The 'Hide Troubleshooting' option is highlighted with a red box.

Setting	State	Comment
Hide Send Feedback	Not configured	No
<b>Hide Troubleshooting</b>	Not configured	No

4. Markieren Sie im Dialogfeld “Problembehandlung ausblenden” das Kontrollkästchen **Aktiviert**. Wenn Sie dieses Kontrollkästchen auswählen, wird die Option zur Problembehandlung vor den Endbenutzern ausgeblendet.



5. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern.

## Versionsupgrade für Chromium Embedded Framework

Die Version des Chromium Embedded Framework (CEF) wurde auf Version 120 aktualisiert. Dieses Versionsupgrade hilft, Sicherheitslücken zu schließen.

## App Protection

**Positivliste für Screenshots** Wenn die Citrix Workspace-App, virtuelle Apps und Desktops oder SaaS-Apps mit der App Protection Anti-Screencapture-Richtlinie aktiviert sind, können Sie ihre Bildschirme mit keinem Screenshottool erfassen.

Ab der Version 2402 der Citrix Workspace-App für Windows können Sie jedoch mit der Funktion “Positivliste für Screenshots” eine App zur Positivliste für Screenshots hinzufügen. Mit dieser Funktion können Sie “Aufgelistete App zulassen” verwenden und den Bildschirm der Ressource erfassen, die mit der App Protection-Richtlinie gegen Screenshots aktiviert ist. Weitere Informationen finden Sie unter [Positivliste für Screenshots](#).



**Ausschlussliste für Prozesse** Wenn Sie einen Prozess oder eine Anwendung auf Ihrem Gerät starten, werden App Protection-DLLs in jeden Prozess eingefügt, sofern der 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. Weitere Informationen finden Sie unter [Ausschlussliste für Prozesse](#).

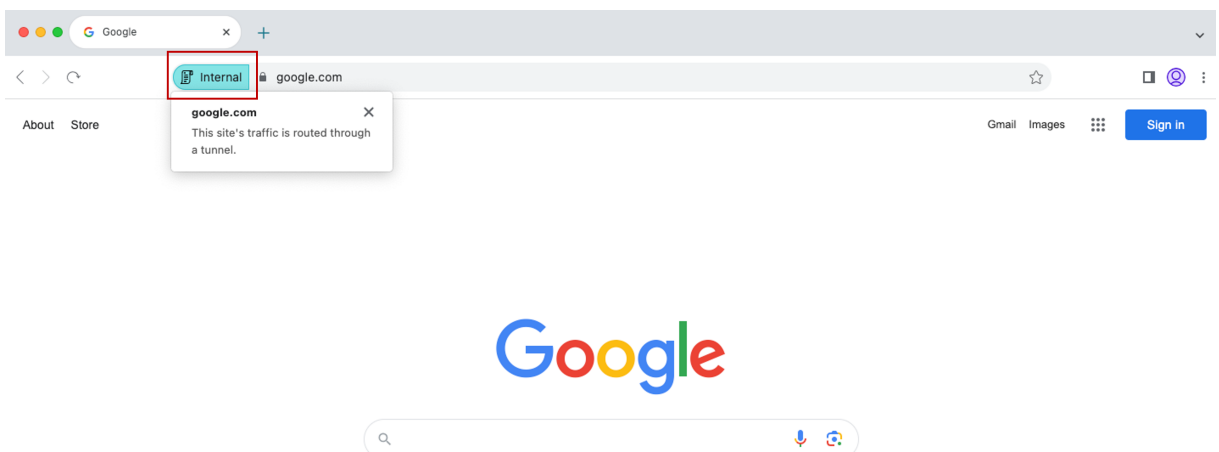
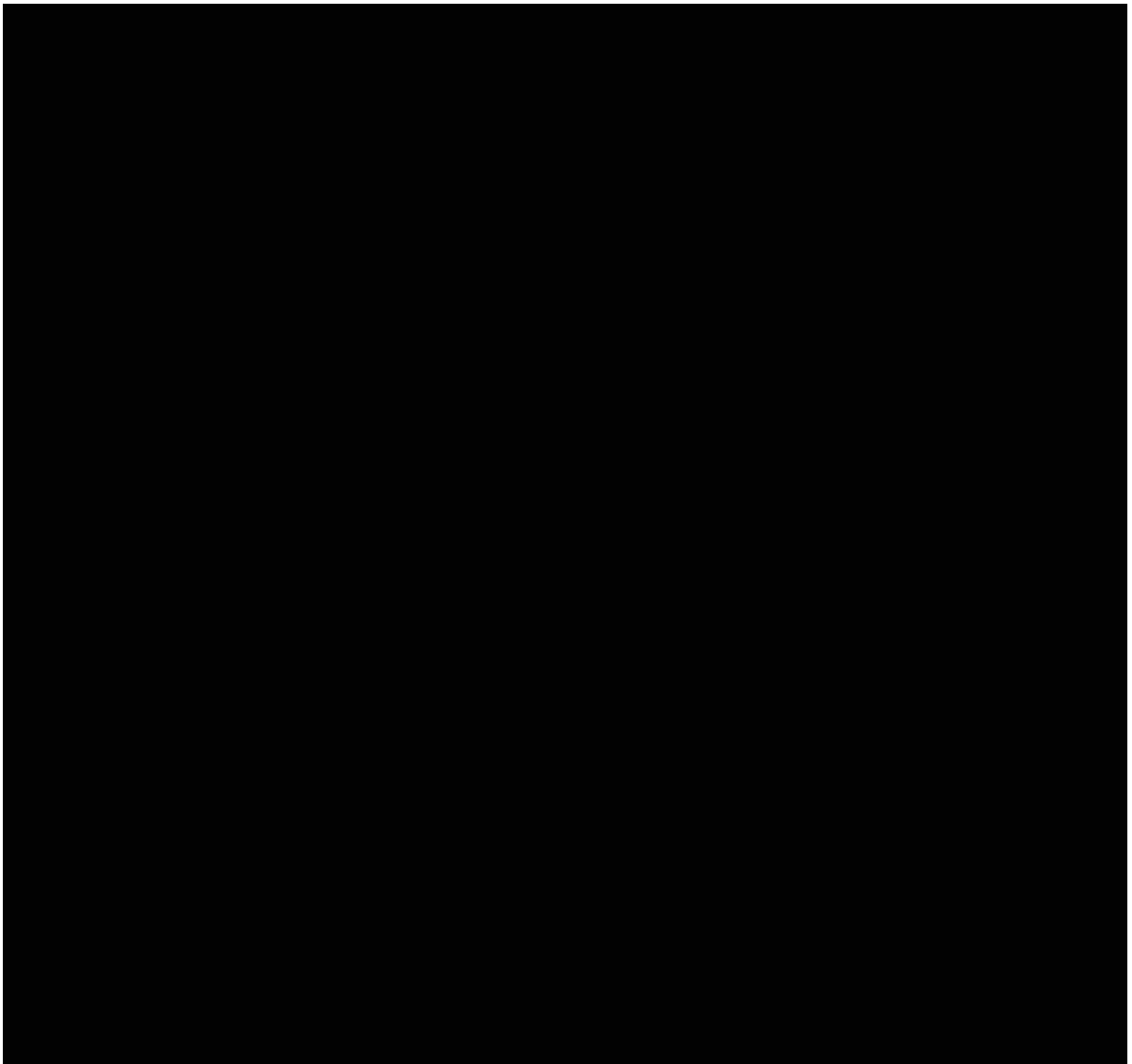
**Ausschlussliste für USB-Filtertreiber** Wenn Sie spezielle externe Tastaturen wie Gaming-Tastaturen mit der Citrix Workspace-App verwenden, kann der App Protection USB-Filtertreiber manchmal Kompatibilitätsprobleme verursachen und Sie daran hindern, die Tastatur zu verwenden.

Ab der Version 2402 der Citrix Workspace-App für Windows können Sie mit der Funktion “Ausschlussliste für USB-Filtertreiber” jedes USB-Gerät ausschließen, das Kompatibilitätsprobleme mit der Citrix Workspace-App hat, indem Sie die Gerätehersteller-ID und die Produkt-ID verwenden. Weitere Informationen finden Sie unter [Ausschlussliste für USB-Filtertreiber](#).

### **Citrix Enterprise Browser**

Diese Version von Citrix Enterprise Browser wird mit der Citrix Workspace-App für Windows 2402 installiert und basiert auf der Chromium-Version 122.

**Sicherheitsindikator beim Besuch von Websites** Citrix Enterprise Browser zeigt jetzt eine Sicherheitsanzeige in der Adressleiste an, wenn Benutzer Websites besuchen. Der Indikator soll Benutzer über die Sicherheitsaspekte der Websites informieren, z. B. ob es sich um eine interne Website handelt oder ob potenzielle Sicherheitseinschränkungen bestehen. Der Indikator bietet weitere Informationen, wenn Sie darauf klicken. Der Indikator wird standardmäßig im Unternehmensbrowser angezeigt und verbessert die Benutzererfahrung.



**Citrix Enterprise Browser führt zusätzliche Einstellungen im Global App Configuration Service ein** Zusätzliche Einstellungen wurden dem Global App Configuration Service (GACS) für die Konfiguration von Citrix Enterprise Browser hinzugefügt.

- Automatisches Ausfüllen der Adresse aktivieren —Ermöglicht Administratoren, die Autofill-Vorschläge für Adressen zu aktivieren oder zu deaktivieren.
- Automatisches Ausfüllen von Kreditkarten aktivieren —Ermöglicht Administratoren, die Vorschläge zum automatischen Ausfüllen von Kreditkarteninformationen zu aktivieren oder zu deaktivieren.
- Automatisches Starten von Protokollen aus Ursprung —Ermöglicht Administratoren, eine Liste von Protokollen anzugeben, mit denen eine externe App von den aufgelisteten Ursprüngen aus gestartet werden kann, ohne dass der Benutzer dazu aufgefordert wird.
- Sicherheitswarnungen für Befehlszeilenkennzeichen aktivieren —Ermöglicht Administratoren das Ein- oder Ausblenden von Sicherheitswarnungen, die angezeigt werden, wenn potenziell gefährliche Befehlszeilen-Flags versuchen, den Enterprise Browser zu starten.
- Standardeinstellung für Cookies verwalten —Ermöglicht Administratoren, Cookies für eine Website zu verwalten.
- Standardeinstellung für Popups verwalten —Ermöglicht Administratoren, Popups von einer Website zu verwalten.
- Installationsquellen für Erweiterungen —Ermöglicht Administratoren, gültige Quellen anzugeben, aus denen Benutzer Erweiterungen, Apps und Designs installieren können.
- Lookalike-Warnseiten deaktivieren —Ermöglicht Administratoren, die bevorzugten Domänen anzugeben, in denen Lookalike-Warnseiten nicht angezeigt werden, wenn der Benutzer Seiten in dieser Domäne besucht.
- Zahlungsmethodenabfrage aktivieren —Ermöglicht es Administratoren, Websites zu ermöglichen, zu überprüfen, ob die Benutzer Zahlungsmethoden gespeichert haben.
- Speichern des Browserverlaufs verwalten —Ermöglicht Administratoren, das Speichern des Enterprise Browser-Verlaufs zu verwalten.
- Suchvorschlag verwalten —Ermöglicht Administratoren, Suchvorschläge in der Adressleiste des Enterprise Browsers zu aktivieren oder zu deaktivieren.
- Export-Lesezeichen aktivieren —Ermöglicht Administratoren, eine Option zum Exportieren der Lesezeichen im Enterprise Browser zu aktivieren.
- Kurzlebige Profile erzwingen —Ermöglicht Administratoren, Benutzerprofildaten zu löschen oder beizubehalten, wenn Benutzer den Enterprise Browser schließen.

Weitere Informationen finden Sie auf der Seite [Citrix Enterprise Browser mit dem Global App Configuration Service verwalten](#) in der Dokumentation zum Citrix Enterprise Browser.

Weitere Informationen zu JSON-Beispieldaten finden Sie unter [JSON-Beispieldaten](#).

## Citrix Endpoint Analysis

In dieser Version ist der EPA-Client mit dem Citrix Workspace-App-Installationsprogramm gebündelt. Um den Client zu installieren, muss die Citrix Workspace-App mit der Befehlszeilenoption `InstalleEPAClient` installiert werden.

Beispiel: `./CitrixworkspaceApp.exe InstalleEPAClient`

### Hinweis:

EPA ist standardmäßig nicht installiert.

In dieser Version ist die EPA-Version 23.11.1.20 verpackt.

## Funktion, die in früheren Releases enthalten war

Dieses Release unterstützt Features, die in der Citrix Workspace-App für Windows von 2204.1 bis 2311.1 enthalten waren, wie unten aufgeführt.

### 2311.1

Dieses Release enthält die folgenden neuen Features:

- Einführung des neuen Citrix Workspace-App-Installationsprogramms
- Unterstützung für Aktivitätsmanager in Cloudstores
- Automatische Auswahl des Videocodecs
- Verlusttoleranzmodus für Audio
- Synchronisierung mehrerer Tastaturen beim Sitzungsstart
- Verbesserte Leistung bei der Browserinhaltsumleitung
- Versionsupgrade für Chromium Embedded Framework
- Wichtiges Update zu App Protection-Dateinamen
- Citrix Enterprise Browser
  - Verbesserte Benutzererfahrung und Ladezeit der Sitzung
  - Verbessertes Wasserzeichendesign
  - Unterstützung für benutzerdefinierte Browsererweiterung
  - Vereinfachtes SSO für Web- und SaaS-Apps über den Global App Configuration Service
  - Passthrough-Authentifizierung im Citrix Enterprise Browser verwalten
  - Verbesserte Funktionen zur Überwachung der Endbenutzeraktivitäten

**Hinweis:**

Ab Version 2311.1 der Citrix Workspace-App für Windows ist die Internet Explorer-basierte Browserinhaltsumleitung veraltet. Die alternative Option besteht darin, die Google Chrome-basierte Browserinhaltsumleitung zu verwenden.

## **Einführung des neuen Citrix Workspace-App-Installationsprogramms**

Die Benutzeroberfläche des Citrix Workspace-App-Installationsprogramms wurde überarbeitet, um ein modernes, einfaches Erscheinungsbild und eine bessere Benutzererfahrung zu bieten. Standardmäßig ist das neue Installationsprogramm aktiviert.

**Voraussetzungen:**

.Net Desktop Runtime 6.0.20 oder höher ist eine zusätzliche Voraussetzung für das neue Installationsprogramm. Weitere Informationen finden Sie unter [Systemanforderungen](#).

Das neue Installationsprogramm ist standardmäßig aktiviert. Weitere Informationen finden Sie unter [Installation über die Benutzeroberfläche](#).

**Hinweis:**

Ab der Version 2311.1 der Citrix Workspace-App für Windows wird `TrolleyExpress` durch `CWAInstaller-<date and timestamp>` ersetzt. Das Protokoll wird beispielsweise unter `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441` aufgezeichnet.

## **Unterstützung für Aktivitätsmanager in Cloudstores**

Die Citrix Workspace-App für Windows unterstützt das Feature "Aktivitätsmanager". Mit diesem Feature können Endbenutzer alle aktiven App- und Desktopsitzungen auf einen Blick anzeigen und damit interagieren. Um aktive Sitzungen im **Aktivitätsmanager** anzuzeigen, klicken Sie auf das **Activity Manager**-Symbol. Sie können die folgenden Aktionen an einer App oder an einem Desktop ausführen, indem sie auf die zugehörige Menüschaltfläche (...) im Aktivitätsmanager klicken.

- **Abmelden:** Zur Abmeldung von der aktuellen Sitzung. Alle Apps in der Sitzung werden geschlossen und alle nicht gespeicherten Dateien gehen verloren.
- **Verbindung trennen:** Die Remotesitzung wird getrennt, die Apps und Desktops sind jedoch weiter im Hintergrund aktiv.
- **Neu starten:** Führt den Desktop herunter und startet ihn neu.
- **Herunterfahren:** Schließt die getrennten Desktops.
- **Beenden erzwingen:** Schaltet Ihren Desktop zwangsweise aus, wenn ein technisches Problem auftritt.

- Klicken Sie im Aktivitätsmanager auf die Schaltfläche **X**, um die aktive App-Sitzung zu beenden.

Weitere Informationen finden Sie unter [Aktivitätsmanager](#).

**Hinweis:**

Diese Funktion ist in der Citrix Workspace-App für Windows nur verfügbar, wenn die [neue Workspace-Benutzeroberfläche](#) aktiviert ist.

### **Automatische Auswahl des Videocodecs**

In dieser Version erkennt die Citrix Workspace-App für Windows jetzt automatisch den am besten zu verwendenden Videocodec. Während der Installation der Citrix Workspace-App für Windows werden die Decodierungsfunktionen des Endpunkts evaluiert. Basierend auf diesen Informationen wählt die Citrix Workspace-App für Windows beim Start der Sitzung den besten Codec für die Verwendung mit dem VDA aus. Die Videocodecs werden in der folgenden Reihenfolge ausgewertet:

1. AV1
2. H.265
3. H.264

Diese Funktion ist verfügbar, wenn die Richtlinie **Videocodec zur Komprimierung verwenden** auf eine der folgenden Einstellungen gesetzt ist:

- **Verwenden, wenn bevorzugt**
- **Für den gesamten Bildschirm**
- **Für aktive Änderungsbereiche**

Weitere Informationen zur Richtlinie **Videocodec zur Komprimierung verwenden** finden Sie unter [Videocodec zur Komprimierung verwenden](#).

Die automatische Auswahl gilt nur für YUV 4:2:0 -Varianten dieser Codecs. YUV 4:2:0 verwendet weniger Bandbreite und beeinträchtigt die Qualität. Wenn die Richtlinieneinstellung **Bildqualität** auf **Zu verlustfrei verbessern** oder **Immer verlustfrei** gesetzt ist und wenn die Richtlinie **Visuell verlustfreie Komprimierung zulassen** auf **aktiviert** gesetzt ist, wird die automatische Auswahl des Videocodecs deaktiviert und stattdessen YUV 4:4:4 H.264 oder H.265 verwendet.

Weitere Informationen zu diesen Richtlinien finden Sie unter:

- [Bildqualität](#)
- [Visuell verlustfreie Komprimierung zulassen](#)

Dieses Feature ist standardmäßig aktiviert.

Weitere Informationen finden Sie unter [Automatische Auswahl des Videocodecs](#).

**H.265** Die Citrix Workspace-App unterstützt die Verwendung des H.265-Videocodecs für die Hardwarebeschleunigung von Remote-Grafiken und -Videos. Der Videocodec H.265 muss sowohl auf dem VDA als auch auf der Citrix Workspace-App unterstützt und aktiviert werden.

Ab Citrix Workspace-App 2311.1 wird dieses Feature mit der Einführung des Features **Automatische Auswahl des Videocodecs** automatisch aktiviert.

Weitere Informationen finden Sie in der [H.265](#)-Dokumentation.

**AV1** Die Citrix Workspace-App unterstützt die Verwendung des AV1-Videocodecs für die Hardwarebeschleunigung von Remote-Grafiken und -Videos. Der Videocodec AV1 muss sowohl auf dem VDA als auch auf der Citrix Workspace-App unterstützt und aktiviert werden.

Ab Citrix Workspace-App 2311.1 wird dieses Feature mit der Einführung des Features **Automatische Auswahl des Videocodecs** automatisch aktiviert.

Weitere Informationen finden Sie in der [AV1](#)-Dokumentation.

### **Verlusttoleranzmodus für Audio**

Ab diesem Release unterstützt die Citrix Workspace-App den Verlusttoleranzmodus (EDT Lossy) für die Audioumleitung. Das Feature verbessert das Echtzeit-Streaming bei Verbindungen über ein Netzwerk mit Paketverlust und hoher Latenz.

Sie müssen VDA-Version 2311 oder höher verwenden. Dieses Feature ist standardmäßig in der Citrix Workspace-App für Windows aktiviert. Es ist jedoch auf dem VDA deaktiviert.

Weitere Informationen finden Sie in der Dokumentation [Verlusttoleranzmodus für Audio](#).

### **Synchronisierung mehrerer Tastaturen beim Sitzungsstart**

Bisher wurde nur die aktive Tastatur auf dem Client mit dem VDA synchronisiert, nachdem die Sitzung im Vollbildmodus gestartet wurde. Wenn Sie in diesem Szenario **Nur einmal beim Sitzungsstart synchronisieren** in Ihrer Citrix Workspace-App konfiguriert hatten und Sie zu einer anderen Tastatur wechseln mussten, war es nötig, die Tastatur manuell auf Ihrem Remotedesktop zu installieren. Wenn Sie **Dynamische Synchronisierung zulassen** in Ihrer Citrix Workspace-App konfiguriert hatten, mussten Sie auch in den Fenstermodus wechseln, die Tastatur auf Ihrem Client ändern und dann zurück in den Vollbildmodus wechseln.

In dieser Version werden alle verfügbaren Tastaturen auf dem Client mit dem VDA synchronisiert, nachdem die Sitzung im Vollbildmodus gestartet wurde. Sie können die erforderliche Tastatur aus der Liste der installierten oder verfügbaren Tastaturen auf dem Client auswählen, nachdem die Sitzung im Vollbildmodus gestartet wurde.

Weitere Informationen finden Sie in der Dokumentation [Mehrere Tastaturen beim Sitzungsstart synchronisieren](#).

### **Verbesserte Leistung bei der Browserinhaltsumleitung**

Bisher verwendete die Browserinhaltsumleitung den clientseitigen Datenträgercache und die zwischengespeicherten Informationen wurden bei einem Upgrade nicht gelöscht. Diese Einstellung führte im Laufe der Zeit zu einer höheren Speicherplatznutzung und zu einem inkonsistenten Verhalten, wenn eine Seite mit der Browserinhaltsumleitung umgeleitet wurde.

In dieser Version verwendet die Browserinhaltsumleitung einen In-Memory-Cache, um dieses Problem zu beheben. Diese Verbesserung hilft, die Leistung der Browserinhaltsumleitung zu verbessern.

Das Feature ist in der Standardeinstellung deaktiviert.

Weitere Informationen finden Sie unter [Verbesserte Leistung bei der Browserinhaltsumleitung](#).

### **Versionsupgrade für Chromium Embedded Framework**

Die Version des Chromium Embedded Framework (CEF) wurde auf Version 117 aktualisiert. Dieses Versionsupgrade hilft, Sicherheitslücken zu schließen.

### **Wichtiges Update zu Datei- und Treibernamen von App Protection**

Ab Citrix Workspace-App für Windows 2311.1 werden die folgenden Datei- und Treibernamen wie folgt aktualisiert:

---

Bestehender Name	Neuer Name
<code>EntryProtect.dll</code>	<code>ctxapdotnet.dll</code>
<code>entryprotect.sys</code>	<code>ctxapdriver.sys</code>
<code>epclient32.dll</code>	<code>ctxapclient32.dll</code>
<code>epclient64.dll</code>	<code>ctxapclient64.dll</code>
<code>epinject.sys</code>	<code>ctxapinject.sys</code>
<code>epusbfilter.sys</code>	<code>ctxapusbfilter.sys</code>
<code>entryprotectdrv</code>	<code>ctxapdriver</code>
<code>epinject6</code>	<code>ctxapinject</code>

---



Diese Dateien werden standardmäßig in %ProgramFiles(x86)%\Citrix\ICA Client installiert.

Wenn Sie einen der obigen Datei- oder Treibernamen zur Positivliste in Ihrer Umgebung hinzugefügt haben, aktualisieren Sie die Positivliste.

### **Verbesserung der Hintergrundunschärfe und -effekte für Microsoft Teams-Optimierung mit HDX**

Ab Version 2311.1 der Citrix Workspace-App können Sie die folgenden Optionen für Hintergrundunschärfe und -effekte auswählen:

- Kein Hintergrundeffekt
- Wählen Sie "Hintergrundunschärfe"
- Wählen Sie "Hintergrundbild"

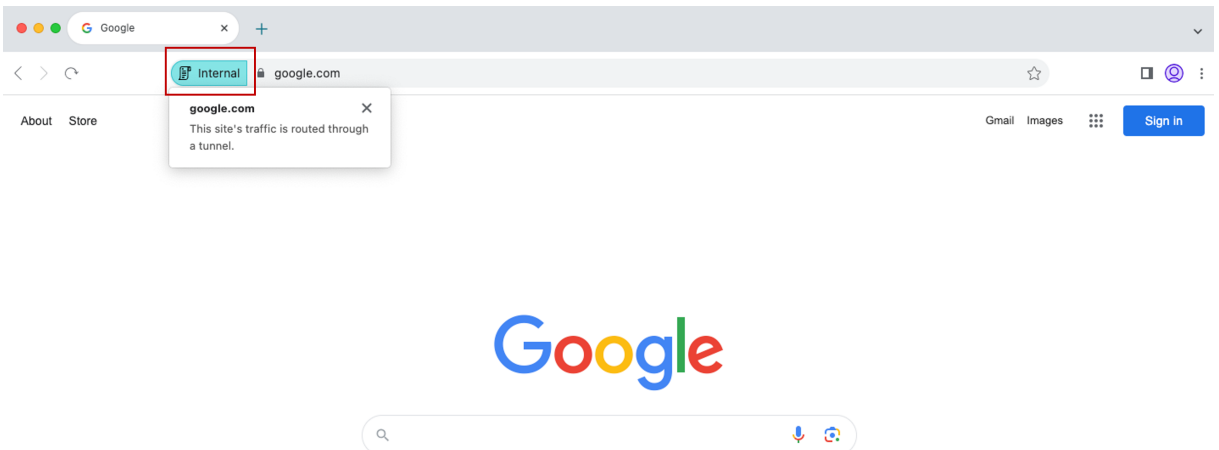
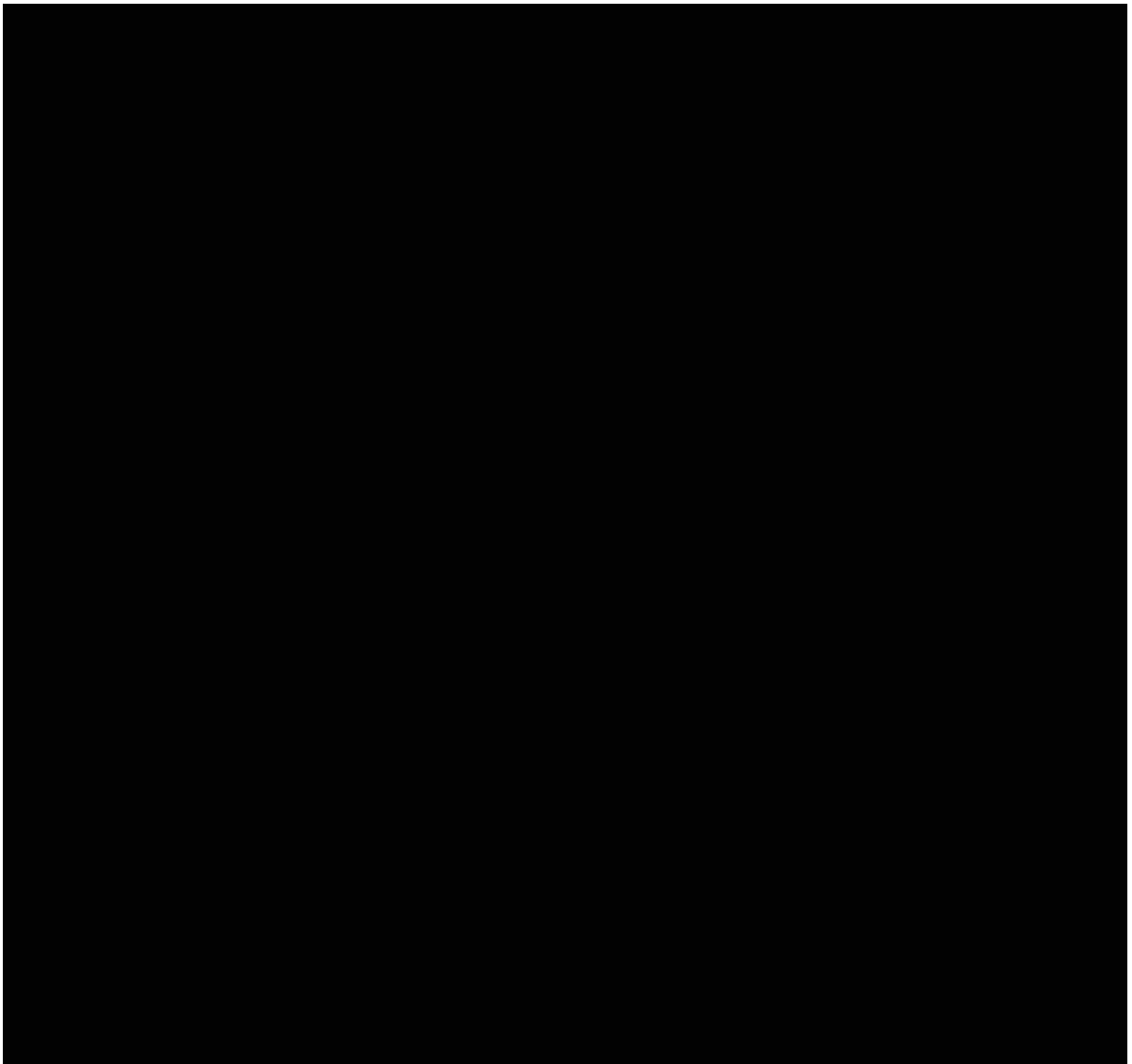
### **Citrix Enterprise Browser**

Dieses Release enthält Citrix Enterprise Browser Version 119.1.1.60 auf Basis der Chromium Version 115. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#)

**Citrix Enterprise Browser führt zusätzliche Einstellungen im Global App Configuration Service ein** Zusätzliche Einstellungen wurden dem Global App Configuration Service (GACS) für die Konfiguration von Citrix Enterprise Browser hinzugefügt. Weitere Informationen finden Sie unter [Citrix Enterprise Browser über GACS verwalten](#).

### **Sicherheitsindikator beim Besuch von Websites**

Citrix Enterprise Browser zeigt jetzt eine Sicherheitsanzeige in der Adressleiste an, wenn Benutzer Websites besuchen. Der Indikator soll Benutzer über die Sicherheitsaspekte der Websites informieren, z. B. ob es sich um eine interne Website handelt oder ob potenzielle Sicherheitseinschränkungen bestehen. Der Indikator bietet weitere Informationen, wenn Sie darauf klicken. Der Indikator wird standardmäßig im Unternehmensbrowser angezeigt und verbessert die Benutzererfahrung.



**Verbesserte Benutzererfahrung** Bisher wurde im Citrix Enterprise Browser ein Wiederverbindungs-fenster angezeigt, wenn Sie nach Ablauf Ihrer Sitzung versuchten, eine Aktion auszuführen. Ab Version 2311.1 der Citrix Workspace-App für Windows (entspricht der Chromium-Version 119.1.1.60) gibt es kein Wiederverbindungs-fenster mehr. Stattdessen erscheint jetzt ein Ladesymbol auf der Registerkarte des Browsers, wenn Sie nach Ablauf Ihrer Sitzung versuchen, eine Aktion auszuführen.

**Verbessertes Wasserzeichendesign** Der Citrix Enterprise Browser verfügt jetzt über ein neues Wasserzeichendesign, das weniger aufdringlich ist und benutzerfreundlicher ist.

**Unterstützung für benutzerdefinierte Browsererweiterung** Citrix Enterprise Browser hat verbesserte Erweiterungsfunktionen. Bisher waren nur Erweiterungen aus dem Chrome Web Store zulässig. Mit dem Citrix Enterprise Browser können Sie jetzt benutzerdefinierte Erweiterungen sicher hinzufügen. Administratoren können benutzerdefinierte Erweiterungen als Teil der Liste der obligatorischen Erweiterungen konfigurieren. Endbenutzer können auf diese Erweiterungen je nach Bedarf entweder über `citrixbrowser://extensions` zugreifen und sie verwenden oder indem sie unter der Schaltfläche **Mehr** auf die Option **Erweiterungen** klicken. Weitere Informationen zur Konfiguration der benutzerdefinierten Erweiterungen finden Sie unter [Obligatorische benutzerdefinierte Erweiterung](#).

**Vereinfachtes SSO für Web- und SaaS-Apps über den Global App Configuration Service** Zuvor wurde Single Sign-On (SSO) für den Citrix Enterprise Browser mithilfe des PowerShell-Moduls konfiguriert. Mit dieser vereinfachten SSO-Funktion können Sie SSO jetzt im Citrix Enterprise Browser konfigurieren, indem Sie eine neu eingeführte Einstellung im Global App Configuration Service (GACS) verwenden. Administratoren können diese neue Einstellung verwenden, um SSO für alle Web- und SaaS-Apps im Citrix Enterprise Browser zu aktivieren. Diese Methode macht das komplexe PowerShell-Modul überflüssig. Weitere Informationen zur Verwaltung von SSO über GACS finden Sie unter [Single Sign-On für Web- und SaaS-Apps über den Global App Configuration Service verwalten](#).

**Hinweis:**

Wir empfehlen Ihnen, Citrix Workspace-App neu zu starten, wenn Sie die Citrix Enterprise Browser-Einstellungen in GACS ändern. Sie können jedoch auch warten, bis die automatische Aktualisierung abgeschlossen ist. Weitere Informationen zur Synchronisierungsdauer der von GACS abgerufenen Richtlinien finden Sie unter [Häufigkeit der Aktualisierung der Einstellungen](#).

**Erweiterung der vereinfachten Single-Sign-On-Funktionalität auf StoreFront** Das Single Sign-On-Feature (SSO) ist jetzt für StoreFront verfügbar und gewährleistet damit eine einheitliche SSO-Benutzeroberfläche. Dank dieses neuen Features müssen sich Benutzer nicht separat zu authentifizieren, wenn sie über StoreFront auf Apps zugreifen. Verwenden Sie denselben Identity Provider

(IdP) für Web- und SaaS-Apps sowie für StoreFront, um dieses SSO-Feature zu ermöglichen. Weitere Informationen zur Verwaltung von SSO über GACS finden Sie unter [Single Sign-On für Web- und SaaS-Apps über den Global App Configuration Service verwalten](#).

**Passthrough-Authentifizierung im Citrix Enterprise Browser verwalten** Die Passthrough-Authentifizierung (PTA) ist ein Feature von Azure AD Connect. PTA ist eine Authentifizierungsmethode, bei der die Benutzeranmeldeinformationen von der Clientmaschine an den Server weitergegeben werden. Man sieht sie nie direkt, weil sie im Backend durchgeführt wird. Bei dieser Methode kommuniziert die Clientmaschine direkt mit dem Authentifizierungsserver, um die Anmeldeinformationen des Benutzers zu überprüfen. PTA wird normalerweise verwendet, wenn Ihre Clientmaschine und der Authentifizierungsserver einander vertrauen und Ihre Clientmaschine als sicher angesehen wird. Weitere Informationen zur Microsoft Azure AD-Passthrough-Authentifizierung finden Sie unter [Microsoft Entra Seamless Single Sign-On](#).

Um die Passthrough-Authentifizierung zu erleichtern, benötigen Sie die Erweiterung “Windows Accounts”, um mit Anwendungen zu interagieren, die Azure AD-basierten Zugriff im Enterprise Browser benötigen. Administratoren müssen diese [Windows Accounts](#)-Erweiterung als Teil der obligatorischen Liste unter **ExtensionInstallForcelist** konfigurieren. Weitere Informationen zur Konfiguration obligatorischer Erweiterungen finden Sie unter [Obligatorische Erweiterung](#).

**Verbesserte Funktionen zur Überwachung der Endbenutzeraktivitäten** Bisher waren Administratoren nicht in der Lage, Endbenutzeraktivitäten wie den Zugriff auf die App und die Art des Datenverkehrs zu überwachen. Ab Citrix Workspace-App für Windows 2311.1 (entspricht Chromium-Version 119.1.1.60) können Sie jetzt auch diese Details überwachen.

- **App-Zugriff:** Der Enterprise Browser bietet Informationen über alle Apps, auf die der Endbenutzer zugegriffen hat, sofern die App im Richtliniendokument aufgeführt ist.
- **Verkehrstyp:** Der Enterprise Browser liefert Informationen darüber, ob Daten direkt oder über die Secure Private Access-Authentifizierung gesendet werden.

Verwenden Sie den Citrix Analytics-Dienst mit Ihrem Citrix Cloud-Konto, um die Endbenutzeraktivitäten vom Enterprise Browser aus zu überwachen. Nachdem Sie sich bei Citrix Cloud angemeldet haben, navigieren Sie zu **Analytics > Sicherheit > Suchen**. Dort nutzen Sie die **Self-Service**-Suche im Abschnitt **Apps und Desktops**. Weitere Informationen zu Citrix Analytics finden Sie unter [Schnelleinstieg](#).

## 2309.1

### Was ist neu

In diesem Release wurden Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

### Citrix Enterprise Browser

Dieses Release enthält Citrix Enterprise Browser Version 117.1.1.13, der auf Chromium Version 117 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

## 2309

### Was ist neu

#### Hinweis:

Ab diesem Release ist Microsoft Edge WebView2 Runtime-Version 117 oder höher erforderlich. Wir empfehlen, die neueste Version zu installieren, um neuere Funktionen und sicherheitsrelevante Korrekturen zu erhalten.

Dieses Release enthält die folgenden neuen Features:

- [Zusätzliche .NET-Voraussetzungen](#)
- [Verbesserter Start von Virtual Apps and Desktops](#)
- [Option "Problembehandlung" zu Taskleiste der Citrix Workspace-App hinzugefügt](#)
  - [Feedback zur Citrix Workspace-App senden](#)
- [Nachhaltigkeitsinitiative der Citrix Workspace-App](#)
- [Tastaturlayoutsynchronisierung mit der Befehlszeilenschnittstelle \(CLI\) konfigurieren](#)
- [Befehl zum Bereinigen und Installieren der Citrix Workspace-App](#)
- [App Protection](#)
  - [Wichtiges Update zu Dateinamen](#)
  - [Richtlinienmanipulationen erkennen](#)
  - [App Protection und Double-Hop-Szenario](#)
- [Citrix Enterprise Browser](#)
  - [Authentifizierung über Citrix Enterprise Browser](#)

**Zusätzliche .NET-Voraussetzungen** Neben .NET Framework 4.8 benötigt die Citrix Workspace-App die x86-Version von .NET Desktop Runtime 6.0 für x86- und x64-Systeme. Weitere Informationen finden Sie unter [.NET-Anforderungen](#).

### Verbesserter Start von Virtual Apps and Desktops

#### Hinweis:

Ab Version 2305.1 der Citrix Workspace-App und höher ist dieses Feature generell für Cloudstores und ab Release 2309 für On-Premises-Stores verfügbar.

Bisher war das Dialogfeld zum Startfortschritt nicht sehr intuitiv für Benutzer. Aufgrund statischer Benachrichtigungen nahmen Benutzer an, dass der Startprozess gestoppt wurde, und schlossen das Dialogfeld.

Das verbesserte Startverhalten von Apps und Desktops macht die Citrix Workspace-App für Windows jetzt informativer und benutzerfreundlicher. Durch zeitnahe und relevante Informationen zum Startstatus bleiben Benutzer aktiv und informiert.

Weitere Informationen finden Sie unter [Verbesserter Start von virtuellen Apps und Desktops](#).

**Option “Problembehandlung” zu Taskleiste der Citrix Workspace-App hinzugefügt** Die Option **Problembehandlung** wurde eingeführt, um die Benutzererfahrung zu verbessern und die Problembehandlung zu vereinfachen. Sie können auf der Taskleiste unten rechts mit der rechten Maustaste auf das Symbol der Citrix Workspace-App klicken und dann **Problembehandlung** auswählen, um darauf zuzugreifen.

Verfügbare Optionen:

- Feedback senden
- Protokolle sammeln
- Konfiguration überprüfen
- App-Daten zurücksetzen
- Hilfe

**Feedback zur Citrix Workspace-App senden** Mit der Option **Feedback senden** können Sie Citrix über Probleme bei der Verwendung der Citrix Workspace-App informieren und Verbesserungsvorschläge für die App einsenden.

Weitere Informationen finden Sie unter [Option “Problembehandlung” zu Taskleiste der Citrix Workspace-App hinzugefügt](#).

**Nachhaltigkeitsinitiative der Citrix Workspace-App** Wenn dieses Feature aktiviert ist, wird eine Aufforderung zum Abmelden von der Desktop-Sitzung angezeigt, sobald ein Benutzer einen virtuellen Desktop schließt. Das Feature kann zur Energieeinsparung beitragen, sofern Windows-Betriebssystemrichtlinien verwendet werden, die VMs herunterfahren, wenn keine Benutzer angemeldet sind.

Weitere Informationen finden Sie unter [Nachhaltigkeitsinitiative der Citrix Workspace-App](#).

**Befehle zum Konfigurieren der Tastaturlayoutsynchronisierung über die Befehlszeilenschnittstelle** Bisher konnten Sie die Tastaturlayoutsynchronisierung nur per GUI oder Aktualisierung der Konfigurationsdatei konfigurieren. Mit diesem Release wurden neue Befehle eingeführt, um die Tastaturlayoutsynchronisierung über die Befehlszeilenschnittstelle zu konfigurieren.

Weitere Informationen finden Sie unter [Tastaturlayoutsynchronisierung mit der Befehlszeilenschnittstelle \(CLI\) konfigurieren](#).

**Befehl zum Bereinigen und Installieren der Citrix Workspace-App** Verwenden Sie den Befehl `/CleanInstall`, um alle nach einer Deinstallation verbleibenden Spuren wie Dateien und Registrierungswerte zu entfernen, und die neue Version der Citrix Workspace-App zu installieren.

Beispiel:

```
1 CitrixWorkspaceApp.exe /CleanInstall
2 <!--NeedCopy-->
```

## Neues zu optimiertem Microsoft Teams

**Angekündigtes EOL für Einzelfenster in Microsoft Teams** Microsoft unterstützt ab 31.01.2024 nur noch den Mehrfenstermodus bei Verwendung von optimiertem Microsoft Teams für VDI. Die Unterstützung der Einzelfenster-Benutzeroberfläche wird eingestellt. Sie müssen eine Version von Citrix Virtual Apps and Desktops und der Citrix Workspace-App verwenden, die den Mehrfenstermodus unterstützt, um bestimmte Funktionen von optimiertem Microsoft Teams weiter nutzen zu können. Weitere Informationen finden Sie unter [Angekündigtes EOL für Einzelfenster in Microsoft Teams](#).

**Angekündigte Einstellung des SDP-Formats (Plan B) von WebRTC** Das aktuelle SDP-Format (Plan B) von WebRTC wird in zukünftigen Versionen nicht mehr von Citrix unterstützt. Sie müssen eine Version der Citrix Workspace-App verwenden, die den Unified Plan unterstützt, um bestimmte Funktionen von optimiertem Microsoft Teams weiter nutzen zu können. Weitere Informationen finden Sie unter [Angekündigte Einstellung des SDP-Formats \(Plan B\) von WebRTC](#).

## App Protection

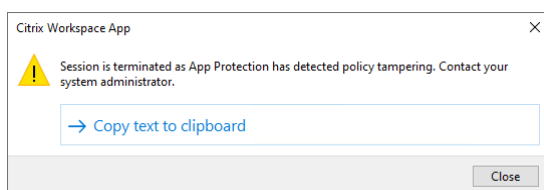
**Wichtiges Update zu Dateinamen** In einem zukünftigen Release der Citrix Workspace-App für Windows werden die folgenden Dateinamen wie folgt aktualisiert:

Alter Dateiname	Neuer Dateiname
EntryProtect.dll	ctxapdotnet.dll
entryprotect.sys	ctxapdriver.sys
epclient32.dll	ctxapclient32.dll
epclient64.dll	ctxapclient64.dll
epinject.sys	ctxapinject.sys
epusbfilter.sys	ctxapusbfilter.sys
entryprotectdrv	ctxapdriver
epinject6	ctxapinject

Diese Dateien werden standardmäßig in %ProgramFiles(x86)%\Citrix\ICA Client installiert.

Wenn Sie einen der obigen Dateinamen zur Positivliste in Ihrer Umgebung hinzugefügt haben, aktualisieren Sie die Positivliste.

**Richtlinienmanipulationen erkennen** 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, und es wird folgende Fehlermeldung angezeigt.



### Hinweis:

Dieses Feature ist erst nach Veröffentlichung der kommenden Version von Citrix Virtual Apps and Desktops verfügbar.



Weitere Informationen zur Erkennung von Richtlinienmanipulationen finden Sie unter [Erkennung von Richtlinienmanipulationen](#).

**Vollständige Desktopfreigabe vom VDA mit Citrix Workspace-App** Bisher war die Desktopfreigabe bei aktiviertem App Protection für optimiertes Microsoft Teams deaktiviert, da App Protection keine Screenshots zulässt.

Ab Version 2309 der Citrix Workspace-App für Windows ist die Desktopfreigabe für optimiertes Microsoft Teams aktiviert, selbst wenn App Protection aktiviert ist.

Weitere Informationen finden Sie unter [Kompatibilität mit der HDX-Optimierung für Microsoft Teams](#).

**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-Features wurden jedoch nicht angewendet.

Eine neue Windows-Gruppenrichtlinie gestattet jetzt das Unterbinden des Öffnens 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**.

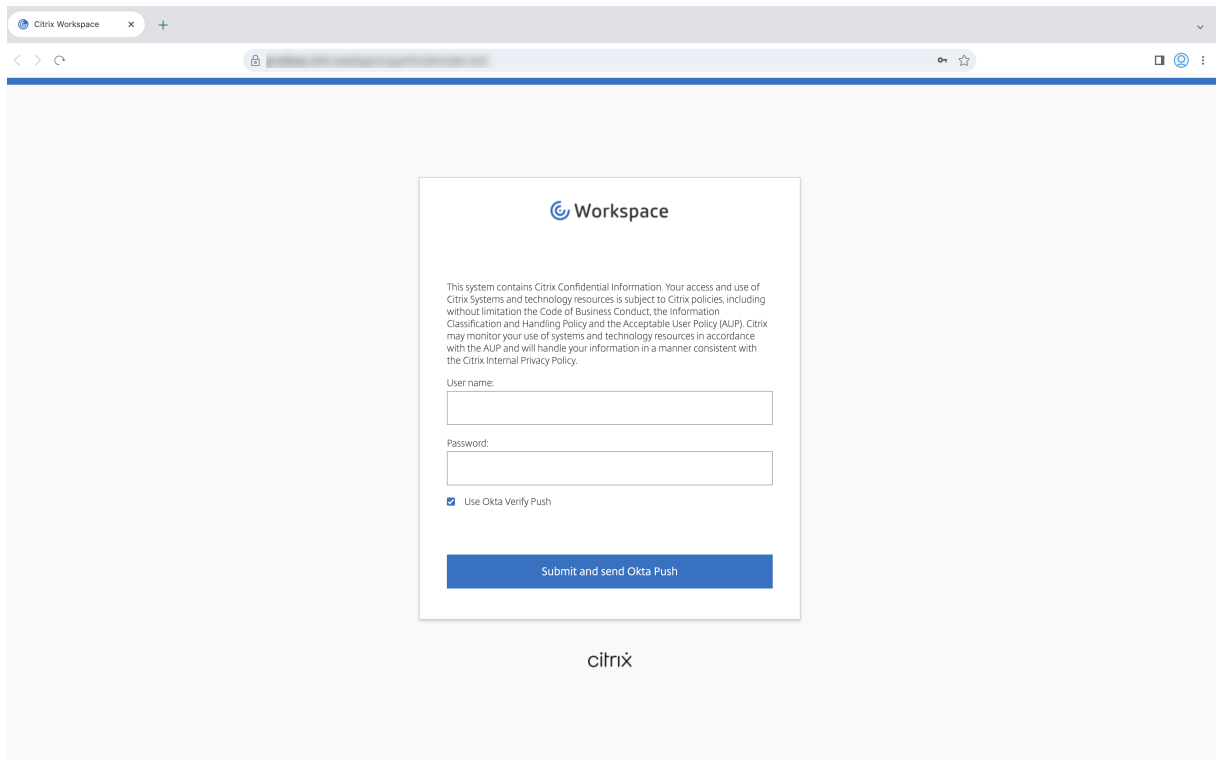
**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 117.1.1.9, der auf Chromium Version 117 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

**Authentifizierung über Citrix Enterprise Browser** Bisher konnten Sie den Enterprise Browser nicht verwenden, wenn das Authentifizierungstoken für die Citrix Workspace-App abgelaufen war. Sie mussten zur Citrix Workspace-App wechseln und sich erneut authentifizieren, um den Enterprise Browser weiterzuverwenden.

Ab Version 2309 der Citrix Workspace-App für Windows (die der Chromium-Version 117.1.1.9 entspricht) können Sie sich im Enterprise Browser selbst authentifizieren, sofern der Store derselbe bleibt. Dadurch erfolgt auch die Authentifizierung für die Citrix Workspace-App. Darüber hinaus bietet das Feature eine nahtlose Anmeldung.

**Hinweis:**

- Das Feature gilt für Workspace-Stores.



### 2307.1

#### Was ist neu

In diesem Release wurden Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

### 2307

#### Was ist neu

#### **Unterstützung für die Wiedergabe kurzer Töne in optimiertem Microsoft Teams hinzugefügt**

Bisher wurden bei aktiviertem sekundären Rufton kurze Signaltöne oder Benachrichtigungen wiederholt wiedergegeben: zum Beispiel der Ton, wenn ein Gast der Microsoft Teams-Besprechung beiträgt. Das Problem ließ sich nur umgehen, indem man Microsoft Teams beendete und neu startete. Dies beeinträchtigte die Benutzererfahrung.

Ab diesem Release unterstützt die Citrix Workspace-App die Wiedergabe der kurzen Töne wie gewünscht. Diese Unterstützung aktiviert auch die sekundäre Ruftonfunktion.

#### **Voraussetzungen:**

Installieren Sie die neueste Version von Microsoft Teams.

**Hinweis:**

Das vorherige Feature ist erst nach Veröffentlichung eines entsprechenden Microsoft Teams-Updates verfügbar. Lesen Sie das Dokumentationsupdate und die Ankündigung in [CTX253754](#).

**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 112.1.1.24, der auf Chromium Version 112 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

**Verknüpfung für Citrix Enterprise Browser** Ab Version 2307 der Citrix Workspace-App für Windows kann ein Administrator konfigurieren und steuern, ob die Citrix Enterprise Browser-Verknüpfung im **Startmenü** angezeigt wird.

**Hinweis:**

Diese Einstellung ist standardmäßig für Workspace-Stores aktiviert.

**Konfiguration** Ein IT-Administrator kann das Vorliegen der Citrix Enterprise Browser-Verknüpfung auf eine der folgenden Arten konfigurieren:

- Gruppenrichtlinienobjekt (GPO)
- Global App Configuration Service (GACS)
- web.config.file.

**Hinweise:**

- Alle Konfigurationsmethoden haben die gleiche Priorität. Aktivieren Sie eine von ihnen, um die Verknüpfung anzuzeigen.
- Wenn Sie die Verknüpfung nicht konfiguriert haben, aber über einen oder mehrere Workspace-Stores verfügen, wird die Verknüpfung automatisch aktiviert.
- Für Endbenutzer wird die Citrix Enterprise Browser-Verknüpfung angezeigt, wenn der Benutzer sie unabhängig von der Konfiguration als bevorzugte App festlegt.
- Um diese Funktion für Workspace-Stores zu deaktivieren, müssen Administratoren eine der folgenden Einstellungen vornehmen:
  - set the **CEBShortcutEnabled** attribute to **false** in the `web.config` file.
  - disable the **Enable Citrix Enterprise Browser shortcut** property in GPO and GACS.

Gruppenrichtlinienobjekt verwenden

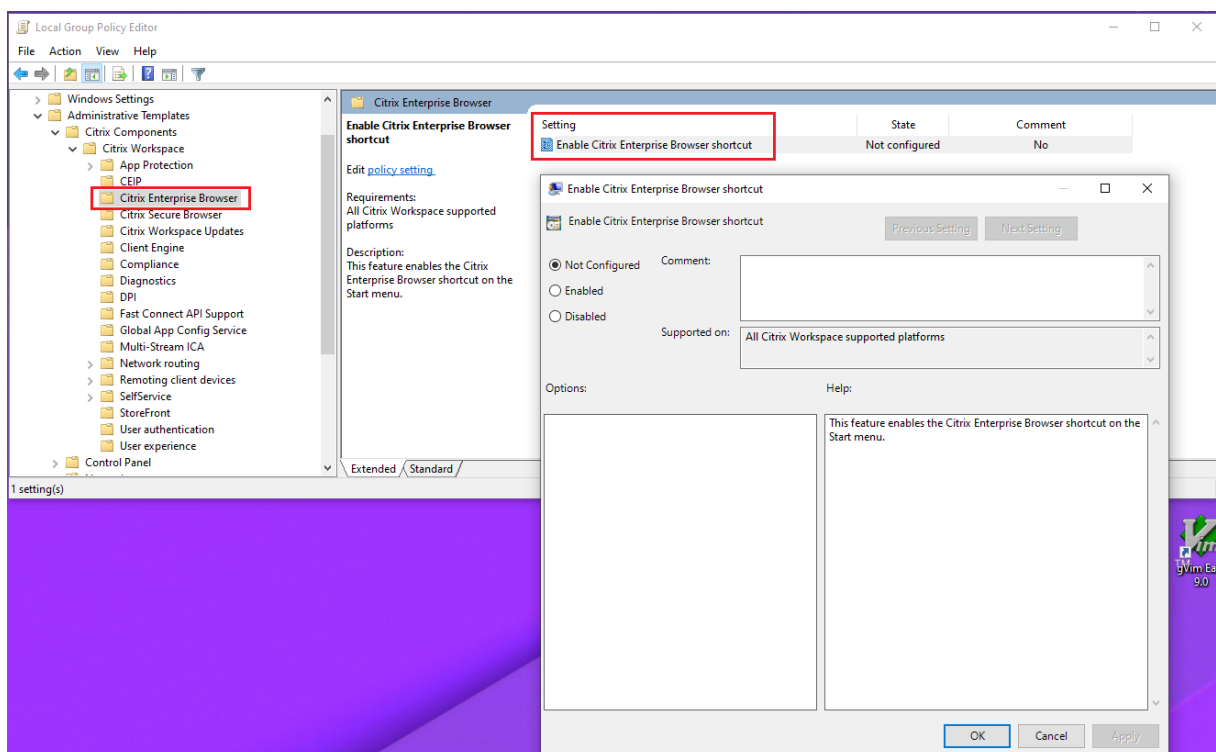
Administratoren können über die Eigenschaft **Citrix Enterprise Browser-Verknüpfung aktivieren** die Anzeige der Citrix Enterprise Browser-Verknüpfung im Startmenü steuern.

**Hinweis:**

Die Konfiguration über das Gruppenrichtlinienobjekt (GPO) ist auf Workspace und StoreFront anwendbar.

Gehen Sie wie folgt vor, um die Citrix Enterprise Browser-Verknüpfung zu aktivieren:

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** > **Citrix Enterprise Browser**.
3. Wählen Sie die Option **Citrix Enterprise Browser-Verknüpfung aktivieren**.



Weitere Informationen zur Verwendung des Gruppenrichtlinienobjekts finden Sie auf der Seite [Administrative Gruppenrichtlinienobjektvorlage](#).

Global App Configuration Service (GACS)

Gehen Sie zu **Workspace-Konfiguration** > **App-Konfiguration** > **Citrix Enterprise Browser** und aktivieren Sie **Citrix Enterprise Browser-Verknüpfung aktivieren**.

Weitere Informationen zur Verwendung der GACS-Benutzeroberfläche finden Sie unter [Benutzeroberfläche](#) in der Dokumentation zu Citrix Enterprise Browser.

**Hinweis:**

Diese Art der Konfiguration gilt für Workspace und StoreFront.

**web.config-Datei:**

Aktivieren Sie das Attribut **CEBShortcutEnabled** unter den Eigenschaften.

```
1 <properties>
2
3     <property name="CEBShortcutEnabled" value="True" />
4
5 </properties>
6 <!--NeedCopy-->
```

**Hinweis:**

Die Konfiguration über `web.config` gilt für StoreFront.

**Verwenden von web.config:**

Gehen Sie wie folgt vor, um die Citrix Enterprise Browser-Verknüpfung zu aktivieren:

1. Öffnen Sie die Datei `web.config` mit einem Texteditor. Die Datei ist normalerweise unter `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Suchen Sie das Benutzerkonto-Element in der Datei (Store ist der Kontoname Ihrer Bereitstellung).  
Beispiel: `<account id=... name="Store">`
3. Navigieren Sie vor dem Tag `</account>` zu den Eigenschaften dieses Benutzerkontos und fügen Sie Folgendes hinzu:

```
1 <properties>
2
3     <property name="CEBShortcutEnabled" value="True" />
4
5 </properties>
6 <!--NeedCopy-->
```

Hier ein Beispiel für die Datei `web.config`:

```
1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6         F84Store"
7         description="" published="true" updaterType="Citrix"
            remoteAccessType="None">
```

```
8     <annotatedServices>
9     <clear />
10    <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
11        <metadata>
12            <plugins>
13                <clear />
14            </plugins>
15            <trustSettings>
16                <clear />
17            </trustSettings>
18            <properties>
19                <property name="CEBShortcutEnabled" value="True
20                    " />
21            </properties>
22        </metadata>
23    </annotatedServiceRecord>
24 </annotatedServices>
25 <metadata>
26     <plugins>
27         <clear />
28     </plugins>
29     <trustSettings>
30         <clear />
31     </trustSettings>
32     <properties>
33         <clear />
34     </properties>
35 </metadata>
36 </account>
37 <!--NeedCopy-->
```

## 2305.1

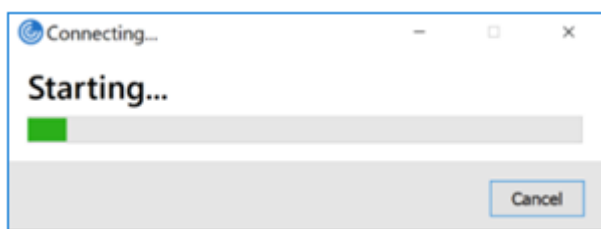
### Was ist neu

#### Verbesserter Start von Virtual Apps and Desktops

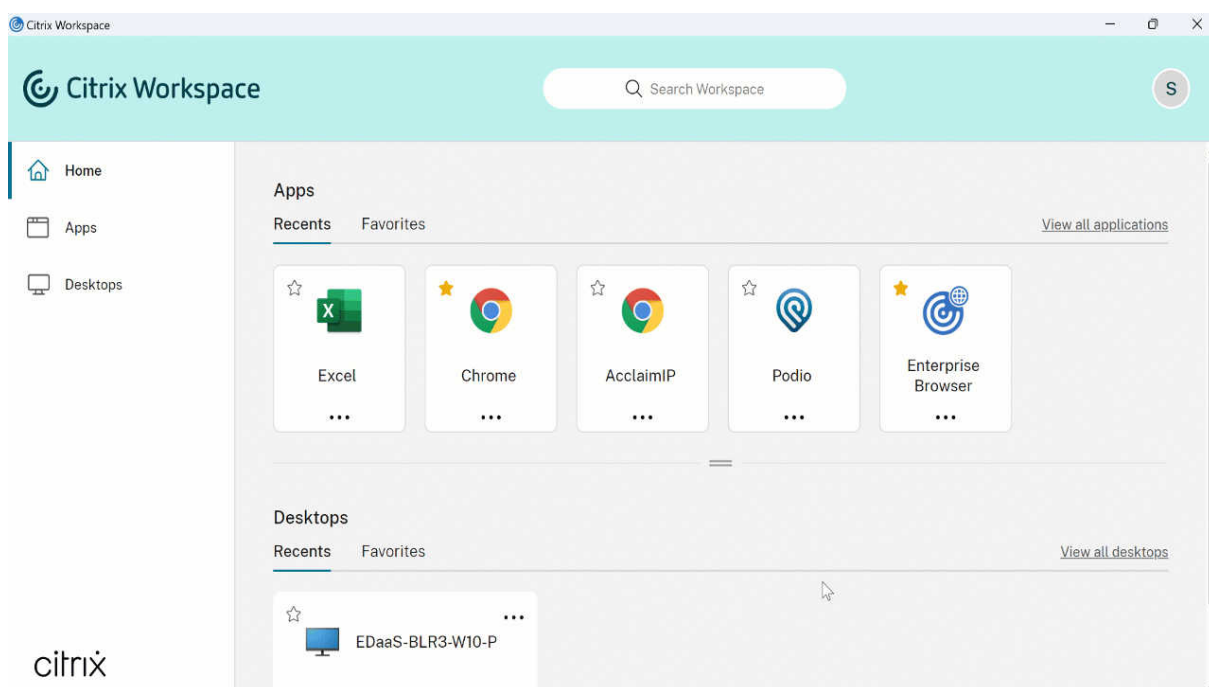
##### Hinweis:

Dieses Feature ist generell für Cloudstores verfügbar und befindet sich in der Technical Preview für On-Premises-Stores.

Bisher war das Dialogfeld zum Startfortschritt nicht sehr intuitiv für Benutzer. Aufgrund statischer Benachrichtigungen nahmen Benutzer an, dass der Startprozess gestoppt wurde, und schlossen das Dialogfeld.



Das verbesserte Startverhalten von Apps und Desktops macht die Citrix Workspace-App für Windows jetzt informativer und benutzerfreundlicher. Durch zeitnahe und relevante Informationen zum Startstatus bleiben Benutzer aktiv und informiert. Die Benachrichtigung wird in der unteren rechten Bildschirmcke angezeigt.



Benutzer erhalten aussagekräftige Benachrichtigungen über den Startfortschritt, anstatt nur ein Wartesymbol zu sehen. Wenn ein Benutzer während eines Startvorgangs versucht, den Browser zu schließen, wird eine Warnmeldung angezeigt.

Ab der Citrix Workspace-App für Windows 2305.1 ist dieses Feature standardmäßig in Cloudstores aktiviert.

Sie können dieses Feature über den Registrierungsschlüssel für die StoreFront-Sitzung (on-premises) aktivieren. Weitere Informationen finden Sie unter [Verbesserter Start von virtuellen Apps und Desktops](#).

**Status des Storebrowse-Befehls verfolgen** Sie können den Ausführungsstatus eines Storebrowse-Befehls in einer Datei verfolgen. Um den Erfolgsstatus zu verfolgen, geben Sie für den Befehl `-f launch` einen eindeutigen Dateinamen an. Dieser Befehl generiert eine Datei mit dem von Ihnen

angegebenen Namen. Der Fehlerstatus ist in der Datei `ica.error` vorhanden, die automatisch erstellt wird.

**Hinweis:**

Stellen Sie sicher, dass Sie dem Dateinamen mit dem Befehl `-f launch` die Erweiterung `.ica` hinzufügen. Andernfalls wird die Datei nicht generiert.

Die Dateien zum Verfolgen von Erfolg und Fehler befinden sich beide in `%LOCALAPPDATA%\citrix\selfservice\cache` und Sie können diese Dateien nach Bedarf überwachen.

Diese Erweiterung ist standardmäßig aktiviert.

Beispiel für die Verwendung des Startbefehls mit Option `-f`:

```
1 -launch -f <uniqueFileName.ica> "launchcommandline"
2 For example:
3 SelfService.exe storebrowse -launch -f uniqueFileName.ica -s store0-5
   c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-
   e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/
   Citrix/Store/resources/v2/
   YTLh0GUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA20TVkZjM5Lk5vdGVwYWQ-/launch/
   ica" -cmdline
4
5 <!--NeedCopy-->
```

**Unterstützung moderner Authentifizierungsmethoden für StoreFront-Stores** Die Citrix Workspace-App 2305.1 für Windows unterstützt moderne Authentifizierungsmethoden für StoreFront-Stores. Nutzen Sie eine der folgenden Methoden zur Authentifizierung bei Citrix StoreFront-Stores:

- Windows Hello und FIDO2-Sicherheitsschlüssel. Weitere Informationen finden Sie unter [Weitere Authentifizierungsmethoden](#).
- Single Sign-On bei Citrix StoreFront-Stores auf in Azure Active Directory (AAD) eingebundenen Maschinen mit AAD als Identitätsanbieter. Weitere Informationen finden Sie unter [Weitere Authentifizierungsmethoden](#).
- Workspace-Administratoren können Richtlinien für den bedingten Zugriff mit Azure Active Directory für Benutzer konfigurieren und erzwingen, die sich bei Citrix StoreFront-Stores authentifizieren. Weitere Informationen finden Sie unter [Unterstützung für bedingten Zugriff mit Azure AD](#).

Um dieses Feature zu aktivieren, müssen Sie Microsoft Edge WebView2 als zugrunde liegenden Browser für die direkte StoreFront- und Gateway-Authentifizierung verwenden.

**Hinweis:**



Achten Sie darauf, dass Sie Microsoft Edge WebView2 Runtime-Version 102 oder höher verwenden.

Mit dem Global App Config Service und der Gruppenrichtlinienobjektvorlage können Sie moderne Authentifizierungsmethoden für StoreFront-Stores aktivieren. Weitere Informationen finden Sie im Abschnitt [Unterstützung moderner Authentifizierungsmethoden für StoreFront-Stores](#).

**Unterstützung für mehr als 200 Gruppen in Azure AD** Ab diesem Release kann ein Azure AD-Benutzer, der Mitglied in mehr als 200 Gruppen ist, ihm zugewiesene Apps und Desktops anzeigen. Bisher konnte er diese Apps und Desktops nicht sehen.

**Hinweis:**

Benutzer müssen sich von der Citrix Workspace-App abmelden und wieder anmelden, um diese Funktion zu aktivieren.

## App Protection

**Verbesserungen beim Keyloggingschutz** Mit dieser Verbesserung 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 Sie 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 Config Service (GACS) 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.

**Wichtiges Update zu Dateinamen** In einem zukünftigen Release der Citrix Workspace-App für Windows werden die folgenden Dateinamen aktualisiert:

- EntryProtect.dll

- entryprotect.sys
- epclient32.dll
- epclient64.dll
- epinject.sys
- epusbfilter.sys
- entryprotectdrv
- epinject6

Diese Dateien sind unter `%ProgramFiles(x86)%\Citrix\ICA Client\` installiert.

Wenn Sie einen dieser Dateinamen zur Positivliste in Ihrer Umgebung hinzugefügt haben, aktualisieren Sie die Positivliste, wenn die neuen Dateinamen angekündigt werden.

**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 105.1.1.27, der auf Chromium Version 105 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

**Unterstützung für Browsererweiterungen** Sie können von Ihrem Administrator zur Verfügung gestellte Erweiterungen sicher dem Citrix Enterprise Browser hinzufügen. Ein Administrator kann die Erweiterungen bereitstellen, verwalten und steuern. Endbenutzer können Erweiterungen in `citrixbrowser://extensions` nach Bedarf anzeigen und verwenden. Informationen zu weitere Einstellungen finden Sie unter [Global App Configuration Service](#).

Weitere Informationen zur Konfiguration finden Sie unter [Unterstützung für Browsererweiterungen](#).

**Änderung der Implementierung von SPA-Richtlinien für interne Web- und SaaS-Apps** Dieses Feature verbessert die Implementierung von Sicherheitsrichtlinien für Web- und SaaS-Apps. Wenn für eine Webseite und für I-Frames innerhalb der Webseite unterschiedliche Richtlinien gelten, gilt jetzt eine strengere Richtlinienimplementierung, bei der eine Einheit aller Richtlinien auf die gesamte Webseite einschließlich I-Frames angewendet wird. Das Wasserzeichen wird jedoch nur auf die Webseite angewendet.

**Citrix Enterprise Browser mit dem Global App Configuration Service verwalten** Der Administrator kann mit dem Global App Configuration Service (GACS) für Citrix Workspace die Citrix Enterprise Browser-Einstellungen zentral bereitstellen.

Global App Configuration Service ermöglicht Administratoren die einfache Konfiguration von Citrix Workspace und die Verwaltung von Citrix Workspace-App-Einstellungen. Mit diesem Feature können

Administratoren über Global App Configuration Service Einstellungen und Systemrichtlinien auf Citrix Enterprise Browser in einem spezifischen Store anwenden. Der Administrator kann jetzt die folgenden Citrix Enterprise Browser-Einstellungen über APIs oder die Verwaltungsoberfläche des GACS konfigurieren und verwalten:

- Enable CEB for all apps: Citrix Enterprise Browser wird als Standardbrowser beim Öffnen von Web- und SaaS-Anwendungen in der Citrix Workspace-App verwendet.
- Enable save passwords: Ermöglicht oder verweigert Endbenutzern die Möglichkeit, Kennwörter zu speichern.
- Enable incognito mode: Aktiviert oder deaktiviert den Inkognitomodus.
- Managed Bookmarks: Ermöglicht Administratoren die Pushbereitstellung von Lesezeichen in Citrix Enterprise Browser.
- Enable developer tools: Aktiviert oder deaktiviert Entwicklertools in Enterprise Browser.
- Delete browsing data on exit: Der Administrator kann vorgeben, welche Daten Citrix Enterprise Browser beim Beenden löscht.
- Extension Install Force list: Der Administrator kann Erweiterungen in Citrix Enterprise Browser installieren.
- Extension Install Allow list: Der Administrator kann eine Liste von Erweiterungen erstellen, die die Benutzer Citrix Enterprise Browser hinzufügen können. Diese Liste verwendet den Chrome Web Store.

Weitere Informationen finden Sie unter [Manage Citrix Enterprise Browser through GACS](#).

#### Hinweise:

- Bei Namen-/Wertpaaren wird zwischen Groß- und Kleinschreibung unterschieden.
- Alle Browsereinstellungen in [Global App Configuration Service](#) sind in den folgenden Kategorien:

```
1 {
2
3     "category": "browser",
4     "userOverride": false,
5     "assignedTo": [
6         "AllUsersNoAuthentication"
7     ]
8 }
9
10
11 <!--NeedCopy-->
```

- Der Administrator kann die Einstellungen auch auf nicht verwaltete Geräte anwenden. Weitere Informationen finden Sie in der Dokumentation zum [Global App Configuration Service](#).

#### Benutzeroberfläche

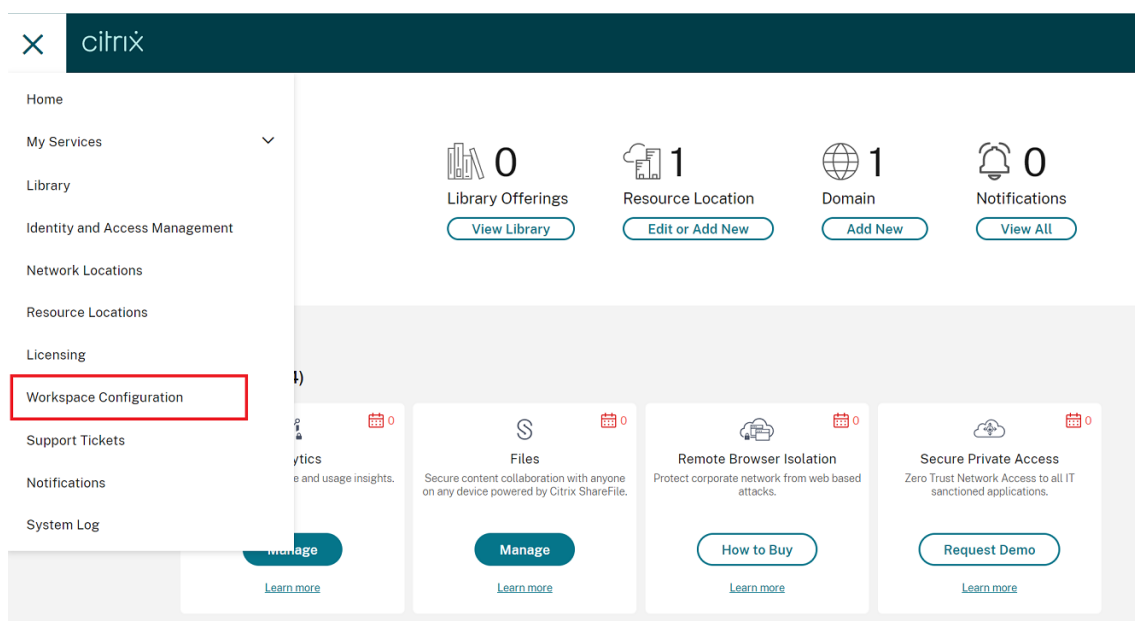
Führen Sie folgende Schritte aus, um den Citrix Enterprise Browser über die Verwaltungsoberfläche des GACS zu konfigurieren:

1. Melden Sie sich mit Ihren Anmeldeinformationen bei [citrix.cloud.com](https://citrix.cloud.com) an.

**Hinweis:**

Im Artikel [Registrierung bei Citrix Cloud](#) finden Sie schrittweise Anleitungen zum Erstellen eines Citrix Cloud-Kontos.

2. Klicken Sie nach der Authentifizierung auf das Menü in der oberen linken Ecke und wählen Sie **Workspacekonfiguration**.



Der Bildschirm **Workspacekonfiguration** wird angezeigt.

3. Klicken Sie auf **App-Konfiguration > Citrix Enterprise Browser**.

Sie können jetzt die Einstellungen für den Citrix Enterprise Browser konfigurieren, ändern und veröffentlichen.

Weitere Informationen finden Sie unter [Manage Citrix Enterprise Browser through GACS](#).

## 2303

### Was ist neu

**Speicherpfad für temporäre Daten für Browserinhaltsumleitungs-Overlay konfigurieren** Ab Version 2303 der Citrix Workspace-App müssen Sie den Pfad des Speichers für temporäre Daten für CEF-basierte Browser (Chromium Embedded Framework) konfigurieren.

Weitere Informationen finden Sie unter [Speicherpfad für temporäre Daten für Browserinhaltsumleitungs-Overlay konfigurieren](#).

**Unterstützung moderner Authentifizierungsmethoden für StoreFront-Stores** Die Citrix Workspace-App 2303 für Windows unterstützt moderne Authentifizierungsmethoden für StoreFront-Stores. Nutzen Sie eine der folgenden Methoden zur Authentifizierung bei Citrix StoreFront-Stores:

- Windows Hello und FIDO2-Sicherheitsschlüssel. Weitere Informationen finden Sie unter [Weitere Authentifizierungsmethoden](#).
- Single Sign-On bei Citrix StoreFront-Stores auf in Azure Active Directory (AAD) eingebundenen Maschinen mit AAD als Identitätsanbieter. Weitere Informationen finden Sie unter [Weitere Authentifizierungsmethoden](#).
- Workspace-Administratoren können Richtlinien für den bedingten Zugriff mit Azure Active Directory für Benutzer konfigurieren und erzwingen, die sich bei Citrix StoreFront-Stores authentifizieren. Weitere Informationen finden Sie unter [Unterstützung für bedingten Zugriff mit Azure AD](#).

Um dieses Feature zu aktivieren, müssen Sie Microsoft Edge WebView2 als zugrunde liegenden Browser für die direkte StoreFront- und Gateway-Authentifizierung verwenden.

**Hinweis:**

Stellen Sie sicher, dass Sie Microsoft Edge WebView2 Runtime-Version 102 oder höher verwenden.

Mit der Gruppenrichtlinienobjektvorlage können Sie moderne Authentifizierungsmethoden für StoreFront-Stores aktivieren. Weitere Informationen finden Sie im Abschnitt [Unterstützung moderner Authentifizierungsmethoden für StoreFront-Stores](#).

**Verbessertes Erlebnis bei optimierten Microsoft Teams-Videokonferenzen** Ab dieser Version ist die Simulcast-Unterstützung standardmäßig für optimierte Microsoft Teams-Videokonferenzen aktiviert. Dadurch werden die Qualität und das Erlebnis bei Videokonferenzen an verschiedenen Endpunkten verbessert, indem die bestgeeignete Auflösung für alle Anrufer gewählt wird.

Dank der Verbesserung kann jeder Benutzer mehrere Videostreams in unterschiedlichen Auflösungen (z. B. 720p, 360p usw.), abhängig von verschiedenen Faktoren wie Endpunktfähigkeit, Netzwerkbedingungen usw. bereitstellen. Der empfangende Endpunkt fordert dann die maximale Auflösung an, die er verarbeiten kann. So ist für jeden Benutzer das optimale Videoerlebnis gewährleistet.

**Hinweis:**

Dieses Feature ist erst nach Veröffentlichung eines Microsoft Teams-Updates verfügbar. Informationen zum voraussichtlichen Releasedatum finden Sie durch Suchen nach der Microsoft

365-Roadmap auf <https://www.microsoft.com/>. Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in [CTX253754](#) Informationen über das Dokumentationsupdate und die Ankündigung.

**Verbesserung von App Protection: DLL-Einschleusungsschutz** App Protection umfasst nun eine Sicherheitsmaßnahme, die die Citrix Workspace-App vor bestimmten nicht autorisierten Dynamic-Link-Bibliotheken (DLL) und nicht vertrauenswürdigen Modulen schützt. Wenn ein solches nicht vertrauenswürdigen Modul eingeschleust wird, erkennt die Citrix Workspace-App den Eingriff und stoppt das Laden des Moduls.

Der DLL-Einschleusungsschutz kann für die folgenden Komponenten aktiviert werden:

- Citrix Authentifizierungsmanager
- Benutzeroberfläche der Citrix Workspace-App
- Citrix Virtual Apps and Desktops

Weitere Informationen finden Sie unter [App Protection](#).

**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.

**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 109.1.1.29, der auf Chromium Version 109 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

**Secure Private Access-Unterstützung für StoreFront** Als Administrator können Sie jetzt Web- und SaaS-Apps in StoreFront mit einer Secure Private Access-Lösung konfigurieren. Nachdem der Administrator die App konfiguriert hat, können Endbenutzer die Web- und SaaS-Apps im Citrix Enterprise Browser mit höherer Sicherheit öffnen.

Weitere Informationen finden Sie unter [Secure Private Access for on-premises](#) in der Dokumentation zu Citrix Secure Private Access.

## 2302

### Was ist neu

**Verbesserte Wiederverbindung für virtuelle Apps und Desktops** Dieses Release bietet eine verbesserte Wiederherstellung von getrennten Verbindungen zu virtuellen Apps und Desktops.

Beim Aktualisieren der getrennten Citrix Workspace-App oder dem Start neuer virtueller Apps oder Desktops innerhalb von Workspace Control durch die Citrix Workspace-App wird folgende Eingabeaufforderung angezeigt:

## Restore session?

You have one or more apps/desktops running from the previous session in Citrix Workspace app. Would you like to restore them?

Remember my preference



Diese Aufforderung wird nur angezeigt, wenn **show reconnection prompt to reconnect sessions** im Global App Configuration Service auf “true” gesetzt ist.

Klicken Sie auf **Wiederherstellen**, um die Verbindung wiederherzustellen und neue und getrennte virtuelle Apps und Desktops zu öffnen. Klicken Sie auf **Abbrechen**, wenn Sie nur neu ausgewählte Apps und Desktops starten möchten.

Wählen Sie **Einstellung speichern**, um die gewählte Einstellung bei der nächsten Anmeldung zu verwenden.

Die zuvor erwähnte neue Eingabeaufforderung **Sitzung wiederherstellen?** erscheint nur, wenn Folgendes gilt:

- Der Benutzer versucht, eine App zu starten, die zu einem Workspace Store gehört,
- für das Feature “Workspace Control” sind keine Administratorrichtlinien oder App-Konfigurationseinstellungen konfiguriert,

- auf dem Client sind die Standardeinstellungen für die Wiederverbindung über Workspace Control festgelegt.

**Hinweis:**

Die Einstellungen unter **Wiederverbindungsoptionen** haben Vorrang vor den Einstellungen, die im Dialogfeld festgelegt sind. Weitere Informationen finden Sie unter [Optionen zum Wiederverbinden über das Dialogfeld "Erweiterte Einstellungen"](#) konfigurieren.

**Client App Management für Zoom-Plug-In** Sie können das Zoom-Plug-In jetzt mit der Funktion "Client App Management" verwalten.

Weitere Informationen finden Sie unter [Client App Management für Zoom-Plug-In](#).

**Aktualisiertes Verhalten bei der Auswahl von Audiogeräten für optimiertes Microsoft Teams**

Ab diesem Release werden Änderungen an den Standardaudiogeräten, die Sie in den Soundeinstellungen auf dem Endpunkt vornehmen, vom optimierten Microsoft Teams im Citrix VDI in der Auswahl der aktuellen Audiogeräte übernommen.

Wenn Sie jedoch in Microsoft Teams ein bestimmtes Gerät auswählen, hat Ihre Auswahl Vorrang und folgt nicht den Standardwerten auf dem Endpunkt. Ihre Auswahl bleibt bestehen, bis Sie den Microsoft Teams-Cache leeren.

**Verbesserung von App Protection** Ab diesem Release ermöglicht Ihnen die Citrix Workspace-App für Windows das Konfigurieren von App Protection mit dem Global App Configuration Service für die Authentifizierung und das Self-Service-Plug-In. Bisher konnten Sie diese Komponenten nur mit dem Gruppenrichtlinienobjekt konfigurieren.

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

**Hinweis:**

Die Konfigurationen im Global App Configuration Service gelten nicht für virtuelle Apps, virtuelle Desktops, Web-Apps und SaaS-Apps. Diese Ressourcen werden weiterhin über den Delivery Controller und Citrix Secure Private Access verwaltet. Weitere Informationen finden Sie unter [Konfigurieren](#) in der Dokumentation zu App Protection.

Weitere Informationen finden Sie im Abschnitt [Verbesserung von App Protection](#).

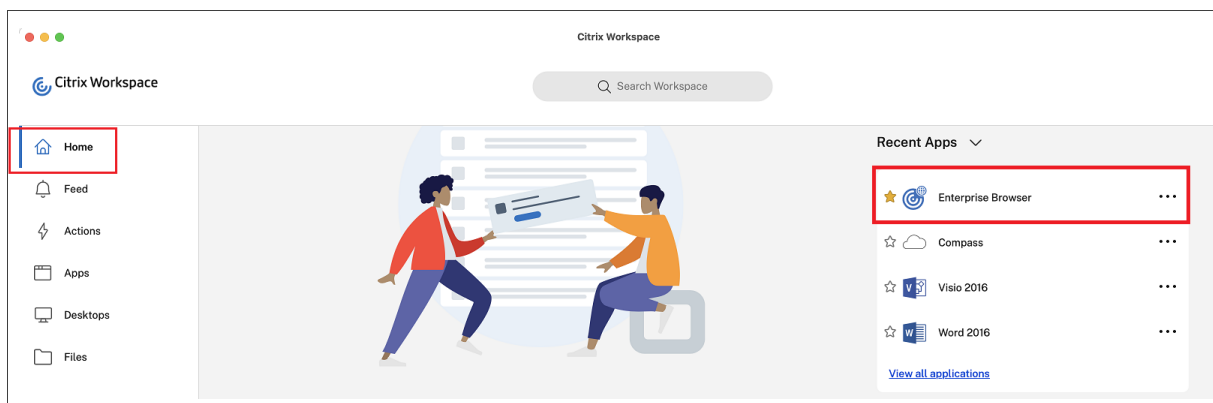
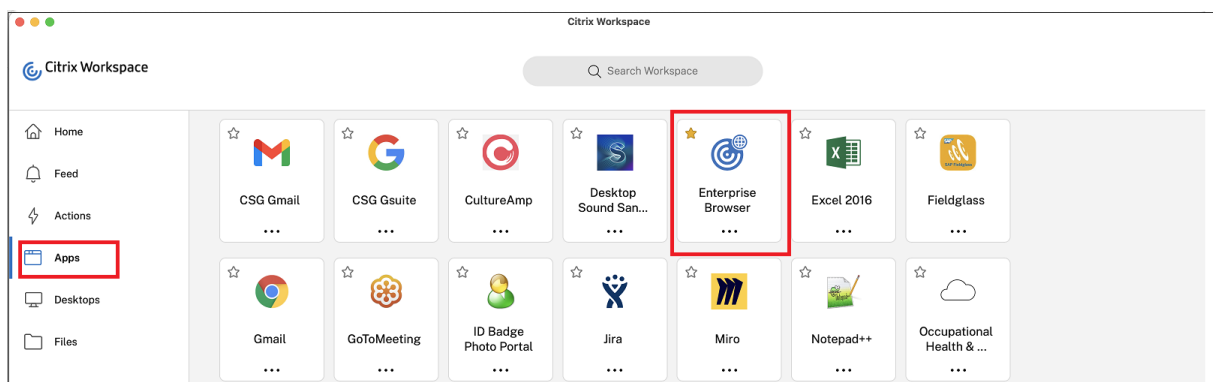
**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 108.1.1.97, der auf Chromium Version 108 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).



**Alle Web- und SaaS-Anwendungen über Citrix Enterprise Browser öffnen** Ab diesem Release des Enterprise Browser (in der Citrix Workspace-App für Windows) werden alle internen Web-Apps und externen SaaS-Apps, die in der Citrix Workspace-App verfügbar sind, in Citrix Enterprise Browser geöffnet.

**Option zum Starten des Citrix Enterprise Browser in der Citrix Workspace-App** Bisher konnten Sie den Citrix Enterprise Browser in der Citrix Workspace-App öffnen, nachdem Sie eine Web- oder SaaS-App geöffnet hatten.

Ab diesem Release können Sie den Citrix Enterprise Browser direkt in der Citrix Workspace-App öffnen, ohne zuvor eine Web- oder SaaS-App zu öffnen. Dieses Feature bietet einfachen Zugriff auf den Citrix Enterprise Browser ohne erforderliche Konfiguration durch Administratoren. Dieses Feature ist standardmäßig verfügbar.



**Hinweis:**

Der Endbenutzer muss durch Secure Private Access über Anspruch auf mindestens eine Web- oder SaaS-App verfügen.

## 2212

### Was ist neu

#### Hinweis:

Ab diesem Release ist Microsoft Edge WebView2 Runtime-Version 102 oder höher erforderlich.  
Weitere Informationen finden Sie unter [Systemanforderungen und Kompatibilität](#).

**Client-App-Verwaltung** Die Citrix Workspace-App 2212 für Windows bietet jetzt Client-App-Verwaltungsfunktionen, mit der die Citrix Workspace-App als einzige Client-App auf dem Endpunkt erforderlich ist, um Agents wie Secure Access Agent und das EPA-Plug-In zu installieren und zu verwalten.

Mit diesen Funktionen können Administratoren erforderliche Agents über eine einzige Verwaltungskonsole mühelos bereitstellen und verwalten.

Weitere Informationen finden Sie unter [Client App Management](#).

**Versionssteuerung für automatische Updates** Administratoren können jetzt angeben, auf welche Version Geräte in der Organisation automatisch aktualisiert werden sollen.

Hierfür legen sie im Global App Config Service in der Eigenschaft "maximumAllowedVersion" die Version fest.

Beispiel für eine JSON-Datei im Global App Config Service:

```
1 {
2
3   "category": "AutoUpdate",
4   "userOverride": false,
5   "assignedTo": [
6     "AllUsersNoAuthentication"
7   ],
8   "settings": [
9     {
10
11       "name": "Auto Update plugins settings",
12       "value": [
13         {
14
15           "pluginSettings": {
16
17             "upgradeToLatest": false,
18             "deploymentMode": "InstallAndUpdate",
19             "stream": "Current",
20             "maximumAllowedVersion": "23.03.0.49",
21             "minimumAllowedVersion": "0.0.0.0",
22             "delayGroup": "Fast"
```

```
23     }
24   ,
25     "pluginName": "WorkspaceApp",
26     "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
27   }
28
29   ]
30 }
31
32 ]
33 }
34
35
36 <!--NeedCopy-->
```

Wenn die Version festgelegt wurde, wird die Citrix Workspace-App auf dem Benutzergerät automatisch auf die Version aktualisiert, die in der Eigenschaft “maximumAllowedVersion” angegeben ist.

**Hinweise:**

- Derzeit sind alle in der vorherigen JSON-Datei genannten Parameter obligatorisch. Für die Einstellung `upgradeToLatest` und die Einstellung `maximumAllowedVersion` müssen Sie Werte gemäß den Anforderungen Ihrer Organisation angeben. Für die übrigen Parameter können Sie Werte verwenden, die der JSON-Beispieldatei ähneln.
- Um die Versionssteuerung für automatische Updates zu aktivieren, muss die Einstellung `upgradeToLatest` im Global App Config Service auf “false” gesetzt sein. Wenn diese Einstellung auf “true” gesetzt ist, wird `maximumAllowedVersion` ignoriert.
- Ändern Sie “pluginId” nicht, da diese ID der Citrix Workspace-App zugeordnet ist.
- Wenn die Version nicht im Global App Config Service konfiguriert ist, wird die Citrix Workspace-App standardmäßig auf die neueste verfügbare Version aktualisiert.

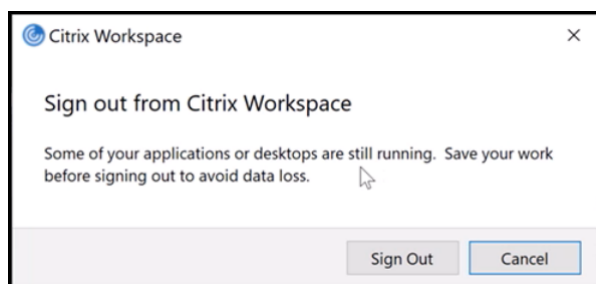
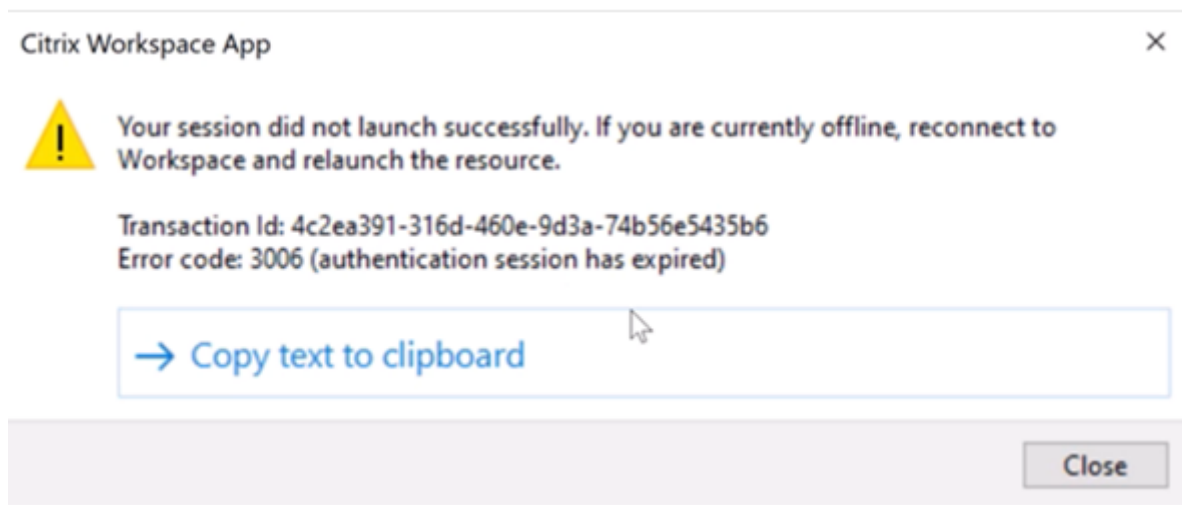
**Anmeldeaufforderung für Verbundidentitätsanbieter erzwingen** Die Citrix Workspace-App berücksichtigt jetzt die Einstellung für “Verbundidentitätsanbietersitzungen”. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX253779](#).

Die Verwendung der Richtlinie “Authentifizierungstoken speichern” ist zum Erzwingen der Anmeldeaufforderung nicht mehr nötig.

**Bessere Wiederverbindung nach Ablauf der Verbindungsleasedatei** Bisher wurde der Endbenutzer nicht benachrichtigt, wenn die Verbindungsleasedatei und das Authentifizierungstoken abliefen.

Ab diesem Release werden eine Fehlermeldung und ein Dialogfeld zur Zustimmung angezeigt. Das Dialogfeld zur Zustimmung wird nur angezeigt, wenn Ressourcen in der Sitzung ausgeführt werden.

Wenn keine Ressourcen ausgeführt werden, wird nur ein Fehlerdialogfeld angezeigt. Sie werden dann ohne Aufforderung zur Zustimmung abgemeldet.



Sie können auf **Abmelden** klicken, um sich von der laufenden Citrix Workspace-App-Sitzung abzumelden, oder auf **Abbrechen**, um mit der Sitzung fortzufahren.

**Hinweis:**

Speichern Sie Ihre Daten, bevor Sie auf **Abmelden** klicken.

**Unterstützung für die standardmäßige Installation von App Protection** App Protection wird jetzt 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.



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

**Hinweis:**

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

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

**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](#).

**Verbesserung von App Protection: Screenshot-Erkennung und Benachrichtigung** Ab diesem Release können Sie eine Benachrichtigung anzeigen, wenn versucht wird, eine geschützte Ressource

per Screenshot zu erfassen. 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 das Tool neu gestartet und die Screenshot-Erfassung erneut versucht wird.

**Desktop Viewer-Optimierung** In diesem Release wurde die Startdauer von Desktop Viewer um 5 Sekunden reduziert. Die **Desktop Viewer**-Symbolleiste wird schnell geöffnet und zeigt möglicherweise den Standardbildschirm für die Windows-Sitzungsanmeldung an. Administratoren können diese Anzeige ausblenden, indem sie über folgenden Registrierungsschlüssel eine Verzögerung in Millisekunden konfigurieren:

- Ort: HKEY\_CURRENT\_USER\SOFTWARE\Citrix\XenDesktop\DesktopViewer
- Name: ExtendConnectScreenMS
- Typ: DWORD
- Wert: 00000000 (Verzögerung in Millisekunden)

**Hinweis:**

Die Registrierungskonfiguration ist optional.

## Citrix Enterprise Browser

**Hinweis:**

Ab Citrix Workspace-App für Windows Version 2210 ist das Feature **Alle Web- und SaaS-Apps über Citrix Enterprise Browser öffnen** deaktiviert.

Dieses Release enthält Citrix Enterprise Browser Version 107.1.1.13, der auf Chromium Version 107 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

- **Citrix Enterprise Browser als Arbeitsbrowser festlegen**

Sie können Citrix Enterprise Browser jetzt als Arbeitsbrowser konfigurieren, um alle Arbeitsslinks zu öffnen. Sie können einen anderen Browser zum Öffnen nicht arbeitsbezogener Links auswählen.

Ein Arbeitslink ist ein den Web- oder SaaS-Apps, die vom Administrator für den Endbenutzer konfiguriert wurden, zugeordneter Link. Wenn ein Benutzer auf einen Link in einer nativen Anwendung klickt und es sich um einen Arbeitslink handelt, wird er im Enterprise Browser geöffnet. Ist es kein Arbeitslink, wird er in dem vom Endbenutzer ausgewählten alternativen Browser geöffnet.

Weitere Informationen finden Sie unter [Festlegen von Citrix Enterprise Browser als Arbeitsbrowser](#).

## 2210.5

### Was ist neu

In diesem Release wurden Probleme behoben, um Leistung, Sicherheit und Stabilität allgemein zu verbessern.

**Verbesserung der automatischen Aktualisierung** Die Citrix Workspace-App unterstützt jetzt automatische Updates, wenn die automatische Proxy-Konfiguration (PAC) und die Erkennung des Webproxy Auto-Discovery Protocol (WPAD) aktiviert sind.

**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 105.2.1.40, der auf Chromium Version 105 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

## 2210

### Was ist neu

**Hintergrundunschärfe für Webcamumleitung** Die Citrix Workspace-App für Windows unterstützt jetzt Hintergrundunschärfe für die Webcamumleitung. Sie können dieses Feature aktivieren, indem Sie **Einstellungen > Verbindungen > Hintergrundunschärfe aktivieren** aktivieren.

**Verbesserung von App Protection für Web- und SaaS-Apps unter Windows 11** Diese Verbesserung von App Protection optimiert die Benutzererfahrung und die Sicherheitsfunktionen für Benutzer von Web- und SaaS-Apps unter Windows 11. Die Verbesserung ist über Citrix Enterprise Browser für Secure Private Access-Kunden verfügbar.

**Videoauflösungen einschränken** Administratoren, die Benutzer auf Clientendpunkten mit niedrigerer Leistung haben, können die eingehenden oder ausgehenden Videoauflösungen einschränken, um die Auswirkung von Codierung und Decodierung von Video auf diesen Endpunkten zu verringern. Ab Citrix Workspace-App 2010 für Windows können Sie diese Auflösungen über die Clientkonfigurationsoptionen einschränken.

**Hinweis:**

Benutzer, die eingeschränkte Auflösungen ausführen, beeinträchtigen die Videoqualität der Konferenz, da der Microsoft Teams-Server gezwungen wird, die niedrigste gemeinsame Auflösung für alle Konferenzteilnehmer zu verwenden.

Mit der Citrix Workspace-App 2210 sind Anrufeinschränkungen auf dem Client standardmäßig deaktiviert. Administratoren müssen die folgenden clientseitigen Konfigurationen unter HKEY\_CURRENT\_USER\SOFTWARE festlegen:

Name	Typ	Erforderlich	Akzeptierte Werte
EnableSimulcast	Ganzzahl	JA	1 - 3 (auf 1 festlegen)
MaxOutgoingResolution	Ganzzahl	JA	180, 240, 360, 540, 720, 1080 (von Microsoft Teams unterstützte Auflösungen)
MaxIncomingResolution	Ganzzahl	JA	180, 240, 360, 540, 720, 1080 (von Microsoft Teams unterstützte Auflösungen)
MaxIncomingStreams	Ganzzahl	JA	1–8
MaxSimulcastLayers	Ganzzahl	JA	1 - 3 (auf 1 festlegen)
MaxVideoFrameRate	Ganzzahl	NEIN	1–30
MaxScreenshareFrameRate	Ganzzahl	NEIN	1–15

Alle Schlüssel sind DWORDs.

**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 105.1.1.27, der auf Chromium Version 105 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).



**Neuer Name für Citrix Workspace Browser** Citrix Workspace Browser heißt jetzt Citrix Enterprise Browser. Das benutzerdefinierte Schema wurde von citrixworkspace:// in citrixbrowser:// geändert.

Die Implementierung dieser Umstellung in unsere Produkte und deren Dokumentation ist ein kontinuierlicher Prozess. Wir danken Ihnen für Ihre Geduld während dieser Umstellung.

- Die Benutzeroberfläche, produktinterne Inhalte sowie Bilder und Anweisungen in der Produktdokumentation werden in den kommenden Wochen aktualisiert.
- Es ist möglich, dass einige Elemente (z. B. Befehle und MSIs) ihre früheren Namen beibehalten, damit vorhandene Kundenskripts auch weiter funktionieren.
- Die zugehörige Produktdokumentation und andere Ressourcen (z. B. Videos und Blogposts), zu denen es Links in dieser Produktdokumentation gibt, verwenden möglicherweise weiterhin die früheren Namen.

**Alle Web- und SaaS-Anwendungen über Citrix Enterprise Browser öffnen** Ab diesem Release werden alle internen Web-Apps und externen SaaS-Apps, die in der Citrix Workspace-App verfügbar sind, in Citrix Enterprise Browser geöffnet.

**Hinweis:**

Ab Citrix Workspace-App für Windows Version 2210 ist das Feature **Alle Web- und SaaS-Apps über Citrix Enterprise Browser öffnen** deaktiviert.

**Unterstützung der automatischen Aktualisierung der Citrix Workspace-App auf dem VDA** Sie können jetzt automatische Updates auf dem VDA aktivieren. Erstellen Sie hierfür den folgenden Registrierungswert:

Auf 32-Bit-Maschinen:

- Registrierungsschlüssel: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- Registrierungswert: AllowAutoUpdateOnVDA
- Registrierungstyp: REG\_SZ
- Registrierungsdaten: True

Auf 64-Bit-Maschinen:

- Registrierungsschlüssel: HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- Registrierungswert: AllowAutoUpdateOnVDA
- Registrierungstyp: REG\_SZ
- Registrierungsdaten: True

**Citrix Enterprise Browser (zuvor “Citrix Workspace Browser”)** Dieses Release enthält Citrix Enterprise Browser Version 103.2.1.10, der auf Chromium Version 103 basiert. Weitere Informationen zu Citrix Enterprise Browser finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

- **Profile in Citrix Enterprise Browser**

Mit Profilen können Sie persönliche Einstellungen wie Verlauf, Lesezeichen und Kennwörter für jedes Citrix Workspace-Konto separat speichern. Das Profil wird basierend auf Ihrem Workspace-Store erstellt und ermöglicht Ihnen eine personalisierte Browsernutzung.

**Hinweis:**

Wenn Sie sich nach dem Upgrade auf Version 103.2.1.10 das erste Mal am Gerät anmelden, werden nur Ihre zuvor gespeicherten Kennwörter entfernt. Wenn Sie sich das erste Mal mit einem anderen Store am Gerät anmelden, gehen alle zuvor gespeicherten Daten verloren.

## 2207

### Was ist neu

**Hintergrundunschärfe und -effekte für Microsoft Teams-Optimierung mit HDX** Die Citrix Workspace-App für Windows unterstützt jetzt Hintergrundunschärfe und -effekte für die Microsoft Teams-Optimierung mit HDX.

Sie können den Hintergrund weichzeichnen oder durch ein benutzerdefiniertes Bild ersetzen, damit zur Vermeidung von Ablenkung die Konzentration auf die Silhouette (Körper und Gesicht) erleichtert wird. Das Feature kann bei persönlichen Anrufen und Telefonkonferenzen verwendet werden.

**Hinweis:**

Dieses Feature ist jetzt in die Benutzeroberfläche und die Schaltflächen von Microsoft Teams integriert. Unterstützung für mehrere Fenster ist eine Voraussetzung, die ein VDA-Update auf 2112 oder höher erfordert. Weitere Informationen finden Sie unter [Meetings und Chat mit mehreren Fenstern](#).

### Einschränkungen:

- Von Administratoren oder Benutzern definierte Hintergrundersetzung wird nicht unterstützt.
- Der Hintergrundeffekt bleibt zwischen den Sitzungen nicht bestehen. Wenn Sie Microsoft Teams schließen und neu starten oder der VDA erneut verbunden wird, wird der Hintergrundeffekt auf “Aus”zurückgesetzt.
- Nachdem die ICA-Sitzung wieder verbunden wurde, ist der Effekt deaktiviert. Die Benutzeroberfläche von Microsoft Teams zeigt jedoch durch ein Häkchen, dass der vorherige Effekt immer noch aktiviert ist. Citrix und Microsoft arbeiten zusammen daran, dieses Problem zu lösen.

- Das Gerät muss mit dem Internet verbunden sein, während das Hintergrundbild ersetzt wird.

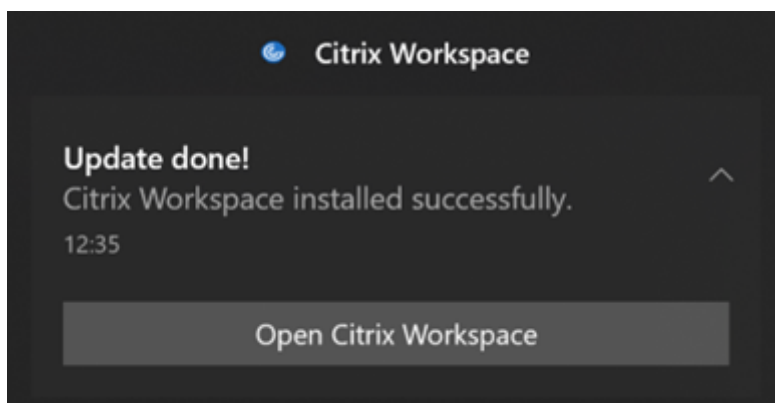
**Hinweis:**

Dieses Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfügbar. Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in im Knowledge Center-Artikel [CTX253754](#) und unter [Microsoft 365-Roadmap](#) Informationen über das Dokumentationsupdate und die Ankündigung.

**Verbesserung der automatischen Updates** Mit dem Feature “Automatische Updates” wird die Citrix Workspace-App automatisch auf die neueste Version aktualisiert, ohne dass ein Benutzereingriff erforderlich ist.

Die Citrix Workspace-App sucht regelmäßig die neueste verfügbare App-Version und lädt sie herunter. Die Citrix Workspace-App ermittelt den besten Zeitpunkt für die Installation basierend auf der Benutzeraktivität, um keine Störungen zu verursachen.

Wenn die Installation abgeschlossen ist, wird die folgende Benachrichtigung angezeigt:



Wenn die Citrix Workspace-App nicht den richtigen Zeitpunkt für die Installation der Updates im Hintergrund findet, wird eine Benachrichtigung angezeigt.

**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 102.1.1.14, der auf Chromium Version 102 basiert.

**Hinweis zum Update der Citrix Workspace-App** Beim Aktualisieren der Citrix Workspace-App für Windows von der vorherigen Version auf 2207 wird der Benutzer aufgefordert, sich anzumelden. Das Anmeldefenster wird nur für den Workspace-Store angezeigt.

## 2206

### Was ist neu

**Verbesserte Grafikleistung** Die Citrix Workspace-App 2206 führt erhebliche Leistungsverbesserungen für integrierte Intel-Grafikprozessoren ein:

- Der Verbrauch des Grafikprozessors wurde reduziert, wodurch die Gesamtleistung verbessert wurde.

Die folgenden Probleme wurden behoben:

- Niedrige Framerate pro Sekunde nach der Wiedergabe eines Videos auf einem Intel-Grafikprozessor der 10. Generation oder höher.
- Helligkeitsunterschied bei Build-To-Lossless oder bei aktiv wechselnden Regionen auf Intel- und AMD-Grafikprozessoren.

**Aktivieren der DPI-Anpassung** Ab der Citrix Workspace-App 2206 für Windows ist die DPI-Anpassung standardmäßig aktiviert. Das bedeutet, dass die Citrix Workspace-App versucht, die Einstellungen der Bildschirmauflösung und DPI-Skala des lokalen Windows-Clients automatisch an die Citrix-Sitzung anzupassen. Im Rahmen dieser Änderung ist die Option “Hohe DPI-Skalierung” unter “Erweiterte Einstellungen” in der Citrix Workspace-App nicht mehr verfügbar. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX460068](#).

**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 101.1.1.12, der auf Chromium Version 101 basiert. Informationen zu Features oder Bugfixes in Citrix Enterprise Browser finden Sie unter [Neue Features](#) in der Dokumentation zu Citrix Enterprise Browser.

## 2205

### Was ist neu

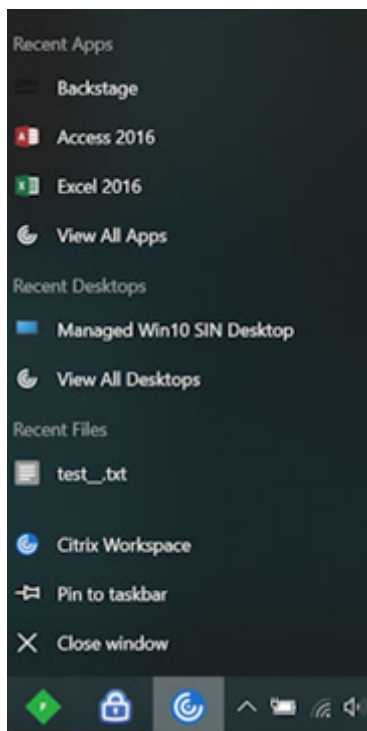
#### Hinweis:

Ab diesem Release ist Microsoft Edge WebView2 Runtime-Version 99 oder höher erforderlich. Weitere Informationen finden Sie unter [Systemanforderungen und Kompatibilität](#).

**Wechsel bei Citrix Casting** Bisher war Citrix Casting bei der Installation der Citrix Workspace-App standardmäßig aktiviert. Ab diesem Release ist Citrix Casting nur dann aktiviert, wenn Sie das Citrix Workspace-App-Installationsprogramm während der Installation mit dem Befehl `/IncludeCitrixCasting` ausführen.

Wenn Sie die Citrix Workspace-App aktualisieren, wird Citrix Casting automatisch aktualisiert. Weitere Informationen zu Citrix Casting finden Sie unter [Citrix Casting](#).

**Schneller Zugriff auf Ressourcen** Ab diesem Release können Sie schnell auf zuletzt verwendete Apps und Desktops zugreifen. Klicken Sie mit der rechten Maustaste auf das Citrix Workspace-Appsymbol in der Taskleiste, um die zuletzt verwendeten Ressourcen im Popup-Menü anzuzeigen und zu öffnen.



### **Abmeldung von benutzerdefinierten Webstores beim Beenden der Citrix Workspace-App**

Wenn das Attribut `signoutCustomWebstoreOnExit` auf "True" festgelegt ist, werden Sie durch Schließen der Citrix Workspace-App von benutzerdefinierten Webstores abgemeldet. Sie können das Attribut `signoutCustomWebstoreOnExit` im **Global App Configuration Service** konfigurieren.

Weitere Informationen finden Sie in der Dokumentation zum [Global App Configuration Service](#).

### **Unterstützung für das Öffnen der Citrix Workspace-App im maximierten Modus**

Ab diesem Release können Sie die Citrix Workspace-App im maximierten Modus öffnen. Anstatt die Citrix Workspace-App jedes Mal manuell zu maximieren, können Sie die Eigenschaft `maximise workspace window` im Global App Configuration Service so festlegen, dass die Citrix Workspace-App standardmäßig im maximierten Modus geöffnet wird.

Weitere Informationen zum Global App Configuration Service finden Sie unter [Erste Schritte](#).

**Storebrowse-Unterstützung für Workspace** Die Citrix Workspace-App für Windows bietet jetzt Storebrowse-Unterstützung für Self-Service, welcher Storebrowse-Benutzern den Zugriff auf Cloud- und Workspace-Features ermöglicht.

**Hinweis:**

- Dieses Feature bietet Storebrowse-Unterstützung nur mit Single Sign-On.
- Die unter [Systemanforderungen und Kompatibilität](#) genannten Voraussetzungen müssen erfüllt sein, damit Benutzer das Feature nutzen können.

Weitere Informationen finden Sie unter [Storebrowse für Workspace](#).

### **Citrix Enterprise Browser**

- Dieses Release enthält Citrix Enterprise Browser Version 99.1.1.8, der auf Chromium Version 99 basiert. Informationen zu Features oder Bugfixes in Citrix Enterprise Browser finden Sie unter [Was ist neu](#) in der Dokumentation zu Citrix Enterprise Browser.
- Die Citrix Workspace-App warnt Sie jetzt beim Schließen aktiver Browserfenster, wenn Sie in der Citrix Workspace-App einen der folgenden Schritte ausführen:
  - Abmelden von einem Store
  - Wechseln zu einem anderen Store
  - Hinzufügen eines neuen Stores
  - Löschen des aktuellen Stores

## **2204.1**

### **Was ist neu**

**Verbesserung der Audioumleitung** Verbesserte Unterstützung der Echounterdrückung für alle Audio-Codecs, einschließlich adaptivem Audio und allen älteren Audio-Codecs.

**Citrix Enterprise Browser** Dieses Release enthält Citrix Enterprise Browser Version 98.1.2.20, der auf Chromium Version 98 basiert. Informationen zu Features oder Bugfixes in Citrix Enterprise Browser finden Sie unter [Was ist neu](#) in der Dokumentation zu Citrix Enterprise Browser.

### **Microsoft Teams-Optimierung**

- **App Protection und Microsoft Teams-Erweiterung:** Microsoft Teams unterstützt eingehende Video- und Bildschirmfreigabe nur, wenn die Citrix Workspace-App für Windows mit aktiviertem App Protection im Desktop Viewer-Modus ist. Im Seamlessmodus veröffentlichte Apps geben keine eingehenden Videos und Bildschirmfreigaben wieder.

## Legacy-Dokumentation

Informationen zu Produktversionen, die das Ende der Lebensdauer erreicht haben, finden Sie in der [Legacy-Dokumentation](#).

## Hinweise zu Drittanbietern

Die Citrix Workspace-App für Windows enthält ggf. Software von Drittanbietern, die gemäß den im folgenden Dokument aufgeführten Bestimmungen lizenziert ist:

[Citrix Workspace-App für Windows –Hinweise zu Drittanbietern](#) (PDF-Download)

## Behobene Probleme

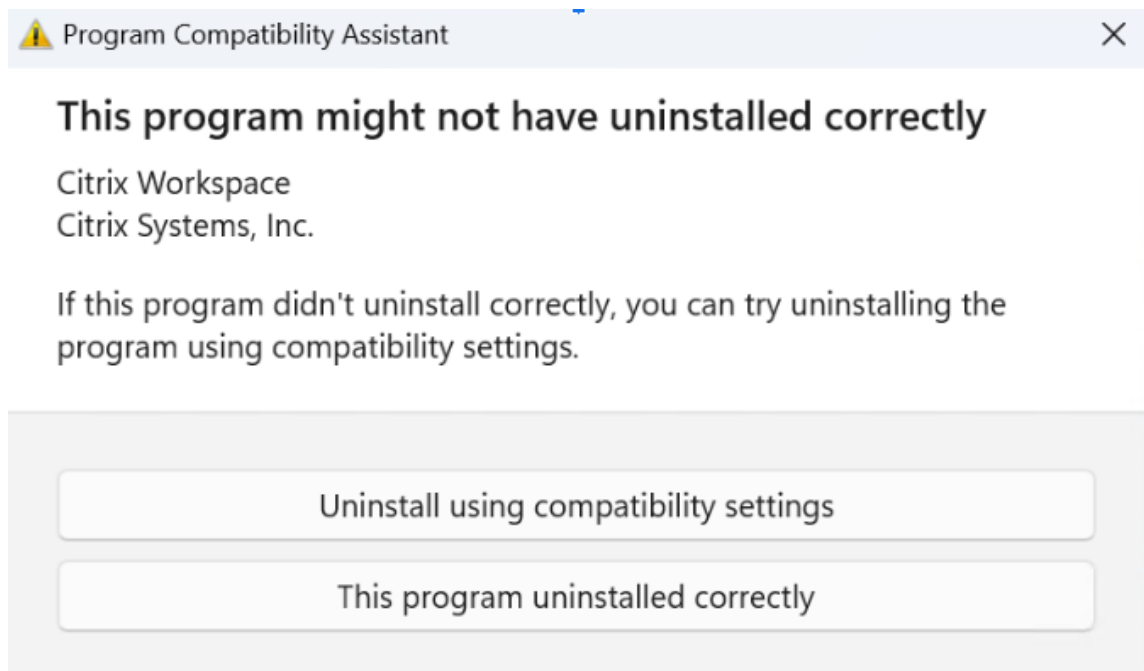
April 22, 2024

### Behobene Probleme in Release 2402 LTSR

- Sie stellen möglicherweise fest, dass auf dem virtuellen Desktop, der im Vollbildmodus geöffnet wird, der Fokus nicht automatisch gesetzt ist. Sie müssen in die Sitzung klicken, um den Fokus wiederzuerlangen. [RFFWIN-32051]
- Beim erneuten Verbinden veröffentlichter Apps wird eine zusätzliche Instanz einer veröffentlichten App geöffnet. [CVADHELP-24485]
- Das Windows Surface-Touchpad und die Softtastatur werden auf dem Anmeldebildschirm der Citrix Workspace-App möglicherweise nicht unterstützt. Dieses Problem tritt auf, wenn Sie sich bei einer Sitzung anmelden, die vom Windows VDA im Vollbildmodus veröffentlicht wurde. Als Workaround öffnen Sie die Sitzung im Fenstermodus und melden Sie sich dann bei der Citrix Workspace-App an. [RFFWIN-32050]
- Zwei Instanzen einer veröffentlichten Anwendung, z. B. app1, werden beobachtet, nachdem app1 getrennt und eine weitere App von demselben VDA aus gestartet wurde. [RFFWIN-32517]
- Für die Version [Windows 10 32bits x86](#) wurde das Kontrollkästchen **Hintergrundunschärfe aktivieren** entfernt, da der Hintergrundunschärfefeffer in dieser Version nicht unterstützt wird. [HDX-60308]
- Das Windows Surface-Touchpad und die Softtastatur werden auf dem Anmeldebildschirm der Citrix Workspace-App möglicherweise nicht unterstützt. Dieses Problem tritt auf, wenn Sie sich bei einer Sitzung anmelden, die vom Windows VDA im Vollbildmodus veröffentlicht wurde. [RFFWIN-32050]

- Der Ton ist möglicherweise beschädigt, wenn mehr als ein Stream gleichzeitig auf derselben Seite abgespielt wird. [HDX-50486]
- Sie erkennen möglicherweise visuelle Artefakte, wenn Sie versuchen, den Bildschirm zu teilen oder den Hauptbildschirm auf der Registerkarte **Monitorlayout** im Bildschirm **Einstellungen** anzupassen. [HDX-59798]
- Windows Media Player (WMP) zeigt einen schwarzen Bildschirm mit aktiviertem Rave auf einem Monitor an, wenn der primäre Monitor nicht der Monitor ganz links ist (wenn mehrere GPUs beteiligt sind). Um dieses Problem zu beheben, wurde der Standard-Renderer von **VMR9** auf **EVR** geändert.  
Wenn Sie **EVR** deaktivieren möchten, erstellen Sie DWORD AllowEvrH264 = 0 unter `Computer \HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream`. [HDX-60494]
- Wenn Sie einen Bildschirm mit Computersound freigeben und mehrere Audioausgabegeräte Ton wiedergeben, kann es vorkommen, dass ein oder mehrere Empfänger Tonartefakte wahrnehmen. [HDX-48213]
- BCR spielt möglicherweise mehrere Audiostreams gleichzeitig statt eines aktiven Streams ab. [HDX-61600]
- Wenn Sie externe Bildschirme verwenden und zu einem einzelnen Bildschirm (z. B. Laptop) wechseln, werden die Menüoptionen, der Text der Benutzeroberfläche und die Dialogfelder der Citrix Workspace-App möglicherweise kleiner als normal angezeigt. [HDX-47575]
- Wenn Sie auf die Version 2402 der Citrix Workspace-App aktualisieren, wird der Befehl `InstallEmbeddedBrowser=N` nicht ausgeführt, wenn der Citrix Enterprise Browser bereits installiert ist. [RFWIN-33169]
- Wenn Sie Mono-Audio für Stereo-Audiostreams verwenden, hören Sie möglicherweise nur einen Audiokanal in einem Ohrhörer, anstatt beide Kanäle auf beiden Ohren zu empfangen. [HDX-56344]
- Bei der Deinstallation der Citrix Workspace-App 2402 LTSR für Windows —Preview-Version über **Systemsteuerung > Programme > Programme und Funktionen** wird das folgende Pop-up angezeigt:





Das Problem tritt zeitweise auf Windows 11-Maschinen auf. Dieses Problem tritt auch nicht bei anderen Deinstallationsmethoden auf, einschließlich der Deinstallation über **Start > Apps > Programme und Funktionen**. Die Deinstallation wurde erfolgreich abgeschlossen, obwohl Sie die vorherige Fehlermeldung erhalten. [RFWIN-32669]

- Der Startvorgang der Citrix Workspace-App wird möglicherweise standardmäßig in veröffentlichten App-Sitzungen ausgeführt. Wenn Sie den Startvorgang in einer veröffentlichten App-Sitzung ausführen möchten, konfigurieren Sie den Registrierungsschlüssel [RunCWAInPublishedAppSessions](#) des Typs `DWORD` in `HKLM/Software/Wow6432Node/Citrix/ICA Client`. [CVADHELP-24070]

## Bekannte Probleme

April 22, 2024

### Bekannte Probleme in Release 2402 LTSR

- In einem Double-Hop-Szenario funktioniert die Taste `ALT + TAB` möglicherweise nicht auf macOS-Clients. [CVADHELP-23085]

## Systemanforderungen und Kompatibilität

April 23, 2024

### Anforderungen

#### Hardwareanforderungen

- Mindestens 2 GB RAM.
- Die folgende Tabelle enthält Informationen zum mindestens erforderlichen Speicherplatz für die Installation der Citrix Workspace-App.

Installationstyp	Erforderlicher Speicherplatz
Neuinstallation	1 GB
Upgrade	1 GB

#### Hinweis:

- Das Installationsprogramm führt die Überprüfung des Speicherplatzes erst aus, wenn Sie das Installationspaket extrahiert haben.
- Wenn bei einer automatischen Installation nicht genug Speicherplatz vorhanden ist, wird das Dialogfeld nicht angezeigt, aber die Fehlermeldung wird im Protokoll `\Citrix\Logs\CTXWorkspaceInstallLogs-*` aufgezeichnet.

#### Softwareanforderungen

- Microsoft Edge WebView2 Runtime-Version 119 oder höher
- .NET Framework 4.8 und .NET Desktop Runtime 6.0.25 oder höher
- Aktuelle Version von Microsoft Visual C++ Redistributable

#### Hinweis:

Um Sicherheitspatches von Microsoft oder anderen Komponenten von Drittanbietern (z. B. .NET Core, .NET Framework, VC Redistributable, Edge Webview) zu verarbeiten, können Sie eine der folgenden Methoden verwenden:

- Aktivieren Sie das automatische Windows-Update auf Clientmaschinen
- IT-Administratoren müssen die Patch-Bereitstellung mit Tools wie SCCM verwalten

### Anforderungen für Microsoft Edge WebView2

- Die Citrix Workspace-App ist in der [Evergreen Bootstrapper](#)-Version von Microsoft Edge WebView2 Runtime enthalten.
- Das Citrix Workspace-App-Installationsprogramm kann Microsoft Edge WebView2 Runtime während der Installation der Citrix Workspace-App installieren. Für diese Installation müssen Sie jedoch mit dem Internet verbunden sein. Alternativ können Sie zunächst das geeignete Offline-Paket von [Microsoft Edge WebView2 Runtime Evergreen Standalone Installer](#) installieren, bevor Sie die Citrix Workspace-App installieren.
- Das Gerät muss Zugriff auf die folgenden URLs haben:
  - [https://\\*.dl.delivery.mp.microsoft.com](https://*.dl.delivery.mp.microsoft.com) zum Download von Microsoft Edge WebView2 Runtime während der Installation der Citrix Workspace-App. Weitere Informationen finden Sie unter [Allow list for Microsoft Edge endpoints](#).
  - <https://msedge.api.cdp.microsoft.com> zur Suche nach einem Microsoft Edge WebView2 Runtime Update
  - Internetverbindung
  - Das Gerät muss Zugriff auf die folgenden URLs haben:

#### Hinweis:

Wenn Sie die Citrix Workspace-App als Nicht-Administrator installieren oder aktualisieren und Microsoft Edge WebView2 Runtime nicht vorhanden ist, wird die Installation mit der folgenden Meldung unterbrochen: “Sie müssen als Administrator angemeldet sein, um die folgenden Voraussetzungspakete installieren zu können: Edge Webview 2 Runtime”.

### .NET-Anforderungen

#### Voraussetzungen

- .NET Framework 4.8 und x86 Version von .NET Desktop Runtime 6.0.25 oder höher. Sie müssen die x86-Version auch auf x64-Systemen installieren.
- Falls Sie .NET zusammen mit der Citrix Workspace-App installieren, stellen Sie sicher, dass eine Internetverbindung besteht.
- Administratorprivilegien

**Hinweis:**

Die Installation schlägt fehl, wenn Sie versuchen, die Citrix Workspace-App ohne Administratorrechte zu installieren oder zu aktualisieren und .NET Framework 4.8 oder höher und .NET Desktop Runtime 6.0.25 oder höher nicht auf dem System vorhanden sind.

**Installationsmethoden**

---

.NET-Version	Bereitstellungsmethode
Die Citrix Workspace-App ab 1904 erfordert .NET Framework Version 4.8. Neben .NET Framework 4.8 benötigt die Citrix Workspace-App ab 2309 die x86-Version von .NET Desktop Runtime 6.0.25 oder höher für x86- und x64-Systeme.	<p>Methode 1: .NET Framework 4.8 und die neueste Version von .NET Desktop Runtime 6.0 werden zusammen mit der Citrix Workspace-App installiert. Diese Installation erfordert als Online-Installation eine Internetverbindung. Das Gerät muss Zugriff auf die Domäne-URL <a href="https://downloadplugins.citrix.com">downloadplugins.citrix.com</a> haben.</p> <p>Methode 2: Für Geräte ohne Internetverbindung können Administratoren ein Offline-Installationsprogramm für die Citrix Workspace-App von der <a href="#">Downloadseite</a> herunterladen. Der Administrator kann diese Anforderungen auch über eine Bereitstellungsmethode wie z. B. SCCM installieren.</p> <p>Methode 3: Administratoren können <a href="#">.NET Framework 4.8</a> und <a href="#">.NET Desktop Runtime 6.0.25</a> separat von der Microsoft-Website installieren, bevor sie die Citrix Workspace-App installieren. Es wird empfohlen, die neueste Version von .NET Desktop Runtime 6.0 (6.0.25 oder höher) herunterzuladen.</p>

---

**Anforderungen für Microsoft Visual C++ Redistributable** Die Citrix Workspace-App erfordert die aktuelle Version von Microsoft Visual C++ Redistributable.

**Hinweis:**

Citrix empfiehlt, die neueste Version von Microsoft Visual C++ Redistributable zu verwenden. Andernfalls wird während eines Upgrades möglicherweise eine Aufforderung zum Neustart

angezeigt.

Ab Version 1904 wird das Installationsprogramm für Microsoft Visual C++ Redistributable nicht mit dem Citrix Workspace-App-Installationsprogramm verpackt. Während der Installation der Citrix Workspace-App überprüft das Installationsprogramm, ob das Microsoft Visual C++ Redistributable-Paket auf dem System vorhanden ist und installiert es gegebenenfalls.

**Hinweis:**

Wenn das Microsoft Visual C++ Redistributable-Paket auf Ihrem System nicht vorhanden ist, schlägt die Installation der Citrix Workspace-App als Nicht-Administrator möglicherweise fehl.

Nur ein Administrator kann das Microsoft Visual C++ Redistributable-Paket installieren.

Informationen zur Behebung von Problemen mit der Installation von .NET Framework oder Microsoft Visual C++ Redistributable finden Sie im Citrix Knowledge Center-Artikel [CTX250044](#).

## Konnektivitätsanforderungen

**Featureflags verwalten** Wenn ein Problem mit der Citrix Workspace-App in der Produktion auftritt, verwenden Sie Feature-Flags und den Drittanbieterdienst LaunchDarkly, um ein betroffenes Feature dynamisch in der Citrix Workspace-App deaktivieren, auch nachdem das Feature bereitgestellt wurde.

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.

Sie können den Datenverkehr für folgende URLs zulassen:

- [events.launchdarkly.com](#)
- [stream.launchdarkly.com](#)
- [clientstream.launchdarkly.com](#)
- [Firehose.launchdarkly.com](#)
- [mobile.launchdarkly.com](#)

Wenn Sie IP-Adressen in einer Positivliste auflisten müssen, konsultieren Sie die Liste der aktuellen IP-Adressbereiche unter [Liste öffentlicher IP-Adressen von LaunchDarkly](#). Mit dieser Liste können Sie sicherstellen, dass Ihre Firewallkonfigurationen automatisch anhand der Infrastrukturupdates aktualisiert werden. Einzelheiten zum Status der Änderungen der Infrastruktur finden Sie auf der [Statusseite von LaunchDarkly](#).

**LaunchDarkly-Systemanforderungen** Überprüfen Sie, ob die Apps mit den folgenden Diensten kommunizieren können, wenn Sie Split-Tunneling in Citrix ADC für die folgenden Dienste auf **OFF** festgelegt haben:

- LaunchDarkly-Dienst.
- APNs-Listenerdienst

**Deaktivieren des LaunchDarkly-Diensts** Sie können den LaunchDarkly-Dienst mit einer Gruppenrichtlinienobjektrichtlinie (GPO-Richtlinie) deaktivieren.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Compliance**.
3. Wählen Sie die Richtlinie **Senden von Daten an Dritte deaktivieren** und legen Sie sie auf "Aktiviert" fest.
4. Klicken Sie auf **Anwenden** und auf **OK**.

## Ports

Informationen zu den erforderlichen Ports finden Sie unter [Gebräuchliche Ports für die Citrix Kommunikation](#).

## Kompatibilitätsmatrix

Die Citrix Workspace-App ist auch kompatibel mit allen derzeit unterstützten Versionen von Citrix Virtual Apps and Desktops, Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) und Citrix Gateway, die in der [Citrix Product Lifecycle Matrix](#) aufgeführt sind.

### Hinweis:

- Das Citrix Gateway Plug-In für die Endpunktanalyse (EPA) wird für Citrix Workspace unterstützt. In der nativen Citrix Workspace-App wird es nur unterstützt, wenn die nFactor-Authentifizierung verwendet wird. Weitere Informationen finden Sie unter [Konfigurieren des EPA-Scans für die Vor- und Nachauthentifizierung als Faktor in der Multifaktorauthentifizierung \(nFactor\)](#) in der Dokumentation zu Citrix ADC.
- Die Installation der Citrix Workspace-App unter Windows wird nur unterstützt, wenn die Kunden regulären oder erweiterten Support von Microsoft haben.
- Die Citrix Workspace-App für Windows wird unter Windows ARM64 nur im Emulatormodus unterstützt.

- Sobald eine Windows 10-Version ihr Dienstende erreicht, wird sie von Microsoft nicht länger unterstützt. Citrix unterstützt die eigene Software nur für Betriebssysteme, die vom Hersteller unterstützt werden. Weitere Informationen zum Dienstende von Windows 10-Versionen finden Sie im [Informationsblatt zum Lebenszyklus von Windows](#).

Die Citrix Workspace-App für Windows ist mit folgenden Windows-Betriebssystemen kompatibel:

---

### **Betriebssystem**

---

Windows 11

Windows 10 (32-Bit- und 64-Bit-Editionen) Weitere Informationen zu kompatiblen Windows 10-Versionen finden Sie unter [Kompatibilität von Windows 10 mit der Citrix Workspace-App für Windows](#).

Windows 10 Enterprise (2016 LTSC 1607, LTSC 2019)

Windows 10 (Home Edition\*, Pro)

Windows Server 2022

Windows Server 2019

Windows Server 2016

---

\*Keine Unterstützung für Domänen-Passthrough-Authentifizierung, Desktop Lock, FastConnect API und Konfigurationen, die in Domänen eingebundene Windows-Maschinen erfordern.

### **Kompatibilität von Windows 10 oder 11 mit der Citrix Workspace-App für Windows**

In der folgenden Tabelle sind die Windows 10-Versionsnummern und die entsprechenden kompatiblen Releases der Citrix Workspace-App für Windows aufgeführt.

---

Windows 10-Versionsnummer	Buildnummer	Version der Citrix Workspace-App
22H2	19045	2206 und höher
21H2	19044	2112.1 und später
21H1	19043.928	2106 und höher
20H2	19042.508	2012 und höher
2004	19041.113	2006.1 und höher
1909	18363.418	1911 und höher

---

Windows 10-Versionsnummer	Buildnummer	Version der Citrix Workspace-App
1903	18362.116	1909 und höher
1809	17763.107	1812 und höher
1803	17134.376	1808 und höher

**Hinweis:**

Windows 10-Versionen sind nur mit den aufgeführten Versionen der Citrix Workspace-App kompatibel. Beispielsweise ist Windows 10 Version 21H1 nicht mit der Version vor 2106 kompatibel.

In der folgenden Tabelle sind die Windows 11-Versionsnummern und die entsprechenden kompatiblen Releases der Citrix Workspace-App für Windows aufgeführt.

Windows 11-Versionsnummer	Buildnummer	Version der Citrix Workspace-App
23H2	22631	2311 und höher
22H2	22621	2209 und höher
21H2	22000	2109.1 und höher

## Installation und Deinstallation

April 22, 2024

Sie können die Citrix Workspace-App von der Citrix [Downloadseite](#) oder der Downloadseite Ihres Unternehmens (falls verfügbar) herunterladen.

Sie können das Paket wie folgt installieren:

- Ausführen eines interaktiven Windows-Installationsassistenten.

Oder

- Eingeben des Dateinamens des Installationsprogramms, der Installationsbefehle und der Installationseigenschaften über die Befehlszeilenschnittstelle. Informationen zum Installieren der Citrix Workspace-App über die Befehlszeilenschnittstelle finden Sie unter [Verwenden von Befehlszeilenparametern](#).



**Hinweis:**

Stellen Sie sicher, dass Sie alle erforderlichen Systemanforderungen installiert haben, wie im Abschnitt [Systemanforderungen](#) beschrieben.

**Installation mit Administrator- und Nicht-Administrator-Rechten:**

Benutzer und Administratoren können die Citrix Workspace-App installieren. Sie benötigen nur dann Administratorrechte, wenn Sie die [Passthrough-Authentifizierung](#), [Single Sign-On](#), [App Protection](#) und [Citrix Ready Workspace Hub](#) mit der Citrix Workspace-App für Windows verwenden.

Die folgende Tabelle zeigt die Unterschiede bei der Installation der Citrix Workspace-App als Administrator oder als Benutzer:

	Installationsordner	Installationstyp
Administrator	64-Bit: C:\Program Files (x86)\Citrix\ICA Client; 32-Bit: C:\Program Files\Citrix\ICA Client	Installation pro System
Benutzer	%USERPROFILE%\AppData\Local\Citrix\ICA Client	Installation pro Benutzer

**Hinweis:**

Administratoren können die vom Benutzer installierte Instanz der Citrix Workspace-App überschreiben und die Installation erfolgreich fortsetzen.

**Befehl zum Bereinigen und Installieren der Citrix Workspace-App**

Verwenden Sie den Befehl `/CleanInstall`, um alle nach einer Deinstallation verbleibenden Spuren wie Dateien und Registrierungswerte zu entfernen, und die neue Version der Citrix Workspace-App zu installieren.

Beispiel:

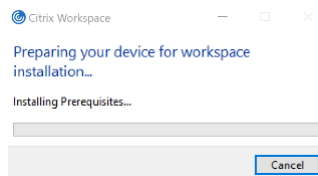
```
1 CitrixWorkspaceApp.exe /CleanInstall
2 <!--NeedCopy-->
```

**Installation über die Benutzeroberfläche**

Sie können die Citrix Workspace-App für Windows manuell installieren, indem Sie das Installationspaket **CitrixWorkspaceApp.exe** ausführen:

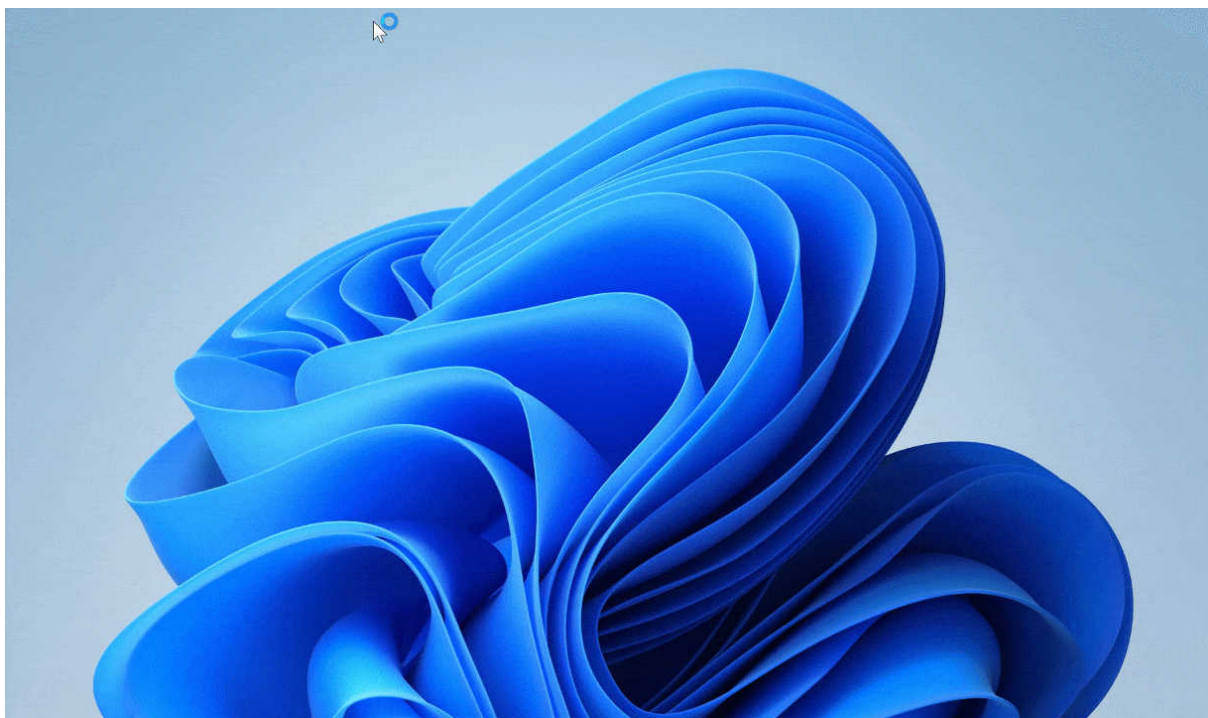
1. Starten Sie die Datei `CitrixWorkspaceApp.exe`.

Das System überprüft die Voraussetzungen für die Citrix Workspace-App und installiert sie bei Bedarf automatisch.



Nach der Installation der Voraussetzungen wird die **Begrüßung zum Citrix Workspace-Installationsprogramm** angezeigt.

2. Klicken Sie auf **Weiter**. Die Seite mit dem **Citrix Lizenzvertrag** wird angezeigt.
3. Lesen und akzeptieren Sie die Citrix Lizenzvereinbarung und fahren Sie mit der Installation fort. Die Installation der Citrix Workspace-App wird fortgesetzt und erfolgreich abgeschlossen.
4. Aktivieren Sie bei einer Installation mit Administratorrechten das Kontrollkästchen **App Protection nach der Installation starten**, falls das Feature App Protection aktiviert werden soll. Die Installation der Citrix Workspace-App wird fortgesetzt und erfolgreich abgeschlossen.

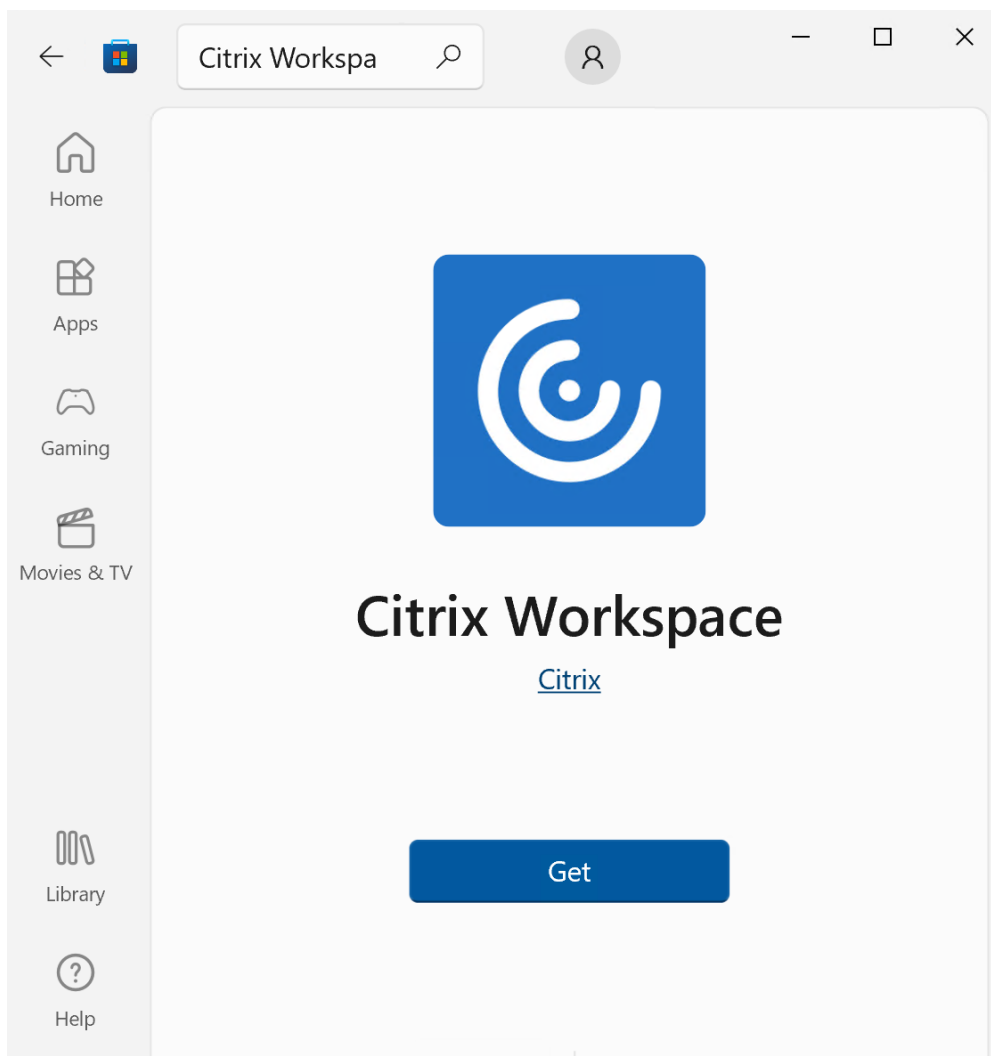


**Wichtig:**

TrolleyExpress wird durch `CWAIInstaller-<date and timestamp>` ersetzt. Das Protokoll wird beispielsweise unter `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441` aufgezeichnet.

## Windows Store verwenden

1. Gehen Sie zum Microsoft Store.
2. Suchen Sie nach Citrix Workspace.



1. Klicken Sie auf **Get**. Die Citrix Workspace-App ist installiert.

## Befehlszeileninstallation

Sie können das Installationsprogramm für die Citrix Workspace-App durch Festlegen verschiedener Befehlszeilenoptionen anpassen. Das Installationspaket wird vor dem Start des Setupprogramms automatisch im Temp-Verzeichnis des Betriebssystems extrahiert. Der benötigte Speicherplatz berücksichtigt Programmdateien, Benutzerdaten und Temp-Verzeichnisse nach dem Start mehrerer Anwendungen.

Um die Citrix Workspace-App über die Windows-Befehlszeile zu installieren, starten Sie die Eingabeaufforderung und geben dann Folgendes auf einer einzigen Zeile ein:

- Name der Installationsdatei,
- Installationsbefehle und
- Installationseigenschaften.

Die verfügbaren Installationsbefehle und -eigenschaften lauten wie folgt:

```
CitrixWorkspaceApp.exe [commands] [properties]
```

### Liste der Befehlszeilenparameter

Die Parameter werden wie folgt klassifiziert:

- [Allgemeine Parameter](#)
- [Update-Parameter](#)
- [Installationsparameter](#)
- [HDX-Parameter](#)
- [Parameter für Einstellungen und Benutzeroberfläche](#)
- [Authentifizierungsparameter](#)

### Allgemeine Parameter

---

Befehl	Beschreibung
? Oderhelp	Listet alle Installationsbefehle und -eigenschaften auf.
/silent	Deaktiviert Installationsdialogfelder und Eingabeaufforderungen während der Installation.
noreboot	Unterdrückt die Aufforderungen zum Neustart während der Installation. Wenn Sie die Neustartaufforderung unterdrücken, werden USB-Geräte, die im ausgesetzten Zustand sind, nicht erkannt. Die USB-Geräte werden erst nach dem Neustart des Geräts aktiviert.

Befehl	Beschreibung
<code>/forceinstall</code>	Dieser Switch ist wirksam, wenn vorhandene Konfigurationen oder Einträge der Citrix Workspace-App bereinigt werden. Verwenden Sie diesen Switch, wenn Sie ein Upgrade von einer nicht unterstützten Version der Citrix Workspace-App durchführen oder wenn die Installation oder das Upgrade fehlschlägt.

**Hinweis:**

Der Switch `forceinstall` ersetzt den Switch `rcu`. Die Befehlszeilenoption `rcu` ist ab Version 1909 veraltet. Weitere Informationen finden Sie unter [Einstellung von Features und Plattformen](#).

**Parameter für automatisches Update****Verfügbares Update erkennen**

- Befehl: `AutoUpdateCheck`
- Beschreibung: Dieser Befehl gibt an, dass die Citrix Workspace für Windows erkennt, wenn ein Update verfügbar ist.

Zulässige Werte:

Werte für AutoUpdateCheck	Beschreibung	Beispiel
Auto (Standard)	Sie werden benachrichtigt, wenn ein Update verfügbar ist.	<code>CitrixWorkspaceApp.exe AutoUpdateCheck=auto.</code>
Manual	Sie werden nicht benachrichtigt, wenn ein Update verfügbar ist. Suchen Sie manuell nach Updates.	<code>CitrixWorkspaceApp.exe AutoUpdateCheck&gt;manual</code>
Deaktiviert	Deaktiviert automatische Updates.	<code>CitrixWorkspaceApp.exe AutoUpdateCheck=disabled.</code>

**Hinweis:**

`AutoUpdateCheck` ist ein obligatorischer Parameter, den Sie festlegen müssen, um andere Parameter wie `AutoUpdateStream`, `DeferUpdateCount` und `AURolloutPriority` zu konfigurieren.

**Updateversion auswählen**

- Befehl `AutoUpdateStream`
- Beschreibung: Wenn Sie die automatische Aktualisierung aktiviert haben, können Sie auswählen, welche Version Sie aktualisieren möchten. Weitere Informationen finden Sie unter [Lifecycle Milestones](#).

Zulässige Werte:

Werte für <code>AutoUpdateStream</code>	Beschreibung	Beispiel
LTSR	Die automatische Aktualisierung auf des Long Term Service Release erfolgt nur kumulativ.	<code>CitrixWorkspaceApp.exe AutoUpdateStream=LTSR</code> .
Current	Die automatische Aktualisierung erfolgt auf die neueste Version der Citrix Workspace-App.	<code>CitrixWorkspaceApp.exe AutoUpdateStream=Current</code>

**Benachrichtigungen über Update ignorieren**

- Befehl: `DeferUpdateCount`
- Beschreibung: Gibt an, wie oft Sie Benachrichtigungen für ein verfügbares Update ignorieren können. Weitere Informationen finden Sie unter [Citrix Workspace-Updates](#).

Zulässige Werte:

DeferUpdateCount-Werte	Beschreibung	Beispiel
-1(Standardwert)	Ermöglicht beliebig oft das Ignorieren von Benachrichtigungen.	<code>CitrixWorkspaceApp.exe DeferUpdateCount=-1</code>

DeferUpdateCount-Werte	Beschreibung	Beispiel
0	Gibt an, dass Sie pro verfügbares Update nur eine Benachrichtigung erhalten. Sie werden nicht erneut an das Update erinnert.	<code>CitrixWorkspaceApp.exe DeferUpdateCount =0</code>
Beliebige andere Zahl "n"	Ermöglicht n-mal das Ignorieren von Benachrichtigungen. Die Option <b>Später erinnern</b> wird gemäß der festgelegten Zahl "n" angezeigt.	<code>CitrixWorkspaceApp.exe DeferUpdateCount =&lt;n&gt;</code>

**Hinweis:**

Ab Version 2207 der Citrix Workspace-App für Windows ist das Feature für automatische Updates verbessert und der Parameter `DeferUpdateCount` gilt nicht mehr.

**Rolloutpriorität festlegen**

- Befehl: `AURolloutPriority`
- Beschreibung: Wenn eine neue App-Version verfügbar ist, stellt Citrix das Update während des Bereitstellungszeitraums bereit. Mit diesem Parameter können Sie steuern, zu welchem Zeitpunkt während des Bereitstellungszeitraums Sie das Update erhalten können.

Zulässige Werte:

AURolloutPriority-Werte	Beschreibung	Beispiel
Auto (Standard)	Sie erhalten Updates während des Bereitstellungszeitraums (von Citrix konfiguriert).	<code>CitrixWorkspaceApp.exe AURolloutPriority =Auto</code>
Fast	Sie erhalten Updates zu Beginn des Bereitstellungszeitraums.	<code>CitrixWorkspaceApp.exe AURolloutPriority =Fast</code>
Medium	Sie erhalten Updates nach Ablauf der Hälfte des Bereitstellungszeitraums.	<code>CitrixWorkspaceApp.exe AURolloutPriority =Medium</code>

AURolloutPriority-Werte	Beschreibung	Beispiel
Slow	Sie erhalten Updates gegen Ende des Bereitstellungszeitraums.	<code>CitrixWorkspaceApp.exe AURolloutPriority=Slow</code>

## Store-Konfigurationsparameter

### Store konfigurieren

- Befehl: [ALLOWADDSTORE](#)
- Beschreibung: Ermöglicht es Ihnen, die Stores (HTTP oder https) basierend auf dem angegebenen Parameter zu konfigurieren.

Zulässige Werte:

ALLOWADDSTORE-Wert	Beschreibung	Beispiel
S (Standardwert)	Sie können nur sichere Stores (mit HTTPS konfiguriert) hinzufügen oder entfernen.	<code>CitrixWorkspaceApp.exe ALLOWADDSTORE=S</code>
A	Sie können sichere (HTTPS) und nicht sichere (HTTP) Stores hinzufügen oder entfernen. Gilt nicht, wenn die Citrix Workspace-App pro Benutzer installiert ist.	<code>CitrixWorkspaceApp.exe ALLOWADDSTORE=A</code>
N	Benutzer können nie einen eigenen Store hinzufügen.	<code>CitrixWorkspaceApp.exe ALLOWADDSTORE=N</code>

### Store-Anmeldeinformationen lokal speichern

- Befehl: [ALLOWSAVEPWD](#)
- Beschreibung: Ermöglicht Ihnen, die Anmeldeinformationen für den Store lokal zu speichern. Dieser Parameter gilt nur für Stores, die das Citrix Workspace-App-Protokoll verwenden.

Zulässige Werte:



ALLOWSAVEPWD-Werte	Beschreibung	Beispiel
• S (Standardwert)	Ermöglicht das Speichern von Kennwörtern nur für sichere Stores, die mit HTTPS konfiguriert sind.	<code>CitrixWorkspaceApp.exe ALLOWSAVEPWD=S</code>
N	Das Speichern von Kennwörtern ist nicht zulässig.	<code>CitrixWorkspaceApp.exe ALLOWSAVEPWD=N</code>
A	Ermöglicht das Speichern von Kennwörtern für sichere Stores (HTTPS) und nicht sichere Stores (HTTP).	<code>CitrixWorkspaceApp.exe ALLOWSAVEPWD=A</code>

## Beispiele für die Store-Konfiguration bei Installation per Befehlszeile

### StoreFront-Store-URL angeben:

```
1 CitrixWorkspaceApp.exe /silent
2 STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR
  App Store
3
4 <!--NeedCopy-->
```

### Angeben der Citrix Gateway Store-URL:

```
1 CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com#
  Storename;On;Store
2 <!--NeedCopy-->
```

Dabei gibt **Storename** den Namen des Stores an, der konfiguriert werden muss.

#### Hinweis:

- Bei einem Setup mit mehreren Stores ist nur eine Citrix Gateway-Store-URL-Konfiguration zulässig und diese muss an erster Stelle in der Liste stehen (Parameter STORE0).
- Die mit dieser Methode konfigurierte Citrix Gateway Store-URL unterstützt keine PNA-Dienste-Sites, die Citrix Gateway verwenden.
- Der Parameter "Discovery" ist nicht erforderlich, wenn Sie eine Citrix Gateway-Store-URL angeben.

### Mehrere Stores konfigurieren:

```
1 CitrixWorkspaceApp.exe STORE0= NetScaler Store;https://ag.mycompany.
  com#Storename;On;NetScaler Store
```

```
2 STORE1="StoreFront Store;https://testserver.net/Citrix/MyBackupStore/
  discovery;on; StoreFrontStore
3 <!--NeedCopy-->
```

#### Hinweis:

- Für eine erfolgreiche Passthrough-Authentifizierung ist es zwingend erforderlich, `discovery` in die Store-URL aufzunehmen.
- Die Citrix Gateway-Store-URL muss der erste Eintrag in der Liste der konfigurierten Store-URLs sein.

## Installationsparameter

### App Protection starten

- Befehl: `startAppProtection`
- Beschreibung: Startet App Protection und bietet mehr Sicherheit, da Clients besser vor Bildschirmerfassungs- und Keylogging-Malware geschützt sind.
- Beispiel: `CitrixWorkspaceApp.exe startAppProtection`

Weitere Informationen finden Sie unter [App Protection](#).

#### Hinweis:

Der Switch `startAppProtection` ersetzt den Switch `includeAppProtection`. Die Option `includeAppProtection` ist veraltet. Weitere Informationen finden Sie unter [Einstellung von Features und Plattformen](#).

### Citrix Enterprise Browser-Binärdateien ausschließen

- Befehl: `InstallEmbeddedBrowser`
- Beschreibung: Schließt die Binärdateien für den Citrix Enterprise Browser aus.
- Beispiel: Führen Sie die Befehlszeilenoption `InstallEmbeddedBrowser=N` aus, um den eingebetteten Browser auszuschließen.

Sie können die Binärdateien für den Citrix Enterprise Browser nur in folgenden Fällen ausschließen:

- Neuinstallation
- Upgrade von einer Version ohne Binärdateien für den Citrix Enterprise Browser.

Wenn Ihre Version der Citrix Workspace-App die Binärdateien für den Citrix Enterprise Browser enthält und Sie auf Version 2002 aktualisieren, werden die Binärdateien für den Citrix Enterprise Browser während des Upgrades automatisch aktualisiert.

## Installationsverzeichnis angeben

- Befehl: `INSTALLDIR`
- Beschreibung: Gibt das benutzerdefinierte Installationsverzeichnis für die Installation der Citrix Workspace-App an. Der Standardpfad ist `C:\Program Files\Citrix`.
- Beispiel: `CitrixWorkspaceApp.exe INSTALLDIR=C:\custom path\Citrix`.

### Hinweis:

Der Ordner **Program Files** ist durch das Betriebssystem geschützt. Wenn Sie einen anderen Ordner verwenden möchten, stellen Sie sicher, dass dieser über die richtigen Berechtigungen verfügt und geschützt ist.

## Eine oder mehrere der spezifischen Komponenten installieren

- Befehl: `ADDLOCAL`
- Beschreibung: Verwenden Sie den Schlüssel `ADDLOCAL`, um eine oder mehrere der bestimmten Komponenten der Citrix Workspace-App zu installieren. Wenn Sie mit diesem Schlüssel bestimmte Komponenten installieren, installiert die Citrix Workspace-App standardmäßig alle obligatorischen Komponenten.

### Hinweis:

Sie sollten den Schlüssel `ADDLOCAL` nur verwenden, um bestimmte Komponenten der Citrix Workspace-App zu installieren. Wenn kein Parameter `ADDLOCAL` angegeben ist, werden standardmäßig alle unterstützten Komponenten während der Installation der Citrix Workspace-App installiert.

In der folgenden Tabelle sind die Komponenten aufgeführt, die vom Schlüssel `ADDLOCAL` unterstützt werden:

ADDLOCAL-Schlüssel	Name der Komponente	Beschreibung
<code>ReceiverInside</code>	Receiver	Bereitstellung von Workspace SDK-Diensten für das Self-Service-Plug-In.
<code>ICA_Client</code>	HDX Engine	Diese Komponente verarbeitet den ICA-Datei- oder Sitzungsstart.
<code>BCR_Client</code>	BCR-Client	Plug-In für die Browserinhaltsumleitung.
<code>USB</code>	USB-Client	Plug-In für die USB-Umleitung.

ADDLOCAL-Schlüssel	Name der Komponente	Beschreibung
<code>DesktopViewer</code>	Desktop Viewer-Client	UI-Framework für virtuelle Desktops.
<code>AM</code>	AuthManager	Authentifizierungsmanager — zur Autorisierung des Benutzers bei der Citrix Workspace-App.
<code>SSON</code>	SSON	Single Sign-On-Komponente zur Unterstützung von Single Sign-On.
<code>SELSERVICE</code>	Self-Service	Plug-In für den Citrix Workspace für den nativen Start.
<code>WebHelper</code>	Web Helper	Hilfsprogramm zum Verbinden des Browsers mit der nativen Workspace-App.
<code>CitrixEnterpriseBrowser</code>	Browser	Mit dem nativen Browser können Benutzer Web- oder SaaS-Apps in der Citrix Workspace-App sicher öffnen.

Beispielsweise können Sie mit dem folgenden Befehl die im Befehl genannten Komponenten installieren:

```
1 CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,BCR_Client,
   USB,DesktopViewer,AM,SSON,SelfService,WebHelper,
   CitrixEnterpriseBrowser
2 <!--NeedCopy-->
```

#### Hinweis:

Das App Protection-Feature ist standardmäßig installiert. Daher ist `AppProtection` keine für ADDLOCAL gültige Option mehr.

### Citrix Casting installieren

#### Wichtig:

Für die Citrix Workspace-App LTSR Version 2402 und höher kann Citrix Casting auch mit dem Befehl `IncludeCitrixCasting` nicht installiert werden. Um dieses Feature verwenden zu können, müssen Sie eine ältere Version der Citrix Workspace-App verwenden. Weitere Informa-

tionen finden Sie auf der Seite [Deprecation](#).

- Befehl: `IncludeCitrixCasting`
- Beschreibung: Installiert Citrix Casting während der Installation.

Weitere Informationen zu Citrix Casting finden Sie unter [Citrix Casting](#).

## HDX-Parameter

### Bidirektionale Inhaltsumleitung einrichten

- Befehl: `ALLOW_BIDIRCONTENTREDIRECTION`
- Beschreibung: Gibt an, ob die bidirektionale Inhaltsumleitung zwischen Client und Host aktiviert ist. Weitere Informationen finden Sie unter [Richtlinieneinstellungen für die bidirektionale Inhaltsumleitung](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Zulässige Werte:

#### ALLOW\_BIDIRCONTENTREDIRECTION-

Wert	Beschreibung	Beispiel
0 (Standardwert)	Gibt an, dass die bidirektionale Inhaltsumleitung deaktiviert ist.	<code>CitrixWorkspaceApp.exe</code> <code>ALLOW_BIDIRCONTENTREDIRECTION=0</code>
1	Gibt an, dass die bidirektionale Inhaltsumleitung aktiviert ist.	<code>CitrixWorkspaceApp.exe</code> <code>ALLOW_BIDIRCONTENTREDIRECTION=1</code>

### Lokalen App-Zugriff einrichten

- Befehl: `FORCE_LAA`
- Beschreibung: Gibt an, dass die Citrix Workspace-App mit der clientseitigen Komponente für den lokalen App-Zugriff installiert ist. Installieren Sie die Citrix Workspace-App mit Administratorrechten, damit diese Komponente funktioniert. Weitere Informationen finden Sie unter [Lokaler App-Zugriff](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Zulässige Werte:

FORCE_LAA-Wert	Beschreibung	Beispiel
0 (Standardwert)	Die Komponente für den lokalen App-Zugriff ist nicht installiert.	<code>CitrixWorkspaceApp.exe FORCE_LAA =0</code>
1	Gibt an, dass die clientseitige Komponente für den lokalen App-Zugriff installiert ist.	<code>CitrixWorkspaceApp.exe FORCE_LAA =1</code>

### URL-Umleitung auf Benutzergeräten einrichten

- Befehl: [ALLOW\\_CLIENTHOSTEDAPPSURL](#)
- Beschreibung: Aktiviert die URL-Umleitung auf einem Benutzergerät. Weitere Informationen finden Sie unter [Lokaler App-Zugriff](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Zulässige Werte:

ALLOW_CLIENTHOSTEDAPPSURL-Wert	Beschreibung	Beispiel
0 (Standardwert)	Deaktiviert die URL-Umleitung auf einem Benutzergerät.	<code>CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL =0</code>
1	Aktiviert die URL-Umleitung auf den Benutzergeräten.	<code>CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL =1</code>

### Symbole für Dokumente oder Dateien anzeigen

- Befehl: [LEGACYFTAICONS](#)
- Beschreibung: Legt fest, ob Sie für Dokumente oder Dateien, die Dateitypzuordnungen für abonnierte Anwendungen haben, Symbole anzeigen möchten.

Zulässige Werte:

LEGACYFTAICONS-Wert	Beschreibung	Beispiel
False (Standardwert)	Anzeige von Symbolen für Dokumente oder Dateien, die Dateitypzuordnungen für abonnierte Anwendungen haben. Wenn dieser Wert auf "false" gesetzt ist, generiert das Betriebssystem ein Symbol für ein Dokument, dem kein bestimmtes Symbol zugewiesen ist. Das vom Betriebssystem generierte Symbol ist ein generisches Symbol, das mit einer kleineren Version des Anwendungssymbols überlagert wird.	<code>CitrixWorkspaceApp.exe LEGACYFTAICONS=False</code>
True	Keine Anzeige von Symbolen für Dokumente oder Dateien, die Dateitypzuordnungen für abonnierte Anwendungen haben.	<code>CitrixWorkspaceApp.exe LEGACYFTAICONS=True</code>

## Parameter für Einstellungen und Benutzeroberfläche

### Verzeichnis für Startmenü- und Desktop-Verknüpfungen einrichten

Befehlswert	Beschreibung	Verzeichnisname	Beispiel
<code>CitrixWorkspaceApp.exe STARTMENUDIR</code>	Gibt das Verzeichnis für die Verknüpfungen im Startmenü an.	Standardmäßig werden Anwendungen unter <b>Start &gt; Alle Programme</b> angezeigt. Sie können den relativen Pfad für die Verknüpfungen im Ordner <code>Programs</code> angeben.	Geben Sie <code>STARTMENUDIR=Workspace</code> an, um Verknüpfungen unter <b>Start &gt; Alle Programme &gt; Workspace</b> zu platzieren.

Befehlswert	Beschreibung	Verzeichnisname	Beispiel
<code>CitrixWorkspaceApp.exe DESKTOPDIR</code>	Gibt das Verzeichnis für Verknüpfungen auf dem Desktop an.	Sie können den relativen Pfad für Verknüpfungen angeben.	Geben Sie <code>DESKTOPDIR=Workspace</code> an, um Verknüpfungen unter <b>Start &gt; Alle Programme &gt; Workspace</b> zu platzieren.

**Hinweis:**

Wenn Sie die Option `DESKTOPDIR` verwenden, legen Sie den Schlüssel `PutShortcutsOnDesktop` auf `True` fest.

**Zugriff auf Self-Service steuern**

- Befehl: `SELFSERVICEMODE`
- Beschreibung: Steuert den Zugriff auf die Self-Service-Benutzeroberfläche der Citrix Workspace-App.

Zulässige Werte:

SELFSERVICEMODE-Wert	Beschreibung	Beispiel
True	Der Benutzer hat Zugriff auf die Self-Service-Benutzeroberfläche.	<code>CitrixWorkspaceApp.exe SELFSERVICEMODE=True</code>
False	Gibt an, dass der Benutzer keinen Zugriff auf die Self-Service-Benutzeroberfläche hat.	<code>CitrixWorkspaceApp.exe SELFSERVICEMODE=False</code>

**Vorabstart von Sitzungen steuern**

- Befehl: `ENABLEPRELAUNCH`
- Beschreibung: Steuert den Vorabstart von Sitzungen. Weitere Informationen finden Sie unter [Dauer des Anwendungsstarts](#).

Zulässige Werte:



ENABLEPRELAUNCH-Wert	Beschreibung	Beispiel
True	Gibt an, dass Sitzungsvorabstart aktiviert ist.	<code>CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True</code>
False	Gibt an, dass Sitzungsvorabstart deaktiviert ist.	<code>CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False</code>

### Tastenkombinationen und Option “Verbindung wiederherstellen” ausblenden

- Befehl: `DisableSetting`
- Beschreibung: Ausblenden der Option **Verknüpfungen und Wiederverbinden** auf der Seite **Erweiterte Einstellungen**. Weitere Informationen finden Sie unter [Ausblenden bestimmter Einstellungen auf der Seite “Erweiterte Einstellungen”](#).

Zulässige Werte:

DisableSetting-Wert	Beschreibung	Beispiel
0 (Standardwert)	Die Optionen <b>Verknüpfungen</b> und <b>Wiederverbinden</b> werden auf der Seite “Erweiterte Einstellungen” angezeigt.	<code>CitrixWorkspaceApp.exe DisableSetting=0</code>
1	Nur die Option <b>Wiederverbinden</b> wird auf der Seite “Erweiterte Einstellungen” angezeigt.	<code>CitrixWorkspaceApp.exe DisableSetting=1</code>
2	Nur die Option <b>Verknüpfungen</b> wird auf der Seite “Erweiterte Einstellungen” angezeigt.	<code>CitrixWorkspaceApp.exe DisableSetting=2</code>
3	Die Optionen <b>Verknüpfungen</b> und <b>Wiederverbinden</b> werden beide auf der Seite “Erweiterte Einstellungen” ausgeblendet.	<code>CitrixWorkspaceApp.exe DisableSetting=3</code>

### Programm zur Verbesserung der Benutzerfreundlichkeit aktivieren

- Befehl: `EnableCEIP`

- Beschreibung: Gibt an, dass Sie am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) teilnehmen. Weitere Informationen finden Sie unter [CEIP](#).

Zulässige Werte:

EnableCEIPcommand-Wert	Beschreibung	Beispiel
True (Standardwert)	Sie nehmen am Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) teil.	<code>CitrixWorkspaceApp.exe EnableCEIP=True</code>
False	Sie nehmen nicht am Citrix Programm zur Verbesserung der Benutzerfreundlichkeit teil.	<code>CitrixWorkspaceApp.exe EnableCEIP=False</code>

### Always-On-Ablaufverfolgung aktivieren

- Befehl: `EnableTracing`
- Beschreibung: Steuert das Feature **Always-On-Ablaufverfolgung**.

Zulässige Werte:

EnableTracing-Wert	Beschreibung	Beispiel
True (Standardwert)	Aktiviert das Feature <b>Always-On-Ablaufverfolgung</b> .	<code>CitrixWorkspaceApp.exe EnableTracing=true</code>
False	Deaktiviert die Funktion <b>Always-On-Ablaufverfolgung</b> .	<code>CitrixWorkspaceApp.exe EnableTracing=false</code>

### Namen für Benutzergerät eingeben

- Befehl: `CLIENT_NAME`
- Beschreibung: Gibt den Namen an, mit dem das Benutzergerät beim Server identifiziert wird.
- `<ClientName>` - Gibt den Namen an, mit dem das Benutzergerät beim Server identifiziert wird. Der Standardname lautet `%COMPUTERNAME%`.
- Beispiel: `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`.

### Clientnamen auf Computernamen einstellen

- Befehl: `ENABLE_DYNAMIC_CLIENT_NAME`
- Beschreibung: Ermöglicht, dass der Clientname mit dem Computernamen übereinstimmt. Wenn Sie den Computernamen ändern, ändert sich auch der Clientname.

Zulässige Werte:

ENABLE_DYNAMIC_CLIENT_NAME-		
Wert	Beschreibung	Beispiel
Yes (Standardwert)	Ermöglicht, dass der Clientname mit dem Computernamen übereinstimmt.	<code>CitrixWorkspaceApp.exe</code> <code>ENABLE_DYNAMIC_CLIENT_NAME=Yes</code>
Nein	Erlaubt nicht, dass der Clientname mit dem Computernamen übereinstimmt. Geben Sie einen Wert für die Eigenschaft <code>CLIENT_NAME</code> ein.	<code>CitrixWorkspaceApp.exe</code> <code>ENABLE_DYNAMIC_CLIENT_NAME=No</code>

## Authentifizierungsparameter

### Single Sign-On einbeziehen

- Befehl: `/includeSSON`
- Beschreibung: Erfordert die Installation als Administrator. Gibt an, dass die Citrix Workspace-App mit der Single Sign-On-Komponente installiert wird. Weitere Informationen finden Sie unter [Domänen-Passthrough-Authentifizierung](#).
- Beispiel: `CitrixWorkspaceApp.exe /includeSSON`

#### Hinweis:

Der Befehl `includeSSON` unterstützt nur die Neuinstallation der Citrix Workspace-App.

### Single Sign-On aktivieren

- Befehl: `ENABLE_SSON`
- Beschreibung: Aktiviert Single Sign-On, wenn die Citrix Workspace-App mit dem Befehl `/includeSSON` installiert wird. Weitere Informationen finden Sie unter [Domänen-Passthrough-Authentifizierung](#).

Zulässige Werte:

ENABLE_SSON-Wert	Beschreibung	Beispiel
Yes (Standardwert)	Gibt an, dass Single Sign-On aktiviert ist.	<code>CitrixWorkspaceApp.exe ENABLE_SSON=Yes</code>
Nein	Gibt an, dass Single Sign-On deaktiviert ist.	<code>CitrixWorkspaceApp.exe ENABLE_SSON=No</code>

## Citrix Workspace-App deinstallieren

### Deinstallation mit einem Windows-basierten Deinstallationsprogramm

Sie können die Citrix Workspace-App für Windows über die **Systemsteuerung** deinstallieren: Weitere Informationen finden Sie im Abschnitt [Citrix Workspace-App für Windows deinstallieren](#).

#### Hinweis:

Bei der Installation der Citrix Workspace-App werden Sie aufgefordert, das Citrix HDX RTME-Paket zu deinstallieren. Klicken Sie auf **OK**, um mit der Deinstallation fortzufahren.

### Deinstallation über die Befehlszeilenschnittstelle

Sie können die Citrix Workspace-App mit dem folgenden Befehl über die Befehlszeile deinstallieren:

```
1 CitrixWorkspaceApp.exe /uninstall
2 <!--NeedCopy-->
```

Führen Sie für die unbeaufsichtigte Deinstallation der Citrix Workspace-App den folgenden Befehl aus:

```
1 CitrixWorkspaceApp.exe /silent /uninstall
2 <!--NeedCopy-->
```

#### Hinweis:

GPO-bezogene Registrierungsschlüssel werden nicht vom Citrix Workspace-App-Installationsprogramm gesteuert und verbleiben daher nach der Deinstallation. Wenn Sie Einträge gefunden haben, aktualisieren Sie diese mit `gpedit` oder löschen Sie sie manuell.

## Problembehandlung

### Fehlercodes

- Fehlercodes im Zusammenhang mit dem Installationsprogramm finden Sie unter [MsiExec.exe und InstMsi.exe Fehlermeldungen](#).
- Informationen zu systembezogenen Fehlercodes finden Sie unter [Systemfehlercodes](#).

### Speicherort des Installationsprotokolls

Standardmäßig sind die Installationsprotokolle am folgenden Speicherort:

---

	Installationsprotokollordner	Installationstyp
Administrator	64-Bit: C:\Program Files (x86)\Citrix\Logs; 32-Bit: C:\Program Files\Citrix\ICA Client	Installation pro System
Benutzer	%USERPROFILE%\AppData\Local\Citrix\Logs	Installation pro Benutzer

---

#### Hinweis:

TrolleyExpress wird durch CWAInstaller-<date and timestamp> ersetzt. Das Protokoll wird beispielsweise unter C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441 aufgezeichnet.

## Problembehandlung

### Fehlercodes

- Fehlercodes im Zusammenhang mit dem Installationsprogramm finden Sie unter [MsiExec.exe und InstMsi.exe Fehlermeldungen](#).
- Informationen zu systembezogenen Fehlercodes finden Sie unter [Systemfehlercodes](#).

### Speicherort des Installationsprotokolls

Standardmäßig sind die Installationsprotokolle am folgenden Speicherort:

	Installationsprotokollordner	Installationstyp
Administrator	64-Bit: C:\Program Files (x86)\Citrix\Logs; 32-Bit: C:\Program Files\Citrix\ICA Client	Installation pro System
Benutzer	%USERPROFILE%\AppData\Local\Citrix\Logs	Installation pro Benutzer

## Zurücksetzen der Citrix Workspace-App

Durch das Zurücksetzen der Citrix Workspace-App werden die Standardeinstellungen wiederhergestellt.

Die folgenden Elemente werden zurückgesetzt, wenn Sie die Citrix Workspace-App zurücksetzen:

- Alle konfigurierten Konten und Stores.
- Apps, die vom Self-Service-Plug-In bereitgestellt werden, ihre Symbole und Registrierungsschlüssel.
- Vom Self-Service-Plug-In erstellte Dateitypzuordnungen.
- Zwischengespeicherte Dateien und gespeicherte Kennwörter.
- Benutzerspezifische Registrierungseinstellungen.
- Maschinenspezifische Installationen und Registrierungseinstellungen.
- Citrix Gateway-Registrierungseinstellungen für die Citrix Workspace-App.

Führen Sie den folgenden Befehl über die Befehlszeilenschnittstelle aus, um die Citrix Workspace-App zurückzusetzen:

```
1 "C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe
   " -cleanUser
2 <!--NeedCopy-->
```

Verwenden Sie für eine unbeaufsichtigte Zurücksetzung folgenden Befehl:

```
1 "C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe
   " /silent -cleanUser
2 <!--NeedCopy-->
```

### Hinweis:

Verwenden Sie den Großbuchstaben U im Parameter.

Das Zurücksetzen der Citrix Workspace-App hat keine Auswirkungen auf Folgendes:

- Installation der Citrix Workspace-App oder des Plug-Ins.

- Maschinenspezifische ICA-Sperreinstellungen.
- Administrative Gruppenrichtlinienobjektvorlage für die Citrix Workspace-App.

## Bereitstellen

April 22, 2024

Sie können die Citrix Workspace-App mit den folgenden Methoden bereitstellen:

- Verwenden Sie Active Directory und Beispielstartskripts, um die Citrix Workspace-App für Windows bereitzustellen. Weitere Informationen über Active Directory finden Sie unter [Verwenden von Active Directory und Beispielskripts](#).
- Installieren Sie vor dem Start von Workspace für Web die Citrix Workspace-App für Windows. Weitere Informationen finden Sie unter [Verwenden von Workspace für Web](#).
- Verwenden Sie ein ESD-Tool zur elektronischen Softwareverteilung wie Microsoft System Center Configuration Manager 2012 R2. Weitere Informationen finden Sie unter [Verwenden von System Center Configuration Manager 2012 R2](#).
- Verwenden Sie Microsoft Endpoint Manager (Intune). Weitere Informationen finden Sie unter [Bereitstellen der Citrix Workspace-App in Microsoft Endpoint Manager \(Intune\)](#).

### Verwenden von Active Directory und Beispielskripts

Sie können Active Directory-Gruppenrichtlinienskripts verwenden, um die Citrix Workspace-App basierend auf Ihrer Organisationsstruktur bereitzustellen. Citrix empfiehlt, die Skripts zu verwenden, anstatt die MSI-Dateien zu extrahieren. Allgemeine Informationen über Startskripts finden Sie in der [Dokumentation von Microsoft](#).

#### Verwenden von Skripten mit Active Directory:

1. Erstellen Sie die Organisationseinheit (OU) für jedes Skript.
2. Erstellen Sie eine Gruppenrichtlinienobjekt (GPO) für die neu erstellte OU.

Informationen zum Erstellen von Organisationseinheiten in einem Azure Active Directory finden Sie unter [Erstellen einer Organisationseinheit \(OU\) in einer verwalteten Azure Active Directory Domain Services-Domäne](#).

### Skripts bearbeiten

Bearbeiten Sie die Skripts mit den folgenden Parametern im Kopfbereich jeder Datei:

- **Current Version of package** - Die angegebene Versionsnummer wird validiert und die Bereitstellung wird fortgesetzt, wenn die Nummer nicht vorhanden ist. Beispiel: Legen Sie `DesiredVersion= 3.3.0.XXXX` fest, um genau der angegebenen Version zu entsprechen. Wenn Sie eine Teilversion angeben, beispielsweise 3.3.0, wird eine Übereinstimmung mit allen Versionen erkannt, die dieses Präfix haben (3.3.0.1111, 3.3.0.7777 usw.).
- **Package Location/Deployment directory** - Hiermit geben Sie die Netzwerkfreigabe mit den Installationspaketen der Citrix Workspace-App an. Die Freigabe wird nicht durch das Skript authentifiziert. Für die Freigabe muss die Leseberechtigung auf JEDER eingestellt sein.
- **Script Logging Directory** - Netzwerkfreigabe, die die kopierten Installationsprotokolle enthält und die Dateien, die nicht durch das Skript authentifiziert wurden. Für die Freigabe muss Schreib- und Leseberechtigung für JEDER eingestellt sein.
- **Package Installer Command Line Options** - Diese Befehlszeilenoptionen werden an den Installer weitergeleitet. Weitere Informationen zur Befehlszeilensyntax finden Sie unter [Verwenden von Befehlszeilenparametern](#).

## Skripts

Der Installer der Citrix Workspace-App bietet Beispiele für Pro-Computer- und Pro-Benutzer-Skripts, um die Citrix Workspace-App zu installieren und zu deinstallieren. Sie finden die Skripts auf der [Downloadseite](#) der Citrix Workspace-App für Windows.

Bereitstellungstyp	Bereitstellen	Entfernen
Pro Computer	<code>CheckAndDeployWorkspacePerMachine.bat</code>	<code>PerMachineRestoreWorkSpaceScript.bat</code>
Pro Benutzer	<code>CheckAndDeployWorkspacePerUser.bat</code>	<code>PerUserRemoveWorkSpacePerUser.bat</code>

## Hinzufügen von Startskripts:

1. Öffnen Sie die Gruppenrichtlinien-Verwaltungskonsole.
2. Wählen Sie **Computerkonfiguration** oder **Benutzerkonfiguration** > **Richtlinien** > **Windows-Einstellungen** > **Skripts**.
3. Wählen Sie im rechten Bereich der Gruppenrichtlinien-Verwaltungskonsole **Anmelden**.
4. Wählen Sie **Dateien anzeigen**, kopieren Sie das entsprechende Skript in den angezeigten Ordner und schließen Sie das Dialogfeld.
5. Klicken Sie in **Eigenschaften** auf **Hinzufügen** und **Durchsuchen**, um das soeben erstellte Skript zu finden und hinzuzufügen.

## Bereitstellen der Citrix Workspace-App für Windows:



1. Verschieben Sie die Benutzergeräte, für die Sie diese Art der Bereitstellung verwenden möchten, in die von Ihnen erstellte Organisationseinheit (OU).
2. Starten Sie das Benutzergerät neu und melden Sie sich an.
3. Stellen Sie sicher, dass das neu installierte Paket unter **Programme und Funktionen** aufgeführt ist.

#### **Entfernen der Citrix Workspace-App für Windows:**

1. Verschieben Sie die Benutzergeräte, die entfernt werden sollen, in die von Ihnen erstellte Organisationseinheit (OU).
2. Starten Sie das Benutzergerät neu und melden Sie sich an.
3. Stellen Sie sicher, dass das neu installierte Paket nicht unter **Programme und Funktionen** aufgeführt ist.

#### **Verwenden von Workspace für Web**

Mit Workspace für Web können Sie über eine Webseite im Browser auf StoreFront-Stores zugreifen.

Bevor Sie über einen Browser eine Verbindung zu einer App herstellen, gehen Sie wie folgt vor:

1. Installieren Sie die Citrix Workspace-App für Windows.
2. Stellen Sie die Citrix Workspace-App über Workspace für Web bereit.

Wenn Workspace für Web erkennt, dass keine kompatible Version der Citrix Workspace-App vorhanden ist, wird eine Aufforderung angezeigt. Darin werden Sie zum Download und zur Installation der Citrix Workspace-App für Windows aufgefordert.

#### **Hinweis:**

Workspace für Web unterstützt keine e-mail-basierte Kontenermittlung.

Verwenden Sie die folgende Konfiguration, um nur zur Eingabe der Serveradresse aufzufordern.

1. Laden Sie [CitrixWorkspaceApp.exe](#) auf den lokalen Computer herunter.
2. Benennen Sie [CitrixWorkspaceApp.exe](#) in [CitrixWorkspaceAppWeb.exe](#) um.
3. Stellen Sie die umbenannte ausführbare Datei mit der normalen Bereitstellungsmethode bereit. Wenn Sie StoreFront verwenden, finden Sie weitere Informationen unter [Konfigurieren von StoreFront mit Konfigurationsdateien](#) in der StoreFront-Dokumentation.

#### **Verwenden von System Center Configuration Manager 2012 R2**

Sie können die Citrix Workspace-App über Microsoft System Center Configuration Manager (SCCM) bereitstellen.

Sie können die Citrix Workspace-App über SCCM mithilfe der folgenden vier Abschnitte bereitstellen:

1. Hinzufügen der Citrix Workspace-App zur SCCM-Bereitstellung
2. Hinzufügen von Verteilungspunkten
3. Bereitstellen der Citrix Workspace-App im Softwarecenter
4. Erstellen von Gerätesammlungen

### Hinzufügen der Citrix Workspace-App zur SCCM-Bereitstellung

1. Kopieren Sie die heruntergeladene Citrix Workspace-App-Software in einen Ordner auf dem Configuration Manager-Server und starten Sie die Configuration Manager-Konsole.
2. Wählen Sie **Softwarebibliothek > Anwendungsverwaltung**. Klicken Sie mit der rechten Maustaste auf **Anwendung** und klicken Sie auf **Anwendung erstellen**.  
Der Assistent zum Erstellen von Anwendungen wird angezeigt.
3. Aktivieren Sie im Bereich **Allgemein** die Option **Anwendungsinformationen manuell angeben** und klicken Sie auf **Weiter**.
4. Im Bereich **Allgemeine Informationen** geben Sie Informationen zur Anwendung ein, zum Beispiel **Name**, **Hersteller** und **Softwareversion**.
5. Im Assistenten zum **Anwendungskatalog** geben Sie zusätzliche Informationen wie Sprache, Anwendungsname und Benutzerkategorie ein. Klicken Sie dann auf **Weiter**.

#### Hinweis:

Benutzer können die Informationen sehen, die Sie hier angeben.

6. Im Bereich **Bereitstellungstyp** klicken Sie auf **Hinzufügen**, um den Bereitstellungstyp für die Citrix Workspace-App zu konfigurieren.  
Der Assistent zum Erstellen von Bereitstellungstypen wird angezeigt.
7. Bereich **Allgemein**: Wählen Sie Windows Installer (\*.msi-Datei) als Bereitstellungstyp. Aktivieren Sie **Informationen zum Bereitstellungstyp manuell angeben** und klicken Sie auf **Weiter**.
8. Bereich **Allgemeine Informationen**: Legen Sie den Bereitstellungstyp fest (z. B.: Workspace-Bereitstellung) und klicken Sie auf **Weiter**.
9. Bereich **Inhalt**:
  - a) Geben Sie den Pfad zum Verzeichnis mit der Citrix Workspace-App-Setupdatei an. Beispiel: Tools auf dem SCCM-Server.
  - b) Geben Sie das **Installationsprogramm** an. Zur Auswahl stehen folgende Optionen:

- `CitrixWorkspaceApp.exe /silent` für die standardmäßige automatische Installation.
- `CitrixWorkspaceApp.exe /silent /includeSSON` zum Aktivieren von Domänen-Passthrough.
- `CitrixWorkspaceApp.exe /silent SELFSERVICEMODE=false` zum Installieren der Citrix Workspace-App im Modus ohne Self-Service.

c) Geben Sie für **Deinstallationsprogramm** den Befehl `CitrixWorkspaceApp.exe /silent /uninstall` ein (zum Aktivieren der Deinstallation über SCCM).

10. Bereich **Erkennungsmethode**: Wählen Sie **Regeln konfigurieren, um zu erkennen, ob dieser Bereitstellungstyp vorhanden ist**, und klicken Sie auf **Klausel hinzufügen**.

Das Dialogfeld "Erkennungsregel" wird angezeigt.

- Wählen Sie als **Einstellungstyp** die Option "Dateisystem".
- Wählen Sie folgende Einstellungen unter **Geben Sie die Datei oder den Ordner an, um diese Anwendung zu erkennen**:
  - **Typ**: Wählen Sie im Dropdownmenü die Option **Datei**.
  - **Pfad**: `%ProgramFiles(x86)%\Citrix\ICA Client\Receiver\`
  - **Datei- oder Ordnername**: `receiver.exe`
  - **Eigenschaft**: Wählen Sie im Dropdownmenü die Option **Version**.
  - **Operator**: Wählen Sie im Dropdownmenü **größer oder gleich**.
  - **Wert**: Geben Sie die Versionsnummer der aktuellen Citrix Workspace-App ein

**Hinweis:**

Diese Regelkombination gilt auch für Upgrades der Citrix Workspace-App für Windows.

11. Wählen Sie im Bereich **Benutzererfahrung** folgende Einstellungen:

- **Installationsverhalten**: Option "Für System installieren"
  - **Anmeldeanforderung**: ob ein Benutzer angemeldet ist
  - **Sichtbarkeit des Installationsprogramms**: Normal
- Klicken Sie auf **Weiter**.

**Hinweis:**

Legen Sie keine Anforderungen und Abhängigkeiten für diesen Bereitstellungstyp fest.

12. Prüfen Sie im Bereich **Zusammenfassung** die gewählten Einstellungen für diesen Bereitstellungstyp. Klicken Sie auf **Weiter**.

Es wird dann ein Erfolg gemeldet.

13. Im **Abschlussfenster** wird unter **Bereitstellungstypen** ein neuer Bereitstellungstyp (Workspace-Bereitstellung) aufgelistet.

14. Klicken Sie auf **Weiter** und klicken Sie auf **Schließen**.

### Hinzufügen von Verteilungspunkten

1. Klicken Sie in der **Configuration Manager**-Konsole mit der rechten Maustaste auf “Citrix Workspace-App” und wählen Sie **Inhalt verteilen**.

Der Assistent für die Verteilung von Inhalt wird angezeigt.

2. Klicken Sie im Bereich “Inhaltsverteilung” auf **Hinzufügen > Verteilungspunkte**.

Das Dialogfeld “Verteilungspunkte hinzufügen” wird angezeigt.

3. Navigieren Sie zum SCCM-Server, auf dem der Inhalt verfügbar ist, und klicken Sie auf **OK**.

Im Abschlussfenster wird eine Erfolgsmeldung angezeigt.

4. Klicken Sie auf **Schließen**.

### Bereitstellen der Citrix Workspace-App im Softwarecenter

1. Klicken Sie mit der rechten Maustaste in der Configuration Manager-Konsole auf “Citrix Workspace-App” und wählen Sie **Bereitstellen**.

Der Assistent zur Softwarebereitstellung wird angezeigt.

2. Wählen Sie **Durchsuchen** für die Sammlung (Gerätesammlung oder Benutzersammlung), wo die Anwendung bereitgestellt werden soll, und klicken Sie auf **Weiter**.

3. Wählen Sie im Bereich **Bereitstellungseinstellungen** für **Aktion** die Einstellung “Installation” und für **Zweck** die Option “Erforderlich”. Dies aktiviert die unbeaufsichtigte Installation. Klicken Sie auf **Weiter**.

4. Legen Sie im Bereich **Zeitplanung** den Zeitplan für die Bereitstellung der Software auf den Zielgeräten fest.

5. Legen Sie im Bereich **Benutzererfahrung** das Verhalten für **Benutzerbenachrichtigungen** fest: Wählen Sie **Änderungen zum Stichtag oder während eines Wartungsfensters ausführen (erfordert Neustart)** und klicken Sie auf **Weiter**, um den Assistenten zur Softwarebereitstellung zu schließen.

Im **Abschlussfenster** wird eine Erfolgsmeldung angezeigt.

Starten Sie die Ziel-Endpunktgeräte neu (nur für die sofortige Installation erforderlich).

Auf Endpunktgeräten wird die Citrix Workspace-App im Softwarecenter unter **Verfügbare Software** angezeigt. Die Installation wird automatisch auf der Basis des konfigurierten Zeitplans ausgelöst. Sie können auch einen späteren Termin festlegen oder die Software bei Bedarf installieren. Der Installationsstatus wird nach dem Start der Installation im **Softwarecenter** angezeigt.

## Erstellen von Gerätesammlungen

1. Starten Sie die **Configuration Manager**-Konsole und klicken Sie auf **Bestand und Kompatibilität > Überblick > Geräte**.

2. Klicken Sie mit der rechten Maustaste auf **Gerätesammlungen** und wählen Sie **Gerätesammlung erstellen**.

Der **Assistent zum Erstellen von Gerätesammlungen** wird angezeigt.

3. Geben Sie im Bereich **Allgemein** den **Namen** für das Gerät ein und klicken Sie auf **Durchsuchen**, um eine begrenzte Sammlung auszuwählen.

Dies bestimmt den Geltungsbereich von Geräten. Es kann eine der von SCCM erstellten Standard-**Gerätesammlungen** verwendet werden.

Klicken Sie auf **Weiter**.

4. Klicken Sie im Bereich **Mitgliedschaftsregeln** auf **Regel hinzufügen**. Diese wird dann zum Filtern der Geräte verwendet.

Der **Assistent zum Erstellen direkter Mitgliedschaftsregeln** wird angezeigt.

- Wählen Sie im Bereich **Ressourcen suchen** einen **Attributnamen**, der den gesuchten Geräten entspricht, und legen Sie einen Wert für den Attributnamen fest, der bei der Geräteauswahl verwendet werden soll.

5. Klicken Sie auf **Weiter**. Wählen Sie im Bereich "Ressourcen auswählen" die Geräte aus, die in der Gerätesammlung enthalten sein müssen.

Im Abschlussfenster wird eine Erfolgsmeldung angezeigt.

6. Klicken Sie auf **Schließen**.

7. Im Bereich "Mitgliedschaftsregeln" wird eine neue Regel aufgelistet. Klicken Sie auf "Weiter".

8. Im Abschlussfenster wird eine Erfolgsmeldung angezeigt. Klicken Sie auf **Schließen**, um den **Assistenten zum Erstellen von Gerätesammlungen** schließen.

Die neue Gerätesammlung ist nun unter **Gerätesammlungen** aufgeführt. Beim Navigieren im Assistenten zur **Softwarebereitstellung** wird die neue Gerätesammlung in den Gerätesammlungen angezeigt.

### Hinweis:

Das Konfigurieren der Citrix Workspace-App mit SCCM kann fehlschlagen, wenn das Attribut **MSIRESTARTMANAGERCONTROL** auf **False** gesetzt ist.

Gemäß unserer Analyse wird dieses Problem nicht durch die Citrix Workspace-App für Windows verursacht. Ein erneuter Versuch kann zudem zum Erfolg der Bereitstellung führen.

## Bereitstellen der Citrix Workspace-App in Microsoft Endpoint Manager (Intune)

Gehen Sie wie folgt vor, um die (native Win-32) Citrix Workspace-App in Microsoft Endpoint Manager (Intune) bereitzustellen:

1. Erstellen Sie die folgenden Ordner:
  - Einen Ordner zum Speichern aller für die Installation erforderlichen Quelldateien. Beispiel: `C:\CitrixWorkspace_Executable`.
  - Einen Ordner für die Ausgabedatei. Ausgabedateien sind in der Datei `.intunewin`. Beispiel: `C:\Intune_CitrixWorkspaceApp`.
  - Einen Ordner für das Microsoft Win32 Content Prep Tool. Beispiel: `C:\Intune_WinAppTool`. Das Tool hilft bei der Konvertierung der Installationsdateien in das `.intunewin`-Format. Sie können das Tool von [Microsoft-Win32-Content-Prep-Tool](#) herunterladen.
2. Konvertieren Sie alle für die Installation benötigten Quelldateien in eine `.intunewin`-Datei:
  - a) Starten Sie die Eingabeaufforderung und gehen Sie zu dem Ordner mit dem Microsoft Win32 Content Prep Tool (Beispiel: `C:\Intune_WinAppTool`).
  - b) Führen Sie den Befehl `IntuneWinAppUtil.exe` aus.
  - c) Geben Sie an der Eingabeaufforderung die folgenden Informationen ein:
    - **Quellordner:** `C:\CitrixWorkspace_Executable`
    - **Setup-Datei:** `CitrixWorkspaceApp.exe`
    - **Ausgabeordner:** `C:\Intune_CitrixWorkspaceApp`Die Datei `.intunewin` wird erstellt.
3. Fügen Sie das Paket zu Microsoft Endpoint Manager (Intune) hinzu:
  - a) Öffnen Sie die Microsoft Endpoint Manager (Intune)-Konsole: <https://endpoint.microsoft.com/#home>.

**Hinweis:**

Die folgende Anweisung kann nur auf <https://endpoint.microsoft.com/#home> ausgeführt werden. Sie können das Paket auch über <https://portal.azure.com> hinzufügen.
  - b) Klicken Sie auf **Apps > Windows app** und dann auf **+Add**.
  - c) Wählen Sie in der Dropdownliste **App type** die Option **Windows app (Win 32)**.
  - d) Klicken Sie auf **App package file**, suchen Sie die Datei `CitrixWorkspaceApp.intunewin` und klicken Sie auf **OK**.

- e) Klicken Sie auf **App information**, geben Sie die erforderlichen Informationen, Namen, Beschreibung und Herausgeber ein und klicken Sie auf **OK**.
- f) Klicken Sie auf **Program**, geben Sie die folgenden Informationen ein und klicken Sie auf **OK**:
- Install command: `CitrixWorkspaceApp.exe /silent`
  - Uninstall command: `CitrixWorkspaceApp.exe /uninstall`
  - Install behavior: System
- g) Klicken Sie auf **Requirement**, geben Sie die erforderlichen Informationen ein und klicken Sie auf **OK**.
- Hinweis:**
- Wählen Sie x64 und x32 aus der Liste der Betriebssystemarchitekturen. Als Betriebssystemversion kann alles ab Win 1607 angegeben werden.
- h) Klicken Sie auf **Detection rules**, wählen Sie **Manually configure detection rules** für **Rules format** und klicken Sie auf **OK**.
- i) Klicken Sie auf **Add**, wählen Sie eine Option für **Rule type** und klicken Sie auf **OK**.
- Wenn für **Rule type** die Option **File** ausgewählt wird, kann der Pfad beispielsweise `C:\Program Files (x86)\Citrix\ICA Client\wfica32.exe` sein.
  - Wenn für **Rule type** die Option **Registry** ausgewählt wird, geben Sie `HKEY_CURRENT_USER\Software\Citrix` für **Path** und **Key exists** für **Detection method** ein.
- j) Klicken Sie auf **Return codes**, überprüfen Sie, ob die Standard-Rückgabecodes gültig sind, und klicken Sie auf **OK**.
- k) Klicken Sie auf **Add**, um die App zu Intune hinzuzufügen.
4. Prüfen des Erfolgs der Bereitstellung:
- a) Klicken Sie auf **Startseite > Apps > Windows**.
- b) Klicken Sie auf **Device install status**.
- Es wird die Zahl der Geräte angezeigt, auf denen die Citrix Workspace-App installiert ist.

## Storekonfiguration

April 22, 2024

## Store

Dieser Artikel ist ein Referenzdokument, mit dem Sie Ihre Umgebung nach der Installation der Citrix Workspace-App einrichten können.

Ein **Store** aggregiert verfügbare Anwendungen und Desktops für einen Benutzer an einem Ort. Ein Benutzer kann mehrere Stores haben und bei Bedarf zwischen Stores wechseln. Ein Administrator stellt die Store-URL mit vorkonfigurierten Ressourcen und Einstellungen bereit. Sie können über die Citrix Workspace-App auf diese Stores zugreifen.

## Arten von Stores

Sie können die folgenden Arten von Stores in der Citrix Workspace-App hinzufügen: Workspace, StoreFront, Citrix Gateway Store und benutzerdefinierter Webstore.

## Workspace

Citrix Workspace ist ein cloudbasierter Unternehmensappstore, der sicheren und einheitlichen Zugriff auf Apps, Desktops und Ressourcen bzw. Inhalte von überall und auf jedem Gerät bietet. Ressourcen können Citrix DaaS, Inhalts-Apps, lokale und mobile Apps, SaaS- und Web-Apps sowie Browser-Apps sein. Weitere Informationen finden Sie unter [Citrix Workspace](#).

## StoreFront

StoreFront ist ein on-premises Unternehmensappstore, der Anwendungen und Desktops von Citrix Virtual Apps and Desktops-Sites in einem einzigen benutzerfreundlichen Store für Benutzer zusammenfasst.

Weitere Informationen finden Sie in der [StoreFront](#)-Dokumentation.

## Citrix Gateway Store

Konfigurieren Sie Citrix Gateway so, dass Benutzer sich von außerhalb mit dem internen Netzwerk verbinden können. Dies können zum Beispiel Nutzer sein, die über das Internet oder von Remotes-tandorten eine Verbindung herstellen.

## Benutzerdefinierte Webstores

Mit diesem Feature können Sie über die Citrix Workspace-App für Windows auf den benutzerdefinierten Webstore Ihrer Organisation zugreifen. Um dieses Feature zu verwenden, muss der Administrator die



Domäne oder den benutzerdefinierten Webstore zu den zulässigen URLs im Global App Configuration Service hinzufügen.

Weitere Informationen zum Konfigurieren von Webstore-URLs für Endbenutzer finden Sie unter [Global App Configuration Service](#).

Sie können die URL des benutzerdefinierten Webstores im Bildschirm **Konto hinzufügen** in der Citrix Workspace-App angeben. Der benutzerdefinierte Webstore wird im nativen Citrix Workspace-App-Fenster geöffnet.

Um den benutzerdefinierten Webstore zu entfernen, gehen Sie zu **Konten > Konten hinzufügen oder entfernen**, wählen Sie die URL des benutzerdefinierten Webstores aus und klicken Sie auf **Entfernen**.

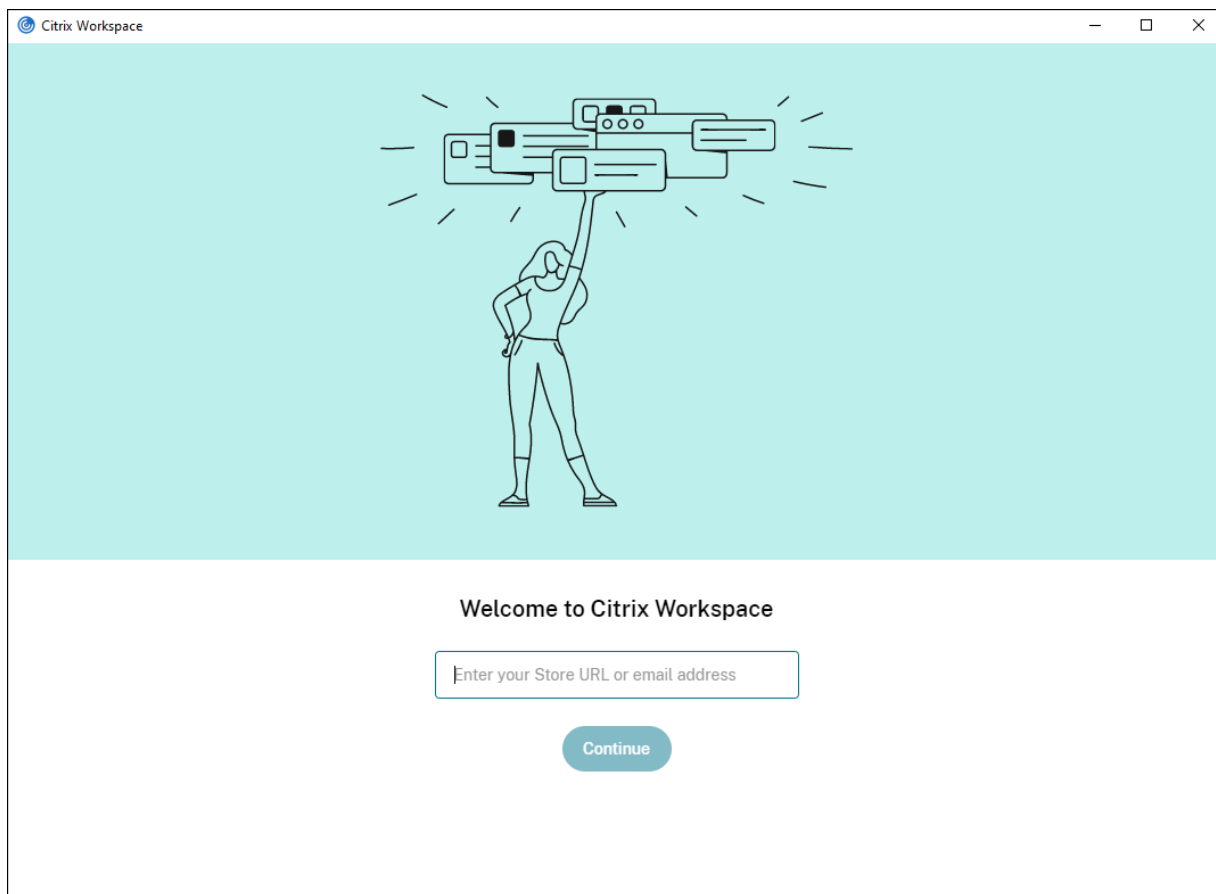
### **Store-URL zur Citrix Workspace-App hinzufügen**

Sie können Benutzern wie folgt die Kontoinformationen mitteilen, die sie zum Zugriff auf die virtuellen Anwendungen und Desktops benötigen:

- Benutzerseitige manuelle Eingabe der bereitgestellten Informationen
- Konfigurieren der e-mail-basierten Kontenermittlung
- Hinzufügen von Stores über die Befehlszeilenschnittstelle
- Provisioningdatei
- Verwenden der administrativen Gruppenrichtlinienobjektvorlage

### **Bereitstellen der manuell einzugebenden Kontoinformationen für Benutzer**

Nach der erfolgreichen Installation der Citrix Workspace-App wird der folgende Bildschirm angezeigt. Die Benutzer müssen eine E-Mail- oder Serveradresse eingeben, um auf die Apps und Desktops zugreifen zu können. Wenn ein Benutzer Angaben für ein neues Konto macht, versucht die Citrix Workspace-App, die Verbindung zu überprüfen. Im Erfolgsfall fordert die Citrix Workspace-App den Benutzer auf, sich bei dem Konto anzumelden.



Stellen Sie sicher, dass Benutzer die nötigen Informationen zum Verbinden mit ihren virtuellen Desktops und Anwendungen haben, damit sie Konten manuell erstellen können.

- Um eine Verbindung zu einem Workspace-Store herzustellen, geben Sie die Workspace-URL an.
- Zum Verbinden mit einem StoreFront-Store teilen Sie Benutzern die URL für den betreffenden Server mit. Beispiel:<https://servername.company.com>.
- Für Verbindungen über Citrix Gateway legen Sie fest, ob Benutzer alle konfigurierten Stores sehen müssen oder nur den Store, für den der Remotezugriff auf ein bestimmtes Citrix Gateway aktiviert ist.
  - Anzeigen aller konfigurierten Stores: Teilen Sie den Benutzern den FQDN für Citrix Gateway mit.
  - Beschränken des Zugriffs auf einen bestimmten Store: Teilen Sie den Benutzern den FQDN für Citrix Gateway und den Storenamen wie folgt mit:

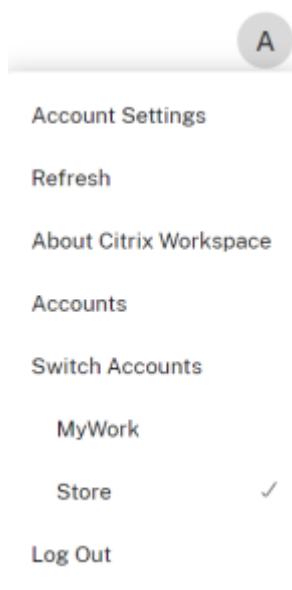
**CitrixGatewayFQDN?MyStoreName:**

Wenn z. B. für den Store “SalesApps” der Remotezugriff auf server1.com aktiviert ist und für den Store **HRApps** der Remotezugriff auf server2.com, dann muss ein Benutzer Folgendes eingeben:

- \* server1.com?SalesApps für den Zugriff auf SalesApps oder
- \* server2.com?HRApps für den Zugriff auf **HRApps**.

Für das Feature **CitrixGatewayFQDN?MyStoreName** muss ein neuer Benutzer ein Konto erstellen, indem er eine URL eingibt. Die e-mail-basierte Kontenermittlung ist nicht verfügbar.

Wenn die Citrix Workspace-App mit der Store-URL konfiguriert ist, kann das Konto über die Option **Konten** im Profilmenu verwaltet werden.



Wenn auf Clientmaschinen, die für die Proxyauthentifizierung konfiguriert sind, die Proxylanmeldeinformationen nicht in der **Windows-Anmeldeinformationsverwaltung** gespeichert sind, werden Sie aufgefordert, die Proxylanmeldeinformationen einzugeben. Die Citrix Workspace-App speichert dann die Anmeldeinformationen des Proxyservers in der **Windows-Anmeldeinformationsverwaltung**. Dies führt zu einer nahtlosen Anmeldeerfahrung, da Sie Ihre Anmeldeinformationen vor dem Zugriff auf die Citrix Workspace-App nicht manuell in der **Windows-Anmeldeinformationsverwaltung** speichern müssen.

### **Konfigurieren der e-mail-basierten Kontenermittlung**

Wenn Sie die Citrix Workspace-App für die e-mail-basierte Kontenermittlung konfigurieren, geben Benutzer ihre E-Mail-Adresse statt einer Server-URL während der Erstinstallation und -konfiguration der Citrix Workspace-App ein. Die Citrix Workspace-App ermittelt das Gerät (Citrix Gateway oder StoreFront-Server), das der E-Mail-Adresse auf der Basis von DNS-Dienst Datensätzen zugeordnet ist. Die App fordert den Benutzer dann zur Anmeldung auf, um auf virtuelle Desktops und Anwendungen zuzugreifen.

Informationen zum Konfigurieren der e-Mail-basierten Kontenermittlung für Citrix Workspace-Stores finden Sie unter [Getting started](#) in der Dokumentation zum Global App Configuration Service. Informationen zum Konfigurieren der e-Mail-basierten Kontenermittlung für Citrix StoreFront- oder Citrix Gateway-Stores finden Sie unter [Configuring email-based account discovery](#).

### **Hinzufügen von Stores über die Befehlszeilenschnittstelle**

Installieren Sie die Citrix Workspace-App für Windows als Administrator an der Befehlszeilenschnittstelle.

Weitere Informationen finden Sie unter der [Liste der Befehlszeilenparameter](#).

### **Bereitstellen von Provisioningdateien für Benutzer**

StoreFront bietet Provisioningdateien, die Benutzer für eine Verbindung mit Stores öffnen können.

Sie können mit StoreFront Provisioningdateien erstellen, die Verbindungsdetails für Konten enthalten. Stellen Sie diese Dateien den Benutzern zur Verfügung, um eine automatische Konfiguration der Citrix Workspace-App zu ermöglichen. Nach der Installation der Citrix Workspace-App öffnen Benutzer einfach die Datei, um die App zu konfigurieren. Wenn Sie Workspace für Web konfigurieren, können Benutzer auch Provisioningdateien für die Citrix Workspace-App von den Sites abrufen.

Weitere Informationen finden Sie unter [Exportieren der Store-Provisioningdateien für Benutzer](#) in der StoreFront-Dokumentation.

**Verwenden der administrativen Gruppenrichtlinienobjektvorlage** Hinzufügen oder Festlegen eines Citrix StoreFront oder Gateways mit der administrativen Gruppenrichtlinienobjektvorlage:

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** > **Klassische administrative Vorlagen (ADM)** > **Citrix Komponenten** > **Citrix Workspace** > **StoreFront**.
3. Wählen Sie **Citrix Gateway-URL\StoreFront-Kontenliste**.
4. Wählen Sie **Aktiviert** und klicken Sie auf **Anzeigen**. Wenn Sie diese Richtlinieneinstellung aktivieren, können Sie eine Liste mit StoreFront-Konten und einer NetScaler Gateway-URL eingeben.
5. Geben Sie die URL in das Feld **Wert** ein.

6. Geben Sie die Store-URL an, die mit der Citrix Workspace-App verwendet wird:

```
STOREx="storename;http[s]://servername.domain/IISLocation/discovery  
;[On, Off]; [storedescription]"
```

Werte:

- x –Ganzzahlen von 0 bis 9 werden verwendet, um einen Store zu identifizieren.
- storename –Name des Stores. Dieser Wert muss mit dem auf dem StoreFront-Server konfigurierten Namen übereinstimmen.
- servername.domain –Der vollqualifizierte Domänenname des Servers, der den Store hostet.
- IISLocation –Der Pfad zum Store in IIS. Die Store-URL muss mit der URL in der StoreFront-Provisioningdatei übereinstimmen. Die Store-URL hat das folgende Format: /Citrix/store/discovery. Um die URL zu erhalten, exportieren Sie eine Provisioningdatei von StoreFront, öffnen Sie die Datei im Editor und kopieren Sie die URL aus dem Element Address.
- [On, Off] - Die Option Off ermöglicht die Bereitstellung deaktivierter Stores. So können Benutzer entscheiden, ob sie darauf zugreifen. Wenn der Status des Stores nicht angegeben ist, ist die Standardeinstellung On.
- storedescription –Eine Beschreibung des Stores, z. B. HR App Store.

7. Fügen Sie die Citrix Gateway-URL hinzu oder geben Sie sie ein. Geben Sie den Namen der URL durch Semikolon getrennt ein:

Beispiel:      `STORE0= HRStore;https://ag.mycompany.com#Storename;On;Store`

Wobei "#Store name" der Name des Stores, hinter dem Citrix Gateway ist.

#### Hinweis:

- Die Citrix Gateway-Store-URL muss an erster Stelle in der Liste stehen (Parameter STORE0).
- Bei einem Setup mit mehreren Stores ist nur eine Citrix Gateway-Store-URL-Konfiguration zulässig.
- Die mit dieser Methode konfigurierte Citrix Gateway Store-URL unterstützt keine PNA-Dienste-Sites, die Citrix Gateway verwenden.
- Der Parameter /Discovery ist nicht erforderlich, wenn Sie eine Citrix Gateway-Store-URL angeben.

Ab Version 1808 werden alle Änderungen an der Richtlinie Citrix Gateway-URL/StoreFront-Kontenliste nach dem Neustart der App in einer Sitzung angewendet. Ein Zurücksetzen ist nicht erforderlich.

**Hinweis:**

Bei der Neuinstallation der Citrix Workspace-App Version 1808 und höher ist ein Zurücksetzen nicht erforderlich. Bei Upgrades auf Version 1808 oder höher müssen Sie die Citrix Workspace-App zurücksetzen, damit die Änderungen wirksam werden.

**Einschränkungen:**

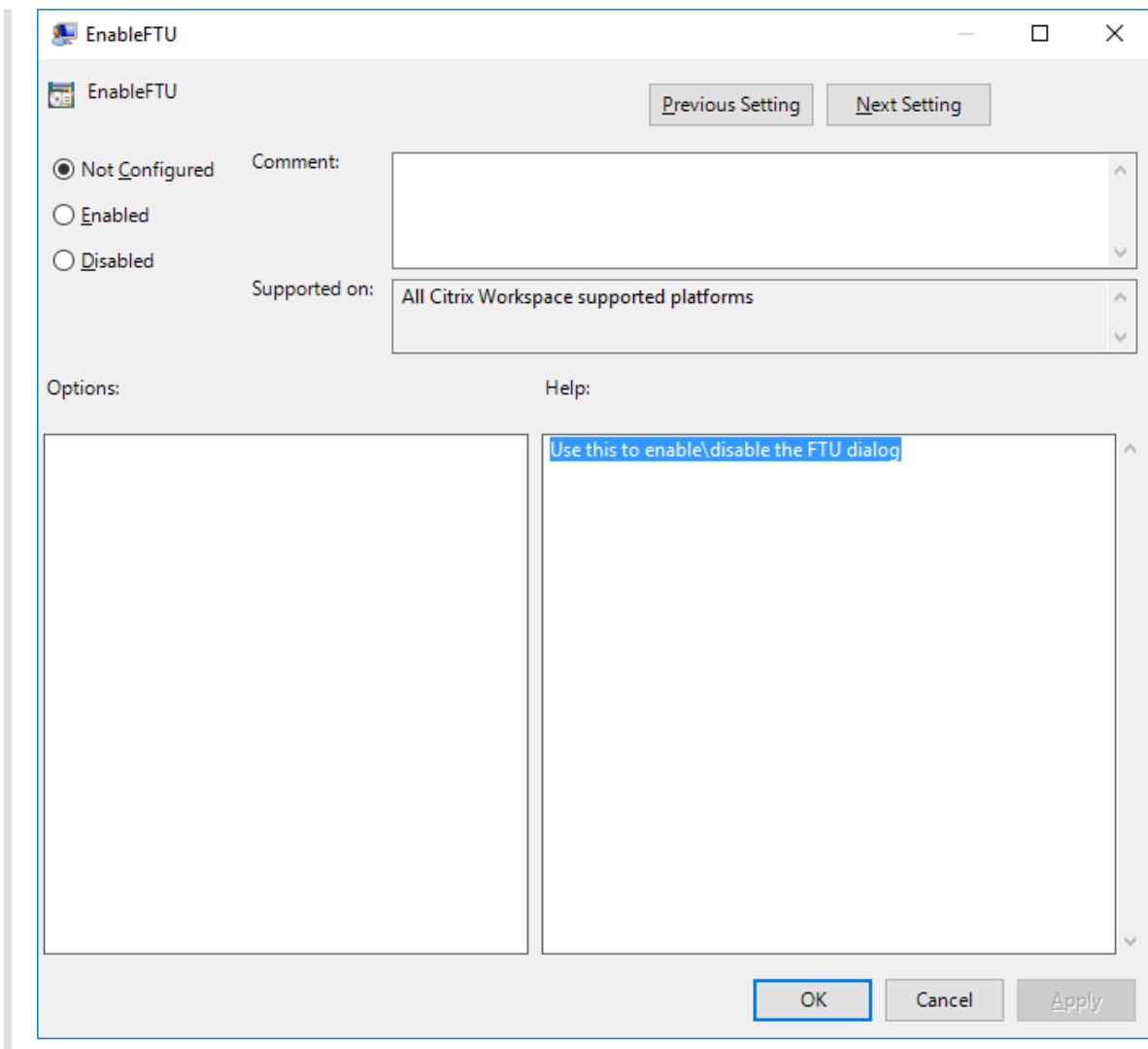
- Die Citrix Gateway-URL muss als Erste aufgeführt werden, gefolgt von den StoreFront-URLs.
- Mehrere Citrix Gateway-URLs werden nicht unterstützt.

**Hinweis:**

Benutzer können auch über einen Webbrowser auf den Store zugreifen. Benutzer können sich über einen Webbrowser beim Citrix Store anmelden und eine virtuelle App oder einen virtuellen Desktop starten. Beim Start der virtuellen App oder des virtuellen Desktops werden die Funktionen der nativ installierten Citrix Workspace-App genutzt.

In diesem Fall sollte die Aufforderung zum **Konto hinzufügen** vor Benutzern verborgen werden. Dies kann mit der folgenden Einstellung erreicht werden:

- **Umbenennen der ausführbaren Citrix Datei:** Benennen Sie die Datei **CitrixWorkspaceApp.exe** in **CitrixWorkspaceAppWeb.exe** um, um das Verhalten des Dialogfelds **Konto hinzufügen** zu ändern. Durch Umbenennen der Datei wird das Dialogfeld **Konto hinzufügen** nicht im **Startmenü** angezeigt.
- **Administrative Gruppenrichtlinienobjektvorlage:** Zum Ausblenden der Option **Konto hinzufügen** im Installationsassistenten der Citrix Workspace-App deaktivieren Sie **EnableFTUpolicy** im Knoten "Self-Service" in der lokalen administrativen Gruppenrichtlinienobjektvorlage (siehe unten). Diese Einstellung gilt pro Maschine, daher ist das Verhalten für alle Benutzer gleich.



## Domain Name Service-Namensauflösung

Wenn die Citrix Workspace-App für Windows den Citrix XML-Dienst verwendet, kann sie einen DNS-Namen anstatt der IP-Adresse eines Servers anfordern.

### Wichtig:

Wenn Ihre DNS-Umgebung nicht speziell für die Verwendung dieser Funktion konfiguriert ist, empfiehlt Citrix, die DNS-Namensauflösung auf dem Server nicht zu aktivieren.

Die DNS-Namensauflösung ist standardmäßig auf dem Server deaktiviert und in der Citrix Workspace-App aktiviert. Wenn die DNS-Namensauflösung auf dem Server deaktiviert ist, wird bei jeder Citrix Workspace-App-Anfrage nach einem DNS-Namen eine IP-Adresse ausgegeben. Die DNS-Namensauflösung muss nicht in der Citrix Workspace-App deaktiviert werden.

Deaktivieren der DNS-Namensauflösung für bestimmte Benutzergeräte:

Wenn Sie in der Serverbereitstellung die DNS-Namensauflösung verwenden und Probleme mit bestimmten Benutzergeräten haben, können Sie die DNS-Namensauflösung für diese Geräte deaktivieren.

**Achtung:**

Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie ein Backup der Registrierung, bevor Sie sie bearbeiten.

1. Fügen Sie eine Registrierungsschlüssel-Zeichenfolge **xmlAddressResolutionType** zu HKEY \\\_LOCAL\\_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing hinzu.
2. Setzen Sie den Wert auf **IPv4-Port**.
3. Wiederholen Sie diesen Vorgang für alle Benutzer der Benutzergeräte.

## Verbinden

Die Citrix Workspace-App bietet Benutzern sicheren Self-Service-Zugriff auf virtuelle Desktops und Anwendungen und bedarfsgesteuerten Zugriff auf Windows-, Web- und SaaS-Anwendungen (Software-as-a-Service). Der Benutzerzugriff wird über Citrix StoreFront oder mit Webinterface erstellte Legacywebseiten verwaltet.

### Herstellen einer Verbindung zu Ressourcen mit der Citrix Workspace-Benutzeroberfläche

Die Homepage der Citrix Workspace-App zeigt virtuelle Desktops und Anwendungen an, die Benutzern basierend auf deren Kontoeinstellungen (d. h. dem Server, mit dem sie eine Verbindung herstellen) und basierend auf den von Citrix Virtual Apps and Desktops- bzw. Citrix DaaS-Administratoren konfigurierten Einstellungen zur Verfügung stehen. Mit der Seite **Einstellungen > Konten** können Sie die URL eines StoreFront-Servers konfigurieren oder bei konfigurierter E-Mail-basierter Kontenermittlung die E-Mail-Adresse eingeben.

Wenn Sie die Verbindung zu einem Store hergestellt haben, zeigt Self-Service folgende Registerkarten an: **Favoriten**, **Desktops** und **Apps**. Um eine Sitzung zu starten, klicken Sie auf das entsprechende Symbol. Um ein Symbol zu **Favoriten** hinzuzufügen, klicken Sie auf das Symbol ... und wählen Sie **Zu Favoriten hinzufügen**.



## URL-Migration von StoreFront zu Workspace

Die URL-Migration von StoreFront zu Workspace ermöglicht es Ihnen, Endbenutzer nahtlos von einem StoreFront-Store zu einem Workspace-Store unter minimaler Benutzerinteraktion zu migrieren.

Angenommen, für alle Endbenutzer wurde ein StoreFront-Store `storefront.com` in der Citrix Workspace-App hinzugefügt. Als Administrator können Sie eine Zuordnung von StoreFront-URL zu Workspace-URL `{'storefront.com':'xyz.cloud.com'}` im Global App Configuration Service konfigurieren. Der Global App Config Service überträgt die Einstellung per Push auf alle Citrix Workspace-App-Instanzen auf verwalteten und nicht verwalteten Geräten, denen die StoreFront-URL `storefront.com` hinzugefügt wurde.

Sobald die Einstellung erkannt wird, fügt die Citrix Workspace-App die zugeordnete Workspace-URL `xyz.cloud.com` als einen weiteren Store hinzu. Wenn der Endbenutzer die Citrix Workspace-App startet, wird der Citrix Workspace-Store geöffnet. Der zuvor hinzugefügte StoreFront-Store `storefront.com` bleibt der Citrix Workspace-App hinzugefügt. Benutzer können mit der Option **Konten wechseln** in der Citrix Workspace-App immer wieder zum StoreFront-Store `storefront.com` wechseln. Administratoren können festlegen, wann der StoreFront-Store `storefront.com` aus der Citrix Workspace-App auf Endpunkten der Benutzer entfernt werden soll. Das Entfernen kann über den Global App Config Service erfolgen.

Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Konfigurieren Sie die StoreFront-zu-Workspace-Zuordnung mit dem Global App Config Service. Weitere Informationen zum Global App Config Service finden Sie unter [Global App Configuration Service](#).
2. Bearbeiten Sie die Nutzlast im App Config Service:

```
1 {
2
3   "serviceURL": {
4
5     "url": "https://storefront.acme.com:443",
6     "migrationUrl": [
7       {
8
9         "url": "https://sampleworkspace.cloud.com:443",
10        "storeFrontValidUntil": "2023-05-01"
11      }
12    ]
13  ]
14 }
15 ,
16 "settings": {
17
18   "name": "Productivity Apps",
19   "description": "Provides access StoreFront to Workspace Migration"
20 }
```

```
20 "useForAppConfig": true,  
21 "appSettings": {  
22  
23   "windows": [  
24     {  
25  
26       "category": "root",  
27       "userOverride": false,  
28       "assignmentPriority": 0,  
29       "assignedTo": [  
30         "AllUsersNoAuthentication"  
31       ],  
32       "settings": [  
33         {  
34  
35           "name": "Hide advanced preferences",  
36           "value": false  
37         }  
38  
39       ]  
40     }  
41  
42   ]  
43 }  
44 }  
45 }  
46 }  
47 }  
48  
49  
50 <!--NeedCopy-->
```

**Hinweis:**

Wenn Sie die Nutzlast zum ersten Mal konfigurieren, verwenden Sie **POST**.

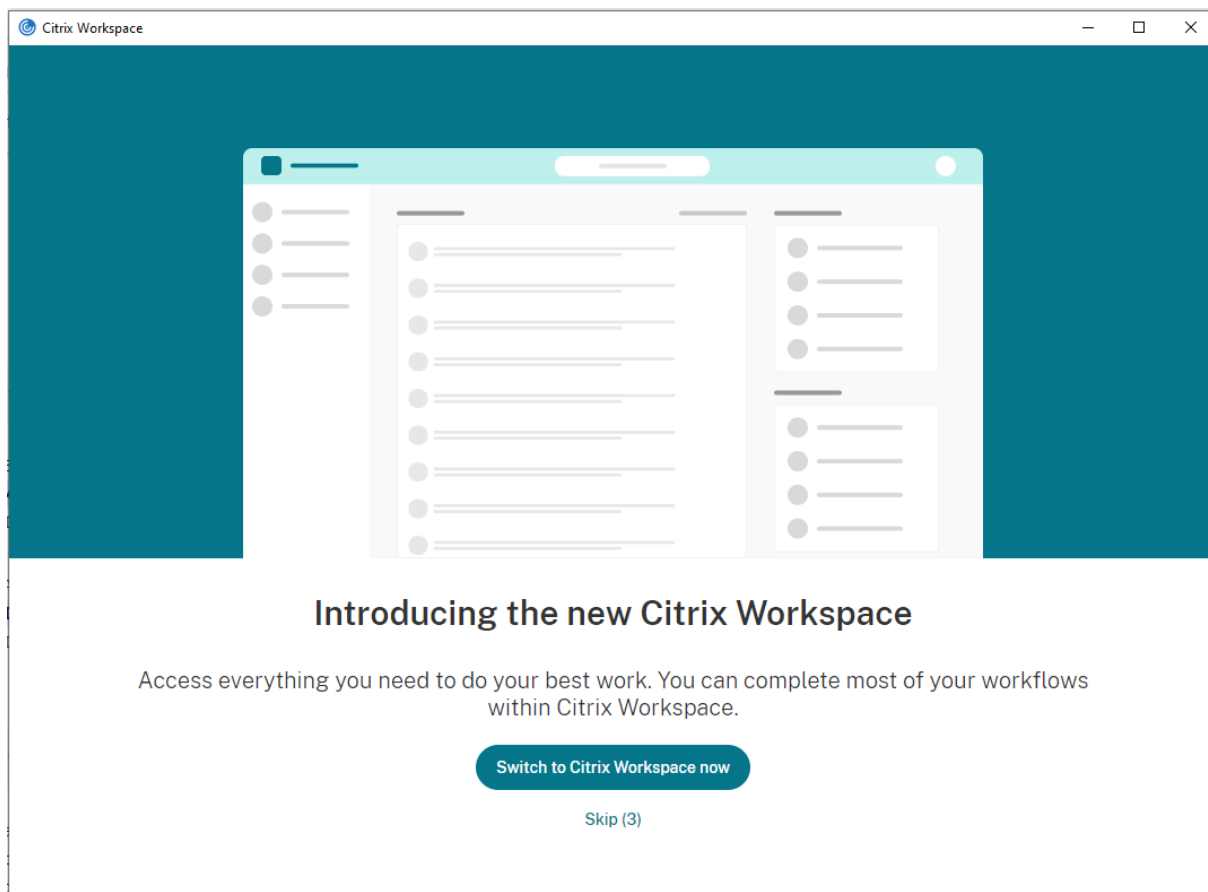
Wenn Sie eine Nutzlastkonfiguration bearbeiten, verwenden Sie **PUT** und stellen Sie sicher, dass Sie die Nutzlast aus allen unterstützten Einstellungen haben.

3. Geben Sie die StoreFront-URL `storefront.com` als Wert für **URL** im Abschnitt **serviceURL** an.
4. Konfigurieren Sie die Workspace-URL `xyz.cloud.com` im Abschnitt **migrationUrl**.
5. Legen Sie mit **storeFrontValidUntil** den Zeitplan für das Entfernen des StoreFront-Stores aus der Citrix Workspace-App fest. Dieses Feld ist optional. Sie können den folgenden Wert entsprechend Ihren Anforderungen festlegen:
  - Gültiges Datum im Format (JJJJ-MM-TT)

**Hinweis:**

Wenn das angegebene Datum in der Vergangenheit liegt, wird der StoreFront-Store bei der URL-Migration sofort entfernt. Wenn das angegebene Datum in der Zukunft liegt, wird der StoreFront-Store zum festgelegten Zeitpunkt entfernt.

Sobald die App Config Service-Einstellungen per Push übertragen werden, wird der folgende Bildschirm angezeigt:



Wenn der Benutzer auf **Jetzt zu Citrix Workspace wechseln** klickt, wird die Workspace-URL der Citrix Workspace-App hinzugefügt und die Authentifizierungsaufforderung wird angezeigt. Benutzer haben eine beschränkte Möglichkeit, den Übergang bis zu drei Mal zu verschieben.

### **Unterstützung für Discovery lokaler Apps in der Citrix Workspace-App**

Ab Release 2112.1 können Administratoren die Discovery und Enumeration lokal installierter Anwendungen in der Citrix Workspace-App konfigurieren. Sie können dieses Feature mit dem Global App Configuration Service konfigurieren. Weitere Informationen zum Konfigurieren dieses Features finden Sie unter [Global App Configuration Service](#).

Diese Funktion ist ideal für Geräte, die im Kioskmodus ausgeführt werden, und für Anwendungen, die nicht innerhalb des Citrix Workspace virtualisiert werden können.

## Updates und Plug-Ins verwalten

April 22, 2024

In diesem Abschnitt wird Folgendes beschrieben:

- [Updates](#)
- [Plug-Ins verwalten](#)

## Aktualisieren

April 22, 2024

### Manuelle Aktualisierung

Wenn Sie die Citrix Workspace-App für Windows bereits installiert haben, laden Sie die neueste Version der App von der [Citrix Downloadseite](#) herunter und installieren Sie sie. Informationen zur Installation finden Sie unter [Installation und Deinstallation](#).

### Automatisches Update

Wenn eine neue Version der Citrix Workspace-App verfügbar ist, sendet Citrix das Update an das System, auf dem die Citrix Workspace-App installiert ist.

#### Hinweis:

- Wenn Sie einen ausgehenden Proxy mit SSL-Interception konfiguriert haben, fügen Sie eine Ausnahme zum Workspace-Server für automatische Updates <https://downloadplugins.citrix.com/> hinzu, damit Sie Updates von Citrix erhalten.
- Automatische Updates sind für Versionen vor Citrix Workspace-App 2104 und Citrix Workspace-App 1912 LTSR CU4 nicht verfügbar.
- Ihr System muss über eine Internetverbindung verfügen, um Updates zu erhalten.
- Standardmäßig sind Citrix Workspace-Updates auf dem VDA deaktiviert. Dies umfasst RDS-

- Server mit mehreren Benutzern, VDI-Maschinen und Maschinen mit Remote-PC-Zugriff.
- Citrix Workspace-Updates sind auf Maschinen deaktiviert, auf denen Desktop Lock installiert ist.
  - Workspace für Web-Benutzer können die StoreFront-Richtlinie nicht automatisch herunterladen.
  - Citrix Workspace-Updates können auf LTSR-Updates beschränkt werden.
  - Citrix HDX RTME für Windows ist in Citrix Workspace-Updates enthalten. Sie erhalten eine Benachrichtigung, wenn HDX RTME-Updates für das LTSR und das aktuelle Release der Citrix Workspace-App verfügbar sind.
  - Ab Version 2105 haben die Citrix Workspace Update-Protokolle neue Pfade. Die Workspace Update-Protokolle sind in C:\Program Files(x86)\Citrix\Logs. Informationen zur Protokollierung finden unter [Protokollsammlung](#).
  - Nicht-Administratoren können die Citrix Workspace-App auf einer vom Administrator installierten Instanz aktualisieren. Klicken Sie dazu im Infobereich mit der rechten Maustaste auf das Symbol der Citrix Workspace-App und wählen Sie **Nach Updates suchen**. Die Option **Nach Updates suchen** ist auf vom Benutzer oder vom Administrator installierten Instanzen der Citrix Workspace-App verfügbar.
  - Sie können auch automatische Updates durchführen, wenn die automatische Proxykonfiguration (PAC) und die Erkennung des Web Proxy Auto-Discovery Protocols (WPAD) aktiviert sind. Dies wird nicht unterstützt, wenn Anmeldeinformationen für die Authentifizierung des Proxys erforderlich sind.
  - Wenn die Verschlüsselungssammlung ohne ECDHE hinzugefügt wird, kann Citrix Workspace den Citrix-Server für automatische Updates nicht erreichen und die folgende Fehlermeldung wird während des automatischen Updates angezeigt:

#### **Keine Verbindung zum Server möglich**

Starten Sie die Citrix Workspace-App für Windows nach einem manuellen oder automatischen Update neu.

Sie können die aktuelle Version der auf Ihrem Gerät installierten Citrix Workspace-App über **Erweiterte Einstellungen** überprüfen oder **DisplayVersion** in der Registrierung unter `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\CitrixOnlinePluginPackWeb` abfragen.

Version in **Erweiterte Einstellungen** anzeigen:

1. Klicken Sie mit der rechten Maustaste im Infobereich auf das Citrix Workspace-App-Symbol.
2. Wählen Sie **Erweiterte Einstellungen**.

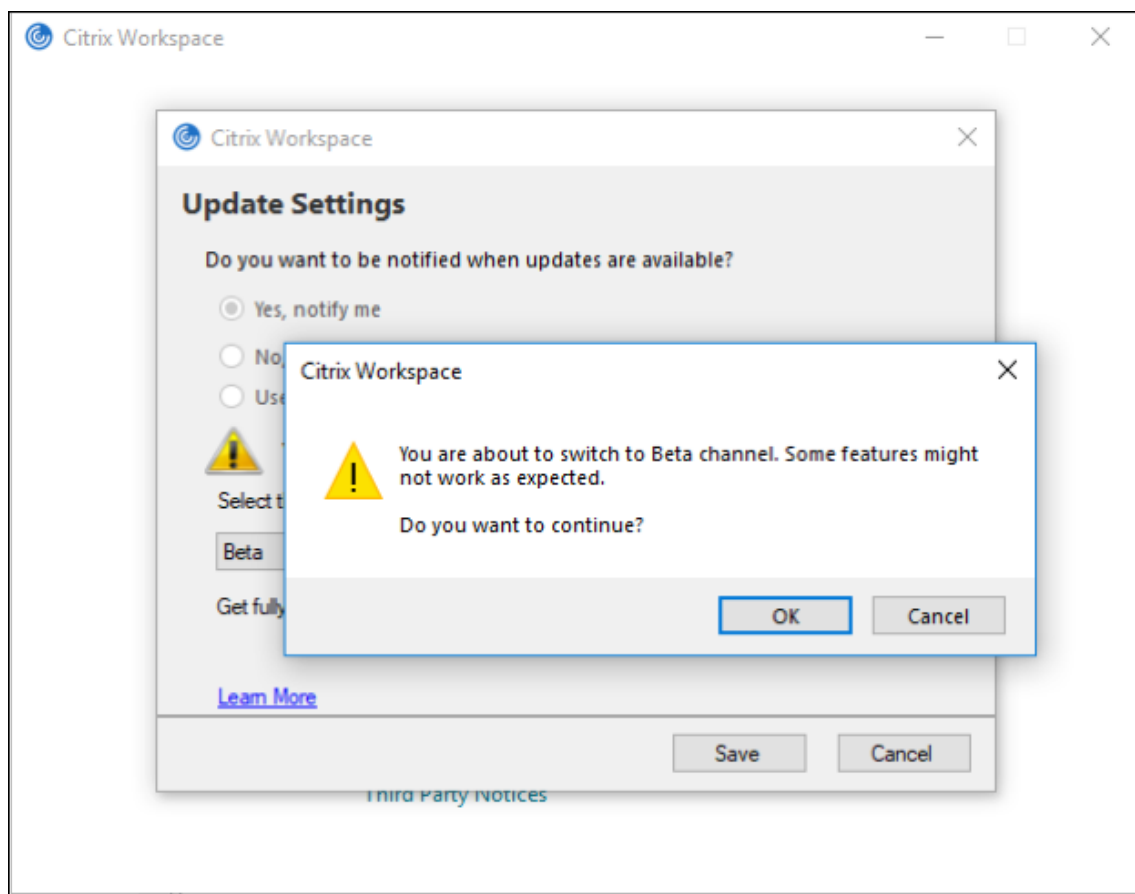
Die Version der Citrix Workspace-App wird im Abschnitt **Info** angezeigt.

### Installieren des Beta-Programms für die Citrix Workspace-App

Sie erhalten eine Updatebenachrichtigung, wenn die Citrix Workspace-App für automatische Updates konfiguriert ist. Führen Sie die folgenden Schritte aus, um den Beta Build auf Ihrem System zu installieren:

1. Öffnen Sie die Citrix Workspace-App über den Infobereich.
2. Navigieren Sie zu **Erweiterte Einstellungen > Citrix Workspace-Updates**.
3. Wählen Sie **Beta** aus der Dropdownliste aus, wenn der Beta Build verfügbar ist, und klicken Sie auf **Speichern**.

Ein Benachrichtigungsfenster wird angezeigt.



4. Klicken Sie auf **OK**, um das Update auf den Beta Build durchzuführen.

Um von einem Beta Build zu einem Releasebuild zu wechseln, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Citrix Workspace-App über den Infobereich.
2. Navigieren Sie zu **Erweiterte Einstellungen > Citrix Workspace-Updates**.

3. Wählen Sie im Bildschirm **Aktualisierungseinstellungen** in der Dropdownliste “Updatekanal” die Option **Release** aus und klicken Sie auf **Speichern**.

**Hinweis:**

- Wenn neue Updates verfügbar sind, wird eine Benachrichtigung zu automatischen Updates angezeigt.
- Kunden können Beta Builds in ihren Umgebungen zu testen, die nicht oder nur eingeschränkt zur Produktion verwendet werden, und Feedback hierzu geben. Citrix akzeptiert keine Supportanfragen für Beta Builds, begrüßt jedoch [Feedback](#) zur Verbesserung der Builds. Basierend auf Schweregrad, Kritikalität und Wichtigkeit behält sich Citrix eine Reaktion auf das Feedback vor. Es wird empfohlen, Beta Builds nicht in Produktionsumgebungen bereitzustellen.

### **Unterstützung der automatischen Aktualisierung der Citrix Workspace-App auf dem VDA**

Ab Version 2209 der Citrix Workspace-App für Windows können Sie die automatische Aktualisierungsfunktion auf dem VDA aktivieren. Zum Aktivieren dieses Features müssen Sie den folgenden Registrierungswert erstellen:

Auf 32-Bit-Maschinen:

- Registrierungsschlüssel: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- Registrierungswert: AllowAutoUpdateOnVDA
- Registrierungstyp: REG\_SZ
- Registrierungsdaten: True

Auf 64-Bit-Maschinen:

- Registrierungsschlüssel: HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- Registrierungswert: AllowAutoUpdateOnVDA
- Registrierungstyp: REG\_SZ
- Registrierungsdaten: True

### **Versionssteuerung für automatische Updates**

Administratoren können jetzt angeben, auf welche Version Geräte in der Organisation automatisch aktualisiert werden sollen.

Hierfür legen sie im Global App Config Service in der Eigenschaft “maximumAllowedVersion” die Version fest.

Beispiel für eine JSON-Datei im Global App Config Service:

```
1 {
2
3   "category": "AutoUpdate",
4   "userOverride": false,
5   "assignedTo": [
6     "AllUsersNoAuthentication"
7   ],
8   "settings": [
9     {
10
11       "name": "Auto Update plugins settings",
12       "value": [
13         {
14
15           "pluginSettings": {
16
17             "upgradeToLatest": false,
18             "deploymentMode": "InstallAndUpdate",
19             "stream": "Current",
20             "maximumAllowedVersion": "23.03.0.49",
21             "minimumAllowedVersion": "0.0.0.0",
22             "delayGroup": "Fast"
23           }
24         ,
25           "pluginName": "WorkspaceApp",
26           "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
27         }
28       ]
29     }
30   ]
31 }
32 ]
33 }
34
35
36 <!--NeedCopy-->
```

Wenn die Version festgelegt wurde, wird die Citrix Workspace-App auf dem Benutzergerät automatisch auf die Version aktualisiert, die in der Eigenschaft “maximumAllowedVersion” angegeben ist.

#### Hinweise:

- Derzeit sind alle in der vorherigen JSON-Datei genannten Parameter obligatorisch. Für die Einstellung `upgradeToLatest` und die Einstellung `maximumAllowedVersion` müssen Sie Werte gemäß den Anforderungen Ihrer Organisation angeben. Für die übrigen Parameter können Sie Werte verwenden, die der JSON-Beispieldatei ähneln.
- Um die Versionssteuerung für automatische Updates zu aktivieren, muss die Einstellung `upgradeToLatest` im Global App Config Service auf “false” gesetzt sein. Bei der Einstellung “true” wird `maximumAllowedVersion` ignoriert.



- Ändern Sie “pluginId” nicht, da dieser Wert der Citrix Workspace-App zugeordnet ist.
- Wenn die Version nicht im Global App Config Service konfiguriert ist, wird die Citrix Workspace-App standardmäßig auf die neueste verfügbare Version aktualisiert.

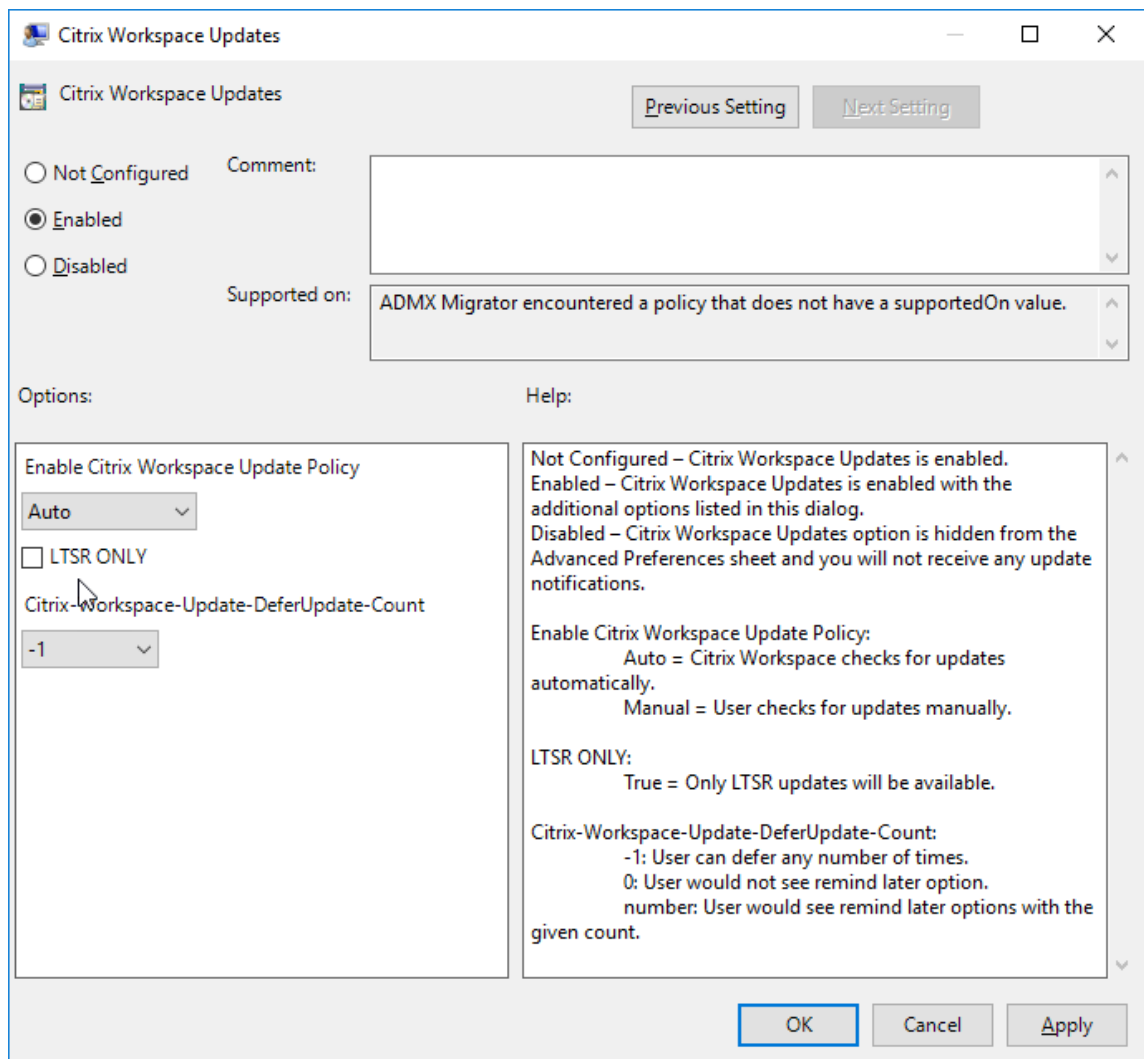
## **Erweiterte Konfiguration für automatische Updates (Citrix Workspace-Updates)**

Sie können Citrix Workspace-Updates mit den folgenden Methoden konfigurieren:

1. Administrative Gruppenrichtlinienobjektvorlage
2. Global App Configuration Service (GACS)
3. Befehlszeilenoberfläche
4. Grafische Benutzeroberfläche (GUI)
5. StoreFront

### **Konfigurieren von Citrix Workspace-Updates mit der administrativen Gruppenrichtlinienobjektvorlage**

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc und navigieren Sie zum Knoten “Computerkonfiguration”.
2. Gehen Sie zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Workspace-Updates**.



3. **Updates aktivieren oder deaktivieren:** Wählen Sie **Aktiviert** oder **Deaktiviert** aus, um Workspace-Updates zu aktivieren oder zu deaktivieren.

**Hinweis:**

Wenn Sie **Deaktiviert** auswählen, werden Sie nicht über neue Updates informiert. Durch die Option **Deaktiviert** wird auch die Option für Workspace-Updates auf der Seite “Erweiterte Einstellungen” ausgeblendet.

4. **Updatebenachrichtigung:** Wenn ein Update verfügbar ist, können Sie wählen, ob Sie automatisch benachrichtigt werden möchten oder manuell danach suchen. Nachdem Sie Workspace-Updates aktiviert haben, wählen Sie eine der folgenden Optionen aus der Dropdownliste **Citrix Workspace-Updaterichtlinie aktivieren:**

- **Auto:** Sie werden benachrichtigt, wenn ein Update zur Verfügung steht (Standardeinstellung). Dies gilt nur für Versionen vor Citrix Workspace-App 2207. In 2207 oder späteren

Versionen erfolgt das Update der Citrix Workspace-App automatisch und Sie werden nicht benachrichtigt, wenn ein Update verfügbar ist.

- **Manual:** Sie werden nicht benachrichtigt, wenn ein Update verfügbar ist. Suchen Sie manuell nach Updates.

5. Aktivieren Sie **Nur LTSR**, um Updates nur für LTSR zu erhalten.

6. Wählen Sie in der Dropdownliste **Citrix-Workspace-Update-DeferUpdate-Count** einen Wert zwischen -1 und 30:

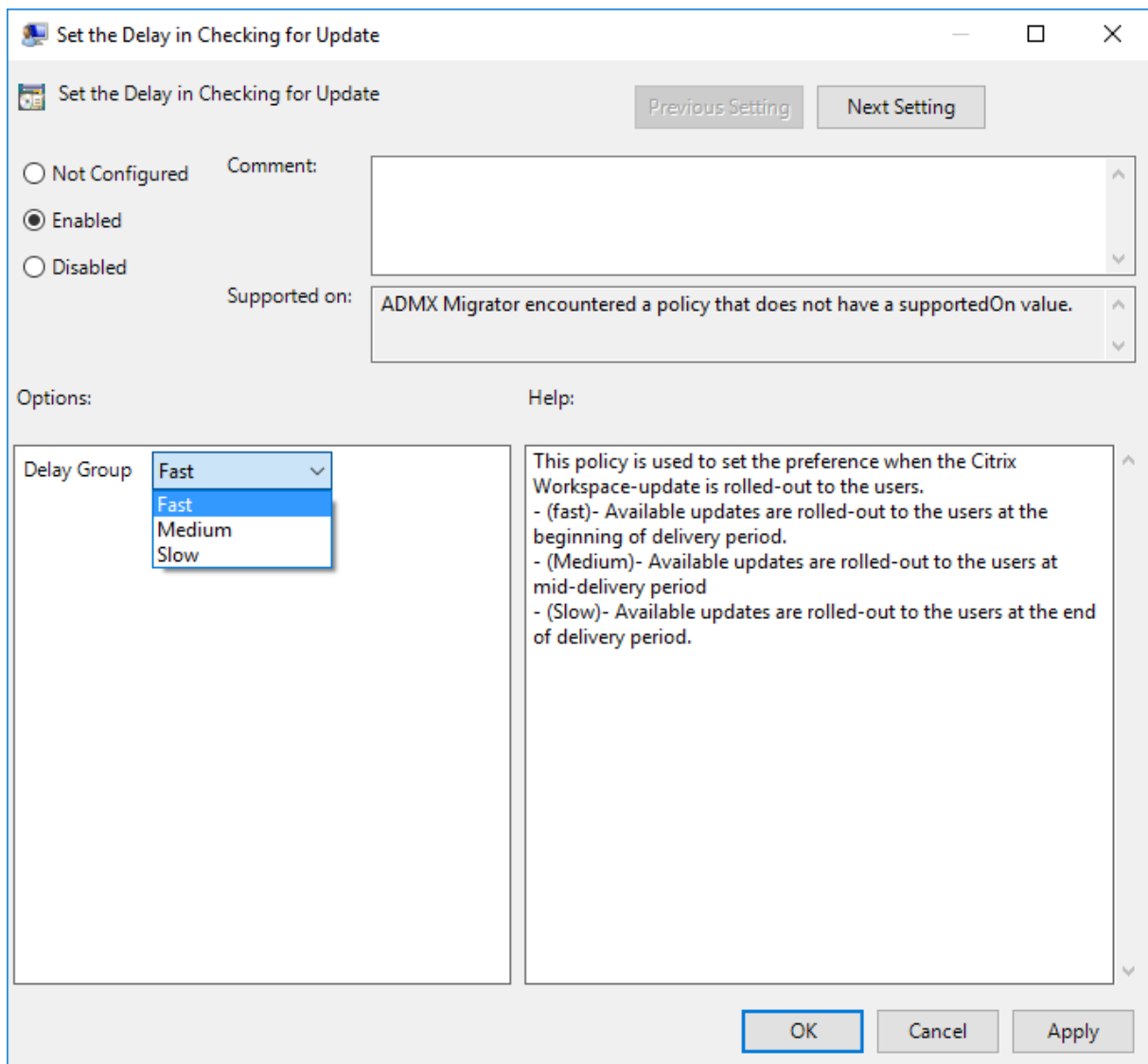
- Beim Wert 0 wird die Option **Später erinnern** nicht angezeigt. Die Eingabeaufforderung **Update verfügbar** wird angezeigt, wenn bei der automatischen Suche ein Update gefunden wird.
- Beim Wert -1 wird die Option **Später erinnern** mit der Eingabeaufforderung **Update verfügbar** angezeigt. Sie können die Update-Benachrichtigung beliebig oft verschieben.
- Der gewählte Wert (1-30) legt fest, wie oft die Option **Später erinnern** mit der Aufforderung **Update verfügbar** angezeigt werden muss. Sie können die Updatebenachrichtigung gemäß dem in diesem Feld definierten Wert verschieben. Die Aufforderung **Update verfügbar** wird zwar weiterhin angezeigt, jedoch ohne die Option **Später erinnern**.

#### Hinweis:

Ab Version 2207 der Citrix Workspace-App für Windows ist das Feature für automatische Updates verbessert und das Feld **Citrix-Workspace-Update-DeferUpdate-Count** ist nicht erforderlich.

**Konfigurieren der Verzögerung bei der Suche nach Updates** Wenn eine neue Version der Citrix Workspace-App verfügbar ist, stellt Citrix das Update während eines bestimmten Bereitstellungszeitraums bereit. Mit dieser Eigenschaft können Sie steuern, in welcher Phase des Bereitstellungszeitraums Sie das Update erhalten.

Führen Sie zum Konfigurieren des Bereitstellungszeitraums `gpedit.msc` aus, um die administrative Vorlage für Gruppenrichtlinienobjekte zu starten. Navigieren Sie unter **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Verzögerung für Prüfung auf Updates festlegen**.



Wählen Sie **Aktiviert** und anschließend in der Dropdownliste neben **Für Gruppe aufschieben** eine der folgenden Optionen:

- Fast –Das Rollout des Updates erfolgt zu Beginn des Bereitstellungszeitraums.
- Medium –Das Rollout des Updates erfolgt in der Mitte des Bereitstellungszeitraums.
- Slow –Das Rollout des Updates erfolgt am Ende des Bereitstellungszeitraums.

**Hinweis:**

Wenn Sie **Deaktiviert** auswählen, werden Sie nicht über verfügbare Updates informiert. Auch die Option für Workspace-Updates auf der Seite "Erweiterte Einstellungen" wird durch **Deaktiviert** ausgeblendet.

## Konfigurieren von Citrix Workspace-Updates über die Befehlszeilenschnittstelle

### Durch Angeben von Befehlszeilenparametern während der Installation der Citrix Workspace-App:

Sie können Workspace-Updates konfigurieren, indem Sie während der Installation der Citrix Workspace-App Befehlszeilenparameter angeben. Weitere Informationen finden Sie unter [Installationsparameter](#).

### Mit Befehlszeilenparametern nach der Installation der Citrix Workspace-App:

Citrix Workspace-Updates können auch nach der Installation der Citrix Workspace-App für Windows konfiguriert werden. Navigieren Sie mit der Windows-Befehlszeile zum Speicherort von `CitrixReceiverUpdater.exe`.

Normalerweise ist `CitrixReceiverUpdater.exe` unter `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver`. Sie können die Binärdatei `CitrixReceiverUpdater.exe` zusammen mit den im Abschnitt [Installationsparameter](#) aufgeführten Befehlszeilenparametern ausführen.

Zum Beispiel:

```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

#### Hinweis:

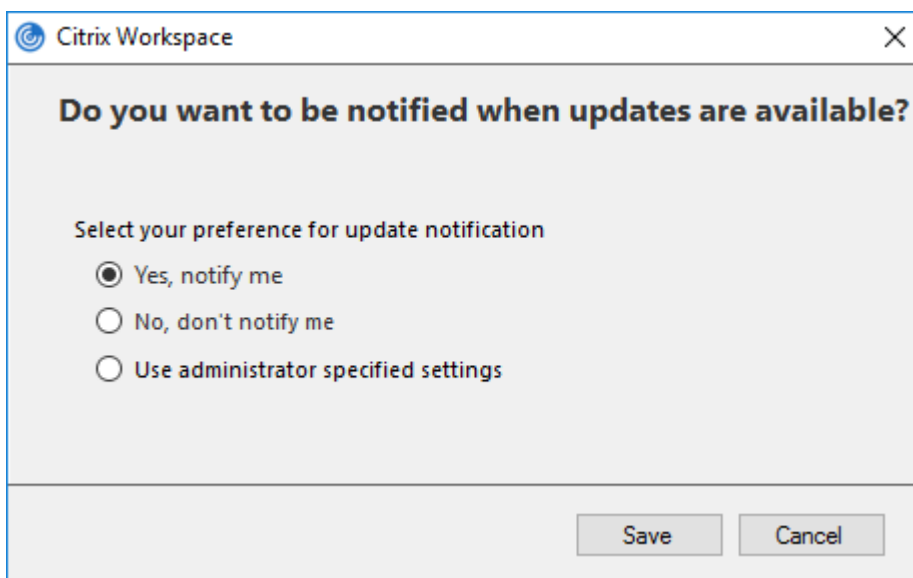
`/AutoUpdateCheck` ist ein obligatorischer Parameter, den Sie festlegen müssen, um andere Parameter wie `/AutoUpdateStream`, `/DeferUpdateCount` und `/AURolloutPriority` zu konfigurieren.

## Konfigurieren von Citrix Workspace-Updates über die grafische Benutzeroberfläche

Ein Benutzer kann die Einstellung für **Citrix Workspace-Updates** im Dialogfeld **Erweiterte Einstellungen** außer Kraft setzen. Diese Konfiguration gilt pro Benutzer und die Einstellungen werden nur für den aktuellen Benutzer angewendet.

1. Klicken Sie mit der rechten Maustaste im Infobereich auf das Citrix Workspace-App-Symbol.
2. Wählen Sie **Erweiterte Einstellungen > Citrix Workspace-Updates**.
3. Wählen Sie eine der folgenden Benachrichtigungseinstellungen:
  - Ja, benachrichtigen: Sie werden benachrichtigt, wenn ein Update für die Citrix Workspace-App verfügbar ist.
  - Nein, nicht benachrichtigen: Sie werden nicht benachrichtigt, wenn ein Update für die Citrix Workspace-App verfügbar ist. Suchen Sie manuell nach Updates.

- Vom Administrator festgelegte Einstellungen verwenden: Verwendet die auf dem StoreFront-Server konfigurierten Einstellungen.



4. Klicken Sie auf **Speichern**.

#### Hinweis:

- Die Optionen **Ja, benachrichtigen** und **Nein, nicht benachrichtigen** gelten nur für Versionen vor Citrix Workspace-App 2207. Ab Version 2207 erfolgt das Update der Citrix Workspace-App automatisch und Sie werden nicht benachrichtigt, wenn ein Update verfügbar ist. Wenn Sie die Option **Nein, nicht benachrichtigen** auswählen, suchen Sie manuell nach Updates.
- Sie können die über das Symbol der Citrix Workspace-App verfügbare Seite "Erweiterte Einstellungen" ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter [Erweiterte Einstellungen](#).

### Konfigurieren von Citrix Workspace-Updates mit StoreFront

1. Öffnen Sie die Datei `web.config` mit einem Text-Editor. Die Datei ist normalerweise im Verzeichnis `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Suchen Sie das Benutzerkonto-Element in der Datei. Der Kontoname Ihrer Bereitstellung ist "Store".

Beispiel: `<account id=... name="Store">`

Vor dem Tag `</account>` navigieren Sie zu den Eigenschaften des Benutzerkontos:

```
1 <properties>
2     <clear/>
```

```
3 </properties>
4 <!--NeedCopy-->
```

3. Fügen Sie das Tag für automatische Updates nach dem Tag `<clear />` ein.

```
1 <account>
2
3   <clear />
4
5   <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6     F84Store"
7     description="" published="true" updaterType="Citrix"
8     remoteAccessType="None">
9     <annotatedServices>
10
11       <clear />
12
13       <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15         <metadata>
16
17           <plugins>
18
19             <clear />
20
21           </plugins>
22
23           <trustSettings>
24
25             <clear />
26
27           </trustSettings>
28
29           <properties>
30
31             <property name="Auto-Update-Check" value="auto" />
32
33             <property name="Auto-Update-DeferUpdate-Count" value
34               ="1" />
35
36               <property name="Auto-Update-LTSR-Only" value
37                 ="FALSE" />
38
39                 <property name="Auto-Update-Rollout-Priority" value=
40                   "fast" />
41
42             </properties>
43
44           </metadata>
45
46         </annotatedServiceRecord>
```

```
44
45     </annotatedServices>
46
47     <metadata>
48
49         <plugins>
50
51             <clear />
52
53         </plugins>
54
55         <trustSettings>
56
57             <clear />
58
59         </trustSettings>
60
61         <properties>
62
63             <clear />
64
65         </properties>
66
67     </metadata>
68
69 </account>
70
71 <!--NeedCopy-->
```

Nachfolgend sind die Bedeutungen der Eigenschaften und ihre möglichen Werte aufgeführt:

- **Auto-update-Check:** Gibt an, dass die Citrix Workspace-App ein Update automatisch erkennt, wenn es verfügbar ist.
  - Auto (default): Überprüft und führt Aktualisierungen automatisch durch
  - Manual: Updates werden nur abgerufen, wenn Benutzer eine Anforderung über das Taskleistenmenü der Citrix Workspace-App stellt.
  - Disabled: Aktualisierungsprüfungen werden nicht durchgeführt.
- **Auto-update-LTSR-only:** Gibt an, dass das Update nur für LTSR gilt.
  - True —Der Updater ignoriert alle Updates, die nicht als gültig für LTSR markiert sind. Es werden nur LTSR-Updates berücksichtigt.
  - False (default) - Der Updater berücksichtigt nur Updates im aktuellen Stream.
- **Auto-update-Rollout-Priority:** Gibt den Bereitstellungszeitraum an, in dem Sie das Update erhalten können.
  - Fast: Das Rollout der Updates an die Benutzer erfolgt zu Beginn des Bereitstellungszeitraums.



- Medium: Das Rollout der Updates erfolgt in der Mitte des Bereitstellungszeitraums.
- Slow: Das Rollout der Updates erfolgt am Ende des Bereitstellungszeitraums.
- **Auto-update-DeferUpdate-Count:** Gibt an, wie oft Sie die Benachrichtigungen für die Updates ignorieren können.

**Hinweis:**

Diese Konfiguration gilt nur für interaktive Updates und nicht, wenn die automatische Aktualisierung aktiviert ist, da Benutzer keine Option zum Aufschieben der Updates erhalten.

- -1: Der Benutzer können die automatische Aktualisierung beliebig oft verschieben.
- 0: Benutzer bekommen die Option "Später erinnern" nicht angezeigt.
- Zahl: Benutzer bekommen die Optionen "Später erinnern" so oft angezeigt, wie durch die Zahl festgelegt wurde.

## Plug-Ins verwalten

April 22, 2024

Die Citrix Workspace-App für Windows bietet Plug-In-Verwaltungsfunktionen, mit der die Citrix Workspace-App als einzige Client-App auf dem Endpunkt erforderlich ist, um Agents wie Secure Access Agent und das EPA-Plug-In zu installieren und zu verwalten.

Mit diesen Funktionen können Administratoren erforderliche Agents über eine einzige Verwaltungskonsole mühelos bereitstellen und verwalten.

Die Plug-In-Verwaltung umfasst die folgenden Schritte:

- Administratoren müssen die auf den Endbenutzergeräten erforderlichen Agents im Global App Configuration Service angeben. Administratoren können den Secure Access Agent und den EPA-Agent angeben.
- Die Citrix Workspace-App ruft die Liste der Agents aus dem Global App Configuration Service ab.
- Basierend auf der vom Global App Configuration Service abgerufenen Liste lädt die Citrix Workspace-App die Agentpakete über den Dienst für automatische Updates herunter. Wenn der Agent nicht auf dem Endpunkt installiert ist, löst die Citrix Workspace-App die Installation des Agents aus. Wenn der Agent bereits installiert ist, löst die Citrix Workspace-App ein Update des Agents aus (wenn die Version des heruntergeladenen Agents höher ist als die installierte Version).

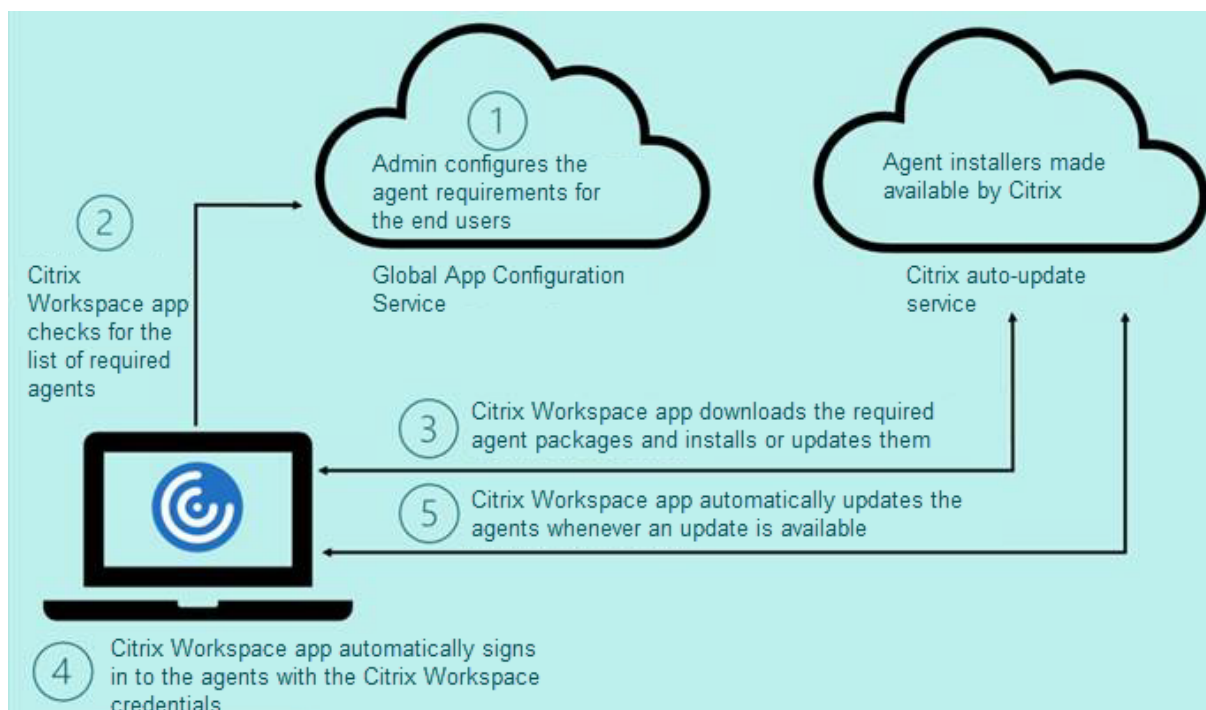
Die Citrix Workspace-App stellt sicher, dass die Agents in der Zukunft automatisch aktualisiert werden, sobald ein Update verfügbar ist.

Die Citrix Workspace-App meldet sich automatisch mit den Citrix Workspace-Anmeldeinformationen bei den Agents an.

**Hinweise:**

- Sind das EPA- und das ZTNA-Plug-In nicht vorhanden, werden sie beim ersten Hinzufügen des Stores oder Kontos heruntergeladen und installiert.
- Sind Store bzw. Konto und die Plug-Ins bereits vorhanden und das Installationsprogramm enthält eine höhere Version, werden die Plug-Ins beim automatischen Update aktualisiert.

Im folgenden Diagramm ist der Workflow dargestellt:



**Wichtig:**

Der Global App Configuration Service ist erforderlich, um die Plug-In-Verwaltung zu aktivieren.

- Bei Cloudstores kann im Bereich **Workspace-Konfiguration** des Citrix Cloud-Verwaltungsportals auf die Benutzeroberfläche des Global App Configuration Service zugegriffen werden. Weitere Informationen finden Sie unter [Citrix Workspace-App konfigurieren](#).
- Informationen zum Onboarding lokaler Stores und zum Einrichten der E-Mail-basierten Erkennung von Cloudstores finden Sie in der Dokumentation zum [Global App Configuration Service](#).

Sie können die Plug-In-Verwaltung mit den folgenden Methoden aktivieren:

- Verwenden der Benutzeroberfläche des Global App Configuration Service: Verwenden Sie diese Methode, um die neueste Version des Clients bereitzustellen.

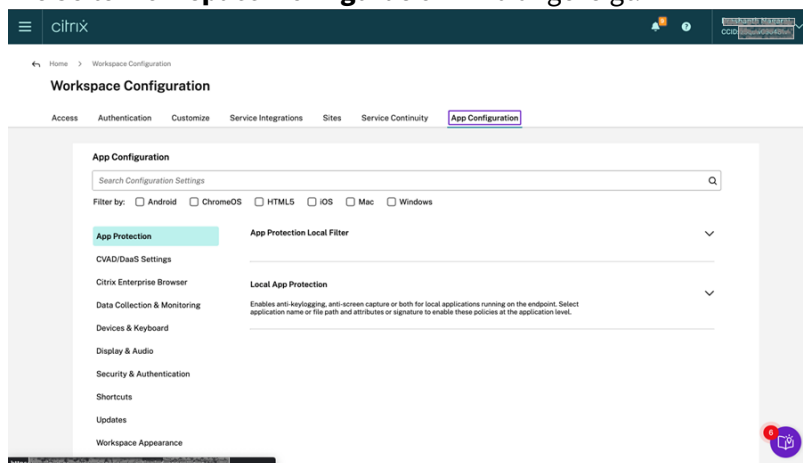
- Verwenden der Global App Configuration Service-API: Verwenden Sie diese Methode, um die Installation mit Parametern zur Steuerung der Version, der Bereitstellungsmodi, des Intervalls für automatischen Updates usw. anzupassen.

### Plug-In-Verwaltung mit Global App Configuration Service-Benutzeroberfläche aktivieren

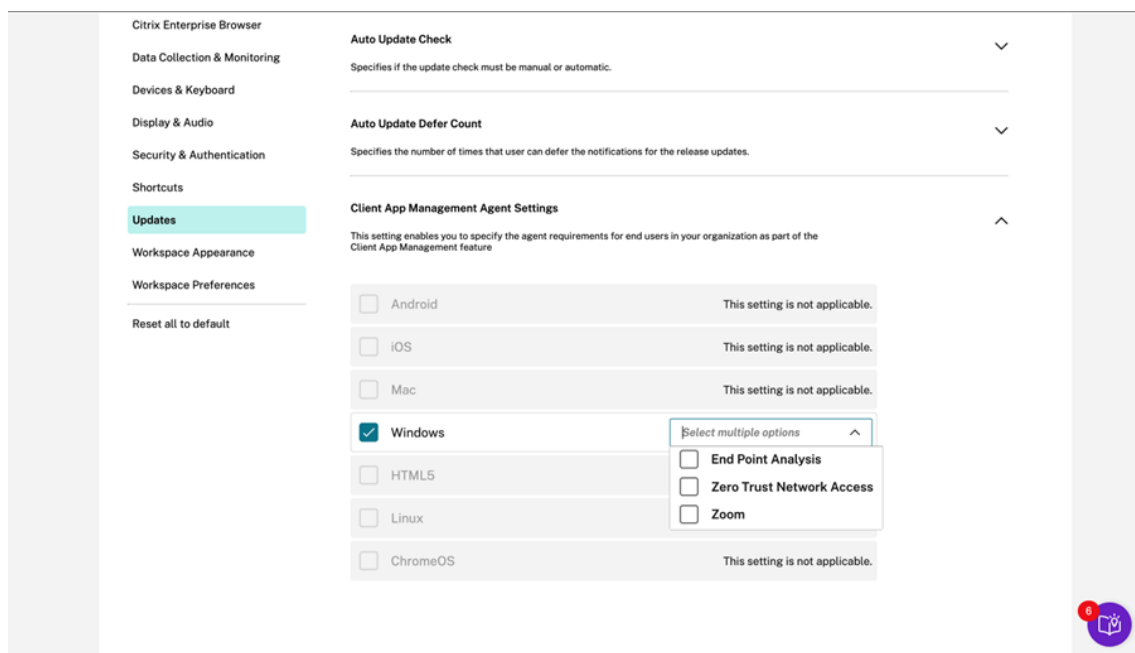
Diese Methode gilt nur für Cloudstores. Agents (EPA/Secure Access, Zoom-Plug-In oder WebEx-Plug-In) können von Administratoren über die Benutzeroberfläche bereitgestellt werden.

1. Melden Sie sich bei [Citrix Cloud](#) an.
2. Wählen Sie im Menü oben links die Option **Workspace-Konfiguration**.

Die Seite **Workspace-Konfiguration** wird angezeigt.



3. Klicken Sie auf die Registerkarte **App-Konfiguration**.
4. Klicken Sie auf **Updates**.
5. Stellen Sie sicher, dass das Kontrollkästchen **Windows** aktiviert ist.
6. Wählen Sie die erforderlichen Agents neben **Windows** in der Dropdownliste **Client App Management Agent Settings**.



## Plug-In-Verwaltung mit Global App Configuration Service-API aktivieren

1. Konfigurieren Sie Einstellungen im Global App Config Service mit der API und weisen Sie sie zu. Weitere Informationen finden Sie unter [Map service URLs and configure settings](#).
2. Die folgende Global App Configuration Service-Einstellung muss für den Store bzw. das Konto für das EPA- und ZTNA/Secure Access Client-Onboarding eingerichtet werden:

```

1  {
2
3    "serviceURL":
4    {
5
6      "url": "https://storefront.acme.com:443"
7    }
8  ,
9    "settings":
10   {
11
12     "description": "Install and update plugins",
13     "name": "Install and update plugins",
14     "useForAppConfig": true,
15     "appSettings":
16     {
17
18       "windows":
19       [
20         {
21
22           "assignedTo":

```

```
23     [
24         "AllUsersNoAuthentication"
25     ],
26     "category": "AutoUpdate",
27     "settings":
28     [
29         {
30
31             "name": "Auto Update plugins settings",
32             "value":
33             [
34                 {
35
36                     "pluginId": "8A8AF6C0-11F6-4343-
37                         BA2D-A85A766170D4",
38                     "pluginName": "Citrix EPA Client",
39                     "pluginSettings":
40                     {
41
42                         "delayGroup": "Fast",
43                         "deploymentMode": "
44                             InstallAndUpdate",
45                         "detectRule": "UpgradeCode:{
46                             37A181F7-870E-4BDF-B0EA-E3B4766119FE }
47                             ",
48                         "isBlocking": true,
49                         "isFTU": true,
50                         "maximumAllowedVersion": "
51                             23.8.1.24",
52                         "minimumAllowedVersion": "
53                             0.0.0.0",
54                         "stream": "Current",
55                         "upgradeToLatest": true
56                     }
57                 }
58             ],
59             "pluginId": "9A8AF6C0-11F6-4343-
60                 BA2D-A85A766170D5",
61             "pluginName": "Citrix Secure Access
62                 Client",
63             "pluginSettings":
64             {
65
66                 "delayGroup": "Fast",
67                 "deploymentMode": "
68                     InstallAndUpdate",
69                 "detectRule": "UpgradeCode:{
70                     F0ED53AB-11BE-4E9C-87E5-CD4A81DA2A4D }
71                     ",
72                 "isBlocking": false,
```

```
69         "isFTU": true,
70         "maximumAllowedVersion": "
71             21.8.0.0",
72         "minimumAllowedVersion": "
73             0.0.0.0",
74         "stream": "Current",
75         "upgradeToLatest": true
76     }
77 ,
78     {
79
80         "pluginId": "C03BAE37-F3AC-4D63-8
81             BC1-3C9CD2BC9E8D",
82         "pluginName": "WebEx VDI
83             AutoUpgrade Plugin",
84         "pluginSettings":
85         {
86             "delayGroup": "Fast",
87             "deploymentMode": "
88                 InstallAndUpdate",
89             "detectRule": "UpgradeCode:{
90                 AA2AACDC-D30B-433F-A602-3E25975010A6 }
91             ",
92             "isBlocking": false,
93             "isFTU": false,
94             "maximumAllowedVersion": "
95                 3.1.0.24263",
96             "minimumAllowedVersion": "0.0.0
97                 ",
98             "stream": "Current",
99             "upgradeToLatest": true
100         }
101     }
102 ],
103     "userOverride": false
104 }
105 ]
106 }
107 ]
108 }
109 }
110 }
111 }
112 }
113 }
114 }
```

115 &lt;!--NeedCopy--&gt;

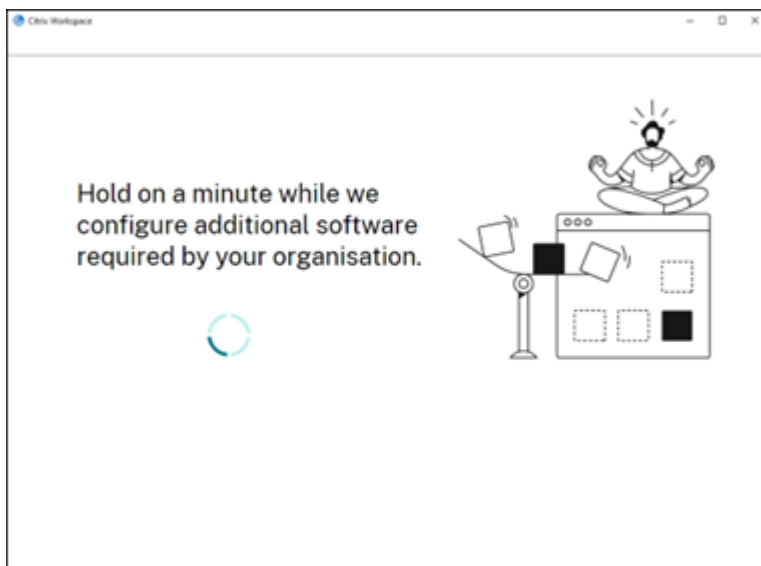
In der folgenden Tabelle werden die Einstellungen, Werte und Beschreibung für die Plug-In-Verwaltung aufgeführt.

Schemaeinstellung	Wert	Beschreibung
isBlocking	"True" oder "False"	Wenn der Parameter "isBlocking" auf "true" festgelegt ist, wird das Plug-In als verbindlich eingestuft und die Anmeldeseite wird nur angezeigt, wenn das erforderliche Plug-In installiert ist. Citrix empfiehlt, EPA als verbindliches Plug-In festzulegen.
pluginName	Anzeigename für das Plug-In. pluginName kann geändert werden.	
pluginId	ID des Plug-Ins (darf nicht geändert werden).	
delayGroup	Fast, Medium, Slow	Intervall, in dem die Plug-Ins automatisch aktualisiert werden müssen.
deploymentMode	InstallAndUpdate/Update	InstallAndUpdate: Das Plugin kann neu installiert und mit der neuen Version aktualisiert werden.Update: Es ist nur ein Update möglich, keine Neuinstallation.
None	Für dieses Plug-In ist keine Aktion erforderlich.	
detectRule	Der Wert darf nicht geändert werden.	Prüft, ob das Plug-In bereits installiert ist.
maximumAllowedVersion	Zulässige Höchstversion des Plug-Ins.	
minimumAllowedVersion	Zulässige Mindestversion des Plug-Ins.	
upgradeToLatest	"True" oder "False"	Muss auf "False" gesetzt werden, um maximumAllowedVersion und minimumAllowedVersion zu unterstützen. True: Die neueste Version des Plug-Ins wird beim Update berücksichtigt.
Stream	Current	Muss auf Current gesetzt werden, um die Plug-Ins zu empfangen, zu installieren oder automatisch zu aktualisieren

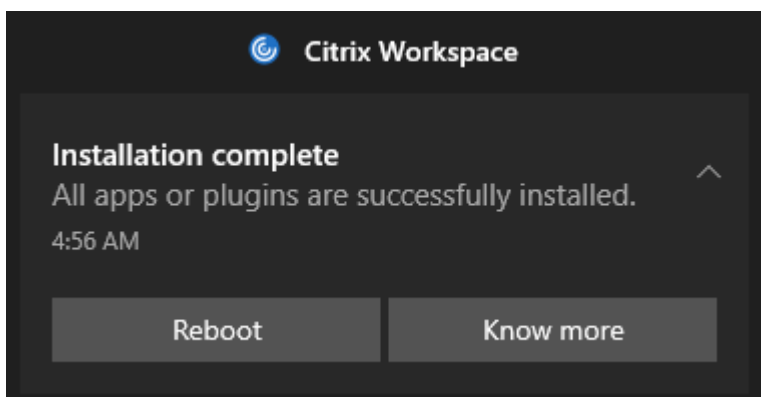
## Arbeitsablauf für Benutzer

1. Download und Installation der Citrix Workspace-App für Windows.
2. Klicken Sie am Ende der Installation auf **Konto hinzufügen**.
3. Fügen Sie den Store/das Konto hinzu, in dem die App-Konfigurationseinstellungen integriert sind.

Die folgende Meldung wird während der Installation der verbindlichen Plug-Ins angezeigt:

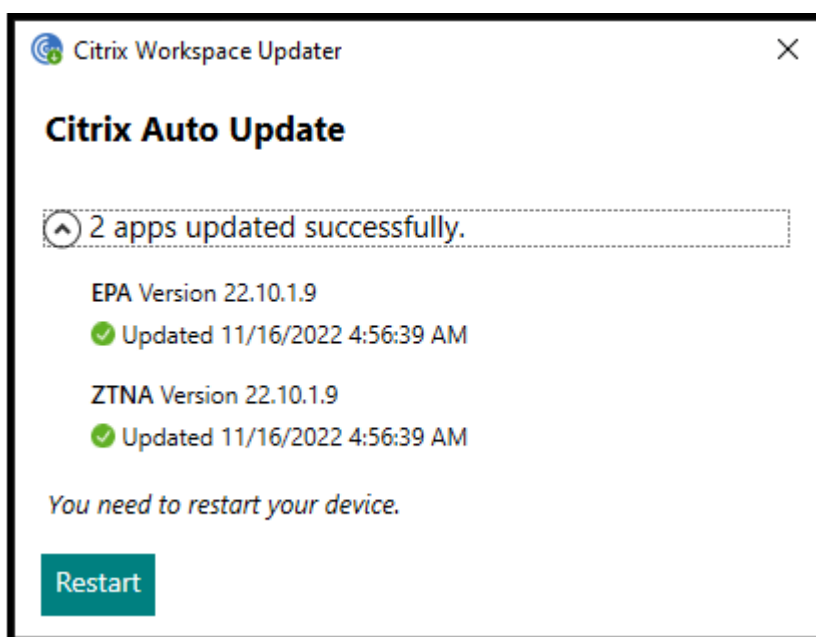


4. Wenn die Installation abgeschlossen ist, wird die folgende Pop-up-Benachrichtigung angezeigt:



5. Klicken Sie auf **Weitere Informationen**, um zu prüfen, welche Plug-Ins installiert wurden.





## Plug-In-Verwaltung für Zoom-Plug-In

Das Herunterladen, Installieren und automatische Update des Zoom-Plug-Ins wird ebenfalls unterstützt und wie die EPA- und ZTNA-Plug-Ins behandelt.

Die folgende Global App Configuration Service-Einstellung muss für den Store bzw. das Konto integriert werden, um das Feature zu nutzen:

```
1 {
2
3   "serviceURL":
4   {
5
6     "url": "https://storefront.acme.com:443"
7   }
8   ,
9   "settings":
10  {
11
12    "description": "Install and update plugins",
13    "name": "Install and update plugins",
14    "useForAppConfig": true,
15    "appSettings":
16    {
17
18      "windows":
19      [
20        {
21
22          "assignedTo":
23          [
```

```
24         "AllUsersNoAuthentication"
25     ],
26     "category": "AutoUpdate",
27     "settings":
28     [
29         {
30
31             "name": "Auto Update plugins settings",
32             "value":
33             [
34                 {
35
36                     "pluginId": "1A4BB471-022C-4C87-
37                         BDCD-0B64FB42869C",
38                     "pluginName": "Zoom VDI AutoUpgrade
39                         Plugin",
40                     "pluginSettings":
41                     {
42
43                         "delayGroup": "Fast",
44                         "deploymentMode": "
45                         InstallAndUpdate",
46                         "detectRule": "UpgradeCode:{
47                         34225638-14F3-4059-BE34-175AC9B35435 }
48                         ",
49                         "isBlocking": false,
50                         "isFTU": false,
51                         "maximumAllowedVersion": "
52                         5.11.2872",
53                         "minimumAllowedVersion": "0.0.0
54                         ",
55                         "stream": "Current",
56                         "upgradeToLatest": true
57                     }
58                 }
59             ]
60         },
61     ],
62     "userOverride": false
63 }
64 }
65 }
66 }
67 }
68 }
69 }
70 }
71 <!--NeedCopy-->
```

## App-Erfahrung

April 22, 2024

In diesem Abschnitt wird Folgendes beschrieben:

- [Anwendungsbereitstellung](#)
- [Verbesserter Start von Virtual Apps and Desktops](#)
- [App-Einstellungen](#)
- [SaaS-Apps](#)
- [Datensammlung und Überwachung](#)

## Anwendungsbereitstellung

April 22, 2024

Mit den folgenden Optionen können Sie die Benutzererfahrung bei der Bereitstellung von Anwendungen mit Citrix Virtual Apps and Desktops und Citrix DaaS verbessern.

- **Webzugriffsmodus:** Ohne jegliche Konfiguration ermöglicht die Citrix Workspace-App browserbasierten Zugriff auf Anwendungen und Desktops. Sie greifen einfach über einen Browser auf Workspace für Web zu und wählen die gewünschten Anwendungen aus. In diesem Modus werden keine Verknüpfungen auf dem Desktop der Benutzer platziert.
- **Self-Service-Modus:** Sie konfigurieren den *Self-Service-Modus* durch Hinzufügen eines StoreFront-Kontos zur Citrix Workspace-App oder durch Verweisen der Citrix Workspace-App auf eine StoreFront-Website. Im Self-Service-Modus können Sie Anwendungen über die Benutzeroberfläche der Citrix Workspace-App abonnieren. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores. Im Self-Service-Modus können Sie nach Bedarf Schlüsselworteinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren.

### Hinweis:

Standardmäßig können Sie in der Citrix Workspace-App Anwendungen zur Anzeige im Startmenü auswählen.

- **Nur-Verknüpfungsmodus:** Administratoren können mit der Citrix Workspace-App Anwendungs- und Desktopverknüpfungen automatisch direkt in das Startmenü oder auf dem Desktop platzieren. Die Platzierung ähnelt der Citrix Workspace-App (Enterprise). Mit dem neuen *Nur-Verknüpfungsmodus* werden die veröffentlichten Anwendungen entsprechend dem gewohnten Windows-Navigationsschema angezeigt.

Weitere Informationen finden Sie unter [Bereitstellungsgruppe erstellen](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

## Konfigurieren des Self-Service-Modus

Sie konfigurieren den Self-Service-Modus durch einfaches Hinzufügen eines StoreFront-Kontos zur Citrix Workspace-App oder durch Verweisen der Citrix Workspace-App auf eine StoreFront-Site. Mit dieser Konfiguration können Benutzer die Anwendungen über die Citrix Workspace-Benutzeroberfläche abonnieren. Diese verbesserte Benutzererfahrung ähnelt der eines mobilen App-Stores.

### Hinweis:

Standardmäßig können Benutzer der Citrix Workspace-App Anwendungen zur Anzeige im Startmenü auswählen.

Im Self-Service-Modus können Sie nach Bedarf Schlüsselpereinstellungen für obligatorische, automatisch bereitgestellte und Highlight-Apps konfigurieren.

Fügen Sie den Beschreibungen, die Sie für Bereitstellungsgruppenanwendungen eingeben, Schlüsselwörter hinzu:

- Um eine App verbindlich zu machen, sodass sie nicht aus der Citrix Workspace-App entfernt werden kann, hängen Sie die Zeichenfolge “KEYWORDS: Mandatory” an die Anwendungsbeschreibung an. Benutzer haben keine Option zum Kündigen des Abonnements verbindlicher Apps.
- Sie können automatisch eine Anwendung für alle Benutzer eines Stores abonnieren, wenn Sie die Zeichenfolge “KEYWORDS: Auto” der Beschreibung anhängen. Wenn Benutzer sich an dem Store anmelden, wird die Anwendung automatisch bereitgestellt, ohne dass die Benutzer sie manuell abonnieren müssen.
- Hängen Sie die Zeichenfolge “KEYWORDS: Featured” der Anwendungsbeschreibung an, um den Benutzern Anwendungen anzukündigen oder häufig verwendete Anwendungen in der Highlightliste von Citrix Workspace anzuzeigen.

## Speicherort für App-Verknüpfung mit Gruppenrichtlinienobjektvorlage konfigurieren

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Self-Service**.
3. Wählen Sie die Richtlinie **Self-Service-Modus verwalten** aus.
  - a) Wählen Sie **Aktiviert**, um die Self-Service-Benutzeroberfläche anzuzeigen.

- b) Wählen Sie **Deaktiviert**, um Apps manuell zu abonnieren. Diese Option blendet die Self-Service-Benutzeroberfläche aus.
4. Wählen Sie die Richtlinie **App-Verknüpfung verwalten** aus.
5. Wählen Sie die gewünschten Optionen aus.
6. Klicken Sie auf **Anwenden** und auf **OK**.
7. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

## Speicherorte für App-Verknüpfungen mit StoreFront-Kontoeinstellungen anpassen

Sie können Verknüpfungen im Startmenü und auf dem Desktop von der StoreFront-Site aus einrichten. Die folgenden Einstellungen können im Abschnitt **<annotatedServices>** der Datei web.config in `C:\inetpub\wwwroot\Citrix\Roaming` hinzugefügt werden:

- Zum Einfügen von Verknüpfungen auf dem Desktop verwenden Sie `PutShortcutsOnDesktop`. Einstellungen: "true" oder "false" (Standardwert ist "false").
- Zum Einfügen von Verknüpfungen im Startmenü verwenden Sie `PutShortcutsInStartMenu`. Einstellungen: "true" oder "false" (Standardwert ist "true").
- Zum Verwenden eines Kategoriepfads im Startmenü verwenden Sie `UseCategoryAsStartMenuPath`. Einstellungen: "true" oder "false" (Standardwert ist "true").

### Hinweis:

In Windows 8, 8.1 und Windows 10 ist die Erstellung von verschachtelten Ordnern im Startmenü nicht zulässig. Die Anwendungen werden stattdessen einzeln oder unter dem Stammordner angezeigt. Die Anwendungen werden nicht in den mit Citrix Virtual Apps and Desktops und Citrix DaaS definierten Unterordnern für Kategorien angezeigt.

- Zum Festlegen eines einzelnen Verzeichnisses für alle Verknüpfungen im Startmenü verwenden Sie `StartMenuDir`. Einstellung: Zeichenfolgewert, der Name des Ordners, in dem die Verknüpfungen gespeichert werden.
- Zum Neuinstallieren modifizierter Apps verwenden Sie `AutoReinstallModifiedApps`. Einstellungen: "true" oder "false" (Standardwert ist "true").
- Zum Anzeigen eines einzelnen Verzeichnisses für alle Verknüpfungen auf dem Desktop verwenden Sie `DesktopDir`. Einstellung: Zeichenfolgewert, der Name des Ordners, in dem die Verknüpfungen gespeichert werden.
- Zum Vermeiden eines Eintrags unter "Programme hinzufügen/entfernen" verwenden Sie `DontCreateAddRemoveEntry`. Einstellungen: "true" oder "false" (Standardwert ist "false").
- Zum Entfernen von Verknüpfungen und des Citrix Workspace-Symbols einer Anwendung, die nicht mehr im Store verfügbar ist, verwenden Sie `SilentlyUninstallRemovedResources`. Einstellungen: "true" oder "false" (Standardwert ist "false").

Fügen Sie die Änderungen in der Datei web.config im **XML**-Abschnitt für das Konto hinzu. Sie finden diesen Abschnitt durch Suchen des Starttags:

```
<account id=... name="Store"
```

Der Abschnitt endet mit dem Tag </account>.

Vor dem Ende des Abschnitts "account" ist der Abschnitt "properties" mit den Eigenschaften:

```
<properties> <clear> <properties>
```

Eigenschaften können in diesen Abschnitt nach dem Tag <clear /> unter Angabe des Namens und Werts (eine Eigenschaft pro Zeile) eingefügt werden. Beispiel:

```
<property name="PutShortcutsOnDesktop" value="True"/>
```

**Hinweis:**

Wenn Eigenschaftenelemente vor dem Tag <clear /> hinzugefügt werden, sind sie u. U. ungültig. Sie können das Tag <clear /> entfernen, wenn Sie einen Eigenschaftsnamen und -wert hinzufügen.

Ausführliches Beispiel für diesen Abschnitt:

```
<properties <property name="PutShortcutsOnDesktop" value="True">  
property name="DesktopDir" value="Citrix Applications">
```

**Wichtig**

Verwenden Sie in einer Multiserverbereitstellung jeweils nur einen Server, um Änderungen an der Konfiguration der Servergruppe vorzunehmen. Stellen Sie sicher, dass die Citrix StoreFront-Verwaltungskonsole nicht auf den anderen Servern der Bereitstellung ausgeführt wird. Zum Abschluss übertragen Sie die Konfigurationsänderungen auf die Servergruppe, sodass die anderen Server der Bereitstellung aktualisiert werden. Weitere Informationen finden Sie in der [StoreFront](#)-Dokumentation.

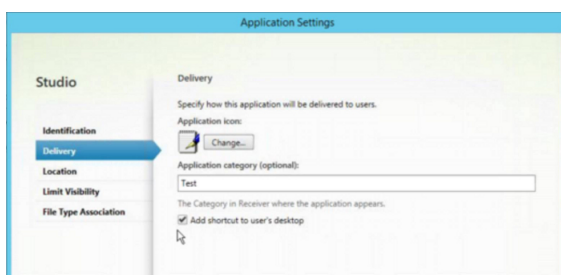
## **Konfigurieren von Speicherorten für App-Verknüpfungen mit Einstellungen pro App in Citrix Virtual Apps and Desktops 7.x**

Mit der Citrix Workspace-App können Anwendungs- und Desktopverknüpfungen direkt in das Startmenü oder auf dem Desktop platziert werden. Diese Konfiguration ähnelt jedoch früheren Versionen von Workspace für Windows. Ab Release 4.2.100 kann jedoch die Platzierung der App-Verknüpfung in Citrix Virtual Apps über Einstellungen pro App gesteuert werden. Diese Funktionalität ist in Umgebungen mit nur einer Handvoll Anwendungen nützlich, die immer am gleichen Ort angezeigt werden sollen.

## Speicherorte für App-Verknüpfungen mit Einstellungen pro App in XenApp 7.6 konfigurieren

Konfigurieren einer Veröffentlichungsverknüpfung pro App in XenApp 7.6:

1. Navigieren Sie in Citrix Studio zum Bildschirm **Anwendungseinstellungen**.
2. Wählen Sie im Bildschirm **Anwendungseinstellungen** die Option **Bereitstellung**. In diesem Bildschirm legen Sie fest, wie Anwendungen Benutzern bereitgestellt werden.
3. Wählen Sie das entsprechende Symbol für die Anwendung. Klicken Sie auf **Ändern**, um zum Speicherort des erforderlichen Symbols zu navigieren.
4. Im Feld **Anwendungskategorie** können Sie optional für die Anwendung eine Kategorie in der Citrix Workspace-App angeben. Wenn Sie beispielsweise Verknüpfungen für Microsoft Office-Anwendungen hinzufügen, geben Sie Microsoft Office ein.
5. Aktivieren Sie das Kontrollkästchen “Verknüpfung auf Benutzerdesktop hinzufügen”.
6. Klicken Sie auf OK.



## Reduzieren von Enumerationsverzögerungen oder digitales Signieren von Anwendungsstubs

Mit der Citrix Workspace-App können Sie in folgenden Fällen die EXE-Stubs von einer Netzwerkfreigabe kopieren:

- Es gibt eine Verzögerung der App-Enumeration bei jeder Anmeldung. Oder:
- Anwendungsstubs müssen digital signiert werden.

Diese Funktionalität umfasst mehrere Schritte:

1. Erstellen Sie die Anwendungsstubs auf der Clientmaschine.
2. Kopieren Sie die Anwendungsstubs an einen allgemeinen Speicherort, der von einer Netzwerkfreigabe aus verfügbar ist.
3. Erstellen Sie bei Bedarf eine Positivliste oder signieren Sie die Stubs mit einem Unternehmenszertifikat.

4. Fügen Sie einen Registrierungsschlüssel hinzu, damit Workspace für Windows die Stubs durch Kopieren von der Netzwerkfreigabe erstellen kann.

Wenn **RemoveappsOnLogoff** und **RemoveAppsonExit** aktiviert sind und die App-Enumeration bei jeder Anmeldung langsam ist, lösen Sie das Problem mit dem folgenden Workaround:

1. Fügen Sie mit dem Registrierungs-Editor (regedit) Folgendes hinzu: `HKEY_CURRENT_USER\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"`.
2. Fügen Sie mit dem Registrierungs-Editor (regedit) Folgendes hinzu: `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"`. HKEY\_CURRENT\_USER hat Vorrang vor HKEY\_LOCAL\_MACHINE.

### Achtung

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Ermöglichen Sie die Verwendung zuvor erstellter und in einer Netzwerkfreigabe gespeicherter EXE-Stubdateien durch den Computer:

1. Erstellen Sie auf einer Clientmaschine EXE-Stubdateien für alle Apps. Zum Erstellen von EXE-Stubdateien fügen Sie mit der Citrix Workspace-App alle Anwendungen zur Maschine hinzu. Die Citrix Workspace-App generiert die EXE-Dateien.
2. Verwenden Sie die EXE-Stubdateien aus `%APPDATA%\Citrix\SelfService`. Sie benötigen nur die Dateien mit der Erweiterung `.exe`.
3. Kopieren Sie die EXE-Dateien in eine Netzwerkfreigabe.
4. Legen Sie für jeden Clientcomputer, der gesperrt werden soll, folgende Registrierungsschlüssel fest:
  - a) `Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\WorkspaceStubs"`
  - b) `Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v`
  - c) `CopyStubsFromCommonStubDirectory /t REG_SZ /d "true"`. Diese Einstellungen sind auch über HKEY\_CURRENT\_USER möglich. HKEY\_CURRENT\_USER hat Vorrang vor HKEY\_LOCAL\_MACHINE.
  - d) Beenden und starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

### Anwendungsbeispiele:

In diesem Abschnitt finden Sie Anwendungsfälle für App-Verknüpfungen.



## Benutzer wählen die gewünschten Apps für das Startmenü selbst aus (Self-Service)

Wenn Sie Dutzende oder sogar Hunderte von Apps haben, lassen Sie Benutzer ihre Anwendungen selbst auswählen und im **Favoriten-** und **Startmenü** hinzufügen:

---

Wenn Benutzer Apps selbst auswählen und dem Startmenü hinzufügen sollen ...

... konfigurieren Sie die Citrix Workspace-App im Self-Service-Modus. In diesem Modus können Sie nach Bedarf Schlüsselworteinstellungen für *obligatorische* und *automatisch bereitgestellte* Apps konfigurieren.

Wenn Benutzer die Apps für das Startmenü selbst auswählen aber auch bestimmte App-Verknüpfungen auf dem Desktop platziert werden sollen ...

... konfigurieren Sie die Citrix Workspace-App ohne Optionen und legen Sie die Einstellungen für die wenigen Apps, die auf dem Desktop platziert werden, einzeln fest. Verwenden Sie *automatisch bereitgestellte* und *obligatorische* Apps nach Bedarf.

---

## Keine App-Verknüpfungen im Startmenü

Wenn ein Benutzer einen Familiencomputer verwendet, sind App-Verknüpfungen möglicherweise nicht erwünscht oder erforderlich. In solchen Fällen ist die einfachste Lösung der Zugriff über einen Browser. Installieren Sie die Citrix Workspace-App hierfür ohne Konfiguration und navigieren Sie zu Workspace für Web. Sie können für die Citrix Workspace-App auch Self-Service-Zugriff konfigurieren, ohne Verknüpfungen zu erstellen.

---

Wenn die Citrix Workspace-App nicht automatisch Anwendungsverknüpfungen im Startmenü platzieren soll ...

... konfigurieren Sie die Citrix Workspace-App mit `PutShortcutsInStartMenu=False`. Die Citrix Workspace-App platziert keine Apps ins Startmenü (selbst bei aktiviertem Self-Service-Modus), sofern Sie sie nicht einzeln über die Einstellungen platzieren.

---

## Alle App-Verknüpfungen im Startmenü oder auf dem Desktop

Wenn Benutzer nur wenige Apps haben, platzieren Sie alle Apps im Startmenü oder auf dem Desktop oder in einem Ordner auf dem Desktop.

Wenn die Citrix Workspace-App automatisch alle Anwendungsverknüpfungen im Startmenü platzieren soll ...

... konfigurieren Sie die Citrix Workspace-App mit `SelfServiceMode=False`. Alle verfügbaren Apps werden dann im Startmenü angezeigt.

Wenn alle Anwendungsverknüpfungen auf dem Desktop platziert werden sollen ...

... konfigurieren Sie die Citrix Workspace-App mit `PutShortcutsOnDesktop=true`. Alle verfügbaren Apps werden dann auf dem Desktop angezeigt.

Wenn alle Verknüpfungen auf dem Desktop in einem Ordner platziert werden sollen ...

... konfigurieren Sie die Citrix Workspace-App mit `DesktopDir=Name des Desktopordners`, in dem die Anwendungen platziert werden sollen.

---

### **Einstellungen pro App in XenApp 6.5 oder 7.x**

Wenn Sie die Speicherorte der Verknüpfungen für alle Benutzer gleich festlegen möchten, verwenden Sie die XenApp-Einstellungen pro App:

---

Wenn Sie unabhängig vom Modus mit den Einstellungen pro App festlegen möchten, wo Anwendungen platziert werden ...

... konfigurieren Sie die Citrix Workspace-App mit `PutShortcutsInStartMenu=false` und aktivieren Sie die Einstellungen pro App

---

### **Apps in Kategorieordnern oder in bestimmten Ordnern**

Wenn Anwendungen in bestimmten Ordnern angezeigt werden sollen, verwenden Sie die folgenden Optionen:

---

Wenn die von der Citrix Workspace-App im Startmenü platzierten

... konfigurieren Sie die Citrix Workspace-App mit `UseCategoryAsStartMenuPath=True`.

Anwendungsverknüpfungen in den zugeordneten Kategorieordnern angezeigt werden sollen ...

Wenn die von der Citrix Workspace-App im Startmenü platzierten Anwendungen in einem bestimmten Ordner angezeigt werden sollen ...

... konfigurieren Sie die Citrix Workspace-App mit `StartMenuDir=Startmenü-Ordnername`.

---

## Apps beim Abmelden oder Beenden entfernen

Wenn ein Endpunkt von mehreren Benutzern genutzt wird und andere Benutzer die Apps nicht sehen sollen, können Sie die Apps beim Abmelden und Beenden des Benutzers entfernen.

---

Wenn die Citrix Workspace-App alle Apps beim Abmelden entfernen soll ...	... konfigurieren Sie die Citrix Workspace-App mit <code>RemoveAppsOnLogoff=True</code> .
Wenn die Citrix Workspace-App alle Apps beim Beenden entfernen soll ...	... konfigurieren Sie die Citrix Workspace-App mit <code>RemoveAppsOnExit=True</code> .

---

## Konfigurieren von lokalem App-Zugriff für Anwendungen

Lokalen App-Zugriff für Anwendungen konfigurieren:

- Wenn eine lokal installierte Anwendung statt einer in der Citrix Workspace-App verfügbaren Anwendung verwendet werden soll, hängen Sie die Zeichenfolge `KEYWORDS:prefer="pattern"` an. Dieses Feature wird als lokaler App-Zugriff bezeichnet.

Bevor Sie eine Anwendung auf dem Computer des Benutzers installieren, sucht die Citrix Workspace-App nach den angegebenen Mustern, um zu erkennen, ob die Anwendung lokal installiert ist. Wenn dies der Fall ist, abonniert die Citrix Workspace-App die Anwendung und erstellt keine Verknüpfung. Wenn der Benutzer die Anwendung vom Citrix Workspace-App-Fenster aus startet, startet die App die lokal installierte (bevorzugte) Anwendung.

Wenn ein Benutzer eine bevorzugte Anwendung außerhalb der Citrix Workspace-App deinstalliert, wird das Abonnement für die Anwendung bei der nächsten Citrix Workspace-App-Aktualisierung gekündigt. Wenn ein Benutzer eine bevorzugte Anwendung über das Citrix Workspace-App-Dialogfeld deinstalliert, kündigt die Citrix Workspace-App das Anwendungsabonnement; die Anwendung wird jedoch nicht deinstalliert.

### Hinweis:

Das Schlüsselwort `“prefer”` wird angewendet, wenn die Citrix Workspace-App eine Anwendung abonniert. Das Hinzufügen des Schlüsselworts, nach dem die Anwendung abonniert ist, hat keine Auswirkung.

Sie können das Schlüsselwort `“prefer”` mehrmals für eine Anwendung angeben. Nur eine Übereinstimmung wird benötigt, damit das Schlüsselwort auf eine Anwendung angewendet wird. Die folgenden Muster können in beliebiger Kombination verwendet werden:

- Wenn eine lokal installierte Anwendung statt einer in der Citrix Workspace-App verfügbaren Anwendung verwendet werden soll, hängen Sie die Zeichenfolge KEYWORDS:prefer="pattern" an. Dieses Feature wird als lokaler App-Zugriff bezeichnet.

Bevor Sie eine Anwendung auf dem Computer des Benutzers installieren, sucht die Citrix Workspace-App nach den angegebenen Mustern, um zu erkennen, ob die Anwendung lokal installiert ist. Wenn dies der Fall ist, abonniert die Citrix Workspace-App die Anwendung und erstellt keine Verknüpfung. Wenn der Benutzer die Anwendung über das Citrix Workspace-App-Dialogfeld startet, startet die App die lokal installierte (bevorzugte) Anwendung.

Wenn ein Benutzer eine bevorzugte Anwendung außerhalb der Citrix Workspace-App deinstalliert, wird das Abonnement für die Anwendung bei der nächsten Citrix Workspace-App-Aktualisierung gekündigt. Wenn ein Benutzer eine bevorzugte Anwendung über die Citrix Workspace-App deinstalliert, kündigt die App das Anwendungsabonnement; die Anwendung wird jedoch nicht deinstalliert.

**Hinweis:**

Das Schlüsselwort "prefer" wird angewendet, wenn die Citrix Workspace-App eine Anwendung abonniert. Das Hinzufügen des Schlüsselworts, nach dem die Anwendung abonniert ist, hat keine Auswirkung.

Sie können das Schlüsselwort "prefer" mehrmals für eine Anwendung angeben. Nur eine Übereinstimmung wird benötigt, damit das Schlüsselwort auf eine Anwendung angewendet wird. Die folgenden Muster können in beliebiger Kombination verwendet werden:

- prefer="ApplicationName"

Das Anwendungsnamenmuster stimmt mit jeder Anwendung überein, die den angegebenen Anwendungsnamen im Verknüpfungsdateinamen hat. Der Anwendungsname kann ein Wort oder ein Satz sein. Für Sätze sind Anführungszeichen erforderlich. Die Übereinstimmung ist nicht für Teilworte oder Dateipfade zulässig; die Groß- und Kleinschreibung wird beachtet. Das Übereinstimmungsmuster für den Anwendungsnamen ist nützlich, wenn ein Administrator manuelle Überschreibungen ausführt.

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
Word	\Microsoft Office\Microsoft Word 2010	Ja
Microsoft Word	\Microsoft Office\Microsoft Word 2010	Ja
Konsole	McAfee\VirusScan Console	Ja
Virus	McAfee\VirusScan Console	Nein

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
Konsole	McAfee\VirusScan Console	Ja

- prefer="\\Folder1\Folder2\...\ApplicationName"

Das Muster des absoluten Pfads stimmt mit dem gesamten Pfad der Verknüpfungsdatei und dem ganzen Anwendungsnamen unter dem Startmenü überein. Der Ordner "Programme" ist ein Unterordner des Startmenüverzeichnis und muss daher im absoluten Pfad für die Zielanwendung in diesem Ordner enthalten sein. Anführungszeichen sind erforderlich, wenn der Pfad Leerstellen enthält. Für die Übereinstimmung wird die Groß-/Kleinschreibung beachtet. Das Übereinstimmungsmuster für den absoluten Pfad ist für Überschreibungen nützlich, die programmatisch in Citrix Virtual Apps and Desktops und Citrix DaaS implementiert werden.

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
\Programme\Microsoft Office\Microsoft Word 2010	\Programme\Microsoft Office\Microsoft Word 2010	Ja
\Microsoft Office	\Programme\Microsoft Office\Microsoft Word 2010	Nein
\Microsoft Word 2010	\Programme\Microsoft Office\Microsoft Word 2010	Nein
\Programme\Microsoft Word 2010	\Programme\Microsoft Word 2010	Ja

- prefer="Folder1\Folder2\...\ApplicationName"

Das Muster des absoluten Pfads stimmt mit dem relativen Pfad unter dem Startmenü überein. Der angegebene relative Pfad muss den Anwendungsnamen enthalten und (optional) den Ordner, in dem die Verknüpfung gespeichert ist. Die Übereinstimmung ist erfolgreich, wenn am Ende des Pfads der Verknüpfungsdatei der angegebene relative Pfad steht. Anführungszeichen sind erforderlich, wenn der Pfad Leerstellen enthält. Für die Übereinstimmung wird die Groß-/Kleinschreibung beachtet. Das Übereinstimmungsmuster für den relativen Pfad ist für Überschreibungen nützlich, die programmatisch implementiert werden.

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
\Microsoft Office\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Ja
\Microsoft Office	\Microsoft Office\Microsoft Word 2010	Nein

KEYWORDS:prefer=	Verknüpfung unter Programme	Übereinstimmung?
\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Ja
\Microsoft Word	\Microsoft Word 2010	Nein

Informationen zu anderen Schlüsselwörtern finden Sie im Abschnitt **Zusätzliche Empfehlungen** unter [Benutzererfahrung in der StoreFront-Dokumentation optimieren](#).

### vPrefer-Start

In älteren Releases können Sie festlegen, dass die Instanz einer auf dem VDA installierten App (= "lokale Instanz" im vorliegenden Dokument) bevorzugt vor der veröffentlichten Anwendung gestartet werden muss, indem Sie in **Citrix Studio** das Attribut KEYWORDS:prefer="application" festlegen.

Ab Version 4.11 können Sie in einem Double-Hop-Szenario (wenn die Citrix Workspace-App auf dem VDA ausgeführt wird, der Ihre Sitzung hostet) steuern, was die Citrix Workspace-App startet:

- die lokale Instanz einer auf dem VDA installierten Anwendung (sofern sie als lokale App verfügbar ist) oder
- eine gehostete Instanz der Anwendung.

vPrefer ist in StoreFront 3.14 und in Citrix Virtual Desktops ab Version 7.17 verfügbar.

Wenn Sie die Anwendung starten, liest die Citrix Workspace-App die Ressourcendaten auf dem StoreFront-Server und wendet die Einstellungen auf der Grundlage des **vprefer**-Flags zum Zeitpunkt der Aufzählung an. Die Citrix Workspace-App sucht in der Windows-Registrierung des VDA nach dem Installationspfad der Anwendung. Falls vorhanden, wird die lokale Instanz der Anwendung gestartet. Andernfalls wird eine gehostete Instanz gestartet.

Wenn Sie eine Anwendung starten, die nicht auf dem VDA ist, wird die gehostete Anwendung von der Citrix Workspace-App gestartet. Weitere Informationen zur Handhabung des lokalen Starts in StoreFront finden Sie unter [Steuern des lokalen Starts von Anwendungen auf veröffentlichten Desktops](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Wenn Sie nicht möchten, dass die lokale Instanz einer Anwendung auf dem VDA gestartet wird, setzen Sie **LocalLaunchDisabled** auf dem Delivery Controller mithilfe von PowerShell auf **True**. Weitere Informationen finden Sie in der Dokumentation zu [Citrix Virtual Apps and Desktops](#).

Das Feature beschleunigt den Anwendungsstart und bietet dadurch eine bessere Benutzererfahrung. Sie können es über die administrative GPO-Vorlage konfigurieren. Standardmäßig ist vPrefer nur in einem Double-Hop-Szenario aktiviert.

#### Hinweis:

Wenn Sie die Citrix Workspace-App zum ersten Mal installieren oder aktualisieren, fügen Sie dem lokalen Gruppenrichtlinienobjekt die neuesten Vorlagendateien hinzu. Weitere Informationen über das Hinzufügen von Vorlagendateien zum lokalen Gruppenrichtlinienobjekt finden Sie unter [Administrative Gruppenrichtlinienobjektvorlage](#). Bei einem Upgrade bleiben die vorhandenen Einstellungen erhalten, während die neuesten Dateien importiert werden.

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Self-Service**.
3. Wählen Sie die Richtlinie **vPrefer**.
4. Wählen Sie **Aktiviert**.
5. Wählen Sie in der Dropdownliste neben **Apps zulassen** eine der folgenden Optionen:
  - **Alle Apps zulassen:** Mit dieser Option wird die lokale Instanz aller Apps auf dem VDA gestartet. Die Citrix Workspace-App sucht nach der installierten Anwendung (einschließlich Windows-eigener Anwendungen wie Editor, Rechner, WordPad, Eingabeaufforderung). Sie startet dann diese Anwendung auf dem VDA (und nicht die gehostete App).
  - **Installierte Apps zulassen:** Mit dieser Option wird die lokale Instanz der installierten App auf dem VDA gestartet. Wenn die App nicht auf dem VDA installiert ist, wird die gehostete App gestartet. Standardmäßig ist die Option **Installierte Apps zulassen** ausgewählt, wenn die **vPrefer**-Richtlinie auf **Aktiviert** festgelegt ist. Diese Option gilt nicht für Windows-eigene Anwendungen wie Editor, Rechner usw.
  - **Netzwerk-Apps zulassen:** Durch diese Option wird die Instanz von Apps gestartet, die in einem freigegebenen Netzwerk veröffentlicht ist.
6. Klicken Sie auf **Anwenden** und auf **OK**.
7. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

#### Einschränkung:

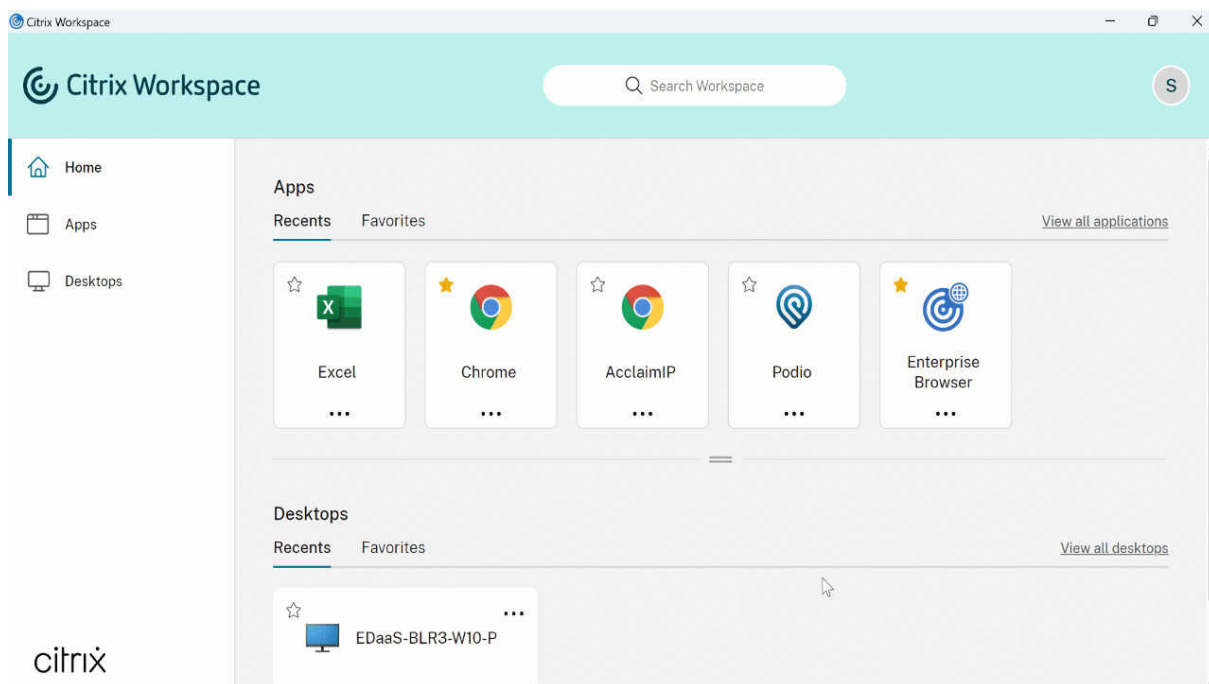
- Workspace für Web unterstützt dieses Feature nicht.

## Verbesserter Start von Virtual Apps and Desktops

April 22, 2024

Diese Funktion ist standardmäßig für Cloud- und on-premises Stores aktiviert. Das verbesserte Startverhalten von Apps und Desktops macht die Citrix Workspace-App für Windows jetzt informativer und benutzerfreundlicher. Durch zeitnahe und relevante Informationen zum Startstatus bleiben

Benutzer aktiv und informiert. Die Benachrichtigung wird in der unteren rechten Bildschirmcke angezeigt.



Benutzer erhalten aussagekräftige Benachrichtigungen über den Startfortschritt, anstatt nur ein Wartesymbol zu sehen. Wenn ein Benutzer während eines Startvorgangs versucht, den Browser zu schließen, wird eine Warnmeldung angezeigt.

## App-Einstellungen

April 22, 2024

### Seite “Erweiterte Einstellungen”

Sie können die Verfügbarkeit und den Inhalt der Seite **Erweiterte Einstellungen** anpassen. Die Seite ist im Kontextmenü des Citrix Workspace-App-Symbols im Infobereich zu finden. Auf diese Weise wird sichergestellt, dass Benutzer nur vom Administrator festgelegte Einstellungen auf ihren Systemen anwenden können. Optionen:

- Ausblenden der gesamten Seite “Erweiterte Einstellungen”
- Ausblenden der folgenden Einstellungen auf der Seite:
  - Datensammlung
  - Connection Center



- Konfigurationsprüfung
- Tastatur und Sprachenleiste
- Hoher DPI-Wert
- Supportinformationen
- Verknüpfungen und Wiederverbinden
- Citrix Casting

## Erweiterte Einstellungen aus dem Kontextmenü ausblenden

Sie können die Seite “Erweiterte Einstellungen” über die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App ausblenden:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Self-Service** > **Erweiterte Einstellungen - Optionen**.
3. Wählen Sie die Richtlinie **Erweiterte Einstellungen deaktivieren**.
4. Wählen Sie **Aktiviert** aus, um die Option “Erweiterte Einstellungen” im Kontextmenü des Citrix Workspace-App-Symbols im Infobereich auszublenden.

### Hinweis:

Standardmäßig ist die Option **Nicht konfiguriert** ausgewählt.

## Ausblenden bestimmter Einstellungen auf der Seite “Erweiterte Einstellungen”

Sie können auf der Seite **Erweiterte Einstellungen** bestimmte vom Benutzer konfigurierbare Einstellungen über die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App ausblenden. Ausblenden der Einstellungen:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Self-Service** > **Erweiterte Einstellungen - Optionen**.
3. Wählen Sie die Richtlinie für die Einstellung, die Sie ausblenden möchten.

Die folgende Tabelle listet die verfügbaren Optionen auf und ihre Wirkung:

---

Optionen	Aktion
Nicht konfiguriert	Anzeigen der Einstellung

---

Optionen	Aktion
Aktiviert	Ausblenden der Einstellung
Deaktiviert	Anzeigen der Einstellung

---

Sie können die folgenden bestimmten Einstellungen auf der Seite “Erweiterte Einstellungen” ausblenden:

- Konfigurationsprüfung
- Connection Center
- Hoher DPI-Wert
- Datensammlung
- Gespeicherte Kennwörter löschen
- Tastatur und Sprachenleiste
- Verknüpfungen und Wiederverbinden
- Supportinformationen
- Citrix Casting

### **Ausblenden der Option zum Zurücksetzen von Workspace auf der Seite “Erweiterte Einstellungen” mit dem Registrierungs-Editor**

Sie können die Option **Workspace zurücksetzen** auf der Seite “Erweiterte Einstellungen” nur mit dem Registrierungs-Editor ausblenden.

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`.
3. Erstellen Sie einen Schlüsselzeichenfolgert **EnableFactoryReset** und legen Sie ihn auf eine der folgenden Optionen fest:
  - True: zeigt die Option “Workspace zurücksetzen” auf der Seite “Erweiterte Einstellungen” an.
  - False: blendet die Option “Workspace zurücksetzen” auf der Seite “Erweiterte Einstellungen” aus.

### **Ausblenden der Option “Citrix Workspace-Updates” auf der Seite “Erweiterte Einstellungen”**

#### **Hinweis:**

Der Richtlinienpfad für die Option “Citrix Workspace-Updates” ist anders als bei anderen Optionen auf der Seite “Erweiterte Einstellungen”.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Citrix Workspace-Updates**.
3. Wählen Sie die Richtlinie **Citrix Workspace-Updates** aus.
4. Wählen Sie **Deaktiviert**, um die Einstellungen für automatische Updates auf der Seite **Erweiterte Einstellungen** auszublenden.

## Citrix Casting

Der Citrix Ready Workspace Hub verbindet die digitale und die physische Umgebung zur Bereitstellung von Apps und Daten in einem sicheren, intelligenten Bereich. Das System verbindet Geräte (oder auch Dinge, z. B. mobile Apps und Sensoren) zur Schaffung einer intelligenten und reaktionsfähigen Umgebung.

Citrix Ready Workspace Hub baut auf der Raspberry Pi 3-Plattform auf. Das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, stellt eine Verbindung zum Citrix Ready Workspace Hub her und ermöglicht die Anzeige von Apps und Desktops auf einem größeren Display. Citrix Casting wird nur unter Microsoft Windows 10 Version 1607 und höher oder auf Windows Server 2016 unterstützt.

Mit Citrix Casting können Sie sofort und sicher auf jede App auf einem Mobilgerät zugreifen und sie auf einem großen Bildschirm anzeigen.

### Hinweis:

- Citrix Casting für Windows unterstützt Citrix Ready Workspace Hub Version 2.40.3839 und höher. Frühere Versionen werden möglicherweise nicht erkannt oder verursachen einen Castingfehler.
- Citrix Casting wird in der Citrix Workspace-App für Windows (Store) nicht unterstützt.

### Voraussetzungen:

- Bluetooth ist zur Hub-Erkennung auf dem Gerät aktiviert.
- Citrix Ready Workspace Hub und Citrix Workspace-App müssen sich im selben Netzwerk befinden.
- Port 55555 ist zwischen dem Gerät mit ausgeführter Citrix Workspace-App und dem Citrix Ready Workspace Hub zugelassen.
- Port 1494 darf für Citrix Casting nicht blockiert sein.
- Port 55556 ist der Standardport für SSL-Verbindungen zwischen Mobilgeräten und dem Citrix Ready Workspace Hub. Sie können in den Einstellungen von Raspberry Pi einen anderen SSL-Port konfigurieren. Wenn der SSL-Port blockiert ist, können die Benutzer keine SSL-Verbindungen zum Workspace Hub herstellen.

- Citrix Casting wird nur unter Microsoft Windows 10 Version 1607 und höher oder auf Windows Server 2016 unterstützt.
- Führen Sie während der Installation den Befehl `/IncludeCitrixCasting` aus, um Citrix Casting zu aktivieren.

## Konfigurieren des Citrix Casting-Starts

### Hinweis:

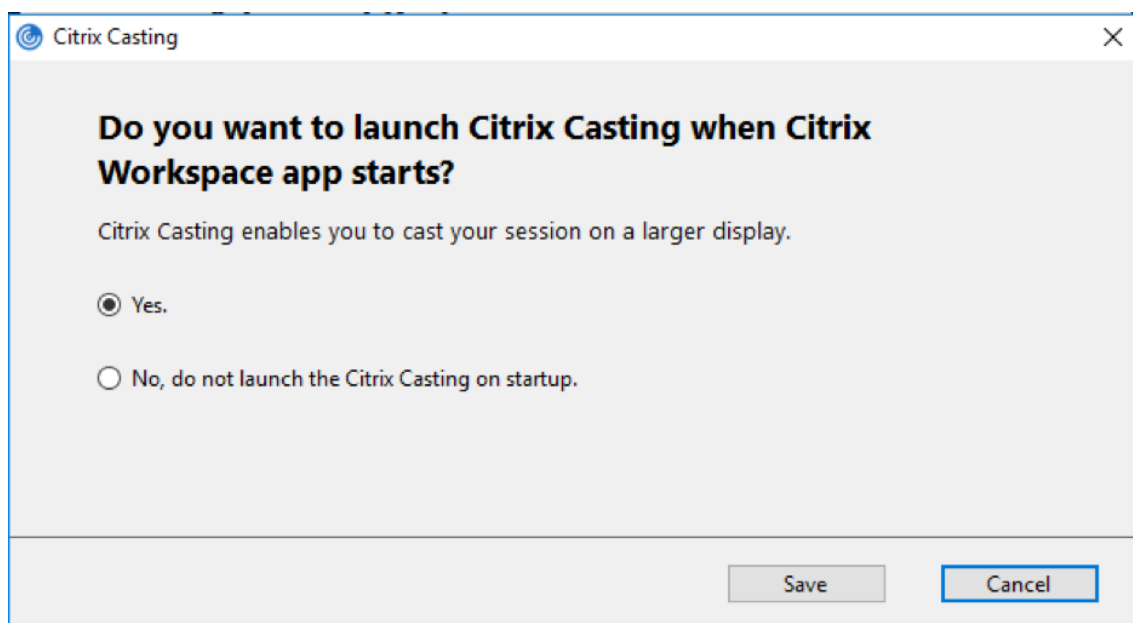
Sie können die Seite “Erweiterte Einstellungen” ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter [Erweiterte Einstellungen](#).

1. Klicken Sie im Infobereich mit der rechten Maustaste auf das Symbol der Citrix Workspace-App und wählen Sie **Erweiterte Einstellungen**.

Das Dialogfeld **Erweiterte Einstellungen** wird angezeigt.

2. Wählen Sie **Citrix Casting**.

Das Dialogfeld **Citrix Casting** wird angezeigt.



3. Wählen Sie eine dieser Optionen:

- Ja – Citrix Casting wird beim Start der Citrix Workspace-App ebenfalls gestartet.
- Nein, Citrix Casting beim Start nicht starten – Gibt an, dass Citrix Casting beim Start der Citrix Workspace-App nicht gestartet wird.

**Hinweis:**

Bei Auswahl der Option **Nein** wird die aktuelle Bildschirmcastingsitzung nicht beendet. Die Einstellung wird erst beim nächsten Start der Citrix Workspace-App wirksam.

4. Klicken Sie auf **Speichern**, um die Änderung zu übernehmen.

### **Citrix Casting mit der Citrix Workspace-App verwenden**

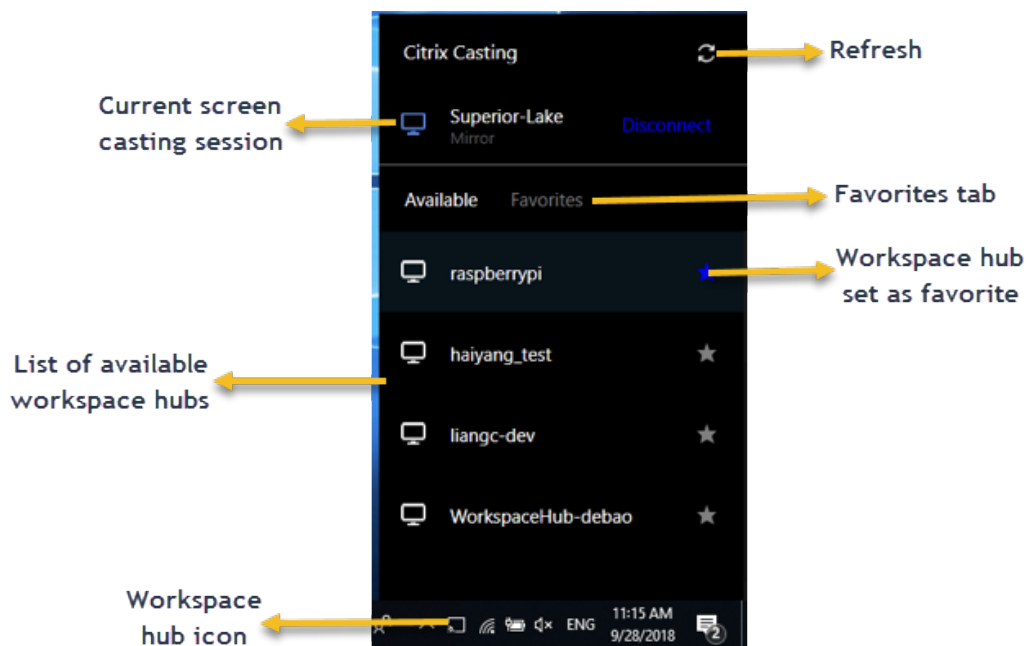
1. Melden Sie sich an der Citrix Workspace-App an und aktivieren Sie Bluetooth auf Ihrem Gerät.  
Die Liste der verfügbaren Hubs wird angezeigt. Die Liste ist nach dem RSSI-Wert des Beaconpakets der Workspace Hubs sortiert.
2. Wählen Sie den Workspace Hub aus, an den Sie Ihre Anzeige übertragen möchten, und wählen Sie eine der folgenden Optionen:
  - Mit **Spiegeln** können Sie den primären Bildschirm duplizieren und die Anzeige an das verbundene Workspace Hub-Gerät übertragen.
  - Mit **Erweitern** können Sie den Bildschirm des Workspace Hub-Geräts als sekundären Bildschirm verwenden.

**Hinweis:**

Beim Beenden der Citrix Workspace-App wird Citrix Casting nicht beendet.

Im Infobereich von **Citrix Casting** sind folgende Optionen verfügbar:

1. Die aktuelle Bildschirmcastingsitzung wird oben angezeigt.
2. Symbol **Aktualisieren**.
3. Wählen Sie **Trennen**, um die aktuelle Bildschirmcastingsitzung auf dem Workspace Hub zu beenden.
4. Mit dem Stern fügen Sie den Workspace Hub zu **Favoriten** hinzu.
5. Klicken Sie mit der rechten Maustaste auf das Workspace Hub-Symbol im Infobereich und wählen Sie **Beenden**, um die Bildschirmcastingsitzung zu trennen und den Citrix Ready Workspace Hub zu beenden.



### Checkliste bei Problemen

Prüfen Sie folgende Faktoren, wenn die Citrix Workspace-App keine verfügbaren Workspace Hubs im Umfeld erkennt oder mit ihnen nicht kommunizieren kann:

1. Citrix Workspace-App und Citrix Ready Workspace Hub sind mit demselben Netzwerk verbunden.
2. Bluetooth ist aktiviert und funktioniert ordnungsgemäß auf dem Gerät, auf dem die Citrix Workspace-App ausgeführt wird.
3. Das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, liegt in Reichweite des Citrix Ready Workspace Hub, also weniger als 10 Meter entfernt und nicht hinter einer Wand oder einem anderen Hindernis.
4. Öffnen Sie einen Browser in der Citrix Workspace-App und geben Sie [http://<hub\\_ip>:55555/device-details.xml](http://<hub_ip>:55555/device-details.xml) ein, um zu überprüfen, ob die Details des Workspace Hub-Geräts angezeigt werden.
5. Klicken Sie in Citrix Ready Workspace Hub auf **Aktualisieren** und versuchen Sie erneut, eine Verbindung zum Workspace Hub herzustellen.

### Bekannte Probleme und Einschränkungen

- Citrix Casting funktioniert nur, wenn das Gerät mit demselben Netzwerk wie der Citrix Ready Workspace Hub verbunden ist.

- Bei Netzwerkproblemen kann es zu einer verzögerten Anzeige auf dem Workspace Hub-Gerät kommen.
- Bei Auswahl von **Erweitern** blinkt der primäre Bildschirm, auf dem die Citrix Ready Workspace-App gestartet wird, mehrmals.
- Im Modus **Erweitern** können Sie die sekundäre Anzeige nicht als primäre Anzeige festlegen.
- Die Bildschirmcastingsitzung wird automatisch beendet, wenn die Anzeigeeinstellungen auf dem Gerät geändert werden. Dies kann beispielsweise auftreten, wenn Sie die Bildschirmauflösung oder Bildschirmausrichtung ändern.
- Wenn das Gerät, auf dem die Citrix Workspace-App ausgeführt wird, während der Bildschirmcastingsitzung gesperrt, inaktiviert oder in den Ruhezustand versetzt wird, wird beim Anmelden ein Fehler angezeigt.
- Mehrere Bildschirmcastingsitzungen werden nicht unterstützt.
- Die von Citrix Casting unterstützte maximale Bildschirmauflösung beträgt 1920 x 1440.
- Citrix Casting unterstützt Citrix Ready Workspace Hub Version 2.40.3839 und höher. Frühere Versionen werden möglicherweise nicht erkannt oder verursachen einen Castingfehler.
- Das Feature wird in der Citrix Workspace-App für Windows (Store) nicht unterstützt.
- Unter Windows 10, Build 1607 wird Citrix Casting im Modus **Erweitert** u. U. nicht richtig positioniert.

Weitere Informationen zu Citrix Ready Workspace Hub finden Sie unter [Citrix Ready Workspace Hub](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

## SaaS-Apps

April 22, 2024

Der sichere Zugriff auf SaaS-Anwendungen bietet eine einheitliche Benutzererfahrung bei der Bereitstellung veröffentlichter SaaS-Anwendungen. SaaS-Anwendungen sind mit Single Sign-On verfügbar. Administratoren können jetzt Netzwerk und Endbenutzergeräte eines Unternehmens vor Malware und Datenlecks schützen. Administratoren können dies erreichen, indem sie den Zugriff auf bestimmte Websites und Websitekategorien filtern.

Die Citrix Workspace-App für Windows unterstützt die Verwendung von SaaS-Apps unter Einsatz des Citrix Secure Private Access. Über diesen Dienst können Administratoren eine geschlossene Erfahrung mit Single Sign-On und Inhaltsinspektion bereitstellen.

Die Bereitstellung von SaaS-Anwendungen über die Cloud hat folgende Vorteile:

- Einfache Konfiguration: einfach zu bedienen, zu aktualisieren und zu nutzen.
- Single Sign-On: mühelose Anmeldung.

- Standardvorlage für verschiedene Anwendungen: vorlagenbasierte Konfiguration beliebiger Anwendungen.

Die Citrix Workspace-App startet die SaaS-Anwendungen in Citrix Enterprise Browser (zuvor “Citrix Workspace Browser”). Informationen finden Sie in der Dokumentation zu [Citrix Enterprise Browser](#).

### **Einschränkungen:**

- Wenn Sie eine veröffentlichte App mit aktivierter Druckoption und deaktivierter Downloadoption starten und einen Druckbefehl an eine gestartete App übergeben, können Sie die betreffende PDF-Datei möglicherweise trotzdem speichern. Sollen Downloads auf jeden Fall unterbunden werden, deaktivieren Sie auch die Druckoption.
- In einer App eingebettete Videos funktionieren möglicherweise nicht.
- Sie können SaaS-Apps nicht mit Storebrowse-Befehlen öffnen.

Weitere Informationen zur Konfiguration von Workspace finden Sie unter [Workspacekonfiguration](#) in der Dokumentation zu Citrix Cloud.

## **Datensammlung und Überwachung**

April 22, 2024

### **Citrix Analytics**

Die Citrix Workspace-App ermöglicht die sichere Übertragung von Protokollen an Citrix Analytics. Wenn die Funktion aktiviert ist, werden die Protokolle auf Citrix Analytics-Servern analysiert und gespeichert. Weitere Informationen zu Citrix Analytics finden Sie unter [Citrix Analytics](#).

### **Verbesserung des Citrix Analytics-Diensts**

Ab diesem Release ermöglicht die Citrix Workspace-App die sichere Übertragung der öffentlichen IP-Adresse des letzten Netzwerk-Hops an den Citrix Analytics-Dienst. Die Daten werden pro Sitzungsstart erfasst. Mit den Daten kann der Citrix Analytics-Dienst analysieren, ob Leistungsprobleme auf bestimmte geografische Bereiche zurückzuführen sind.

Standardmäßig werden die IP-Adressprotokolle an den Citrix Analytics-Dienst gesendet. Sie können diese Option jedoch in der Citrix Workspace-App mit dem Registrierungs-Editor deaktivieren.

Um die Übertragung von IP-Adressprotokollen zu deaktivieren, navigieren Sie zum folgenden Registrierungspfad und legen Sie den Schlüssel `SendPublicIPAddress` auf **Aus** fest.



- Navigieren Sie auf 64-Bit-Windows-Maschinen zu: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`.
- Navigieren Sie auf 32-Bit-Windows-Maschinen zu: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`.

**Hinweis:**

- Die IP-Adressübertragung gelingt nicht immer perfekt. Zwar überträgt die Citrix Workspace-App jede IP-Adresse, auf der sie gestartet wird, jedoch sind einige der Adressen möglicherweise nicht korrekt.
- Stellen Sie in geschlossenen Kundenumgebungen, in denen die Endpunkte innerhalb eines Intranets betrieben werden, sicher, dass die URL `https://locus.analytics.cloud.com/api/locateip` auf dem Endpunkt auf einer Positivliste steht.

Die Citrix Workspace-App überträgt Daten von ICA-Sitzungen, die Sie über einen Browser starten, sicher an den Citrix Analytics-Dienst.

Weitere Informationen dazu, wie die Leistungsanalyse diese Informationen verwendet, finden Sie unter [Self-Service Search for Performance](#).

### **Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP)**

---

Erfasste Daten	Beschreibung	Verwendungszweck
Konfigurations- und Nutzungsdaten	Das Citrix-Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) sammelt Konfigurations- und Nutzungsdaten in der Citrix Workspace-App für Windows und sendet die Daten automatisch an Citrix und Google Analytics.	Diese Daten helfen Citrix, Qualität, Funktionalität und Leistung der Citrix Workspace-App zu verbessern, Ressourcen für Produktentwicklungszwecke angemessen zuzuweisen, Servicelevel aufrechtzuerhalten und Personal- und Infrastrukturinvestitionen zu verwalten.

---

#### **Erfasste Daten**

Wie oben erwähnt, erfasst Citrix Konfigurations- und Nutzungsdaten der Citrix Workspace-App, um die Qualität, Funktionalität und Leistung der Workspace-App zu verbessern und um zu ermöglichen, dass

Citrix Ressourcen für Produktentwicklungszwecke sowie zur Aufrechterhaltung der Servicelevel und zur Verwaltung von Personal- und Infrastrukturinvestitionen angemessen zuweist. Die Daten werden nur in aggregierter Form verwendet und analysiert. Kein Benutzer oder dessen Computer wird herausgegriffen und es wird keine Analyse für bestimmte Endbenutzer auf der Grundlage der CEIP-Daten durchgeführt.

Folgende CEIP-Datenelemente werden von Google Analytics und Citrix Analytics erfasst:

---

Betriebssystemversion*	Citrix Workspace-App-Version*	Authentifizierungskonfiguration	Spalte der Citrix Workspace-App
Sitzungsstartmethode	Verbindungsfehler	Verbindungsprotokoll	VDA-Informationen
Installerkonfiguration	Status des Installers	Clienttastaturlayout	Storekonfiguration
Einstellung für automatische Aktualisierung	Nutzung des Connection Centers	Konfiguration von App Protection	Grund für das Offline-Banner
Gerätemodell/Eigenschaften	Citrix Virtual Apps and Desktops-Sitzungsstartstatus	Name der virtuellen App/des Desktops	Status für automatische Updates
Verbindungsleasedetails	Nutzung des Features zur URL-Migration von StoreFront zu Workspace	Citrix Enterprise Browser - Nutzung	Auto-Updatekanal
Details zum Timeout bei Inaktivität	Citrix Enterprise Browser-Version		

---

### Einstellungen für die Datensammlung

Ab Version 2205 können sowohl Benutzer als auch Administratoren das Senden von CEIP-Daten beenden (mit Ausnahme der beiden Datenelemente, die wie im Hinweis unten angegeben blockiert werden können), indem sie die folgenden Schritte ausführen.

1. Klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Citrix Workspace-App-Symbol.
2. Wählen Sie **Erweiterte Einstellungen**.  
Das Dialogfeld **Erweiterte Einstellungen** wird angezeigt.
3. Wählen Sie **Datensammlung**.
4. Wählen Sie **Nein, danke**, um CEIP zu deaktivieren und die Teilnahme abzulehnen.
5. Klicken Sie auf **Speichern**.

Als Administrator können Sie auch zum folgenden Registrierungseintrag navigieren und den Wert wie vorgeschlagen festlegen:

**Pfad:** HKEY\_LOCAL\_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP

**Schlüssel:** Enable\_CEIP

**Wert:** False

**Hinweis:**

Wenn Sie **Nein, danke** auswählen oder den Schlüssel `Enable_CEIP` auf `False` festlegen, um auch die letzten beiden CEIP-Datenelemente (Betriebssystemversion und Version der Citrix Workspace-App) nicht zu senden, navigieren Sie zum folgenden Registrierungseintrag und legen Sie den Wert fest:

**Pfad:** HKEY\_LOCAL\_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP

**Schlüssel:** DisableHeartbeat

**Wert:** True

### Weitere Informationen

Citrix verarbeitet Ihre Daten gemäß den Bedingungen Ihres Vertrags mit Citrix und schützt sie, wie im [Citrix Services Security Exhibit](#) festgelegt. Das Citrix Services Security Exhibit ist im [Citrix Trust Center](#) verfügbar.

## Sicherheit und Authentifizierung

April 22, 2024

In diesem Abschnitt wird Folgendes beschrieben:

- [Sicherheit](#)
- [Sichere Kommunikation](#)
- [Authentifizierung](#)
  - [Domänen-Passthrough-Zugriffsmatrix](#)
  - [Domänen-Passthrough-Authentifizierung an Citrix Workspace mit On-Premises-Citrix Gateway als Identitätsanbieter](#)
  - [Domänen-Passthrough-Authentifizierung an Citrix Workspace mit Azure Active Directory als Identitätsanbieter](#)

- [Domänen-Passthrough-Authentifizierung an Citrix Workspace mit Okta als Identitätsanbieter](#)

## Sicherheit

April 22, 2024

### App Protection

App Protection ist ein Zusatzfeature, das erweiterte Sicherheit bei der Verwendung von Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) bietet. Sie verringert das Risiko, dass Clients Keylogging und Screenshot-Malware zulassen. App Protection verhindert das Exfiltrieren von Benutzeranmeldeinformationen und anderen vertraulichen Informationen auf dem Bildschirm. Die Funktion verhindert, dass Benutzer und Angreifer Screenshots erstellen und Keylogger verwenden, um vertrauliche Informationen zu lesen und zu nutzen. Weitere Informationen finden Sie unter [App Protection](#).

#### Haftungsausschluss

Richtlinien von App Protection 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.

Informationen zur Konfiguration von App Protection in der Citrix Workspace-App für Windows finden Sie in dem Abschnitt zur Citrix Workspace-App für Windows im Artikel [Konfiguration](#).

#### Hinweis:

App Protection wird nur bei einem Upgrade auf Version 1912 und höher unterstützt.

### Verbesserte ICA-Dateisicherheit

Dieses Feature bietet erhöhte Sicherheit für die Handhabung von ICA-Dateien beim Starten von Sitzungen mit virtuellen Apps und Desktops.

Mit der Citrix Workspace-App können Sie die ICA-Datei beim Starten einer Sitzung mit virtuellen Apps und Desktops im Systemspeicher speichern statt auf dem lokalen Datenträger.

Diese Funktion zielt darauf ab, Oberflächenangriffe und Malware auszuschließen, die die ICA-Datei missbrauchen könnten, wenn sie lokal gespeichert wird. Das Feature ist auch in Sitzungen mit virtuellen Apps und Desktops verfügbar, die im Workspace für Web gestartet werden.

## Konfiguration

Die ICA-Dateisicherheit wird auch unterstützt, wenn über das Internet auf Citrix Workspace oder StoreFront zugegriffen wird. Die Clienterkennung ist eine Voraussetzung für das Funktionieren des Features, wenn darauf über das Internet zugegriffen wird. Wenn Sie über einen Browser auf StoreFront zugreifen, aktivieren Sie die folgenden Attribute in der Datei `web.config` in StoreFront-Bereitstellungen:

---

StoreFront-Version	Attribut
2.x	<code>pluginassistant</code>
3.x	<code>protocolHandler</code>

---

Klicken Sie bei der Anmeldung am Store über den Browser auf **Workspace-App ermitteln**. Wenn die Aufforderung nicht angezeigt wird, löschen Sie die Browsercookies und versuchen Sie es erneut.

Wenn es sich um eine Workspace-Bereitstellung handelt, finden Sie die Einstellungen für die Clienterkennung unter **Kontoeinstellungen > Erweitert > Startpräferenz für Apps und Desktops**.

Sie können zusätzliche Maßnahmen ergreifen, damit Sitzungen nur mit der ICA-Datei gestartet werden, die im Systemspeicher gespeichert ist. Verwenden Sie eine der folgenden Methoden:

- Administrative Gruppenrichtlinienobjektvorlage auf dem Client
- Global App Config Service
- Workspace für Web.

## Verwenden des Gruppenrichtlinienobjekts:

Gehen Sie wie folgt vor, um Sitzungsstarts von ICA-Dateien zu blockieren, die auf dem lokalen Datenträger gespeichert sind:

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 > Clientengine**.

3. Wählen Sie die Richtlinie **Sitzungsstart mit ICA-Datei sichern** und legen Sie sie auf **Aktiviert** fest.
4. Klicken Sie auf **Anwenden** und auf **OK**.

#### **Verwenden des Global App Config Service:**

Sie können den globalen App Config Service über die Citrix Workspace-App 2106 verwenden.

Gehen Sie wie folgt vor, um Sitzungsstarts von ICA-Dateien zu blockieren, die auf dem lokalen Datenträger gespeichert sind:

Setzen Sie das Attribut **Block Direct ICA File Launches** auf **True**.

Weitere Informationen zum Global App Config Service finden Sie in der Dokumentation zum [Global App Config Service](#).

#### **Workspace für Web verwenden:**

Gehen Sie wie folgt vor, um den Download der ICA-Datei auf den lokalen Datenträger zu unterbinden, wenn Sie Workspace für Web verwenden:

Führen Sie das PowerShell-Modul aus. Siehe [Configure DisallowICADownload](#).

#### **Hinweis:**

Die Richtlinie **DisallowICADownload** ist für StoreFront-Bereitstellungen nicht verfügbar.

### **Inaktivitätstimeout für Workspace-Sitzungen**

Mit dem Inaktivitätstimeout können Administratoren festlegen, nach wie viel Zeit inaktive Benutzer automatisch von der Citrix Workspace-Sitzung abgemeldet werden. Sie werden automatisch von Workspace abgemeldet, wenn Maus, Tastatur oder Toucheingabe im angegebenen Zeitintervall inaktiv sind. Das Inaktivitätstimeout hat keine Auswirkungen auf aktive Sitzungen mit virtuellen Apps oder Desktops oder auf Citrix StoreFront-Stores.

Der Wert für das Inaktivitätstimeout kann zwischen einer Minute und 1440 Minuten liegen. Standardmäßig ist das Inaktivitätstimeout nicht konfiguriert. Administratoren können die Eigenschaft "inactivityTimeoutInMinutes" mit einem PowerShell-Modul konfigurieren. Klicken Sie [hier](#), um die PowerShell-Module für die Citrix Workspace-Konfiguration herunterzuladen.

Für die Endbenutzererfahrung gilt Folgendes:

- Drei Minuten vor der Abmeldung wird eine Benachrichtigung in Ihrem Sitzungsfenster angezeigt. Sie können angemeldet bleiben oder sich abmelden.
- Die Benachrichtigung wird nur angezeigt, wenn der konfigurierte Wert für das Inaktivitätstimeout größer oder gleich fünf Minuten ist.

- Benutzer können auf **Angemeldet bleiben** klicken, um die Benachrichtigung zu schließen und die App weiter zu verwenden. In diesem Fall wird der Inaktivitätstimer auf den konfigurierten Wert zurückgesetzt. Sie können auch auf **Abmelden** klicken, um die Sitzung für den aktuellen Store zu beenden.

**Hinweis:**

Administratoren können das Inaktivitätstimeout nur für Workspace-Sitzungen (Cloud) konfigurieren.

## Sichere Kommunikation

April 22, 2024

Zum Sichern der Kommunikation zwischen dem Citrix Virtual Apps and Desktops-Server und der Citrix Workspace-App können Sie Citrix Workspace-App-Verbindungen mit verschiedenen sicheren Technologien wie den Folgenden integrieren:

- Citrix Gateway: Weitere Informationen finden Sie im vorliegenden Abschnitt und in der Dokumentation zu Citrix Gateway und StoreFront.
- Eine Firewall: Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden.
- Transport Layer Security (TLS) Versionen 1.0 bis 1.3 werden unterstützt.
- Vertrauenswürdige Server zum Herstellen von Vertrauensbeziehungen in Citrix Workspace-App-Verbindungen.
- ICA-Dateisignierung
- Schutz durch lokale Sicherheitsautorität
- Proxyserver nur für Citrix Virtual Apps-Bereitstellungen: Ein SOCKS-Proxyserver oder ein sicherer Proxyserver. Proxyserver helfen, den Zugriff auf und vom Netzwerk zu beschränken. Sie verarbeiten außerdem die Verbindungen zwischen der Citrix Workspace-App und dem Server. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.
- Ausgehender Proxy

### Citrix Gateway

Citrix Gateway (ehemals Access Gateway) sichert Verbindungen mit StoreFront-Stores. Administratoren können hiermit zudem präzise den Benutzerzugriff auf Desktops und Anwendungen steuern.

Herstellen einer Verbindung mit Desktops und Anwendungen über Citrix Gateway:

1. Nutzen Sie eine der folgenden Methoden, um die vom Administrator erhaltene Citrix Gateway-URL einzugeben:

- Bei der ersten Verwendung der Self-Service-Benutzeroberfläche werden Sie aufgefordert, die URL im Dialogfeld **Konto hinzufügen** einzugeben.
- Wenn Sie die Self-Service-Benutzeroberfläche später verwenden, geben Sie die URL ein, indem Sie auf **Einstellungen > Konten > Hinzufügen** klicken.
- Beim Herstellen einer Verbindung mit dem Befehl “storebrowse” geben Sie die URL in der Befehlszeile ein.

Über die URL wird das Gateway und optional ein bestimmter Store angegeben:

- Zum Herstellen einer Verbindung mit dem ersten Store, den die Citrix Workspace-App findet, verwenden Sie eine URL im folgenden Format:

- <https://gateway.company.com>

- Zum Herstellen einer Verbindung mit einem bestimmten Store verwenden Sie eine URL im folgenden Format: <https://gateway.company.com?<storename>>. Diese dynamische URL besitzt kein standardmäßiges Format, verwenden Sie kein Gleichheitszeichen (=) in der URL. Beim Herstellen einer Verbindung mit einem bestimmten Store mit storebrowse müssen Sie die URL im storebrowse-Befehl eventuell in Anführungszeichen setzen.

1. Wenn Sie dazu aufgefordert werden, stellen Sie eine Verbindung mit dem Store (über das Gateway) unter Verwendung Ihres Benutzernamens, Kennworts und Sicherheitstokens her. Weitere Informationen zu diesem Schritt finden Sie in der Citrix Gateway-Dokumentation.

Wenn die Authentifizierung abgeschlossen ist, werden Ihre Desktops und Anwendungen angezeigt.

## Herstellen einer Verbindung durch eine Firewall

Firewalls entscheiden anhand der Zieladresse und des Zielports von Datenpaketen, ob diese Pakete weitergeleitet werden. Wenn Sie eine Firewall verwenden, kann die Citrix Workspace-App für Windows über die Firewall mit dem Webserver und dem Citrix Server kommunizieren.

### Allgemeine Citrix Kommunikationsports

---

Quelle	Typ	Port	Details
Citrix Workspace-App	TCP	80/443	Kommunikation mit StoreFront



---

Quelle	Typ	Port	Details
ICA oder HDX	TCP/UDP	1494	Zugriff auf Anwendungen und virtuelle Desktops
ICA oder HDX mit Sitzungszuverlässigkeit	TCP/UDP	2598	Zugriff auf Anwendungen und virtuelle Desktops
ICA oder HDX über TLS	TCP/UDP	443	Zugriff auf Anwendungen und virtuelle Desktops

---

Weitere Informationen zu den Ports finden Sie im Knowledge Center-Artikel [CTX101810](#).

## TLS (Transport Layer Security)

Transport Layer Security (TLS) ersetzt das SSL-Protokoll (Secure Sockets Layer). Die IETF (Internet Engineering Taskforce) hat den Standard zu TLS umbenannt, als diese Organisation die Verantwortung für die Entwicklung von TLS als offenem Standard übernahm.

TLS sichert die Datenkommunikation mit Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfen der Nachrichtenintegrität. Einige Organisationen, u. a. amerikanische Regierungsstellen, verlangen das Sichern der Datenkommunikation mit TLS. Diese Organisationen verlangen ggf. auch die Verwendung überprüfter Kryptografie, wie FIPS 140. FIPS 140 ist ein Standard für die Kryptografie.

Um die TLS-Verschlüsselung als Kommunikationsmedium zu verwenden, müssen Sie das Benutzergerät und die Citrix Workspace-App konfigurieren. Weitere Informationen zum Sichern der StoreFront-Kommunikation finden Sie unter [Sicherheit](#) in der StoreFront-Dokumentation. Informationen zum Sichern des VDA finden Sie unter [Transport Layer Security \(TLS\)](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Sie können die folgenden Richtlinien zu folgenden Zwecken verwenden:

- Erzwingen der Verwendung von TLS: Es wird empfohlen, TLS für Verbindungen über nicht vertrauenswürdige Netzwerke zu verwenden, einschließlich des Internets.
- Erzwingen der Verwendung von FIPS (Federal Information Processing Standards): genehmigte Kryptografie gemäß den Empfehlungen im Dokument NIST SP 800-52. Diese Optionen sind standardmäßig deaktiviert.
- Erzwingen der Verwendung einer bestimmten Version von TLS und bestimmter TLS-Verschlüsselungssammlungen: Citrix unterstützt die Protokolle TLS 1.0, TLS 1.1 und TLS 1.2.

- Herstellen von Verbindungen mit bestimmten Servern.
- Überprüfen, ob das Serverzertifikat widerrufen wurde.
- Überprüfen auf eine bestimmte Serverzertifikatausstellungsrichtlinie.
- Auswählen eines bestimmten Clientzertifikats, wenn der Server für die Anforderung konfiguriert ist.

Die Citrix Workspace-App für Windows unterstützt die folgenden Verschlüsselungssammlungen für das TLS 1.2-Protokoll:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Informationen zu den unterstützten Verschlüsselungssammlungen finden Sie im Knowledge Center-Artikel [CTX250104](#).

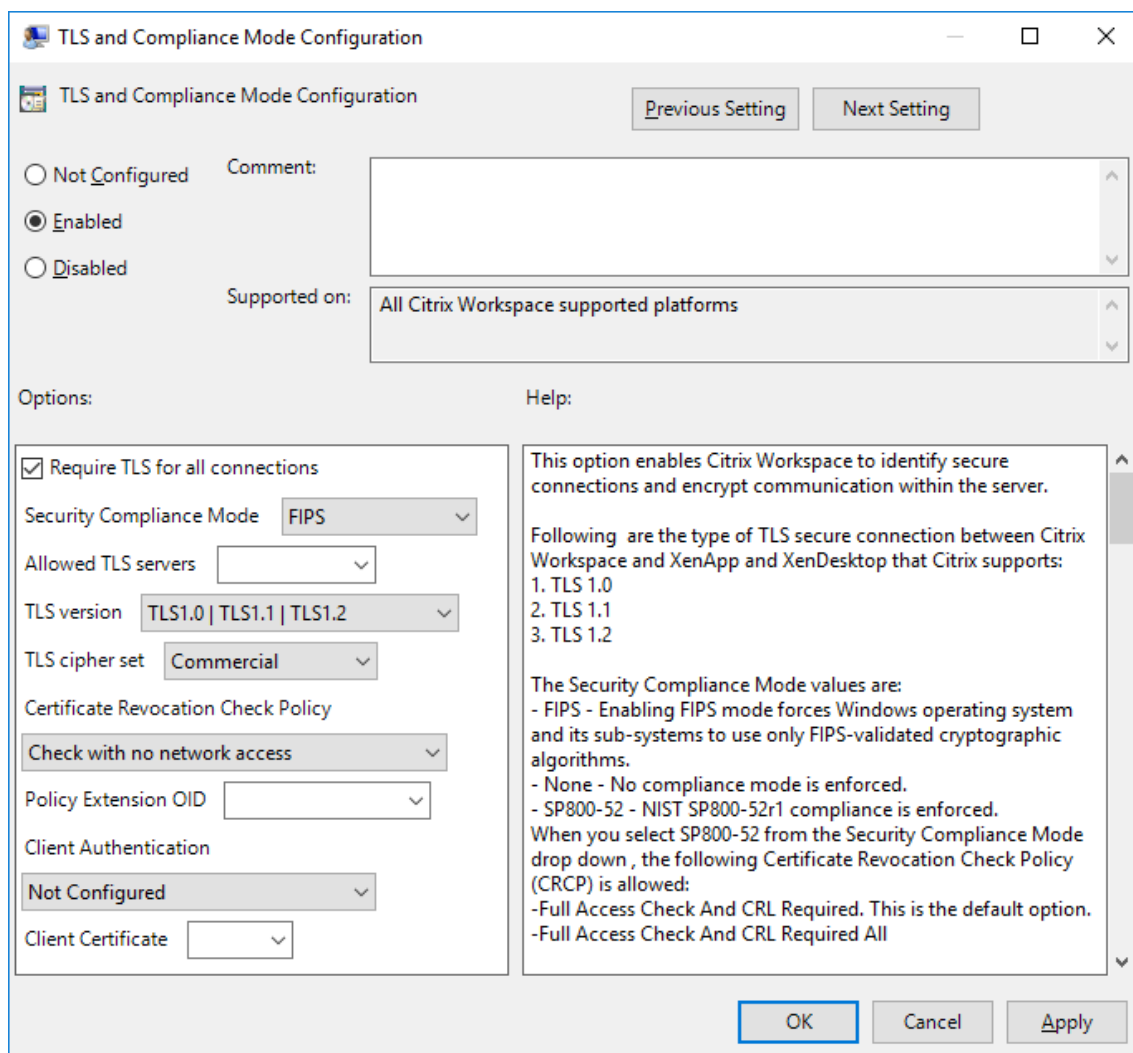
#### **Wichtig:**

Die folgenden Verschlüsselungssammlungen sind aus Sicherheitsgründen veraltet:

- Verschlüsselungssammlungen RC4 und 3DES
- Verschlüsselungssammlungen mit dem Präfix “TLS\_RSA\_”
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009d)
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009c)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003d)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)
- TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005)
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a)

#### **Unterstützung für TLS**

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Netzwerkrouting**. Wählen Sie dann die Richtlinie **Konfiguration von TLS und Konformitätsmodus**.



3. Wählen Sie **Aktiviert**, um sichere Verbindungen zu aktivieren und die Kommunikation auf dem Server zu verschlüsseln. Legen Sie folgende Optionen fest:

**Hinweis:**

Citrix empfiehlt TLS für sichere Verbindungen.

- a) Aktivieren Sie **TLS für alle Verbindungen verwenden**. Damit erzwingen Sie, dass die Citrix Workspace-App TLS für alle Verbindungen mit veröffentlichten Anwendungen und Desktops verwendet.
- b) Wählen Sie im Menü **Sicherheitskonformitätsmodus** die geeignete Option aus:
  - i. **Ohne:** Es wird kein Konformitätsmodus erzwungen.
  - ii. **SP800-52:** Wählen Sie **SP800-52** für Konformität mit NIST SP 800-52. Wählen Sie diese Option nur, wenn Server oder Gateway gemäß den Empfehlungen in NIST SP 800-52 konfiguriert sind.

**Hinweis:**

Bei Auswahl von **SP800-52** wird automatisch FIPS-validierte Kryptografie verwendet, selbst wenn **FIPS aktivieren** nicht ausgewählt ist. Aktivieren Sie auch die Windows-Sicherheitsoption **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden**. Andernfalls kann die Citrix Workspace-App u. U. keine Verbindung zu den veröffentlichten Anwendungen und Desktops herstellen.

Wenn Sie **SP800-52** auswählen, legen Sie die Einstellung für **Richtlinie ‘Zertifikatsprüfung’** auf **Volle Zugriffsprüfung und CRL erforderlich** fest.

Wenn Sie **SP800-52** auswählen, überprüft die Citrix Workspace-App, ob das Serverzertifikat den Empfehlungen in NIST SP 800-52 entspricht. Wenn dies nicht der Fall ist, kann die Citrix Workspace-App möglicherweise keine Verbindung herstellen.

- i. **FIPS aktivieren:** Wählen Sie diese Option, um die Verwendung von FIPS-validierter Kryptografie zu erzwingen. Aktivieren Sie auch die Windows-Sicherheitsoption aus der Gruppenrichtlinie des Betriebssystems **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden**. Andernfalls kann die Citrix Workspace-App u. U. keine Verbindung zu veröffentlichten Anwendungen und Desktops herstellen.
- c) Wählen Sie im Dropdownmenü neben **Zulässige TLS-Server** die Portnummer aus. Verwenden Sie eine durch Trennzeichen getrennte Liste, um sicherzustellen, dass die Citrix Workspace-App Verbindungen nur zu angegebenen Servern herstellt. Sie können Platzhalter und Portnummern angeben. Beispielsweise ermöglicht \*.citrix.com: 4433 die Verbindung mit allen Servern auf Port 4433, deren allgemeiner Name mit .citrix.com endet. Die Genauigkeit der Informationen in einem Sicherheitszertifikat wird durch den Aussteller des Zertifikats bestätigt. Wenn Citrix Workspace den Aussteller nicht erkennt oder ihm nicht traut, wird die Verbindung abgelehnt.
- d) Wählen Sie im Menü **TLS-Version** eine der folgenden Optionen:
  - **TLS 1.0, TLS 1.1 oder TLS 1.2:** Dies ist die Standardeinstellung. Diese Option wird nur empfohlen, wenn die Kompatibilität mit TLS 1.0 eine Geschäftsanforderung ist.
  - **TLS 1.1, TLS 1.2:** Mit dieser Option stellen Sie sicher, dass TLS 1.1 oder TLS 1.2 für Verbindungen verwendet wird.
  - **TLS 1.2:** Diese Option wird empfohlen, wenn TLS 1.2 eine Geschäftsanforderung ist.
- a) **TLS-Verschlüsselungssatz:** Um die Verwendung von bestimmten TLS-Verschlüsselungssätzen zu erzwingen, wählen Sie “Behörden”(GOV), “Kommerziell”(COM) oder “Alle”(ALL). Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX250104](#).

- b) Wählen Sie im Menü **Richtlinie 'Zertifikatssperrüberprüfung'** eine der folgenden Optionen aus:
- **Prüfung ohne Netzwerkzugriff:** Es wird eine Überprüfung der Zertifikatssperrliste durchgeführt. Es werden nur lokale Zertifikatssperrlisten-Stores verwendet. Alle Verteilungspunkte werden ignoriert. Eine Überprüfung der Zertifikatssperrliste zum Verifizieren des Serverzertifikats, das vom Ziel-SSL-Relay bzw. Citrix Secure Web Gateway-Server bereitgestellt ist, ist nicht obligatorisch.
  - **Volle Zugriffsprüfung:** Es wird eine Überprüfung der Zertifikatssperrliste durchgeführt. Lokale Zertifikatssperrlisten-Speicher und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Eine Überprüfung der Zertifikatssperrliste zum Verifizieren des Serverzertifikats, das vom Zielservers bereitgestellt wird, ist nicht kritisch.
  - **Volle Zugriffsprüfung und CRL erforderlich:** Die Zertifikatssperrliste wird ohne Stamm-Zertifizierungsstelle überprüft. Lokale Zertifikatssperrlisten-Speicher und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden aller erforderlichen Zertifikatssperrlisten ist für die Überprüfung wichtig.
  - **Volle Zugriffsprüfung und alle CRL erforderlich:** Die Zertifikatssperrliste und die Stamm-Zertifizierungsstelle werden überprüft. Lokale Zertifikatssperrlisten-Speicher und alle Verteilungspunkte werden verwendet. Wenn Sperrinformationen für ein Zertifikat gefunden werden, wird die Verbindung abgelehnt. Das Finden aller erforderlichen Zertifikatssperrlisten ist für die Überprüfung wichtig.
  - **Keine Prüfung:** Es wird keine Überprüfung der Zertifikatssperrliste durchgeführt.
- a) Mit der **Richtlinienerweiterungs-OID** können Sie die Citrix Workspace-App auf Verbindungen mit Servern beschränken, auf denen eine bestimmte Zertifikatausstellungsrichtlinie festgelegt ist. Wenn Sie **Richtlinienerweiterungs-OID** auswählen, akzeptiert die Citrix Workspace-App nur Serverzertifikate mit dieser Richtlinienerweiterungs-OID.
- b) Wählen Sie im Menü zur **Clientauthentifizierung** eine der folgenden Optionen aus:
- **Deaktiviert:** Die Clientauthentifizierung ist deaktiviert.
  - **Zertifikatauswähler anzeigen:** Der Benutzer wird immer aufgefordert, ein Zertifikat auszuwählen.
  - **Wenn möglich automatisch auswählen:** Die Aufforderung wird nur angezeigt, wenn mehrere Zertifikate zur Identifizierung ausgewählt werden können.
  - **Nicht konfiguriert:** Gibt an, dass die Clientauthentifizierung nicht konfiguriert ist.

- **Angegebenes Zertifikat verwenden:** Verwenden Sie das unter “Clientzertifikat” festgelegte Clientzertifikat.
- a) Geben Sie mit der Einstellung **Clientzertifikat** den Fingerabdruck des identifizierenden Zertifikats an, damit Benutzer nicht unnötig aufgefordert werden.
- b) Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.

Informationen zur Matrix der internen und externen Netzwerkverbindungen finden Sie im Knowledge Center-Artikel [CTX250104](#).

## Vertrauenswürdige Server

### Erzwingen vertrauenswürdiger Serververbindungen

Die Richtlinie “Vertrauenswürdige Serverkonfiguration” dient dazu, Vertrauensstellungen bei Verbindungen der Citrix Workspace-App zu identifizieren und durchzusetzen.

Mit dieser Richtlinie können Sie steuern, wie der Client die veröffentlichte Anwendung oder den veröffentlichten Desktop identifiziert, zu dem eine Verbindung hergestellt wird. Der Client bestimmt eine Vertrausebene, die bei einer Verbindung “Vertrauensregion” genannt wird. Die Vertrauensregion bestimmt dann, wie der Client für die Verbindung konfiguriert wird.

Durch Aktivieren dieser Richtlinie werden Verbindungen zu Servern verhindert, die sich nicht in den vertrauenswürdigen Regionen befinden.

Die Regionsidentifizierung basiert standardmäßig auf der Adresse des Servers, zu dem der Client eine Verbindung herstellt. Der Server muss Mitglied der Zone vertrauenswürdiger Sites von Windows sein, um Mitglied der **Vertrauensregion** sein zu können. Sie können dies mit der Einstellung **Windows-Internetzone** konfigurieren.

Alternativ kann die Serveradresse mithilfe der Einstellung **Adress** ausdrücklich als vertrauenswürdige eingestuft werden. Bei der Serveradresse muss es sich um eine kommasetrennte Liste von Servern handeln (die Verwendung von Platzhaltern wird unterstützt –z. B. `cps*.citrix.com`).

Aktivieren der vertrauenswürdigen Serverkonfiguration über die administrative Gruppenrichtlinienobjektvorlage

#### Voraussetzung:

Beenden Sie alle Citrix Workspace-App-Komponenten, einschließlich Connection Center.

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Erweitern Sie den Knoten **Computerkonfiguration** und navigieren Sie zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Netzwerkrouting > Vertrauenswürdige Serverkonfiguration konfigurieren**.

3. Wählen Sie **Aktiviert**, um die Regionsidentifizierung in der Citrix Workspace-App durchzusetzen.
4. Wählen Sie **Vertrauenswürdige Serverkonfiguration erzwingen**. Der Client muss dann die Identifizierung mit einem vertrauenswürdigen Server durchführen.
5. Wählen Sie im Dropdownmenü zu **Windows-Internetzone** die Client-Serveradresse aus. Diese Einstellung gilt nur für die Zone vertrauenswürdiger Sites von Windows.
6. Legen Sie im Feld **Adresse** die Client-Serveradresse für die Zone vertrauenswürdiger Sites außer Windows fest. Sie können eine durch Trennzeichen getrennte Liste verwenden.
7. Klicken Sie auf **OK** und **Übernehmen**.

Wenn diese Richtlinie aktiviert ist und der Server sich nicht in der vertrauenswürdigen Region befindet, wird die Verbindung verhindert und eine Fehlermeldung angezeigt.

Der angegebene Server muss der Windows-**Zone für vertrauenswürdige Sites** hinzugefügt werden, damit die Verbindung hergestellt werden kann. Fügen Sie den Server beispielsweise entweder als “http://” oder als “https://” für SSL-Verbindungen hinzu.

#### Hinweis:

Bei SSL-Verbindungen muss der allgemeine Name des Zertifikats vertrauenswürdig sein. Bei anderen Verbindungen müssen alle einzelnen Server, die kontaktiert werden, vertrauenswürdig sein.

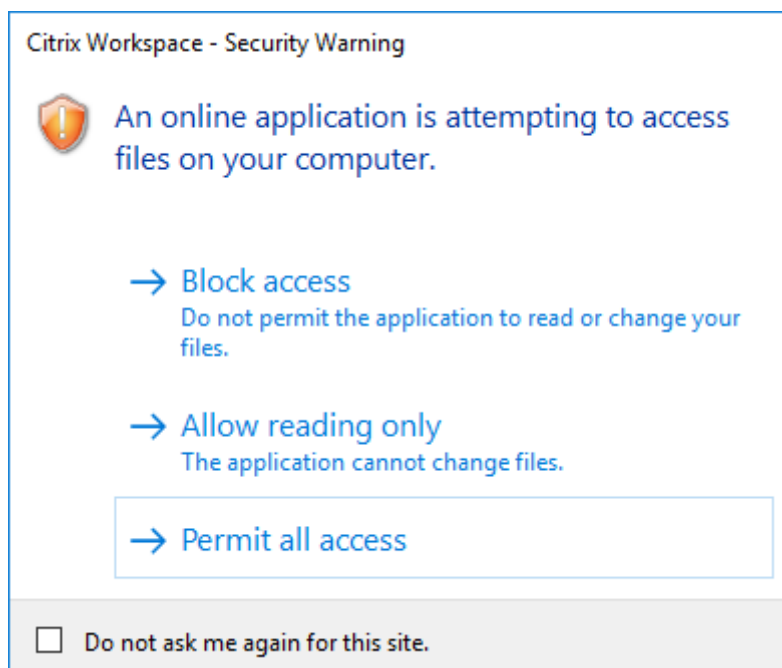
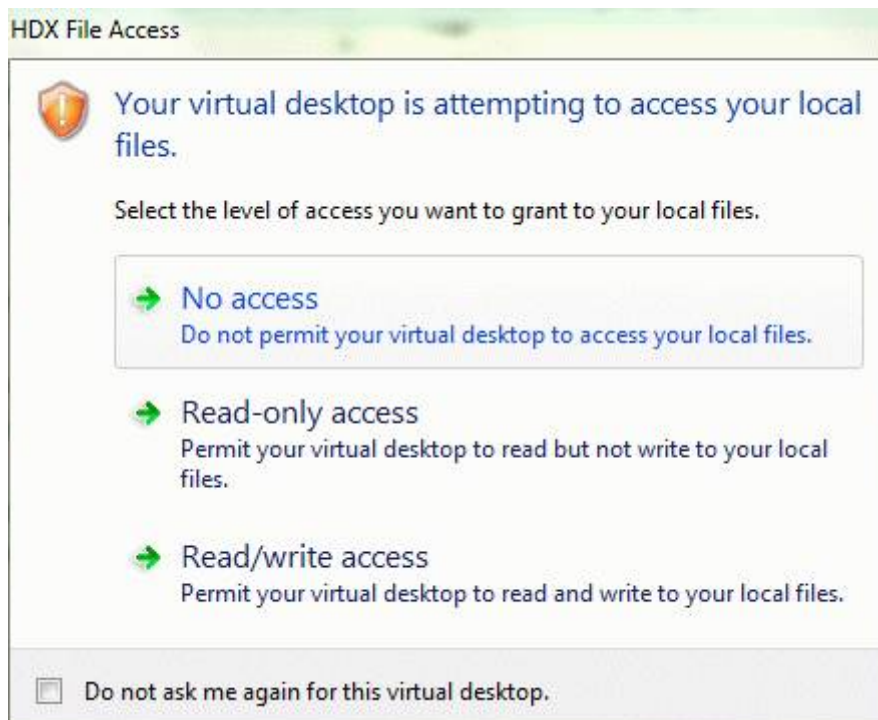
Stellen Sie außerdem sicher, dass der interne StoreFront-FQDN der Zone “Lokales Intranet” oder “Vertrauenswürdige Sites” hinzugefügt wird. Weitere Informationen finden Sie unter **Ändern der Internet Explorer-Einstellungen** im Abschnitt [Authentifizierung](#).

### Client Selective Trust

Neben dem Zulassen oder Verhindern von Verbindungen zu den Servern verwendet der Client die Regionen auch, um den SSO-Zugriff auf Dateien, das Mikrofon oder die Webcam zu identifizieren.

Regionen	Ressourcen	Zugriffsebene
Internet	Datei, Mikrofon, Webcam	Benutzer bei Zugriff auffordern, SSO nicht zulässig
Intranet	Mikrofon, Webcam	Benutzer bei Zugriff auffordern, SSO zulässig
Eingeschränkte Sites	Alle	Kein Zugriff und Verbindung kann verhindert werden
Vertrauenswürdig	Mikrofon, Webcam	Lesen oder Schreiben, SSO zulässig

Wenn der Benutzer den Standardwert für eine Region ausgewählt hat, wird möglicherweise das folgende Dialogfeld angezeigt:







Administratoren können dieses Standardverhalten ändern, indem sie die Registrierungsschlüssel für **Client Selective Trust** entweder mithilfe der Gruppenrichtlinie oder in der Registrierung erstellen und konfigurieren. Weitere Informationen zum Konfigurieren von Client Selective Trust-Registrierungsschlüsseln finden Sie im Knowledge Center-Artikel [CTX133565](#).

## ICA-Dateisignierung

Die ICA-Dateisignierung schützt vor unautorisierten Anwendungs- oder Desktopstarts. Die Citrix Workspace-App prüft, ob eine vertrauenswürdige Quelle die Anwendung oder den Desktop gestartet hat und verhindert basierend auf administrativen Richtlinien das Starten von Ressourcen auf nicht vertrauenswürdigen Servern. Sie können die ICA-Dateisignierung über die administrative Vorlage für Gruppenrichtlinienobjekte oder StoreFront konfigurieren. Das Feature der ICA-Dateisignierung ist in der Standardeinstellung nicht aktiviert.

Informationen zum Aktivieren der ICA-Dateisignierung für StoreFront finden Sie unter [Aktivieren der ICA-Dateisignierung](#) in der StoreFront-Dokumentation.

## Konfigurieren der ICA-Dateisignatur

### Hinweis:

Wenn CitrixBase.admx\adml nicht dem lokalen Gruppenrichtlinienobjekt hinzugefügt wird, ist die **Richtlinie zum Aktivieren der ICA-Dateisignierung** evtl. nicht vorhanden.

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**.
3. Wählen Sie die Richtlinie **ICA-Dateisignierung aktivieren** und dann nach Bedarf eine der folgenden Optionen:
  - a) Aktiviert: gibt an, dass Sie den Fingerabdruck des Signaturzertifikats der Positivliste der vertrauenswürdigen Zertifikatfingerabdrücke hinzufügen können.
  - b) Vertrauenswürdige Zertifikate: Klicken Sie auf **Anzeigen**, um den Fingerabdruck des Signaturzertifikats aus der Positivliste zu entfernen. Sie können die Fingerabdrücke von Signaturzertifikaten von den Eigenschaften des Signaturzertifikats kopieren und einfügen.
  - c) Sicherheitsrichtlinie: Folgende Optionen sind im Menü verfügbar.
    - i. Nur signierte Starts zulassen (sicherer): lässt nur richtig signierte Anwendungs- und Desktopstarts von einem vertrauenswürdigen Server zu. Im Falle einer ungültigen Signatur wird eine Sicherheitswarnung angezeigt. Die Sitzung wird dann wegen fehlender Autorisierung nicht gestartet.
    - ii. Benutzer bei nicht signierten Starts auffordern (weniger sicher): Eine Nachricht wird angezeigt, wenn eine nicht signierte oder ungültig signierte Sitzung gestartet wird. Sie können den Start fortsetzen oder abbrechen (Standard).
4. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

### **Auswählen und Verteilen eines digitalen Signaturzertifikats:**

Bei der Auswahl eines digitalen Signaturzertifikats empfehlen wir eine Auswahl aus der folgenden Prioritätsliste:

1. Erwerben Sie ein codesigniertes Zertifikat oder ein SSL-Signaturzertifikat einer öffentlichen Zertifizierungsstelle.
2. Wenn Ihr Unternehmen eine private Zertifizierungsstelle hat, erstellen Sie ein codesigniertes oder SSL-Signaturzertifikat mit der privaten Zertifizierungsstelle.
3. Verwenden Sie ein vorhandenes SSL-Zertifikat.
4. Erstellen Sie ein Stammzertifikat der Zertifizierungsstelle und verteilen es mit einem Gruppenrichtlinienobjekt oder einer manuellen Installation auf die Benutzergeräte.

### **Schutz durch lokale Sicherheitsautorität**

Die lokale Sicherheitsautorität von Windows, die Informationen zu allen Aspekten der lokalen Sicherheit auf einem System enthält, wird von der Citrix Workspace-App unterstützt. Diese Unterstützung ermöglicht einen Systemschutz durch die lokale Sicherheitsautorität für gehostete Desktops.

## Herstellen von Verbindungen über Proxyserver

Mit Proxyservern wird der eingehende und ausgehende Netzwerkzugriff beschränkt und die Verbindung zwischen der Citrix Workspace-App für Windows und Servern gehandhabt. Die Citrix Workspace-App unterstützt die Protokolle SOCKS und Secure Proxy.

Für die Kommunikation mit dem Server verwendet die Citrix Workspace-App die Proxyservereinstellungen, die remote auf dem Server konfiguriert sind, auf dem Workspace für Web ausgeführt wird.

Bei der Kommunikation mit dem Webserver verwendet die Citrix Workspace-App die Einstellungen für den Proxyserver, die über die **Internetoptionen** des Standardwebrowsers auf dem Benutzergerät konfiguriert wurden. Konfigurieren Sie die **Internetoptionen** des Standardwebrowsers auf dem Benutzergerät entsprechend.

Informationen zum Erzwingen von Proxyeinstellungen mit der ICA-Datei in StoreFront finden Sie im Knowledge Center-Artikel [CTX136516](#).

## Unterstützung für den ausgehenden Proxy

SmartControl ermöglicht Administratoren das Konfigurieren und Durchsetzen von Richtlinien, die sich auf die Umgebung auswirken. Beispielsweise können Sie verhindern, dass Benutzer ihren Remotedesktops weitere Laufwerke zuordnen. Sie können diese Granularität mit dem SmartControl-Feature auf dem Citrix Gateway erreichen.

Das Szenario ändert sich jedoch, wenn die Citrix Workspace-App und Citrix Gateway zu separaten Unternehmenskonten gehören. In diesem Fall kann die Clientdomäne das SmartControl-Feature nicht anwenden, da das Gateway in der Domäne fehlt. Sie können den ausgehenden ICA-Proxy verwenden. Mit dem ausgehenden ICA-Proxy können Sie das SmartControl-Feature auch dann verwenden, wenn die Citrix Workspace-App und Citrix Gateway in verschiedenen Organisationen bereitgestellt sind.

Die Citrix Workspace-App unterstützt Sitzungsstarts mit dem NetScaler LAN-Proxy. Verwenden Sie das ausgehende Proxy-Plug-In, um einen einzelnen statischen Proxy zu konfigurieren, oder wählen Sie zur Laufzeit einen Proxyserver aus.

Es gibt folgende Konfigurationsmethoden für ausgehende Proxys:

- Statischer Proxy: Der Proxyserver wird durch Angabe eines Proxy-Hostnamen und der Portnummer konfiguriert.
- Dynamischer Proxy: Ein einzelner Proxyserver wird mit der Proxy-Plug-In-DLL unter einem oder mehreren Proxyservern ausgewählt.

Sie können den ausgehenden Proxy mit der administrativen Gruppenrichtlinienobjektvorlage oder dem Registrierungs-Editor konfigurieren.

Weitere Informationen zum ausgehenden Proxy finden Sie unter [Unterstützung für den ausgehenden ICA-Proxy](#) in der Citrix Gateway-Dokumentation.

## Unterstützung für den ausgehenden Proxy - Konfiguration

### Hinweis:

Wenn statische und dynamische Proxys konfiguriert sind, hat die Konfiguration des dynamischen Proxys Vorrang.

### Konfigurieren des ausgehenden Proxys mit der administrativen GPO-Vorlage:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Workspace > Netzwerkrouting**.
3. Wählen Sie eine der folgenden Optionen:
  - Statischer Proxy: Wählen Sie die Richtlinie **NetScaler LAN-Proxy manuell konfigurieren**. Wählen Sie **Aktiviert** und geben Sie den Hostnamen und die Portnummer ein.
  - Dynamischer Proxy: Wählen Sie die Richtlinie **NetScaler LAN-Proxy mit DLL konfigurieren**. Wählen Sie **Aktiviert** und geben Sie den vollständigen Pfad zur DLL-Datei ein. Beispiel: `C:\Workspace\Proxy\ProxyChooser.dll`.
4. Klicken Sie auf **Anwenden** und auf **OK**.

### Konfigurieren des ausgehenden Proxys mit dem Registrierungs-Editor:

#### • Statischer Proxy:

- Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler`.
- Erstellen Sie folgende DWORD-Wertschlüssel:

```
"StaticProxyEnabled"=dword:00000001
```

```
"ProxyHost"="testproxy1.testdomain.com"
```

```
"ProxyPort"=dword:000001bb
```

#### • Dynamischer Proxy:

- Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxy`.
- Erstellen Sie folgende DWORD-Wertschlüssel:

```
"DynamicProxyEnabled"=dword:00000001
```

```
"ProxyChooserDLL"="c:\\Workspace\\Proxy\\ProxyChooser.dll"
```

## Verbindungen und Zertifikate

### Verbindungen

- HTTP-Store
- HTTPS-Store
- Citrix Gateway 10.5 und höher

### Zertifikate

#### Hinweis:

Die Citrix Workspace-App für Windows ist digital signiert. Die digitale Signatur ist mit einem Zeitstempel versehen. Das Zertifikat ist also auch nach Ablauf gültig.

- Privat (selbstsigniert)
- Stamm
- Platzhalter
- Zwischenzertifikat

### Private (selbstsignierte) Zertifikate

Wenn ein privates Zertifikat auf dem Remotegateway vorhanden ist, installieren Sie das Stammzertifikat der Zertifizierungsstelle des Unternehmens auf dem Benutzergerät, mit dem auf Citrix-Ressourcen zugegriffen wird.

#### Hinweis:

Wenn das Zertifikat des Remotegateways sich beim Herstellen der Verbindung nicht verifizieren lässt, wird eine Warnung über ein nicht vertrauenswürdiges Zertifikat angezeigt. Die Warnung wird angezeigt, wenn das Stammzertifikat im lokalen Schlüsselspeicher fehlt. Wenn der Benutzer weiterarbeitet, werden die Apps angezeigt, können jedoch nicht gestartet werden.

### Stammzertifikate

Für in Domänen eingebundene Computer können Sie ZS-Zertifikate mit der administrativen Gruppenrichtlinienobjektvorlage verteilen und als vertrauenswürdig einstufen.

Für nicht domänengebundene Computer können Unternehmen ein benutzerdefiniertes Installationspaket erstellen und damit das Zertifikat der Zertifizierungsstelle verteilen und installieren. Wenden Sie sich bei Fragen an den Systemadministrator.

## Zertifikate mit Platzhalterzeichen

Zertifikate mit Platzhalterzeichen werden für einen Server in derselben Domäne verwendet.

Die Citrix Workspace-App unterstützt Zertifikate mit Platzhalterzeichen. Verwenden Sie Zertifikate mit Platzhalterzeichen gemäß den jeweils gültigen Sicherheitsrichtlinien Ihres Unternehmens. Eine Alternative zu Zertifikaten mit Platzhalterzeichen sind Zertifikate, die eine Liste der Servernamen und die SAN-Erweiterung (Subject Alternative Name) enthalten. Private und öffentliche Zertifizierungsstellen stellen diese Zertifikate aus.

## Zwischenzertifikate

Wenn die Zertifikatkette ein Zwischenzertifikat enthält, muss das Zwischenzertifikat dem Citrix Gateway-Serverzertifikat angehängt werden. Weitere Informationen finden Sie unter [Konfigurieren von Zwischenzertifikaten](#).

## Zertifikatsperrliste

Mit der Zertifikatsperrliste (Certificate Revocation List, CRL) kann die Citrix Workspace-App überprüfen, ob das Zertifikat des Servers widerrufen wurde. Durch die Überprüfung des Zertifikats wird die kryptografische Authentifizierung für den Server und die allgemeine Sicherheit der TLS-Verbindung zwischen Benutzergerät und Server verbessert.

Sie können die Überprüfung der Zertifikatsperrlisten in mehreren Stufen einstellen. Sie können die Citrix Workspace-App beispielsweise so konfigurieren, dass nur die lokale Zertifikatsperrliste oder die lokale und die Netzwerkzertifikatsperrliste überprüft werden. Sie können die Überprüfung der Zertifikate auch so konfigurieren, dass Benutzer sich nur anmelden können, wenn alle Zertifikatsperrlisten überprüft wurden.

Wenn Sie die Überprüfung der Zertifikate auf Ihrem lokalen Computer konfigurieren, beenden Sie die Citrix Workspace-App und stellen Sie sicher, dass alle Citrix Workspace-Komponenten einschließlich **Connection Center** geschlossen sind.

Weitere Informationen finden Sie unter [TLS \(Transport Layer Security\)](#).

## Unterstützung zur Abwehr von Man-in-the-Middle-Angriffen

Mit der Citrix Workspace-App für Windows können Sie das Risiko eines Man-in-the-Middle-Angriffs mit dem Microsoft Windows-Feature **Enterprise Certificate Pinning** reduzieren. Ein Man-in-the-Middle-Angriff ist eine Art von Cyberangriff, bei dem der Angreifer heimlich Nachrichten zwischen zwei Parteien, die glauben, direkt miteinander zu kommunizieren, abfängt und weiterleitet.

Bisher konnte bei der Kontaktaufnahme mit dem Store-Server nicht überprüft werden, ob die erhaltene Antwort von dem Server stammt, den Sie kontaktieren wollten oder nicht. Mit dem Feature **Enterprise Certificate Pinning** von Microsoft Windows können Sie die Gültigkeit und Integrität des Servers überprüfen, indem Sie das Zertifikat anheften.

Die Citrix Workspace-App für Windows ist so vorkonfiguriert, dass sie anhand der Regeln für das Anheften von Zertifikaten weiß, welches Serverzertifikat für eine bestimmte Domäne oder Site zu erwarten ist. Wenn das Serverzertifikat nicht mit dem vorkonfigurierten Serverzertifikat übereinstimmt, verhindert die Citrix Workspace-App für Windows, dass die Sitzung stattfindet.

Informationen zur Bereitstellung des Features **Enterprise Certificate Pinning** finden Sie in der [Microsoft-Dokumentation](#).

**Hinweis:**

Sie müssen wissen, wann das Zertifikat abläuft und die Gruppenrichtlinien und Zertifikatsvertrauenslisten entsprechend aktualisieren. Andernfalls können Sie die Sitzung möglicherweise nicht starten, auch wenn kein Angriff erfolgt.

## Authentifizierung

April 22, 2024

Sie können verschiedene Authentifizierungsmethoden für die Citrix Workspace-App konfigurieren, u. a. Domänen-Passthrough-Authentifizierung (Single Sign-On), Smartcardauthentifizierung und Kerberos-Passthrough-Authentifizierung.

### Domänen-Passthrough-Authentifizierung (Single Sign-On)

Mit Domänen-Passthrough (Single Sign-On) können Sie sich bei einer Domäne authentifizieren und Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) verwenden, ohne sich erneut authentifizieren zu müssen.

**Hinweis:**

Wenn Sie die Richtlinie **Enable MPR notifications for the System** in der Gruppenrichtlinienobjektvorlage deaktivieren, wird die Authentifizierungsfunktion für Domänen-Passthrough (Single Sign-On) unter Windows 11 nicht unterstützt.

Dieses Feature ist in der Citrix Workspace-App für Windows Version 2012 und höher verfügbar.

Wenn Domänen-Passthrough (Single Sign-On) aktiviert ist, werden Ihre Anmeldeinformationen zwischengespeichert, sodass Sie eine Verbindung mit anderen Citrix Anwendungen herstellen können,

ohne sich jedes Mal anmelden zu müssen. Stellen Sie sicher, dass nur Software auf Ihrem Gerät ausgeführt wird, die den Unternehmensrichtlinien entspricht, um das Risiko für die Anmeldeinformationen zu verringern.

Wenn Sie sich bei der Citrix Workspace-App anmelden, werden Ihre Anmeldeinformationen zusammen mit den Apps und Desktops sowie Startmenüeinstellungen an StoreFront übergeben. Nach der Konfiguration von Single Sign-On können Sie sich bei der Citrix Workspace-App anmelden und Sitzungen mit virtuellen Apps und Desktops starten, ohne Ihre Anmeldeinformationen erneut eingeben zu müssen.

Sie müssen bei allen Webbrowsern Single Sign-On mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren. Weitere Informationen zum Konfigurieren von Single Sign-On mit der administrativen Gruppenrichtlinienobjektvorlage finden Sie unter [Konfigurieren von Single Sign-On mit Citrix Gateway](#).

Sie können Single Sign-On sowohl bei der Neuinstallation als auch bei einem Upgrade konfigurieren, indem Sie eine der folgenden Optionen verwenden:

- Befehlszeilenoberfläche
- Grafische Benutzeroberfläche (GUI)

**Hinweis:**

Die Begriffe “Domänen-Passthrough”, “Single Sign-On” und “SSON” werden in diesem Dokument synonym verwendet.

## Single Sign-On während der Neuinstallation konfigurieren

Konfigurieren Sie Single Sign-On während einer Neuinstallation mit folgenden Schritten:

1. Konfiguration in StoreFront.
2. Konfigurieren Sie XML-Vertrauensdienste auf dem Delivery Controller.
3. Ändern der Internet Explorer-Einstellungen.
4. Installieren der Citrix Workspace-App mit Single Sign-On.

## Single Sign-On in StoreFront konfigurieren

Mit Single Sign-On können Sie sich bei einer Domäne authentifizieren und das von dieser Domäne bereitgestellte Citrix Virtual Apps and Desktops und Citrix DaaS verwenden, ohne sich für jede App oder jeden Desktop neu authentifizieren zu müssen.

Wenn Sie mit dem **Storebrowse**-Hilfsprogramm einen Store hinzufügen, werden Ihre Anmeldeinformationen zusammen mit den für Sie enumerierten Apps und Desktops (einschließlich Startmenüeinstellungen) an den Citrix Gateway-Server übergeben. Nach dem Konfigurieren von Single Sign-On



können Sie den Store hinzufügen, Ihre Apps und Desktops enumerieren und erforderliche Ressourcen starten, ohne Ihre Anmeldeinformationen mehrmals eingeben zu müssen.

Abhängig von der Citrix Virtual Apps and Desktops-Bereitstellung kann die Single Sign-On-Authentifizierung über die Verwaltungskonsole in StoreFront konfiguriert werden.

In der folgenden Tabelle finden Sie verschiedene Anwendungsfälle und die entsprechende Konfiguration:

Anwendungsfall	Konfigurationsdetails	Weitere Informationen
SSON ist in StoreFront konfiguriert	Starten Sie Citrix Studio, navigieren Sie zu <b>Store</b> > <b>Authentifizierungsmethoden verwalten - Store</b> und aktivieren Sie <b>Domänen-Passthrough-Authentifizierung</b> .	Wenn die Citrix Workspace-App nicht mit Single Sign-On konfiguriert ist, ändert sich die Authentifizierungsmethode automatisch von <b>Domänen-Passthrough-Authentifizierung</b> in <b>Benutzername und Kennwort</b> , sofern verfügbar.
Wenn Workspace für Web erforderlich ist	Starten Sie <b>Stores</b> > <b>Workspace für Websites</b> > <b>Authentifizierungsmethoden verwalten</b> und aktivieren Sie <b>Domänen-Passthrough-Authentifizierung</b> .	Wenn die Citrix Workspace-App nicht mit Single Sign-On konfiguriert ist, ändert sich die Authentifizierungsmethode automatisch von <b>Domänen-Passthrough-Authentifizierung</b> in <b>Benutzername und Kennwort</b> , sofern verfügbar.

### Single Sign-On mit Citrix Gateway konfigurieren

Sie aktivieren Single Sign-On mit Citrix Gateway über die administrative Gruppenrichtlinienobjektvorlage. Sie müssen jedoch sicherstellen, dass Sie die Standardauthentifizierung und die Einzelfaktorauthentifizierung (nFactor mit 1 Faktor) auf dem Citrix Gateway aktiviert haben.

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung**. Wählen Sie dann die Richtlinie **Single Sign-On für Citrix Gateway**.

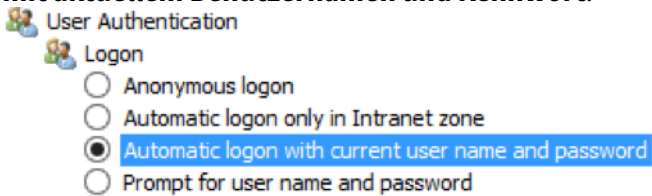
3. Wählen Sie **Aktiviert**.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

### XML-Vertrauensdienste auf dem Delivery Controller konfigurieren

Führen Sie in Citrix Virtual Apps and Desktops und Citrix DaaS als Administrator den folgenden PowerShell-Befehl auf dem Delivery Controller aus:

```
asnpx Citrix* ; Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True
```

### Ändern der Internet Explorer-Einstellungen

1. Fügen Sie den StoreFront-Server der Liste der vertrauenswürdigen Sites im Internet Explorer hinzu. Schrittfolge zum Hinzufügen:
  - a) Starten Sie **Internetoptionen** über die Systemsteuerung.
  - b) Klicken Sie auf **Sicherheit > Lokales Intranet** und dann auf **Sites**.  
Das Fenster **Lokales Intranet** wird angezeigt.
  - c) Wählen Sie **Erweitert**.
  - d) Fügen Sie die URL des StoreFront-FQDN mit den entsprechenden HTTP- oder HTTPS-Protokollen hinzu.
  - e) Klicken Sie auf **Anwenden** und auf **OK**.
2. Ändern Sie im **Internet Explorer** die Einstellungen unter **Benutzerauthentifizierung**. Schrittfolge zum Modifizieren:
  - a) Starten Sie **Internetoptionen** über die Systemsteuerung.
  - b) Klicken Sie auf die Registerkarte **Sicherheit > Lokales Intranet**.
  - c) Klicken Sie auf **Stufe anpassen**. Das Fenster **Sicherheitseinstellungen –lokales Intranet-zone** wird angezeigt.
  - d) Wählen Sie im Bereich **Benutzerauthentifizierung** die Option **Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort**.

The screenshot shows the 'User Authentication' section with the following options:

    - Anonymous logon
    - Automatic logon only in Intranet zone
    - Automatic logon with current user name and password
    - Prompt for user name and password
  - e) Klicken Sie auf **Anwenden** und auf **OK**.

## Single Sign-On über die Befehlszeilenschnittstelle konfigurieren

Installieren Sie die Citrix Workspace-App mit dem Switch `/includeSSON` und starten Sie die Citrix Workspace-App neu, damit die Änderungen wirksam werden.

## Single Sign-On mit der GUI konfigurieren

1. Suchen Sie die Installationsdatei der Citrix Workspace-App (`CitrixWorkspaceApp.exe`).
2. Doppelklicken Sie auf `CitrixWorkspaceApp.exe`, um das Installationsprogramm zu starten.
3. Wählen Sie im **Installationsassistenten zum Aktivieren von Single Sign-On** die Option **Single Sign-On aktivieren**.
4. Klicken Sie auf **Weiter** und folgen Sie den Anweisungen, um die Installation abzuschließen.

Sie können sich jetzt ohne Eingabe von Benutzeranmeldeinformationen mit der Citrix Workspace-App bei einem vorhandenen Store anmelden (oder einen neuen Store konfigurieren).

## Single Sign-On in Workspace für Web konfigurieren

Sie können Single Sign-On in Workspace für Web mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren.

1. Öffnen Sie die administrative GPO-Vorlage von Workspace für Web, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung**.
3. Wählen Sie die Richtlinie **Lokaler Benutzername und Kennwort** und legen Sie sie auf **Aktiviert** fest.
4. Klicken Sie auf **Passthrough-Authentifizierung aktivieren**. Mit dieser Option kann Workspace für Web Ihre Anmeldeinformationen für die Authentifizierung auf dem Remoteserver verwenden.
5. Klicken Sie auf **Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen**. Mit dieser Option werden alle Authentifizierungseinschränkungen umgangen und das Passthrough von Anmeldeinformationen für alle Verbindungen ermöglicht.
6. Klicken Sie auf **Anwenden** und auf **OK**.
7. Starten Sie Workspace für Web neu, um die Änderungen zu übernehmen.

Stellen Sie sicher, dass Single Sign-On aktiviert ist, indem Sie den **Task-Manager** starten und prüfen, ob der Prozess `ssonsvr.exe` ausgeführt wird.

## Single Sign-On mit Active Directory konfigurieren

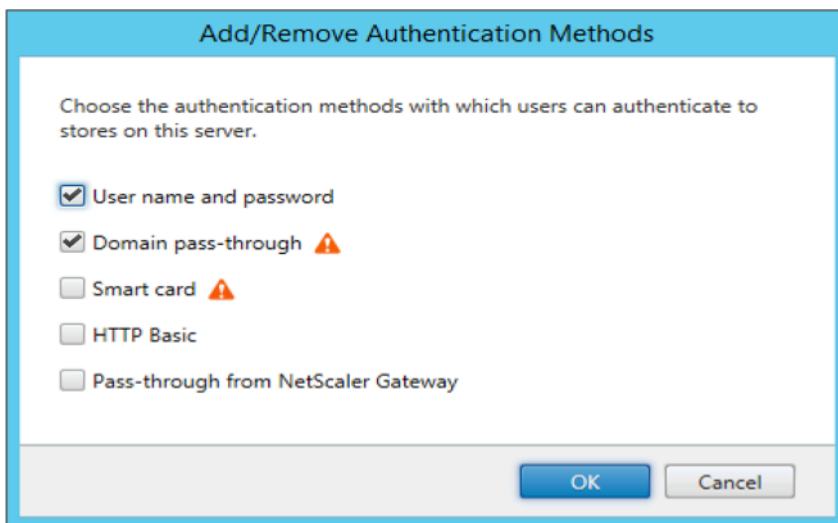
Führen Sie die folgenden Schritte aus, um die Citrix Workspace-App für die Passthrough-Authentifizierung mit der Active Directory-Gruppenrichtlinie zu konfigurieren. In diesem Szenario können Sie die Authentifizierung per Single Sign-On auch ohne Enterprise-Software-Bereitstellungstools wie Microsoft System Center Configuration Manager erzielen.

1. Laden Sie die Installationsdatei für die Citrix Workspace-App ([CitrixWorkspaceApp.exe](#)) auf eine geeignete Netzwerkfreigabe herunter. Die Maschinen, auf denen die Citrix Workspace-App installiert werden soll, müssen darauf Zugriff haben.
2. Laden Sie die Vorlage [CheckAndDeployWorkspacePerMachineStartupScript.bat](#) von der [Downloadseite für die Citrix Workspace-App für Windows](#) herunter.
3. Bearbeiten Sie den Inhalt, damit der Speicherort und die Version von [CitrixWorkspaceApp.exe](#) korrekt sind.
4. Geben Sie in der **Active Directory-Gruppenrichtlinienverwaltungskonsole** als Startskript [CheckAndDeployWorkspacePerMachineStartupScript.bat](#) ein. Weitere Informationen zum Bereitstellen der Startskripts finden Sie im Abschnitt [Active Directory](#).
5. Navigieren Sie im Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Vorlagen hinzufügen/entfernen**, um die Datei [receiver.adml](#) hinzuzufügen.
6. Nachdem Sie die Vorlage [receiver.adml](#) hinzugefügt haben, navigieren Sie zu **Computerkonfiguration > Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung**. Weitere Informationen über das Hinzufügen von Vorlagendateien finden Sie unter [Administrative Gruppenrichtlinienobjektvorlage](#).
7. Wählen Sie die Richtlinie **Lokaler Benutzername und Kennwort** und legen Sie sie auf **Aktiviert** fest.
8. Wählen Sie **Passthrough-Authentifizierung aktivieren** und klicken Sie auf **Übernehmen**.
9. Starten Sie die Maschine neu, damit die Änderungen wirksam werden.

## Single Sign-On in StoreFront konfigurieren

### Konfigurieren in StoreFront

1. Starten Sie **Citrix Studio** auf dem StoreFront-Server und wählen Sie **Stores > Authentifizierungsmethoden verwalten –Store**.
2. Wählen Sie dann **Domänen-Passthrough**.



## Authentifizierungstoken

Authentifizierungstoken werden verschlüsselt und auf dem lokalen Datenträger gespeichert, sodass Sie Ihre Anmeldeinformationen beim Neustart des Systems oder der Sitzung nicht erneut eingeben müssen. Die Citrix Workspace-App bietet eine Option, mit der das Speichern von Authentifizierungstoken auf dem lokalen Datenträger deaktiviert werden kann.

Mit einer neuen Richtlinie für ein Gruppenrichtlinienobjekt (GPO) kann das Speichern von Authentifizierungstoken konfiguriert und so die Sicherheit erhöht werden.

### Hinweis:

Diese Konfiguration ist nur in Cloud-Bereitstellungen anwendbar.

### Speicherung von Authentifizierungstoken über die GPO-Richtlinie deaktivieren:

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** > **Self-Service**.
3. Wählen Sie in der Richtlinie **Authentifizierungstoken speichern** eine der folgenden Optionen aus:
  - **Aktiviert:** Gibt an, dass die Authentifizierungstoken auf dem Datenträger gespeichert werden. Die Standardeinstellung ist "Aktiviert".
  - **Deaktiviert:** Gibt an, dass die Authentifizierungstoken nicht auf dem Datenträger gespeichert sind. Geben Sie Ihre Anmeldeinformationen erneut ein, wenn Ihr System oder Ihre Sitzung neu gestartet wird.

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

Ab Version 2106 bietet die Citrix Workspace-App eine weitere Option, mit der das Speichern von Authentifizierungstoken auf dem lokalen Datenträger deaktiviert werden kann. Mit dem Global App Configuration Service können Sie die vorhandene GPO-Konfiguration und das Speichern von Authentifizierungstoken auf dem lokalen Datenträger deaktivieren.

Legen Sie im Global App Configuration Service das Attribut `Store Authentication Tokens` auf `False` fest.

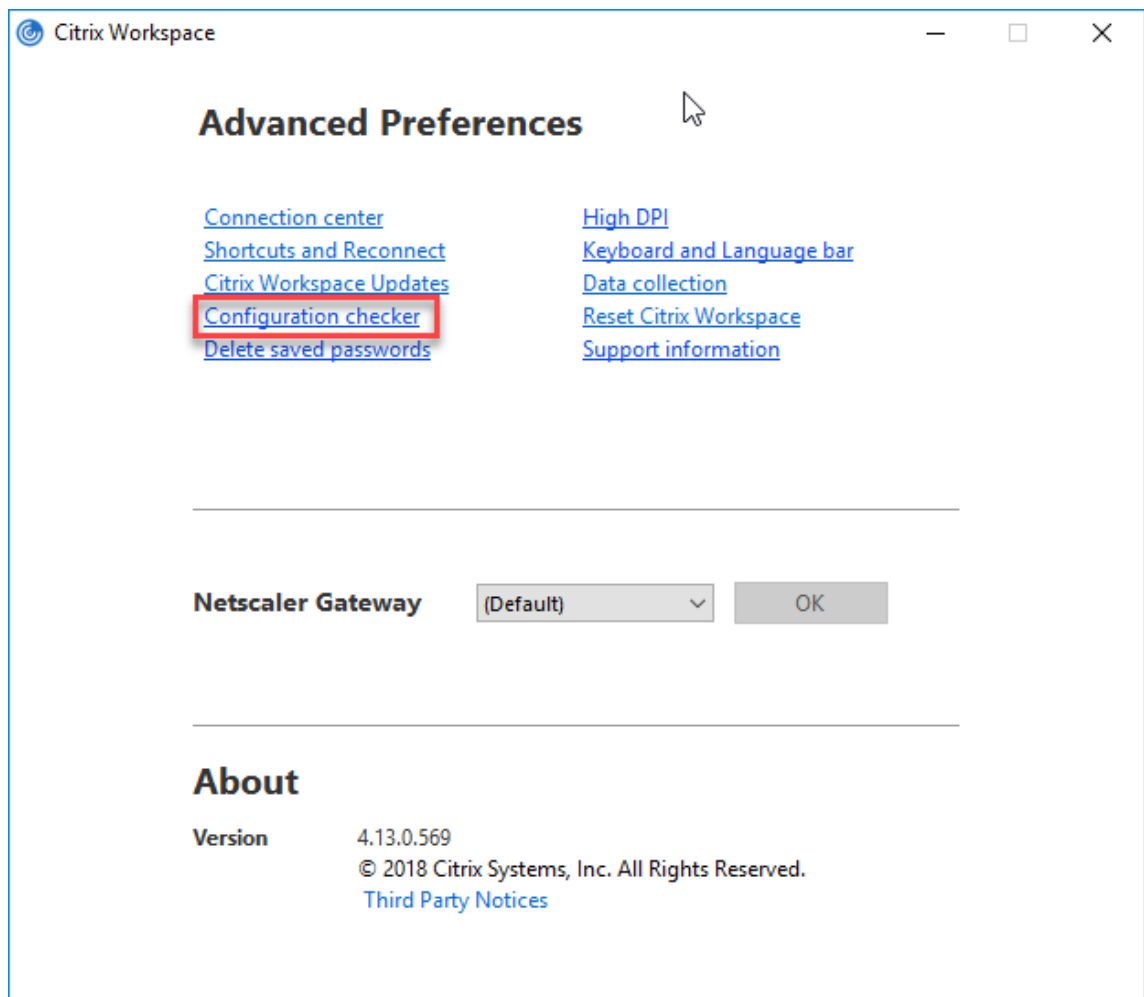
Sie können diese Einstellung mithilfe des Global App Configuration Service und einer der folgenden Methoden konfigurieren:

- GACS-UI: siehe [Citrix Workspace-App konfigurieren](#)
- API: siehe [Citrix Developer-Dokumentation](#)

### **Konfigurationsprüfung**

Mit der Konfigurationsprüfung können Sie testen, ob Single Sign-On ordnungsgemäß konfiguriert ist. Der Test wird für verschiedene Prüfpunkte der Single Sign-On-Konfiguration ausgeführt und die Konfigurationsergebnisse werden angezeigt.

1. Klicken Sie mit der rechten Maustaste im Infobereich auf das Symbol der Citrix Workspace-App und dann auf **Erweiterte Einstellungen**.  
Das Dialogfeld **Erweiterte Einstellungen** wird angezeigt.
2. Klicken Sie auf **Konfigurationsprüfung**.  
Das Fenster **Citrix Konfigurationsprüfung** wird angezeigt.



3. Wählen Sie **SSONChecker** im Bereich **Auswählen** aus.
4. Klicken Sie auf **Ausführen**. Eine Fortschrittsanzeige mit dem Status des Tests wird angezeigt.

Das Fenster der **Konfigurationsprüfung** enthält die folgenden Spalten:

1. **Status:** zeigt das Ergebnis eines Tests auf einem bestimmten Prüfpunkt an.
  - Ein grünes Häkchen bedeutet, dass der Prüfpunkt ordnungsgemäß konfiguriert ist.
  - Ein blaues I bedeutet, dass zu dem Prüfpunkt Informationen vorhanden sind.
  - Ein rotes X bedeutet, dass der Prüfpunkt nicht ordnungsgemäß konfiguriert ist.
2. **Anbieter:** zeigt den Namen des Moduls an, auf dem der Test ausgeführt wird. In diesem Fall Single Sign-On.
3. **Suite:** die Kategorie des Tests. Beispiel: Installation.
4. **Test:** der Name des Tests, der ausgeführt wird.
5. **Details:** zusätzliche Informationen zum Test (für bestandene und für fehlgeschlagene Tests).

Der Benutzer erhält weitere Informationen zu den einzelnen Prüfpunkten und den entsprechenden Ergebnissen.

Die folgenden Tests werden durchgeführt:

1. Installation mit Single Sign-On.
2. Erfassen der Anmeldeinformationen.
3. Registrierung von Netzwerkanbieter: Das Testergebnis für “Registrierung von Netzwerkanbieter” hat nur dann ein grünes Häkchen, wenn “Citrix Single Sign-On” als erster Netzwerkanbieter festgelegt ist. Wenn “Citrix Single Sign-On” an einer weiteren Stelle in der Liste steht, werden neben dem Testergebnis für “Registrierung von Netzwerkanbieter” ein blaues I und zusätzliche Informationen angezeigt.
4. Single Sign-On-Prozess wird ausgeführt.
5. Gruppenrichtlinie: Diese Richtlinie ist standardmäßig auf dem Client konfiguriert.
6. Interneteinstellungen für Sicherheitszonen: Sie müssen die Store-/XenApp-Dienst-URL der Liste der Sicherheitszonen in den Internetoptionen hinzufügen.  
Wenn die Sicherheitszonen per Gruppenrichtlinie konfiguriert sind, erfordern Änderungen in der Richtlinie das erneute Öffnen des Fensters **Erweiterte Einstellungen**, damit die Änderungen wirksam werden und der richtige Teststatus angezeigt wird.
7. Authentifizierungsmethode für StoreFront.

#### Hinweis:

- Wenn Sie auf Workspace für Web zugreifen, gelten die Testergebnisse nicht.
- Wenn die Citrix Workspace-App mit mehreren Stores konfiguriert ist, wird der Test für die Authentifizierungsmethode für alle konfigurierten Stores ausgeführt.
- Sie können die Testergebnisse als Berichte speichern. Das Standardberichtformat ist TXT.

#### Ausblenden der Konfigurationsprüfung im Fenster “Erweiterte Einstellungen”

1. Öffnen Sie die administrative GPO-Vorlage der Citrix Workspace-App, indem Sie `gpedit.msc` ausführen.
2. Navigieren Sie zu **Citrix Komponenten > Citrix Workspace > Self-Service > DisableConfigChecker**.
3. Klicken Sie auf **Aktiviert**, um die Option **Konfigurationsprüfung** im Fenster **Erweiterte Einstellungen** auszublenden.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Führen Sie den Befehl `gpupdate /force` aus.

#### Einschränkung:

Die Konfigurationsprüfung enthält nicht den Prüfpunkt für die Konfiguration von “An XML-Dienst gesendeten Anfragen vertrauen” auf Citrix Virtual Apps and Desktops-Servern.



**Beacontest** Mit der Citrix Workspace-App können Sie einen Beacontest durchführen. Hierfür verwenden Sie den in der **Konfigurationsprüfung** enthaltenen Beacon Checker. Über den Beacontest können Sie prüfen, ob der Beacon (ping.citrix.com) erreichbar ist. Mit dem Test können Sie eine der vielen möglichen Ursachen für eine langsame Ressourcenenumeration (Beacon nicht verfügbar) eliminieren. Um den Test auszuführen, klicken Sie mit der rechten Maustaste auf die Citrix Workspace-App im Infobereich und wählen Sie **Erweiterte Einstellungen > Konfigurationsprüfung**. Wählen Sie in der Liste der vorhandenen Tests die Option **Beacon checker** und klicken Sie auf **Ausführen**.

Der Test kann folgende Ergebnisse haben:

- Erreichbar: Die Citrix Workspace-App kann den Beacon erfolgreich kontaktieren.
- Nicht erreichbar: Die Citrix Workspace-App kann den Beacon nicht kontaktieren.
- Teilweise erreichbar: Die Citrix Workspace-App kann den Beacon sporadisch kontaktieren.

#### **Hinweis:**

- Die Testergebnisse gelten nicht für Workspace für Web.
- Sie können die Testergebnisse als Bericht speichern. Das Standardberichtformat ist TXT.

## **Domänen-Passthrough-Authentifizierung (Single Sign-On) mit Kerberos**

Dieser Abschnitt gilt nur für Verbindungen zwischen der Citrix Workspace-App für Windows und StoreFront, Citrix Virtual Apps and Desktops und Citrix DaaS.

Die Citrix Workspace-App für Windows unterstützt Kerberos für Domänen-Passthrough-Authentifizierung (Single Sign-On) in Bereitstellungen mit Smartcardverwendung. Kerberos ist eine der in der **integrierten Windows-Authentifizierung (IWA)** enthaltenen Authentifizierungsmethoden.

Bei Aktivierung handhabt Kerberos die Authentifizierung ohne Kennwörter für die Citrix Workspace-App und verhindert so trojanerartige Angriffe auf Benutzergeräte, die den Zugriff auf Kennwörter zum Ziel haben. Benutzer nutzen eine beliebige Authentifizierungsmethode (z. B. biometrische Authentifizierungsmethoden wie ein Fingerabdrucklesegerät), um sich anzumelden und auf veröffentlichte Ressourcen zuzugreifen.

Sind die Citrix Workspace-App, StoreFront sowie Citrix Virtual Apps and Desktops und Citrix DaaS für die Smartcard-Authentifizierung konfiguriert, geschieht bei der Anmeldung bei der Citrix Workspace-App mit einer Smartcard Folgendes:

1. Die App erfasst die Smartcard-PIN beim Single Sign-On.
2. Die App authentifiziert den Benutzer mit IWA (Kerberos) bei StoreFront. StoreFront stellt der Citrix Workspace-App dann Informationen zum verfügbaren Citrix Virtual Apps and Desktops und Citrix DaaS bereit.

**Hinweis:**

Aktivieren Sie Kerberos, um eine zusätzliche PIN-Eingabeaufforderung zu vermeiden. Wird die Kerberos-Authentifizierung nicht verwendet, führt die Citrix Workspace-App mit den Smartcard-Anmeldeinformationen eine Authentifizierung bei StoreFront durch.

3. Die HDX Engine (zuvor "ICA-Client") übergibt die Smartcard-PIN an den VDA, um den Benutzer an der Citrix Workspace-App-Sitzung anzumelden. Citrix Virtual Apps and Desktops und Citrix DaaS stellen dann die angeforderten Ressourcen bereit.

Zur Verwendung der Kerberos-Authentifizierung mit der Citrix Workspace-App prüfen Sie, ob die Kerberos-Konfiguration folgenden Punkten entspricht.

- Kerberos funktioniert nur zwischen Citrix Workspace-App und Servern, die zu denselben oder vertrauenswürdigen Windows Server-Domänen gehören. Den Servern wird zudem für Delegierungszwecke vertraut. Dies können Sie über das Verwaltungstool für Active Directory-Benutzer und -Computer konfigurieren.
- Kerberos muss sowohl in der Domäne als auch in Citrix Virtual Apps and Desktops und Citrix DaaS aktiviert sein. Um hohe Sicherheitsstandards und die Verwendung von Kerberos zu gewährleisten, deaktivieren Sie in der Domäne alle IWA-Optionen außer Kerberos.
- Die Kerberos-Anmeldung ist nicht verfügbar für Remotedesktopdienste-Verbindungen, die eine Standardauthentifizierung nutzen, stets vorgegebene Anmeldeinformationen verwenden oder immer zur Eingabe des Kennworts auffordern.

**Warnung:**

Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

### **Domänen-Passthrough-Authentifizierung (Single Sign-On) mit Kerberos für die Verwendung mit Smartcards**

Lesen Sie zuerst die Informationen im Abschnitt [Sichern der Bereitstellung](#) in der Citrix Virtual Apps and Desktops-Dokumentation, bevor Sie fortfahren.

Wenn Sie die Citrix Workspace-App für Windows installieren, fügen Sie die folgende Befehlszeilenoption hinzu:

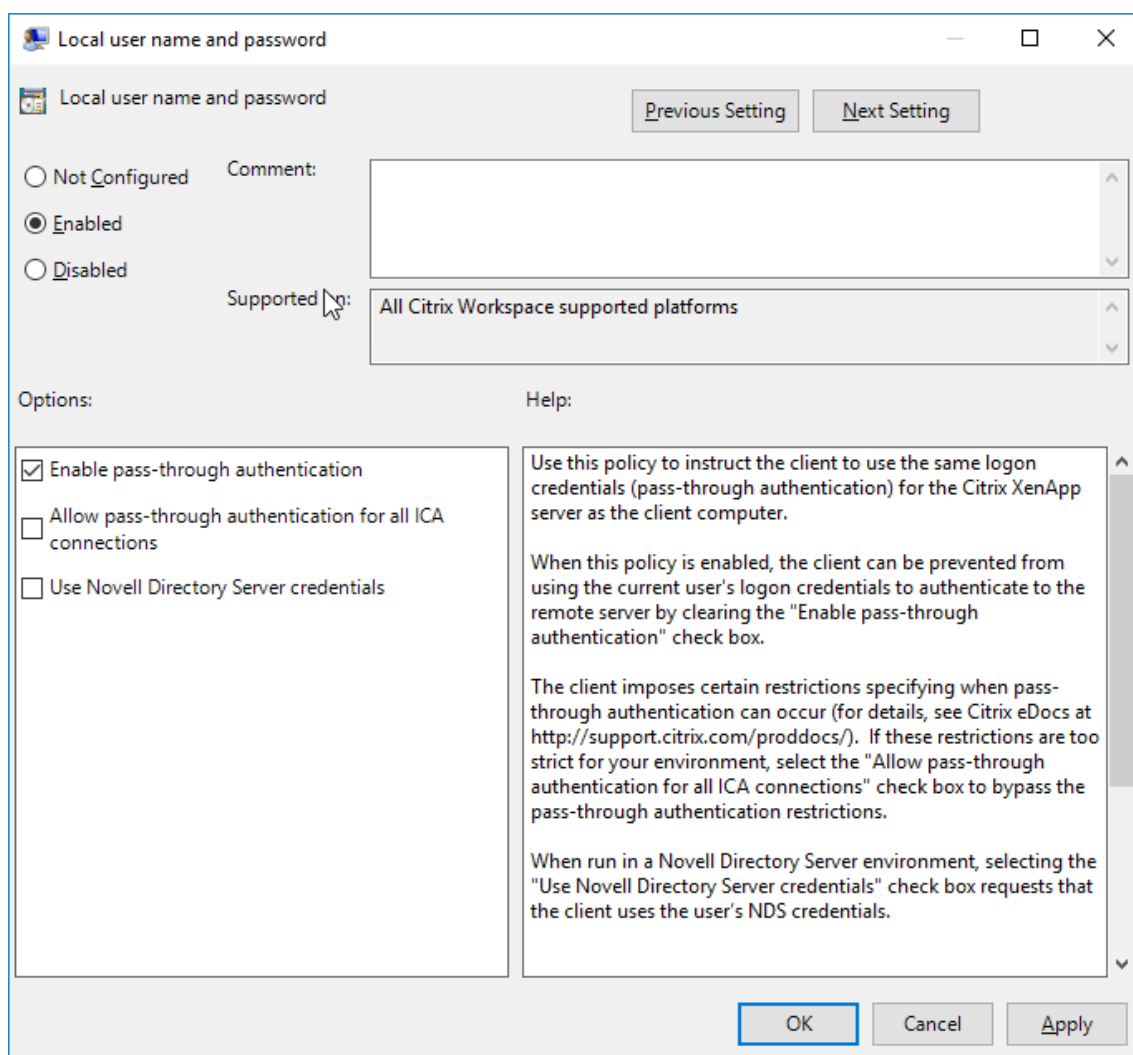
- `/includeSSON`

Mit dieser Option wird die Single Sign-On-Komponente auf dem in die Domäne eingebundenen Computer installiert, sodass der Workspace mit IWA (Kerberos) die Authentifizierung bei StoreFront durchführen kann. Die Single Sign-On-Komponente speichert die Smartcard-PIN, mit der die HDX Engine eine Remoteverbindung zwischen Smartcard-Hardware und -Anmeldeinformationen und Citrix Virtual Apps and Desktops und Citrix DaaS herstellt. Citrix Virtual Apps and Desktops und Citrix DaaS wählen automatisch ein Zertifikat von der Smartcard aus und rufen die PIN von der HDX Engine ab.

Die verwandte Option `ENABLE_SSON` ist standardmäßig aktiviert.

Wenn Sie Single Sign-On aufgrund einer Sicherheitsrichtlinie auf einem Gerät nicht aktivieren können, konfigurieren Sie die Citrix Workspace-App mit der administrativen Gruppenrichtlinienobjektvorlage.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Wählen Sie **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort**.
3. Wählen Sie **Passthrough-Authentifizierung aktivieren**.
4. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.



### StoreFront konfigurieren:

Wenn Sie den Authentifizierungsdienst auf dem StoreFront-Server konfigurieren, aktivieren Sie die Option **Domänen-Passthrough**. Mit dieser Einstellung wird die integrierte Windows-Authentifizierung aktiviert. Die Option "Smartcard" muss nur aktiviert werden, wenn Sie auch Clients haben, die nicht in Domänen eingebunden sind und mit Smartcards eine Verbindung mit StoreFront herstellen.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter [Konfigurieren des Authentifizierungsdiensts](#) in der StoreFront-Dokumentation.

### Unterstützung für bedingten Zugriff mit Azure Active Directory

Der bedingte Zugriff ist ein Tool, mit dem Azure Active Directory Organisationsrichtlinien durchsetzt. Workspace-Administratoren können Richtlinien für den bedingten Zugriff mit Azure Active Directory für Benutzer konfigurieren und erzwingen, die sich bei der Citrix Workspace-App authentifizieren. Auf

der Windows-Maschine, auf der die Citrix Workspace-App ausgeführt wird, muss Microsoft Edge WebView2 Runtime-Version 99 oder höher installiert sein.

Ausführliche Informationen und Anweisungen zum Konfigurieren von Richtlinien für den bedingten Zugriff mit Azure Active Directory finden Sie in der **Dokumentation zum bedingten Azure AD-Zugriff** unter [Docs.microsoft.com/de-de/azure/active-directory/conditional-access/](https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/).

**Hinweis:**

Dieses Feature wird nur für Workspace (Cloud)-Bereitstellungen unterstützt.

## Unterstützung moderner Authentifizierungsmethoden für StoreFront-Stores

Mit der Gruppenrichtlinienobjektvorlage können Sie die Unterstützung für moderne Authentifizierungsmethoden für StoreFront-Stores aktivieren. Sie können dieses Feature mit dem Global App Configuration Service aktivieren.

Nutzen Sie eine der folgenden Methoden zur Authentifizierung bei Citrix StoreFront-Stores:

- Windows Hello und FIDO2-Sicherheitsschlüssel. Weitere Informationen finden Sie unter [Weitere Authentifizierungsmethoden](#).
- Single Sign-On bei Citrix StoreFront-Stores auf in Azure Active Directory (AAD) eingebundenen Maschinen mit AAD als Identitätsanbieter. Weitere Informationen finden Sie unter [Weitere Authentifizierungsmethoden](#).
- Workspace-Administratoren können Richtlinien für den bedingten Zugriff mit Azure Active Directory für Benutzer konfigurieren und erzwingen, die sich bei Citrix StoreFront-Stores authentifizieren. Weitere Informationen finden Sie unter [Unterstützung für bedingten Zugriff mit Azure AD](#).

Um dieses Feature zu aktivieren, müssen Sie Microsoft Edge WebView2 als zugrunde liegenden Browser für die direkte StoreFront- und Gateway-Authentifizierung verwenden.

**Hinweis:**

Stellen Sie sicher, dass Sie Microsoft Edge WebView2 Runtime-Version 102 oder höher verwenden.

Mit dem Global App Config Service und der Gruppenrichtlinienobjektvorlage können Sie moderne Authentifizierungsmethoden für StoreFront-Stores aktivieren.

### Global App Config Service verwenden

Aktivieren des Features:

1. Wählen Sie im **Citrix Cloud**-Menü zunächst **Workspacekonfiguration** und dann **App-Konfiguration**.
2. Klicken Sie auf **Sicherheit & Authentifizierung**.
3. Stellen Sie sicher, dass das Kontrollkästchen **Windows** aktiviert ist.
4. Wählen Sie in der Dropdownliste **Microsoft Edge WebView für StoreFront-Authentifizierung** neben **Windows** die Option **Aktiviert**.

#### Microsoft Edge WebView For StoreFront Authentication

This policy allows to control the WebView where the StoreFront authentication related web content is loaded. Microsoft Edge WebView2 provides support for modern authentication methods for StoreFront authentication.

<input type="checkbox"/>	Android	This setting is not applicable.
<input type="checkbox"/>	iOS	This setting is not applicable.
<input type="checkbox"/>	Mac	This setting is not applicable.
<input checked="" type="checkbox"/>	Windows	Enabled
<input type="checkbox"/>	HTML5	This setting is not applicable.
<input type="checkbox"/>	Linux	This setting is not applicable.

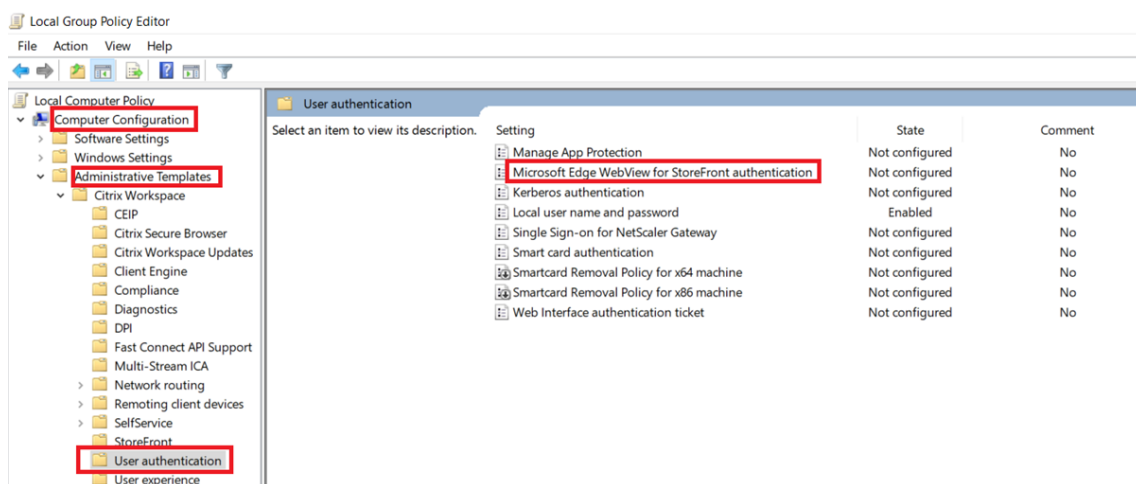
#### Hinweis:

Wenn Sie in der Dropdownliste **Microsoft Edge WebView für StoreFront-Authentifizierung** neben **Windows** die Option **Deaktiviert** auswählen, wird Internet Explorer WebView in der Citrix Workspace-App verwendet und die modernen Authentifizierungsmethoden für Citrix StoreFront-Stores werden nicht unterstützt.

#### GPO verwenden

Aktivieren des Features:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Workspace > Benutzerauthentifizierung**.
3. Klicken Sie auf die Richtlinie **Microsoft Edge WebView für StoreFront-Authentifizierung** und setzen Sie sie auf **Aktiviert**.



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

Wenn diese Richtlinie deaktiviert ist, verwendet die Citrix Workspace-App Internet Explorer Web-View. Die modernen Authentifizierungsmethoden für Citrix StoreFront-Stores werden dann nicht unterstützt.

## Weitere Authentifizierungsmethoden

Sie können die folgenden Authentifizierungsmethoden mit der Citrix Workspace-App konfigurieren. Damit die folgenden Authentifizierungsmethoden wie erwartet funktionieren, muss auf der Windows-Maschine, auf der die Citrix Workspace-App ausgeführt wird, Microsoft Edge WebView2 Runtime-Version 99 oder höher installiert sein.

1. Windows Hello-basierte Authentifizierung: Anweisungen zum Konfigurieren der Windows Hello-basierten Authentifizierung finden Sie im Artikel **Configure Windows Hello for Business Policy settings - Certificate Trust** unter [“Docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings”](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings).

### Hinweis:

Windows Hello-basierte Authentifizierung mit Domänen-Passthrough (Single Sign-On) wird nicht unterstützt.

2. Authentifizierung mit FIDO2-Sicherheitsschlüsseln: FIDO2-Sicherheitsschlüssel ermöglichen Unternehmensmitarbeitern eine nahtlose Authentifizierung ohne Eingabe von Benutzernamen oder Kennwort. Sie können die Authentifizierung mit FIDO2-Sicherheitsschlüsseln für Citrix Workspace konfigurieren. Wenn sich Benutzer bei Citrix Workspace mit ihrem Azure AD-Konto mit einem FIDO2-Sicherheitsschlüssel authentifizieren sollen, lesen Sie den Artikel **Enable passwordless security key sign-in** unter [Docs.microsoft.com/de-de/azure/active-directory/authentication/howto-authentication-passwordless-security-key](https://docs.microsoft.com/de-de/azure/active-directory/authentication/howto-authentication-passwordless-security-key).

3. Sie können Single Sign-On (SSO) für Citrix Workspace-App auch von in Microsoft Azure Active Directory (AAD) eingebundenen Maschinen mit AAD als Identitätsanbieter konfigurieren. Weitere Informationen zum Konfigurieren von Azure Active Directory-Domänendiensten finden Sie im Artikel **Configuring Azure Active Directory Domain services** unter [Docs.microsoft.com/de-de/azure/active-directory-domain-services/overview](https://docs.microsoft.com/de-de/azure/active-directory-domain-services/overview). Weitere Informationen zum Verbinden von Azure Active Directory mit Citrix Cloud finden Sie unter [Verbinden von Azure Active Directory mit Citrix Cloud](#).

## Smartcard

Citrix Workspace-App für Windows unterstützt folgende Smartcardauthentifizierung.

- **Passthrough-Authentifizierung (Single Sign-On):** Die Passthrough-Authentifizierung erfasst die Smartcard-Anmeldeinformationen, wenn Benutzer sich bei der Citrix Workspace-App anmelden. Die Citrix Workspace-App verwendet die erfassten Anmeldeinformationen wie folgt:
  - Benutzer von in Domänen eingebundenen Geräten, die sich mit einer Smartcard bei der Citrix Workspace-App anmelden, können virtuelle Desktops und Anwendungen ohne erneute Authentifizierung starten.
  - Ist die Citrix Workspace-App auf nicht in Domänen eingebundenen Geräten, die die Smartcard-Anmeldeinformationen verwenden, müssen die Benutzer zum Starten eines virtuellen Desktops oder einer virtuellen Anwendung die Anmeldeinformationen erneut eingeben.

StoreFront und die Citrix Workspace-App müssen beide für die Passthrough-Authentifizierung konfiguriert werden.

- **Bimodale Authentifizierung:** Bei der bimodalen Authentifizierung können die Benutzer zwischen einer Smartcard und der Eingabe des Benutzernamens und des Kennworts wählen. Das Feature eignet sich für Fälle, wenn keine Smartcard verwendet werden kann. Beispielsweise wenn das Anmeldezertifikat abgelaufen ist. Für die bimodale Authentifizierung müssen dedizierte Stores pro Site eingerichtet werden, damit die Methode **DisableCtrlAltDel** zur Smartcardverwendung auf **False** festgelegt werden kann. Die bimodale Authentifizierung erfordert eine StoreFront-Konfiguration.

Mit der bimodalen Authentifizierung kann der StoreFront-Administrator die Authentifizierung über Benutzernamen/Kennwort und per Smartcard bei dem gleichen Store durch Auswahl in der StoreFront-Konsole zulassen. Weitere Informationen finden Sie in der [StoreFront-Dokumentation](#).

- **Mehrere Zertifikate:** Mehrere Zertifikate können für eine Smartcard genutzt werden und wenn mehrere Smartcards verwendet werden. Wird eine Smartcard in einen Kartenleser eingeführt, gel-



ten die Zertifikate für alle Anwendungen, die auf dem Gerät ausgeführt werden, einschließlich der Citrix Workspace-App.

- **Clientzertifikatauthentifizierung:** Citrix Gateway und StoreFront müssen für die Clientzertifikatauthentifizierung konfiguriert werden.
  - Für den Zugriff auf StoreFront über Citrix Gateway ist nach dem Entfernen der Smartcard eine erneute Authentifizierung erforderlich.
  - Wenn die SSL-Konfiguration von Citrix Gateway auf **Mandatory client certificate authentication** (Verbindliche Clientzertifikatauthentifizierung) festgelegt ist, ist der Betrieb sicherer. Die verbindliche Clientzertifikatauthentifizierung ist jedoch nicht mit der bimodalen Authentifizierung kompatibel.
- **Double-Hop-Sitzungen:** Wenn ein Double Hop benötigt wird, wird eine Verbindung zwischen Citrix Workspace-App und dem virtuellen Desktop des Benutzers hergestellt.
- **Smartcard-aktivierte Anwendungen:** In smartcard-aktivierten Anwendungen, wie Microsoft Outlook und Microsoft Office, können Benutzer Dokumente, die in Sitzungen mit virtuellen Apps und Desktops verfügbar sind, digital signieren oder verschlüsseln.

#### **Einschränkungen:**

- Zertifikate müssen auf der Smartcard und nicht auf dem Benutzergerät gespeichert sein.
- Die Zertifikatauswahl wird in der Citrix Workspace-App nicht gespeichert, es wird jedoch bei entsprechender Konfiguration die PIN gespeichert. Die PIN wird im nicht ausgelagerten Speicher für die Dauer der Benutzersitzung zwischengespeichert. Sie wird nicht auf der Festplatte gespeichert.
- Die Citrix Workspace-App stellt die Verbindung mit einer Sitzung nicht wieder her, wenn eine Smartcard eingesteckt wird.
- Wenn die Citrix Workspace-App für die Smartcardauthentifizierung konfiguriert ist, wird VPN-Single Sign-On oder Sitzungsvorabstart nicht unterstützt. Für die Verwendung eines VPN mit der Smartcardauthentifizierung installieren Sie das Citrix Gateway Plug-In. Melden Sie sich über eine Webseite an und authentifizieren Sie sich bei jedem Schritt mit den Smartcards und PINs. Die Passthrough-Authentifizierung bei StoreFront mit dem Citrix Gateway Plug-In ist für Smartcardbenutzer nicht verfügbar.
- Die Kommunikation des Updater-Tools der Citrix Workspace-App mit citrix.com und Merchandising Server ist nicht kompatibel mit der Smartcardauthentifizierung auf Citrix Gateway.

#### **Warnung**

Einige Konfigurationen erfordern Registrierungsänderungen. Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie

dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

### Single Sign-On für die Smartcardauthentifizierung aktivieren:

Fügen Sie zum Konfigurieren der Citrix Workspace-App für Windows bei der Installation die folgende Befehlszeilenoption hinzu:

- `ENABLE_SSON=Yes`

Single Sign-On ist ein anderer Begriff für Passthrough-Authentifizierung. Wenn diese Einstellung aktiviert ist, zeigt die Citrix Workspace-App keine zweite PIN-Eingabeaufforderung an.

- Navigieren Sie im Registrierungs-Editor zum folgenden Pfad und legen Sie die Zeichenfolge `SSONCheckEnabled` auf `False` fest, wenn die Single Sign-On-Komponente nicht installiert ist.

```
HKEY_CURRENT_USER\Software{ Wow6432 } \Citrix\AuthManager\protocols  
\integratedwindows\
```

```
HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\  
protocols\integratedwindows\
```

Der Schlüssel verhindert, dass der Authentifizierungsmanager der Citrix Workspace-App nach der Single Sign-On-Komponente sucht, sodass die Citrix Workspace-App die Authentifizierung bei StoreFront durchführen kann.

Zum Aktivieren der Smartcardauthentifizierung bei StoreFront anstelle von Kerberos installieren Sie die Citrix Workspace-App für Windows mit folgenden Befehlszeilenoptionen:

- `/includeSSON` installiert die Single Sign-On-Authentifizierung (Passthrough-Authentifizierung). Aktiviert das Zwischenspeichern der Anmeldeinformationen und die Verwendung der domänenbasierten Passthrough-Authentifizierung.
- Meldet der Benutzer sich beim Endpunkt mit einer anderen Authentifizierungsmethode an (z. B. über Benutzernamen und Kennwort), verwenden Sie folgende Befehlszeile:

```
/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

Diese Art der Authentifizierung verhindert, dass die Anmeldeinformationen bei der Anmeldung erfasst werden. Gleichzeitig kann die Citrix Workspace-App die PIN bei der Anmeldung an der Citrix Workspace-App speichern.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Wählen Sie **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung > Lokaler Benutzername und Kennwort**.

3. Wählen Sie **Passthrough-Authentifizierung aktivieren**. Je nach Konfiguration und Sicherheitseinstellungen müssen Sie möglicherweise die Option **Passthrough-Authentifizierung für alle ICA-Verbindungen zulassen** aktivieren, damit die Passthrough-Authentifizierung funktioniert.

#### **StoreFront konfigurieren:**

- Wenn Sie den Authentifizierungsdienst konfigurieren, aktivieren Sie das Kontrollkästchen **Smartcard**.

Weitere Informationen zur Verwendung von Smartcards mit StoreFront finden Sie unter [Konfigurieren des Authentifizierungsdiensts](#) in der StoreFront-Dokumentation.

#### **Aktivieren der Benutzergeräte für die Smartcardverwendung:**

1. Importieren Sie das Stammzertifikat der Zertifizierungsstelle in den Schlüsselspeicher des Geräts.
2. Installieren Sie die kryptografische Middleware.
3. Installieren und konfigurieren Sie die Citrix Workspace-App.

#### **Ändern der Zertifikatauswahl:**

Wenn mehrere Zertifikate gültig sind, fordert die Citrix Workspace-App den Benutzer standardmäßig auf, ein Zertifikat aus der Liste auszuwählen. Sie können die Citrix Workspace-App jedoch auch so konfigurieren, dass das Standardzertifikat (gemäß Smartcardanbieter) oder das Zertifikat mit dem spätesten Ablaufdatum verwendet wird. Wenn keine gültigen Anmeldezertifikate vorhanden sind, wird der Benutzer benachrichtigt und kann eine alternative Anmeldemethode (falls vorhanden) verwenden.

Ein gültiges Zertifikat muss die drei folgenden Merkmale haben:

- Die aktuelle Uhrzeit auf dem lokalen Computer liegt im Gültigkeitszeitraum des Zertifikats.
- Der **öffentliche Schlüssel des Subjekts** muss den RSA-Algorithmus verwenden und eine Schlüssellänge von 1024, 2048 oder 4096 Bit haben.
- Die Schlüsselverwendung muss die digitale Signatur enthalten.
- Der alternative Antragstellernamen muss den Benutzerprinzipalnamen (UPN) enthalten.
- Die erweiterte Schlüsselverwendung muss Smartcard-Anmeldung und Clientauthentifizierung oder alle Schlüsselverwendungen enthalten.
- Eine der Zertifizierungsstellen in der Ausstellerkette des Zertifikats muss mit einem der zulässigen Distinguished Names übereinstimmen, den der Server im TLS-Handshake sendet.

Ändern Sie mit einer der folgenden Methoden, wie Zertifikate ausgewählt werden:

- Geben Sie in der Befehlszeile der Citrix Workspace-App die Option `AM_CERTIFICATESELECTIONMODE` `={ Prompt | SmartCardDefault | LatestExpiry }` an.

Prompt ist der Standard. Wenn mehrere Zertifikate die Anforderungen erfüllen, fordert Citrix Workspace für `SmartCardDefault` oder `LatestExpiry` den Benutzer zur Auswahl eines Zertifikats auf.

---

Fügen Sie dem	<code>SmartCardDefault</code>	<code>LatestExpiry</code> }.
---------------	-------------------------------	------------------------------

Registrierungsschlüssel  
`HKEY_CURRENT_USER` OR  
`HKEY_LOCAL_MACHINE\`  
`Software\[Wow6432Node`  
`\Citrix\AuthManager`  
den folgenden Schlüsselwert  
hinzu:  
`CertificateSelectionMode={`  
Prompt

---

•

In `HKEY_CURRENT_USER` definierte Werte haben Priorität über Werte in `HKEY_LOCAL_MACHINE`, um dem Benutzer die Auswahl des Zertifikats zu erleichtern.

#### **CSP-PIN-Aufforderungen verwenden:**

Die PIN-Aufforderungen, die den Benutzern angezeigt werden, werden standardmäßig von der Citrix Workspace-App für Windows und nicht von dem Smartcard-Kryptografiedienstanbieter bereitgestellt. Die Citrix Workspace-App fordert die Benutzer bei Bedarf zur Eingabe einer PIN auf und übergibt die PIN an den Smartcard-Kryptografiedienstanbieter. Wenn die Site oder Smartcard strengere Sicherheitsanforderungen hat, z. B. kein Zwischenspeichern der PIN pro Prozess oder pro Sitzung zulässt, können Sie in der Citrix Workspace-App konfigurieren, dass die PIN-Eingabe, einschließlich der Aufforderung für eine PIN, von den Komponenten des Kryptografiedienstanbieters verwaltet wird.

Ändern Sie mit einer der folgenden Methoden, wie die PIN-Eingabe gehandhabt wird:

- Geben Sie in der Befehlszeile der Citrix Workspace-App die Option `AM_SMARTCARDPINENTRY=CSP` an.
- Fügen Sie dem Registrierungsschlüssel `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager` den folgenden Schlüsselwert hinzu: `SmartCardPINEntry=CSP`.

#### **Änderungen bei der Unterstützung und Entfernung von Smartcards**

Eine Citrix Virtual Apps-Sitzung wird abgemeldet, wenn Sie die Smartcard entfernen. Wenn Smartcard als Authentifizierungsmethode für die Citrix Workspace-App konfiguriert ist, müssen Sie die

entsprechende Richtlinie in der Citrix Workspace-App für Windows konfigurieren, damit das Abmelden der Citrix Virtual Apps-Sitzung erzwungen werden kann. Der Benutzer bleibt an der Citrix Workspace-App-Sitzung angemeldet.

**Einschränkung:**

Wenn Sie sich an der Citrix Workspace-App per Smartcardauthentifizierung anmelden, wird der Benutzername als **Angemeldet** angezeigt.

**Schnelle-Smartcard-Feature** Das Schnelle-Smartcard-Feature ist eine Verbesserung gegenüber der alten HDX PC/SC-basierten Smartcardumleitung. Das Feature verbessert die Leistung, wenn Smartcards in WANs mit hoher Latenz verwendet werden.

Schnelle Smartcards werden nur unter Windows VDA unterstützt.

**Aktivieren der schnellen Smartcardanmeldung in der Citrix Workspace-App:**

Die schnelle Smartcardanmeldung ist standardmäßig auf dem VDA aktiviert und in der Citrix Workspace-App standardmäßig deaktiviert. Um die schnelle Smartcardanmeldung zu aktivieren, fügen Sie den folgenden Parameter in die Datei `default.ica` der zugeordneten StoreFront-Site ein:

```
1 copy[WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

**Deaktivieren der schnellen Smartcardanmeldung in der Citrix Workspace-App:**

Um die schnelle Smartcardanmeldung in der Citrix Workspace-App zu deaktivieren, entfernen Sie den Parameter `SmartCardCryptographicRedirection` aus der Datei `default.ica` der zugeordneten StoreFront-Site.

Weitere Informationen finden Sie unter [Smartcards](#).

**Automatische Authentifizierung für Citrix Workspace**

Die Citrix Workspace-App führt eine Richtlinie für ein Gruppenrichtlinienobjekt (GPO) ein, um die automatische Authentifizierung für Citrix Workspace zu aktivieren. Diese Richtlinie ermöglicht es der Citrix Workspace-App, sich beim Systemstart automatisch bei Citrix Workspace anzumelden. Verwenden Sie diese Richtlinie nur, wenn Domänen-Passthrough (Single Sign-On) für Citrix Workspace auf in Domänen eingebundenen Geräten konfiguriert ist. Dieses Feature ist in der Citrix Workspace-App für Windows Version 2012 und höher verfügbar.

Damit diese Richtlinie funktioniert, müssen die folgenden Kriterien erfüllt sein:

- Single Sign-On muss aktiviert sein.

- Der Schlüssel `SelfServiceMode` muss im Registrierungs-Editor auf `Off` festgelegt sein.

#### **Aktivieren der automatischen Authentifizierung:**

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 Workspace** > **Self-Service**.
3. Klicken Sie auf die Richtlinie **Automatische Authentifizierung für Citrix Workspace** und legen Sie sie auf **Aktiviert** fest.
4. Klicken Sie auf **Anwenden** und auf **OK**.

#### **Zwischenspeicherung von Kennwörtern und Benutzernamen in Citrix Workspace-App für Windows deaktivieren**

Standardmäßig verwendet Citrix Workspace für Windows automatisch den zuletzt eingegebenen Benutzernamen. Um das automatische Einfügen des Benutzernamens in das entsprechende Feld zu deaktivieren, bearbeiten Sie die Registrierung auf dem Benutzergerät:

1. Erstellen Sie einen REG\_SZ-Wert unter `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Remember`
2. Geben Sie als Wert "false" an.

Um das Kontrollkästchen **Kennwort speichern** zu deaktivieren und die automatische Anmeldung zu verhindern, erstellen Sie den folgenden Registrierungsschlüssel auf der Clientmaschine, auf der die Citrix Workspace-App für Windows installiert ist:

- Pfad: `HKEY_LOCAL_MACHINE\Software\wow6432node\Citrix\AuthManager`
- Typ: REG\_SZ
- Name: `SavePasswordMode`
- Wert: `Never`

#### **Hinweis:**

Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine falsche Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Informationen zum Verhindern des Zwischenspeicherns von Anmeldeinformationen für StoreFront-Stores finden Sie in der StoreFront-Dokumentation unter [Deaktivieren der Zwischenspeicherung von Kennwörtern und Benutzernamen in der Citrix Workspace-App für Windows](#).

## Unterstützung für mehr als 200 Gruppen in Azure AD

Ab diesem Release kann ein Azure AD-Benutzer, der Mitglied in mehr als 200 Gruppen ist, ihm zugewiesene Apps und Desktops anzeigen. Bisher konnte er diese Apps und Desktops nicht sehen.

### Hinweis:

Benutzer müssen sich von der Citrix Workspace-App abmelden und wieder anmelden, um diese Funktion zu aktivieren.

## Unterstützung der Proxyauthentifizierung

Bisher konnten Sie sich auf Clientcomputern, die für die Proxyauthentifizierung konfiguriert waren, nicht bei der Citrix Workspace-App authentifizieren, wenn die Proxyanmeldeinformationen nicht in der **Windows-Anmeldeinformationsverwaltung** gespeichert waren.

Für Citrix Workspace-App für Windows Version 2102 und höher gilt: Wenn auf Clientmaschinen, die für die Proxyauthentifizierung konfiguriert sind, die Proxyanmeldeinformationen nicht in der **Windows-Anmeldeinformationsverwaltung** gespeichert sind, werden Sie aufgefordert, die Proxyanmeldeinformationen einzugeben. Die Citrix Workspace-App speichert dann die Anmeldeinformationen des Proxyservers in der **Windows-Anmeldeinformationsverwaltung**. Dies führt zu einer nahtlosen Anmeldeerfahrung, da Sie Ihre Anmeldeinformationen vor dem Zugriff auf die Citrix Workspace-App nicht manuell in der Windows-Anmeldeinformationsverwaltung speichern müssen.

## User-Agent

Die Citrix Workspace-App sendet einen User-Agent in Netzwerkanforderungen, mit dem Authentifizierungsrichtlinien konfiguriert werden können, einschließlich der Umleitung der Authentifizierung an andere Identitätsanbieter (IdPs).

### Hinweis:

Die Versionsnummern, die in der folgenden Tabelle als Teil des User-Agents erwähnt werden, sind Beispiele und werden automatisch auf der Grundlage der von Ihnen verwendeten Versionen aktualisiert.

In der folgenden Tabelle werden Szenarien mit Beschreibung und User-Agent beschrieben:

Szenario	Beschreibung	User-Agent
<b>Allgemeine HTTP-Anforderungen</b>	Netzwerkanforderungen der Citrix Workspace-App erhalten in der Regel einen User-Agent. Zum Beispiel Netzwerkanforderungen wie <code>GET /Citrix/Roaming/Accounts</code> und <code>GET /AGServices/discover</code> .	<code>CitrixReceiver/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965) SelfService/23.5.0.63 (Release)X1Class CWACapable</code>
<b>Cloudstore</b>	Wenn ein Benutzer einen Cloudstore zur Citrix Workspace-App hinzufügt, werden Netzwerkanforderungen mit einem bestimmten User-Agent gesendet. Zum Beispiel Netzwerkanforderungen mit Pfad <code>/core/connect/authorize</code> .	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50 CWA/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965)</code>
<b>On-Premises-Store mit Gateway Advanced Auth mithilfe von Edge WebView</b>	Wenn sich ein Benutzer mithilfe von Edge WebView bei dem mit Advanced Auth konfigurierten Gateway in der Citrix Workspace-App authentifiziert, werden Netzwerkanforderungen mit einem bestimmten User-Agent gestellt. Zum Beispiel Netzwerkanforderungen, die <code>GET /nf/auth/doWebview.do</code> und <code>GET /logon/LogonPoint/tmindex.html</code> beinhalten.	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54 CWAWEBVIEW/23.2.0.2111 Windows/10.0 (22H2 Build 19045.2364)</code>



Szenario	Beschreibung	User-Agent
<b>On-Premises-Store mit Gateway Advanced Auth mithilfe von IE WebView</b>	Wenn sich ein Benutzer mithilfe von Internet Explorer WebView bei dem mit Advanced Auth konfigurierten Gateway in der Citrix Workspace-App authentifiziert, werden Netzwerkanforderungen mit einem bestimmten User-Agent gestellt. Zum Beispiel Netzwerkanforderungen, die <code>GET /nf/auth/doWebview.do</code> und <code>GET /logon/LogonPoint/tmindex.html</code> beinhalten.	<code>Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko, CWAWebView/23.5.0.43</code>
<b>Benutzerdefinierter Webstore</b>	Wenn ein Benutzer einen benutzerdefinierten Webstore zur Citrix Workspace-App hinzufügt, sendet die App einen User-Agent.	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50 CWA/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965)</code>

## Domänen-Passthrough-Zugriffsmatrix

April 22, 2024

Wenn Sie Citrix Workspace verwenden und Domänenpassthrough verwenden möchten, können Sie anhand der Tabellen in den Unterabschnitten ablesen, in welchen Szenarien Domänenpassthrough möglich ist.

Die Spaltenüberschriften haben folgende Bedeutung:

- Endpunkt verbunden mit: Gibt das Verzeichnis an, mit dem der Endpunkt verbunden ist. Das

Verzeichnis ermöglicht die Steuerung des Zugriffs auf On-Premises-Ressourcen. Dabei kann es sich um ein On-Premises-Active Directory (AD), ein Azure Active Directory (AAD) oder ein Hybridverzeichnis handeln.

- Identitätsanbieter (IdP): Entität, die zur Bereitstellung von Authentifizierungsdiensten für Citrix Workspace verwendet wird. Sie ermöglicht die Herstellung einer Verbindung zu den Ressourcen.
- Verbundauthentifizierungsdienst (FAS): Weitere Informationen finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).
- Virtual Delivery Agent (VDA): Weitere Informationen finden Sie unter [Installieren von VDAs](#).
- VDA verbunden mit: Gibt das Verzeichnis an, mit dem das VDA-Gerät verbunden ist. Weitere Informationen finden Sie unter [Identitäts- und Zugriffsverwaltung](#).
- Single Sign-On (SSO) bei Citrix Workspace/VDA: “Ja” oder “Nein” gibt an, ob Domänenpassthrough an Citrix Workspace oder den VDA unterstützt wird.
- Citrix Workspace-App: Informationen zum Bereitstellen von Single Sign-On finden Sie unter [Konfigurieren von Single Sign-On während der Neuinstallation](#).

**Hinweis:**

Möglicherweise benötigen Sie die neueste Version der Citrix Workspace-App, um Domänenpassthrough für einige der folgenden Szenarien zu ermöglichen.

**Unterstützung von Domänen-Passthrough für Citrix Workspace**

Endpunkt verbunden mit	IdP	VDA verbunden mit	SSO an Citrix Workspace	SSO an VDA	Dokumentation
AD	On-Premises Citrix Gateway	AD	Ja	Citrix Workspace App/FAS	<a href="#">Domänen-Passthrough-Authentifizierung an Citrix Workspace mit On-Premises-Citrix Gateway als Identitätsanbieter</a>

Endpunkt verbunden mit	IdP	VDA verbunden mit	SSO an Citrix Workspace	SSO an VDA	Dokumentation
AD	Adaptive Authentifizierung	AD	Ja	Citrix Workspace App/FAS	Zum Konfigurieren der adaptiven Authentifizierung lesen Sie <a href="#">Adaptive Authentifizierung</a> und folgen Sie den Anweisungen unter <a href="#">Domänen-Passthrough-Authentifizierung an Citrix Workspace mit On-Premises-Citrix Gateway als Identitätsanbieter.</a>

Endpunkt verbunden mit	IdP	VDA verbunden mit	SSO an Citrix Workspace	SSO an VDA	Dokumentation
AD	Citrix Gateway im Verbund mit einem anderen IdP (AAD/Okta)	AD	Ja	Citrix Workspace App/FAS	Konfigurieren Sie IdP gemäß <a href="#">Configure SAML single sign-on</a> und lesen Sie die Dokumentation zu dem zum Konfigurieren von Domänenpassthrough verwendeten IdP.
AD	Okta	AD	Ja	Citrix Workspace App/FAS	<a href="#">Domänen-Passthrough-Authentifizierung an Citrix Workspace mit Okta als Identitätsanbieter.</a>
AD/Hybrid	AAD (AD mit AAD Connect)	AD	Ja	Citrix Workspace App/FAS **	<a href="#">Domänen-Passthrough-Authentifizierung an Citrix Workspace mit Azure Active Directory als Identitätsanbieter.</a>

Endpunkt verbunden mit	IdP	VDA verbunden mit	SSO an Citrix Workspace	SSO an VDA	Dokumentation
AD	Beliebiger SAML-basierter IdP (z. B. ADFS)	AD	Ja	Citrix Workspace App/FAS	Weitere Informationen finden Sie unter <a href="#">Verbinden von SAML als Identitätsanbieter mit Citrix Cloud</a> und in der Dokumentation des zum Konfigurieren von Domänenpassthrough verwendeten IdP.
AD	AD	AD	Nein	Nicht unterstützt	Nicht verfügbar
AD	AD+OTP	AD	Nein	Nicht unterstützt	Nicht verfügbar
AD	AAD	AAD	Nein	Nicht unterstützt	Nicht verfügbar

Endpunkt verbunden mit	IdP	VDA verbunden mit	SSO an Citrix Workspace	SSO an VDA	Dokumentation
AAD	AAD ohne On-Premises-AD	AD	Ja	FAS	Citrix Workspace verwendet Microsoft Edge WebView, was SSO beim Workspace ermöglicht. SSO am VDA wird über FAS unterstützt. Weitere Informationen finden Sie unter <a href="#">Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst (FAS)</a> .

Endpunkt verbunden mit	IdP	VDA verbunden mit	SSO an Citrix Workspace	SSO an VDA	Dokumentation
AAD	AAD	AAD	Ja	Der Benutzer muss Anmeldeinformationen eingeben.	Citrix Workspace verwendet Microsoft Edge WebView, was SSO beim Workspace ermöglicht. SSO beim VDA wird nicht unterstützt.
Gehört keiner Domäne an	IdP, der kennwortlose Authentifizierung unterstützt – Link	AD	Nein	FAS	Citrix Workspace verwendet Microsoft Edge WebView, was SSO beim Workspace ermöglicht. SSO am VDA wird über FAS unterstützt. Weitere Informationen finden Sie unter <a href="#">Weitere Methoden der Authentifizierung bei Citrix Workspace</a> .

**Hinweise:**

- Der Client muss für AD erreichbar sein, damit Kerberos funktioniert.
- \*\*Citrix Single Sign-On (SSONSVR.exe) funktioniert nur mit dem Benutzernamen oder Kennwort auf dem Client. Wenn sich der Benutzer mit Windows Hello anmeldet, ist FAS erforderlich.
- Die Authentifizierung erfolgt in der Cloud möglicherweise nicht gänzlich automatisch, wenn LLT aktiviert oder die Richtlinie zur Annahme durch die Endbenutzer konfiguriert ist.
- Es wird empfohlen, FAS passend für Nicht-Windows-Plattformen zu konfigurieren.

**Unterstützung von Domänen-Passthrough für StoreFront**

Endpunkt verbunden mit	IdP	VDA verbunden mit	SSO an Citrix Workspace	SSO an VDA	Dokumentation
AD	StoreFront	AD	Ja	Citrix Workspace-App	<a href="#">Domänen-Passthrough-Authentifizierung</a>
AD/Hybrid/Windows Hello for Business	StoreFront	AD	Ja (1)	Citrix Workspace-App/FAS (2)	<a href="#">Domänen-Passthrough-Authentifizierung und Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst (FAS)</a>
AD	Citrix Gateway —Erweiterte Authentifizierung	AD	Ja	Citrix Workspace-App (3)	



AD	Standardauthentifizierung mit Citrix Gateway	AD-Zertifizierung	Ja	Citrix Workspace-App (4)	<a href="#">Domänen-Passthrough-Authentifizierung.</a>
----	----------------------------------------------	-------------------	----	--------------------------	--------------------------------------------------------

---

**Hinweise:**

1. Navigieren Sie im Registrierungs-Editor zum folgenden Pfad und legen Sie die Zeichenfolge `SSONCheckEnabled` auf `False` fest, wenn die Single Sign-On-Komponente nicht installiert ist.

`HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\`

The key prevents the Citrix Workspace app authentication manager from checking for the single sign-on component and allows Citrix Workspace app to authenticate to StoreFront.

2. Wenn Sie sich mit Windows Hello anmelden, sind FAS und eine Registrierungskonfiguration zum Aktivieren von SSO erforderlich.
3. Der Client muss für AD erreichbar sein, da Kerberos verwendet wird.
4. Funktioniert auch, wenn der Client für AD nicht erreichbar ist. Keine Verwendung von Kerberos.

## Domänen-Passthrough-Authentifizierung an Citrix Workspace mit On-Premises-Citrix Gateway als Identitätsanbieter

April 22, 2024

**Wichtig:**

Dieser Artikel unterstützt Sie beim Konfigurieren der Domänen-Passthrough-Authentifizierung. Wenn Sie bereits ein On-Premises-Gateway als IdP eingerichtet haben, fahren Sie mit dem unter [Konfigurieren von Domänen-Passthrough als Authentifizierungsmethode in Citrix Gateway](#) beschriebenen Verfahren fort.

Citrix Cloud unterstützt die Verwendung eines On-Premises-Citrix Gateways als Identitätsanbieter für die Authentifizierung von Abonnenten, wenn diese sich bei ihrem Workspace anmelden.

Vorteile der Authentifizierung mit Citrix Gateway:

- Fortdauernde Authentifizierung von Benutzern über das vorhandene Citrix Gateway, damit sie über Citrix Workspace auf die Ressourcen in der On-Premises-Bereitstellung von Virtual Apps and Desktops zugreifen können.
- Verwenden Sie die Funktionen “Authentifizierung”, “Autorisierung” und “Auditing” von Citrix Gateway mit Citrix Workspace.
- Stellen Sie den Benutzerzugriff auf erforderliche Ressourcen über Citrix Workspace-Features wie Passthrough-Authentifizierung, Smartcards, Sicherheitstoken, Richtlinien für bedingten Zugriff, Verbund usw. bereit.

Die Authentifizierung mit Citrix Gateway wird für folgende Produktversionen unterstützt:

- Citrix Gateway 13.1.4.43 Advanced Edition oder höher

**Voraussetzungen:**

- Cloud Connectors: Sie benötigen mindestens zwei Server zum Installieren der Citrix Cloud Connector-Software.
- Active Directory und die Domäne muss registriert sein.
- Anforderungen für Citrix Gateway
  - Verwenden Sie erweiterte Richtlinien, da klassische Richtlinien veraltet sind.
  - Beim Konfigurieren des Gateways für die Authentifizierung von Abonnenten bei Citrix Workspace fungiert das Gateway als OpenID Connect-Anbieter. Nachrichten zwischen Citrix Cloud und Gateway entsprechen dem OIDC-Protokoll, was auch die digitale Signatur von Token umfasst. Daher müssen Sie ein Zertifikat zur Signatur dieser Token konfigurieren.
  - Zeitsynchronisierung: Citrix Gateway muss mit der NTP-Zeit synchronisiert werden.

Einzelheiten finden Sie unter [Voraussetzungen](#) in der Citrix Cloud-Dokumentation.

Bevor Sie die OAuth IdP-Richtlinie erstellen, müssen Sie Citrix Workspace oder Cloud zur Verwendung des Gateways als Authentifizierungsoption im IdP einrichten. Einzelheiten hierzu finden Sie unter [Verbinden eines On-Premises-Citrix Gateways mit Citrix Cloud](#). Wenn Sie die Einrichtung vornehmen, werden die Client-ID, das Geheimnis und die Umleitungs-URL generiert, die zum Erstellen der OAuth-IdP-Richtlinie erforderlich sind.

Die Domänen-Passthrough-Authentifizierung für Workspace für Web ist aktiviert, wenn Sie Internet Explorer, Microsoft Edge, Mozilla Firefox und Google Chrome verwenden. Die Domänen-Passthrough-Authentifizierung wird nur aktiviert, wenn der Client erfolgreich erkannt wurde.

**Hinweis:**

Wenn der HTML5-Client von einem Benutzer bevorzugt oder vom Administrator erzwungen wird, wird die Domänen-Passthrough-Authentifizierungsmethode nicht aktiviert.

Beim Starten der StoreFront-URL in einem Browser wird die Aufforderung **Receiver ermitteln** angezeigt.

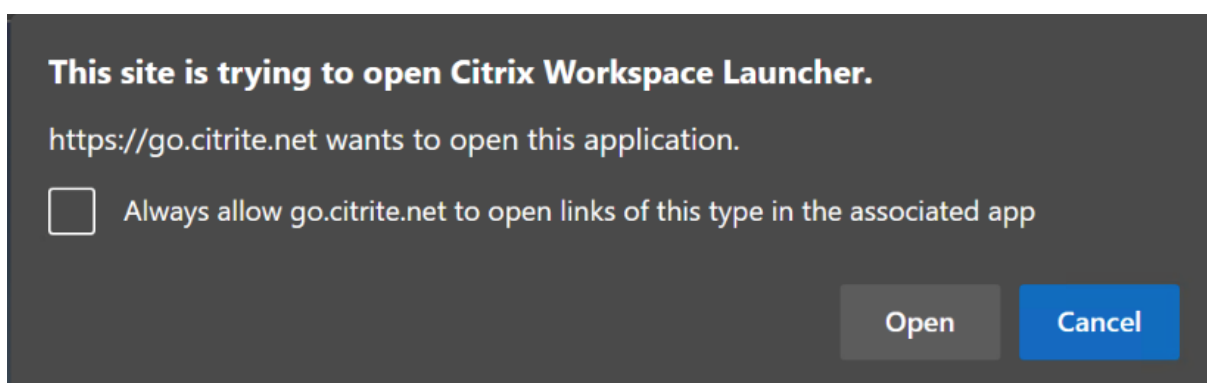
Wenn die Geräte verwaltet werden, konfigurieren Sie die Gruppenrichtlinie so, dass diese Aufforderung deaktiviert wird, anstatt die Clienterkennung zu deaktivieren. Weitere Informationen:

- [URLAllowlist](#) in der Microsoft-Dokumentation.
- [URLAllowlist](#) in der Google Chrome-Dokumentation.

**Hinweis:**

Der von der Citrix Workspace-App verwendete Protokollhandler ist **receiver**. Konfigurieren Sie dies als eine zugelassene URL.

Die Benutzer können auch das im folgenden Beispiel einer StoreFront-URL in der Aufforderung zur Clienterkennung gezeigte Kontrollkästchen aktivieren. Durch Aktivieren dieses Kontrollkästchens wird die Aufforderung auch bei anschließenden Starts vermieden.



Nachfolgend wird erläutert, wie Citrix Gateway als IdP eingerichtet werden kann.

## **Erstellen einer OAuth-IdP-Richtlinie im On-Premises-Citrix Gateway**

Das Erstellen einer OAuth-IdP-Authentifizierungsrichtlinie umfasst die folgenden Aufgaben:

1. Erstellen eines OAuth-IdP-Profiles
2. Hinzufügen einer OAuth-IdP-Richtlinie
3. Binden der OAuth-IdP-Richtlinie an einen virtuellen Server
4. Globales Binden des Zertifikats

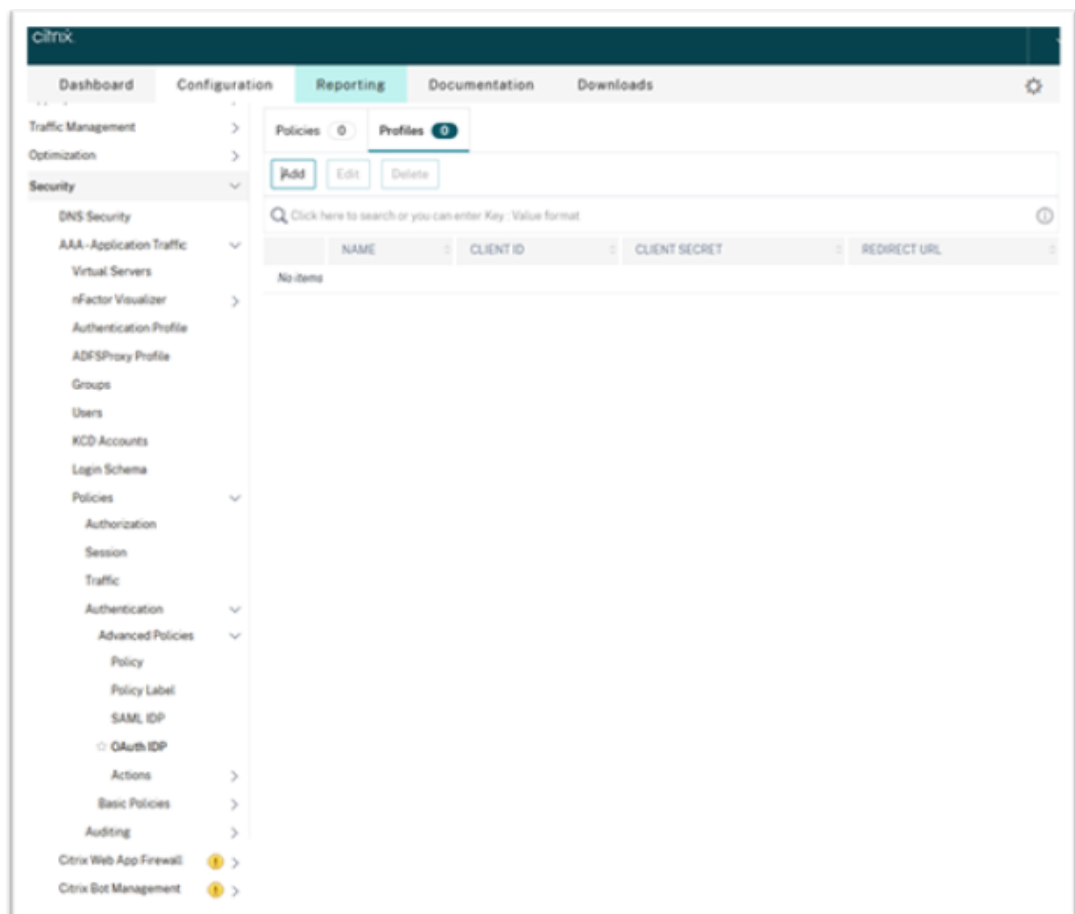
### **Erstellen eines OAuth-IdP-Profiles**

1. Um ein OAuth-IdP-Profil mithilfe der CLI zu erstellen, geben Sie an der Eingabeaufforderung Folgendes ein:

```
1 add authentication OAuthIdPProfile <name> [-clientID <string>][-  
  clientSecret ][-redirectURL <URL>][-issuer <string>][-audience  
  <string>][-skewTime <mins>] [-defaultAuthenticationGroup <  
  string>]  
2  
3 add authentication OAuthIdPPolicy <name> -rule <expression> [-  
  action <string> [-undefAction <string>] [-comment <string>][-  
  logAction <string>]  
4  
5 add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=  
  aaa,dc=local"  
6  
7 ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password  
  > -ldapLoginName sAMAccountName  
8  
9 add authentication policy <name> -rule <expression> -action <  
  string>  
10  
11 bind authentication vserver auth_vs -policy <ldap_policy_name> -  
  priority <integer> -gotoPriorityExpression NEXT  
12  
13 bind authentication vserver auth_vs -policy <OAuthIdPPolicyName> -  
  priority <integer> -gotoPriorityExpression END  
14  
15 bind vpn global -certkey <>  
16  
17 <!--NeedCopy-->
```

2. Zum Erstellen eines OAuth-IdP-Profiles mit der GUI gehen Sie folgendermaßen vor:

- a) Melden Sie sich bei dem Verwaltungsportal Ihres On-Premises-Citrix Gateways an und gehen Sie zu **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > OAuth IDP**.



- b) Klicken Sie auf der Seite **OAuth IdP** auf die Registerkarte **Profiles** und dann auf **Add**.
- c) Konfigurieren Sie das OAuth-IdP-Profil.

**Hinweis:**

- Kopieren Sie die Client-ID-, das Geheimnis und Umleitungs-URL auf der Registerkarte **Citrix Cloud > Identitäts- und Zugriffsverwaltung > Authentifizierung** und fügen Sie sie ein, um die Verbindung mit Citrix Cloud herzustellen.
- Geben Sie die Gateway-URL korrekt in das Feld **Issuer Name** ein. Beispiel: <https://GatewayFQDN.com>.
- Kopieren Sie die Client-ID und fügen Sie sie in das Feld **Audience** ein.
- **Send Password:** Aktivieren Sie diese Option für SSO. Standardmäßig ist diese Option deaktiviert.

- d) Legen Sie auf der Seite **Create Authentication OAuth IdP Profile** Werte für die folgenden Parameter fest und klicken Sie auf **Create**.
- **Name:** Name des Authentifizierungsprofils. Muss mit einem Buchstaben, einer Zahl oder dem Unterstrich (\_) beginnen. Der Name darf ausschließlich Buchstaben, Zahlen

Bindestriche (-), Punkte (.), Rautenzeichen (#), Leerzeichen ( ), At-Zeichen (@), das Gleichheitszeichen (=), Doppelpunkte (:) und Unterstriche enthalten. Sie können den Namen nicht mehr ändern, wenn das Profil erstellt ist.

- **Client ID:** Eindeutige Zeichenfolge zur SP-Identifizierung. Der Autorisierungsserver leitet die Clientkonfiguration von dieser ID ab. Maximale Länge: 127.
- **Client Secret:** Geheime Zeichenfolge, die vom Benutzer und Autorisierungsserver erstellt wird. Maximale Länge: 239.
- **Redirect URL:** Endpunkt auf dem SP, auf dem der Code / das Token gepostet werden muss.
- **Issuer Name:** Name des Servers, dessen Token akzeptiert werden sollen. Maximale Länge: 127. Beispiel: <https://GatewayFQDN.com>.
- **Audience:** Zielempfänger für das vom IdP gesendete Token. Der Empfänger überprüft dieses Token.
- **Skew Time** Zeitversatz (in Minuten), den Citrix ADC für ein eingehendes Token zulässt. Beispiel: Bei einem Wert von 10 ist das Token ab aktuelle Zeit minus 10 Minuten bis aktuelle Zeit plus 10 Minuten, also insgesamt 20 Minuten gültig. Standardwert: 5.
- **Default Authentication Group:** Gruppe, die zur Liste der internen Gruppen der Sitzung hinzugefügt wird, wenn das Profil vom IdP ausgewählt wird, und die im nFactor-Flow verwendet werden kann. Sie kann im Ausdruck (AAA.USER.IS\_MEMBER\_OF(xxx")) für Authentifizierungsrichtlinien verwendet werden, um den nFactor-Flow zu identifizieren, der mit einer vertrauenden Partei zusammenhängt. Maximale Länge: 63

Der Sitzung für dieses Profil wird eine Gruppe hinzugefügt, um die Richtlinienbewertung und das Anpassen von Richtlinien zu vereinfachen. Die Gruppe ist die Standardgruppe, die zusätzlich zu extrahierten Gruppen ausgewählt wird, wenn die Authentifizierung erfolgreich ausgeführt wird. Maximale Länge: 63.

The screenshot shows the Citrix console interface for creating an OAuth IDP profile. The top navigation bar includes 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The main heading is 'Create Authentication OAuth IDP Profile'. The form contains the following fields and options:

- Name\***: gatewayIDP
- Client ID\***: cclientid
- Client Secret\***: cclientsecret
- Redirect URL\***: https://redirecUrl
- Issuer Name**: (empty)
- Audience**: cclientid
- Skew Time (mins)**: 5
- Default Authentication Group**: testGroup
- Relying Party Metadata URL**: (empty)
- Refresh Interval**: 50
- Encrypt Token**
- Signature Service**: (empty)
- Attributes**: (empty)
- Send Password**

At the bottom, there are 'Create' and 'Close' buttons.

### Hinzufügen einer OAuth IdP-Richtlinie

1. Klicken Sie auf der Seite "OAuth IdP" auf die Registerkarte **Profiles** und dann auf **Add**.
2. Legen Sie auf der Seite **Create Authentication OAuth IdP Policy** Werte für die folgenden Parameter fest und klicken Sie auf **Create**.
  - **Name**: Name der Authentifizierungsrichtlinie.
  - **Action**: Name des zuvor erstellten Profils.
  - **Log Action**: Name der Nachrichtenprotokollaktion, die verwendet werden soll, wenn eine Anforderung mit dieser Richtlinie übereinstimmt. Kein Pflichtfeld.
  - **Undefined-Result Action**: Aktion, die ausgeführt werden soll, wenn das Ergebnis der Richtlinienbewertung nicht definiert ist (UNDEF). Kein Pflichtfeld.
  - **Expression**: Standardsyntaxausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anfrage zu antworten. Beispiel: true.
  - **Comments**: Kommentare zu der Richtlinie.

The screenshot shows the Citrix management console interface for creating an OAuth IDP Policy. The navigation bar includes Dashboard, Configuration, Reporting, Documentation, and Downloads. The main heading is 'Create Authentication OAuth IDP Policy'. The form contains the following fields and controls:

- Name\***: A text input field containing 'gatewayIDP\_pol'.
- Action\***: A dropdown menu with 'gatewayIDP' selected, accompanied by 'Add' and 'Edit' buttons.
- Log Action**: A dropdown menu with an empty selection, accompanied by 'Add' and 'Edit' buttons.
- Undefined Result Action**: A dropdown menu with an empty selection.
- Expression\***: A text area containing 'true', with an 'Expression Editor' link and an 'Evaluate' button.
- Comments**: A text input field.
- Buttons**: 'Create' and 'Close' buttons at the bottom of the form.

**Hinweis:**

Wenn sendPassword auf ON (standardmäßig OFF) festgelegt ist, werden Benutzeranmeldedaten verschlüsselt und über einen sicheren Kanal an Citrix Cloud weitergeleitet. Werden Benutzeranmeldedaten über einen sicheren Kanal übergeben, können Sie SSO für Citrix Virtual Apps and Desktops beim Start aktivieren.

### Binden Sie die OAuthIDP-Richtlinie und die LDAP-Richtlinie an den virtuellen Authentifizierungsserver

Jetzt müssen Sie die OAuth IdP-Richtlinie an den virtuellen Authentifizierungsserver auf dem On-Premises-Citrix Gateway binden.

1. Melden Sie sich bei dem Verwaltungsportal Ihres On-Premises-Citrix Gateways an und gehen Sie zu **Configuration > Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Actions > LDAP**.
2. Klicken Sie auf der Seite **LDAP Actions** auf **Add**.
3. Legen Sie auf der Seite "Create Authentication LDAP Server" Werte für die folgenden Parameter fest und klicken Sie auf **Create**.
  - **Name:** Name der LDAP-Aktion.
  - **ServerName/ServerIP :** FQDN oder IP des LDAP-Servers.



- Wählen Sie die entsprechenden Werte für **Security Type, Port, Server Type, Time-Out**.
  - Stellen Sie sicher, dass die **Authentication** aktiviert ist.
  - **Base DN:** Basis, von der aus die LDAP-Suche gestartet wird Beispiel: `dc=aaa,dc=local`.
  - **Administrator Bind DN:** Benutzername der Bindung an den LDAP-Server. Beispiel: `admin@aaa.local`.
  - **Administrator Password/Confirm Password:** Kennwort zum Binden von LDAP.
  - Klicken Sie auf **Test Connection**, um Ihre Einstellungen zu testen.
  - **Server Logon Name Attribute:** Wählen Sie "sAMAccountName".
  - Die anderen Felder sind nicht obligatorisch und können daher nach Bedarf konfiguriert werden.
4. Gehen Sie zu **Configuration > Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Policy**.
  5. Klicken Sie auf der Seite **Authentication Policies** auf **Add**.
  6. Legen Sie auf der Seite **Create Authentication Policy** Werte für die folgenden Parameter fest und klicken Sie auf **Create**.
    - **Name:** Name der LDAP-Authentifizierungsrichtlinie.
    - **Action Type:** Wählen Sie LDAP.
    - **Action:** Wählen Sie die LDAP-Aktion.
    - **Expression:** Standardsyntaxausdruck, den die Richtlinie verwendet, um auf eine bestimmte Anfrage zu antworten. Beispiel: `true**`.

### Globales Binden des Zertifikats an das VPN

Das globale Binden des Zertifikats an das VPN erfordert CLI-Zugriff auf das On-Premises-Citrix Gateway. Melden Sie sich mit Putty (o. ä.) unter Einsatz von SSH beim On-Premises-Citrix Gateway an.

1. Starten Sie ein Befehlszeilendienstprogramm wie Putty.
2. Melden Sie sich unter Einsatz von SSH beim On-Premises-Citrix Gateway an.
3. Geben Sie den folgenden Befehl ein:

```
show vpn global
```

#### Hinweis:

Es muss kein Zertifikat gebunden werden.

```
Done
> show vpn global

1)      VPN Clientless Access Policy Name: ns_cvpa_owa_policy   Priority: 95000
        Bindpoint: REQ_DEFAULT
2)      VPN Clientless Access Policy Name: ns_cvpa_sp_policy   Priority: 96000
        Bindpoint: REQ_DEFAULT
3)      VPN Clientless Access Policy Name: ns_cvpa_sp2013_policy   Priority: 97000
        Bindpoint: REQ_DEFAULT
4)      VPN Clientless Access Policy Name: ns_cvpa_default_policy   Priority: 100000
        Bindpoint: REQ_DEFAULT

Done
```

4. Um die Zertifikate des On-Premises-Citrix Gateways aufzulisten, geben Sie den folgenden Befehl ein:

```
show ssl certkey
```

5. Wählen Sie das geeignete Zertifikat und geben Sie den folgenden Befehl ein, um es global an das VPN zu binden:

```
bind vpn global -certkey cert_key_name
```

“cert\_key\_name” ist der Name des Zertifikats.

6. Geben Sie den folgenden Befehl ein, um zu überprüfen, ob das Zertifikat global an das VPN gebunden ist:

```
show vpn global
```

```
Done
> show vpn global
Certificate: Gateway_ ██████████

1)      VPN Clientless Access Policy Name: ns_cvpa_owa_policy   Priority: 95000
        Bindpoint: REQ_DEFAULT
2)      VPN Clientless Access Policy Name: ns_cvpa_sp_policy   Priority: 96000
        Bindpoint: REQ_DEFAULT
3)      VPN Clientless Access Policy Name: ns_cvpa_sp2013_policy   Priority: 97000
        Bindpoint: REQ_DEFAULT
4)      VPN Clientless Access Policy Name: ns_cvpa_default_policy   Priority: 100000
        Bindpoint: REQ_DEFAULT

Done
```

## Konfigurieren von Domänen-Passthrough als Authentifizierungsmethode in Citrix Gateway

Wenn Sie die Einrichtung des Citrix Gateways als IdP abgeschlossen haben, führen Sie die folgenden Schritte aus, um Domänen-Passthrough als Authentifizierungsmethode im Citrix Gateway zu konfigurieren.

Wenn Domänen-Passthrough als Authentifizierungsmethode festgelegt ist, verwendet der Client Kerberos-Tickets zur Authentifizierung anstelle von Anmeldeinformationen.

Citrix Gateway unterstützt sowohl Identitätswechsel als auch die eingeschränkte Kerberos-Delegierung (KCD). In diesem Artikel wird die KCD-Authentifizierung beschrieben. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX236593](#).

Konfigurieren Sie Domänen-Passthrough mit folgenden Schritten:

1. Konfiguration der eingeschränkten Kerberos-Delegierung
2. Clientkonfiguration

### **Konfiguration der eingeschränkten Kerberos-Delegierung**

1. Erstellen Sie einen KCD-Benutzer in Active Directory

Kerberos funktioniert mit einem Ticketsystem zur Authentifizierung von Benutzern für Ressourcen und umfasst einen Client, einen Server und ein Schlüsselverteilungszentrum (KDC).

Damit Kerberos funktioniert, muss der Client ein Ticket beim KDC anfordern. Der Client muss sich zunächst mit Benutzernamen, Kennwort und Domäne beim KDC authentifizieren, bevor er ein Ticket anfordert (AS-Anforderung).

The screenshot shows the 'kcduser Properties' dialog box with the 'General' tab selected. The fields are as follows:

- Member Of: (empty)
- Dial-in: (empty)
- Environment: (empty)
- Sessions: (empty)
- Remote control: (empty)
- Remote Desktop Services Profile: (empty)
- Personal Virtual Desktop: (empty)
- COM+: (empty)
- General: (selected)
- Address: (empty)
- Account: (empty)
- Profile: (empty)
- Telephones: (empty)
- Delegation: (empty)
- Organization: (empty)

Fields for user information:

- First name:  Initials:
- Last name:
- Display name:
- Description:
- Office:
- Telephone number:  Other...
- Email:
- Web page:  Other...

Buttons: OK, Cancel, Apply, Help

2. Ordnen Sie dem neuen Benutzer den Service Principal Name (SPN) zu.

Der Gateway-SPN wird vom Client zur Authentifizierung verwendet.

- Service Principal Name (SPN): Ein Service Principal Name (SPN) ist eine eindeutige ID einer Dienstinstanz. Die Kerberos-Authentifizierung verwendet den SPN, um eine Dienstinstanz einem Dienstanmeldekonto zuzuordnen. Diese Funktion ermöglicht es einer Clientanwendung, die Dienstaauthentifizierung eines Kontos anzufordern, selbst wenn der Client nicht über den Kontonamen verfügt.

SetSPN ist die Anwendung zum Verwalten von SPNs auf Windows-Geräten. Mit SetSPN können Sie SPN-Registrierungen anzeigen, bearbeiten und löschen.

a) Öffnen Sie auf dem Active Directory-Server eine Eingabeaufforderung.

- b) Geben Sie an der Eingabeaufforderung den folgenden Befehl ein:

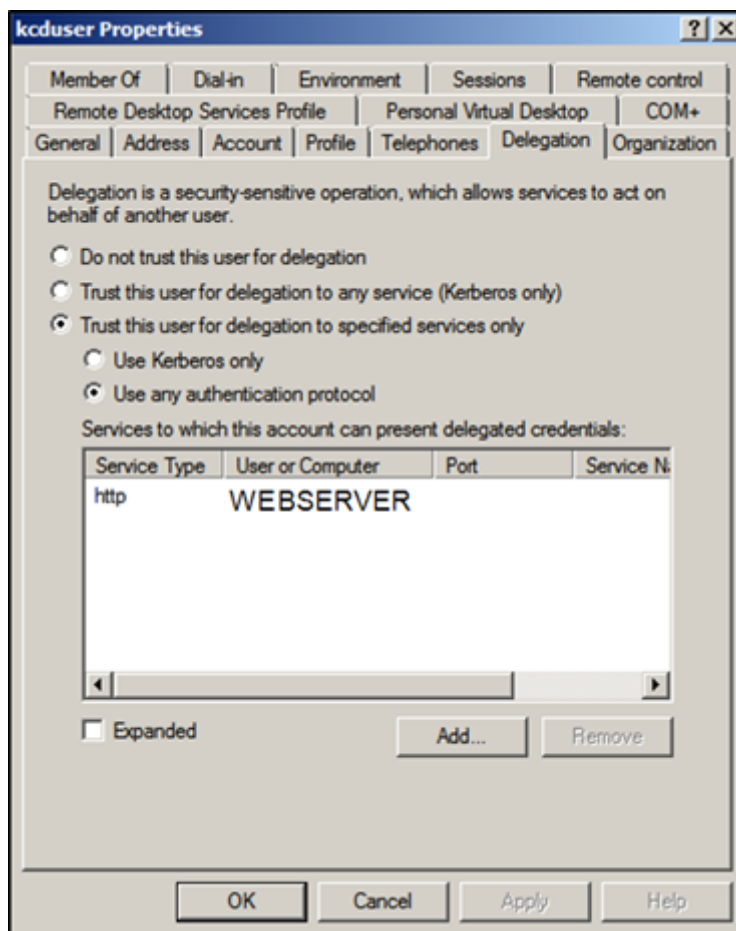
```
setspn -A http/<LB fqdn> <domain\Kerberos user>
```

- c) Führen Sie den folgenden Befehl aus, um die SPNs für den Kerberos-Benutzer zu bestätigen:

```
setspn -l <Kerberos user>
```

Die Registerkarte für die Delegation wird angezeigt, nachdem Sie den Befehl `setspn` ausgeführt haben.

- d) Wählen Sie **Benutzer bei Delegationen angegebener Dienste vertrauen** und **Beliebiges Authentifizierungsprotokoll verwenden**. Fügen Sie den Webserver hinzu und wählen Sie den HTTP-Dienst aus.



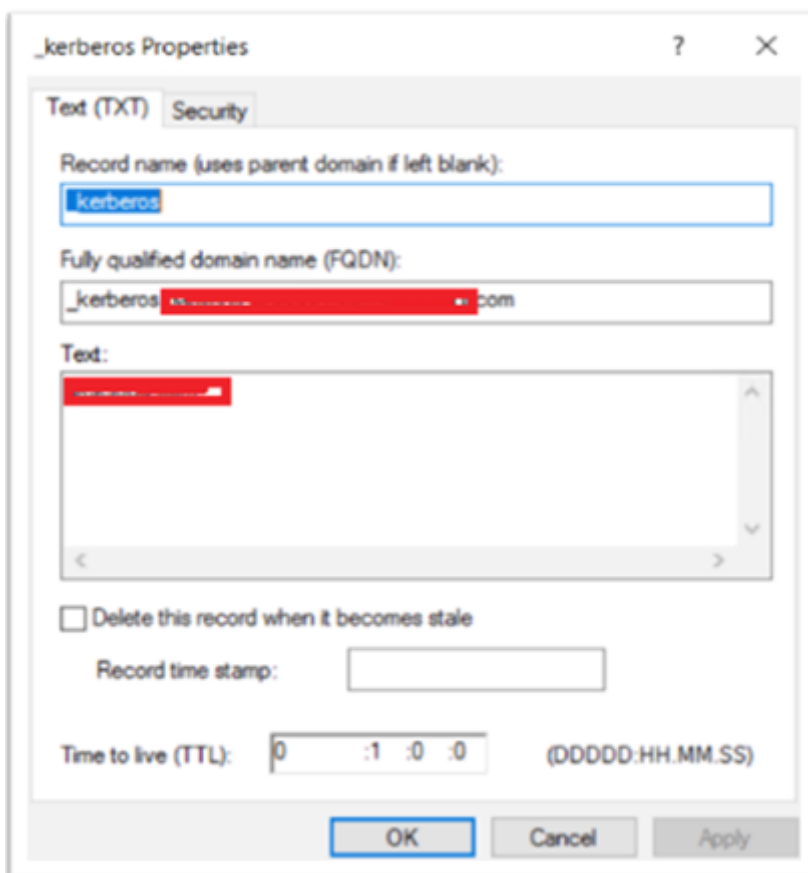
3. Erstellen Sie einen DNS-Eintrag für den Client, um den SPN des Gateways zu finden:

Fügen Sie einen TXT-DNS-Eintrag in Active Directory hinzu.

**Hinweis:**

Der Name muss mit “\_Kerberos” beginnen, die Daten müssen der Domainname sein. Als

FQDN muss Kerberos angezeigt werden..



Ein mit einer Windows-Domäne verbundener Client verwendet `_kerberos.fqdn`, um Tickets anzufordern. Wenn der Client beispielsweise mit `citrite.net` verbunden ist, kann das Betriebssystem Tickets für alle Websites mit `*.citrite.net` erhalten. Bei externen Gateway-Domänen (z. B. `gateway.citrix.com`) kann das Clientbetriebssystem das Kerberos-Ticket jedoch nicht erhalten.

Daher müssen Sie einen DNS TXT-Eintrag erstellen, anhand dessen der Client nach `_kerberos.gateway.citrix.com` suchen und das Kerberos-Ticket für die Authentifizierung abrufen kann.

4. Konfigurieren Sie Kerberos als Authentifizierungsfaktor.
  - a) Erstellen Sie ein KCD-Konto für den NetScaler-Benutzer. Im vorliegenden Beispiel erfolgt dies manuell, Sie können aber auch eine Keytab-Datei erstellen.

**Hinweis:**

Wenn Sie alternative Domänen (interne und externe Domäne) verwenden, müssen Sie den Dienst-SPN auf `HTTP/PublicFQDN.com@InternalDomain.ext`

festlegen.

- **Realm** - Kerberos-Bereich. Normalerweise das Suffix der internen Domäne.
- **User Realm:** Dies ist das interne Domänensuffix des Benutzers.
- **Enterprise Realm:** Dies muss nur in bestimmten KDC-Bereitstellungen angegeben werden, in denen KDC den Enterprise-Benutzernamen anstelle des Prinzipalnamens erwartet.
- **Delegated User:** NetScaler-Benutzerkonto für KCD, das Sie zuvor in AD erstellt haben. Stellen Sie sicher, dass das Kennwort korrekt ist.

← | Configure KCD Account

Name  
kcduser

Use Keytab File

Realm\*  
READINESS.LAB

User Realm  
[Empty]

Enterprise Realm  
[Empty]

Service SPN  
[Empty]

User Certificate  
Choose File [Empty]

CA Certificate  
Choose File [Empty]

Delegated User  
kcduser

Password for Delegated User

- b) Stellen Sie sicher, dass das Sitzungsprofil das richtige KCD-Konto verwendet. Binden Sie die Sitzungsrichtlinie an den virtuellen Authentifizierungs-, Autorisierungs- und Auditingserver.

← | Configure Session Profile

Name  
mysso

Unchecked Override Global check box indicates that the value is inherited from Global Session Parameters.

	Override Global
Session Time-out (mins) 10 ?	<input checked="" type="checkbox"/>
Default Authorization Action* ALLOW	<input checked="" type="checkbox"/>
Single Sign-on to Web Applications* ON	<input checked="" type="checkbox"/>
Credential Index* PRIMARY	<input checked="" type="checkbox"/>
Single Sign-on Domain readiness	<input checked="" type="checkbox"/>
HTTPOnly Cookie* YES	<input type="checkbox"/>
Enable Persistent Cookie* OFF	<input type="checkbox"/>
Persistent Cookie Validity	<input type="checkbox"/>
KCD Account kcduser	<input checked="" type="checkbox"/>
Home Page	<input type="checkbox"/>

- c) Binden Sie die Authentifizierungsrichtlinie an den virtuellen Authentifizierungs-, Autorisierungs- und Auditingserver. Bei den Authentifizierungs-, Autorisierungs- und Auditmethoden dieser Richtlinien wird kein Kennwort vom Client abgerufen, weshalb KCD verwendet werden muss. Es müssen allerdings weiterhin der und die Domäneninformationen im UPN-Format abgerufen werden.



**Hinweis:**

Sie können die IP-Adresse oder den EPA-Scan verwenden, um domänengebundene und nicht domänengebundene Geräte zu unterscheiden und Kerberos oder reguläres LDAP als Authentifizierungsfaktor zu verwenden.

**Konfigurieren des Clients**

Gehen Sie wie folgt vor, um Single Sign-On beim VDA zu ermöglichen.

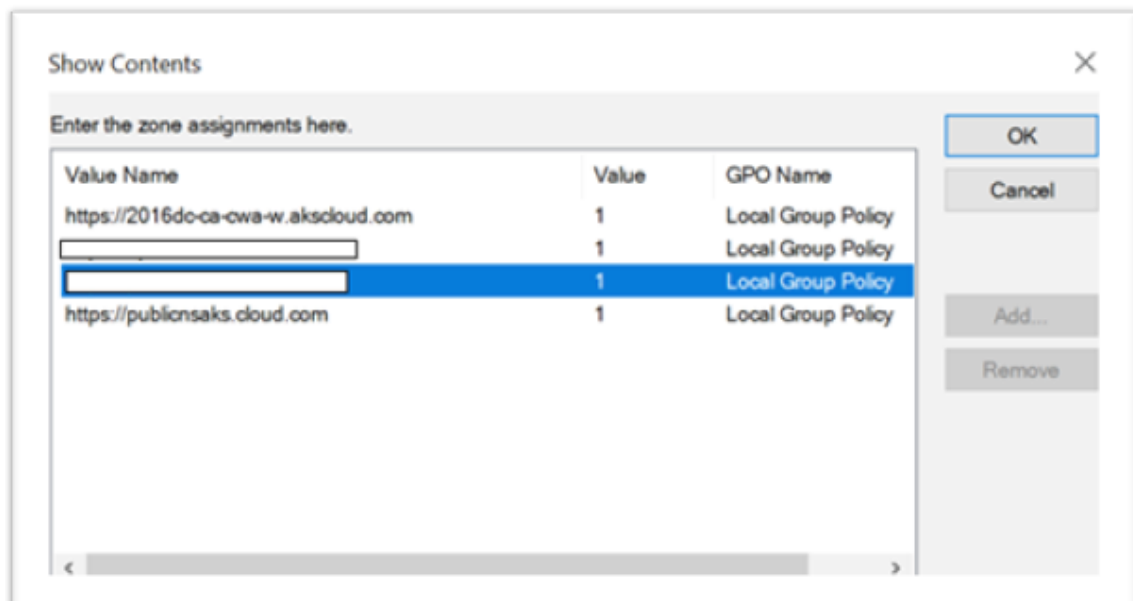
**Voraussetzungen:**

- Domänengebundene Maschine
- Citrix Workspace 2112.1 oder höher mit aktiviertem SSO
- Vertrauen erforderlicher URLs (Prüfung, ob die Verbindungen geschützt sind)
- Validieren Sie Kerberos von Client und AD. Das Clientbetriebssystem muss mit AD verbunden sein, um Kerberos-Tickets abzurufen.

Nachfolgenden sind einige der URLs aufgeführt, denen im Browser vertraut werden muss:

- Gateway-URL oder -FQDN
- AD-FQDN
- Workspace-URL für SSO aus browserbasierten Starts.

1. Wenn Sie Internet Explorer, Microsoft Edge oder Google Chrome verwenden, gehen Sie wie folgt vor:
  - a) Starten Sie den Browser.
  - b) Öffnen Sie den Editor für lokale Gruppenrichtlinien auf dem Client.



- a) Gehen Sie zu **Computerkonfiguration > Windows-Komponente > Internet Explorer > Internetsystemsteuerung > Sicherheit**.
  - b) Öffnen Sie die Liste der Site-zu-Zonen-Zuweisungen und fügen Sie alle aufgelisteten URLs mit dem Wert eins (1) hinzu.
  - c) (Optional) Führen Sie `Gpupdate` aus, um Richtlinien anzuwenden.
2. Wenn Sie Mozilla Firefox verwenden, gehen Sie wie folgt vor:
- a) Öffnen Sie den Browser.
  - b) Geben Sie `about:config` in die Suchleiste ein.
  - c) Akzeptieren Sie das Risiko und fahren Sie fort.
  - d) Geben Sie in das Suchfeld **negotiate** ein.
  - e) Überprüfen Sie in der Liste der angezeigten Daten, ob **network.negotiate-auth.trusted-uris** auf den Domänenwert festgelegt ist.



Damit ist die Konfiguration auf der Clientseite abgeschlossen.

3. Melden Sie sich mit der Citrix Workspace-App oder dem Browser bei Workspace an.

Dabei darf keine Eingabe eines Benutzernamens oder Kennworts auf einem mit der Domäne verbundenen Gerät angefordert werden.

## Problembehandlung bei Kerberos

### Hinweis:

Sie müssen Domänenadministrator sein, um diesen Überprüfungsschritt ausführen zu können.

Führen Sie an der Eingabeaufforderung oder in Windows PowerShell den folgenden Befehl aus, um die Kerberos-Ticketüberprüfung für den SPN-Benutzer zu überprüfen:

```
KLIST get host/FQDN of AD
```

## Domänen-Passthrough-Authentifizierung an Citrix Workspace mit Azure Active Directory als Identitätsanbieter

April 22, 2024

Sie können Single Sign-On (SSO) bei Citrix Workspace mithilfe von Azure Active Directory (AAD) als Identitätsanbieter mit domänenverbundenen, Hybrid- und Azure AD-registrierten Endpunkten/VMs implementieren.

Mit dieser Konfiguration können Sie auch Windows Hello für SSO bei Citrix Workspace mit bei AAD-registrierten Endpunkten verwenden.

- Sie können sich mit Windows Hello bei der Citrix Workspace-App authentifizieren.
- FIDO2-basierte Authentifizierung bei der Citrix Workspace-App.
- Single Sign-On bei der Citrix Workspace-App von Microsoft AAD-verbundenen Maschinen (AAD = IdP) und bedingter Zugriff mit AAD.

Um SSO für virtuelle Apps und Desktops zu erreichen, können Sie entweder FAS bereitstellen oder die Citrix Workspace-App wie folgt konfigurieren.

### Hinweis:

SSO bei den Citrix Workspace-Ressourcen ist nur mit Windows Hello möglich. Sie werden jedoch aufgefordert, einen Benutzernamen und ein Kennwort einzugeben, wenn Sie auf Ihre veröffentlichten virtuellen Apps und Desktops zugreifen. Um diese Aufforderung zu lösen, können Sie FAS und SSO für virtuelle Apps und Desktops bereitstellen.

### Voraussetzungen:

1. Verbinden Sie Azure Active Directory mit Citrix Cloud. Weitere Informationen finden Sie unter [Verbinden von Azure Active Directory mit Citrix Cloud](#) in der Citrix Cloud-Dokumentation.

2. Aktivieren Sie Azure AD-Authentifizierung für den Zugriff auf Workspace. Weitere Informationen finden Sie unter [Aktivieren der Azure AD-Authentifizierung für Workspaces](#) in der Citrix Cloud-Dokumentation.

Gehen Sie für Single Sign-On bei Citrix Workspace folgendermaßen vor:

1. Konfigurieren Sie die Citrix Workspace-App mit includeSSON.
2. Deaktivieren Sie das Attribut `prompt=login` in Citrix Cloud.
3. Konfigurieren Sie die Azure Active Directory-Passthrough-Authentifizierung mit Azure Active Directory Connect.

## Konfigurieren der Citrix Workspace-App für die Unterstützung von SSO

### Voraussetzungen:

- Citrix Workspace Version 2109 oder höher.

#### Hinweis:

Wenn Sie FAS für SSO verwenden, ist die Konfiguration von Citrix Workspace nicht erforderlich.

1. Installieren Sie die Citrix Workspace-App über die Verwaltungsbefehlszeile mit der Option `includeSSON`:

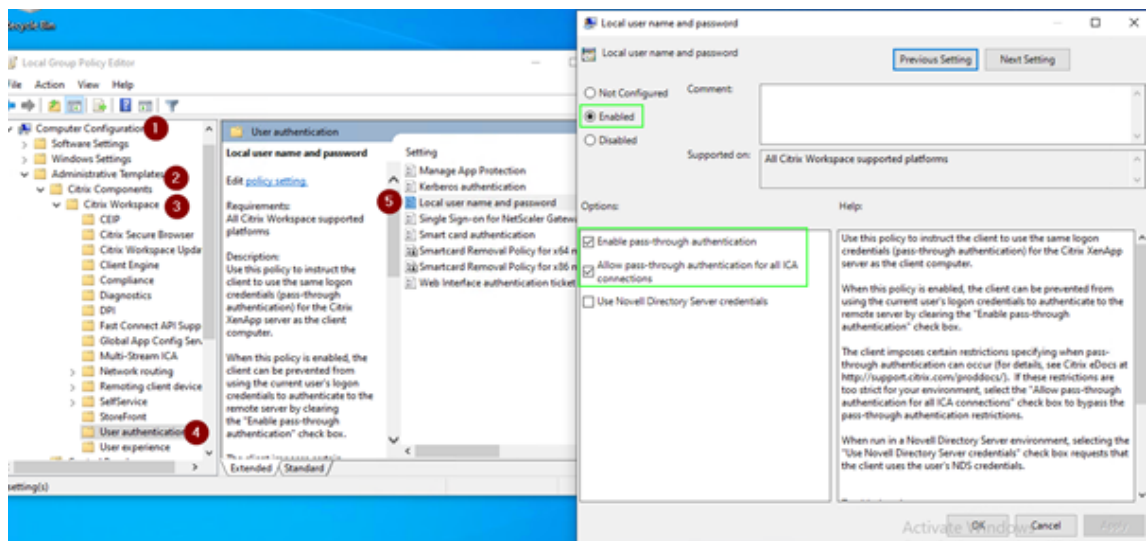
```
CitrixWorkspaceApp.exe /includeSSON
```

2. Melden Sie sich vom Windows-Client ab und melden Sie sich an, um den SSON-Server zu starten.
3. Klicken Sie auf **Computerkonfiguration** > **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung**, um das Citrix Workspace-Gruppenrichtlinienobjekt so zu ändern, dass **Lokaler Benutzername und Kennwort** zugelassen ist.

#### Hinweis:

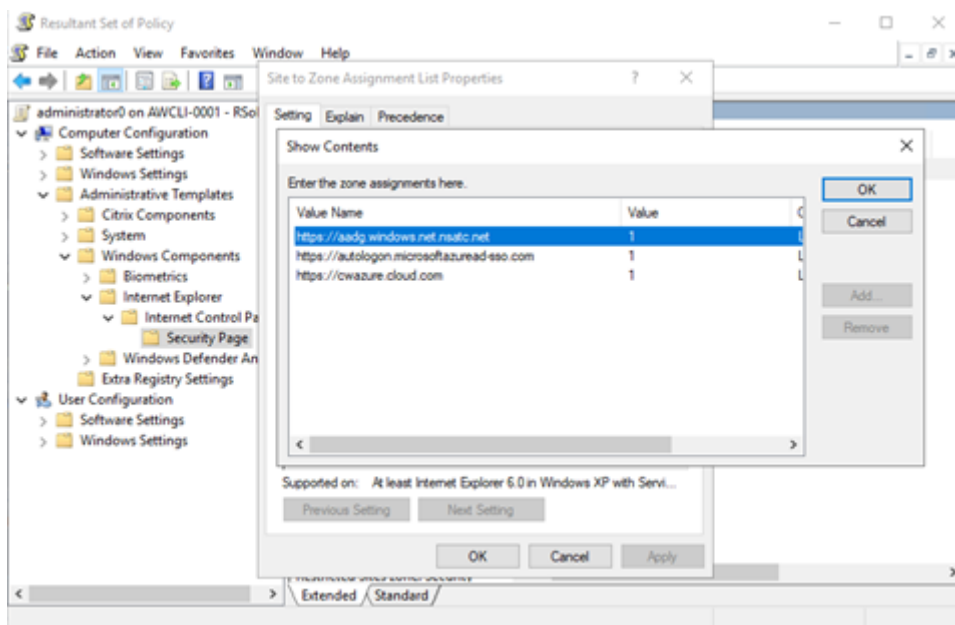
Diese Richtlinien können über Active Directory auf das Clientgerät übertragen werden. Dieser Schritt ist nur erforderlich, wenn Sie über den Webbrowser auf Citrix Workspace zugreifen.

4. Aktivieren Sie die Einstellung gemäß dem Screenshot.



5. Fügen Sie die folgenden vertrauenswürdigen Websites über das GPO hinzu:

- <https://aadg.windows.net.nsatc.net>
- <https://autologon.microsoftazuread-ss0.com>
- <https://xxxtenantxxx.cloud.com>: Workspace-URL



**Hinweis:**

Single Sign-On für AAD ist deaktiviert, wenn die Registrierung **AllowSSOForEdgeWebview-** in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` auf "false" gesetzt ist.

## Deaktivieren des Parameters “prompt=login” in Citrix Cloud

Standardmäßig ist `prompt=login` für Citrix Workspace aktiviert, wodurch die Authentifizierung erzwungen wird, selbst wenn der Benutzer **angemeldet bleibt** oder das Gerät mit Azure AD verbunden ist.

Sie können `prompt=login` in Ihrem Citrix Cloud-Konto deaktivieren. Gehen Sie zu [Workspace Configuration\Customize\Preferences-Federated Identity Provider Sessions](#) und deaktivieren Sie die Umschaltfläche.

Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX253779](#).

The screenshot shows the Citrix Cloud management interface. At the top, there is a navigation bar with the Citrix logo and a hamburger menu. Below it, a breadcrumb trail shows 'Home > Workspace Configuration' with a red circle '1' next to 'Workspace Configuration'. The main heading is 'Workspace Configuration'. Below the heading, there are several tabs: 'Access', 'Authentication' (with a red circle '2'), 'Customize' (highlighted with a red box), 'Service Integrations', 'Sites', 'Service Continuity', and 'App Configuration'. Under the 'Customize' tab, there are three sub-sections: 'Appearance', 'Features' (with a red circle '3'), and 'Preferences' (highlighted with a red box). Below the 'Preferences' section, there is a heading 'Workspace Sessions' and a sub-heading 'Federated Identity Provider Sessions'. Under this sub-heading, there is a toggle switch labeled 'Disabled' (with a red circle '4') and a red 'X' icon. Below the toggle switch, there is a paragraph of text explaining the configuration.

### Hinweis:

Wenn AAD auf Geräten, die mit AAD oder hybriden AAD verbundenen sind, als IdP für Workspace verwendet wird, fordert die Citrix Workspace-App nicht zur Eingabe von Anmeldeinformationen auf. Benutzer können sich automatisch mit einem Arbeits- oder Schulkonto anmelden.

Um Benutzern die Anmeldung mit einem anderen Konto zu ermöglichen, legen Sie die folgende Registrierung auf “false” fest.

Erstellen und fügen Sie eine Registrierungszeichenfolge REG\_SZ mit dem Namen **AllowSSO-ForEdgeWebview** unter `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` oder `Computer\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle` hinzu und legen Sie den Wert auf “False” fest. Wenn sich Benutzer von der Citrix Workspace-App abmelden, können sie sich bei der nächsten Anmeldung auch mit einem anderen Konto anmelden.

## Konfigurieren der Azure Active Directory-Passthrough-Authentifizierung mit Azure Active Directory Connect

- Wenn Sie Azure Active Directory Connect zum ersten Mal installieren, wählen Sie auf der Seite **Benutzeranmeldung** als Anmeldemethode **Passthrough-Authentifizierung**. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter [Azure Active Directory-Passthrough-Authentifizierung: Schnellstart](#).
- Wenn Microsoft Azure Active Directory Connect vorhanden ist:
  1. Wählen Sie den Task **Benutzeranmeldung ändern** und klicken Sie auf **Weiter**.
  2. Wählen Sie **Passthrough-Authentifizierung** als Anmeldemethode aus.

### Hinweis:

Sie können diesen Schritt überspringen, wenn das Clientgerät mit Azure AD verbunden oder mit einer Hybrideinbindung konfiguriert ist. Wenn das Gerät mit AD verbunden ist, wird für die Domänen-Passthrough-Authentifizierung die Kerberos-Authentifizierung verwendet.

## Domänen-Passthrough-Authentifizierung an Citrix Workspace mit Okta als Identitätsanbieter

April 22, 2024

Sie können Single Sign-On bei Citrix Workspace unter Einsatz von Okta als Identitätsanbieter (IdP) implementieren.

### Voraussetzungen:

- Citrix Cloud
  - Cloud Connectors

### Hinweis:

Wenn Sie neu bei Citrix Cloud sind, definieren Sie einen Ressourcenstandort und sorgen Sie dafür, dass die Connectors konfiguriert sind. Es wird empfohlen, mindestens zwei Cloud Connectors in Produktionsumgebungen bereitzustellen. Weitere Informationen zur Installation von Citrix Cloud Connectors finden Sie unter [Cloud Connector-Installation](#).

- Citrix Workspace
- Verbundauthentifizierungsdienst (optional). Weitere Informationen finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst](#).

erst (FAS).

- Citrix DaaS (früher Citrix Virtual Apps and Desktops Service)
- VDA mit AD-Domänenbindung oder mit physischem AD verbundene Geräte
- Okta-Mandant
  - Okta IWA Agent (Integrierte Windows-Authentifizierung)
  - Okta Verify (optional, Okta Verify kann vom App Store heruntergeladen werden)
- Active Directory

1. Bereitstellen des Okta AD Agent:

- a) Klicken Sie im Okta Admin-Portal auf **Directory > Directory Integrations**.
- b) Klicken Sie auf **Add Directory > Add Active Directory**.
- c) Informieren Sie sich über die Installationsanforderungen, indem Sie dem Workflow folgen, der die Agentarchitektur und die Installationsanforderungen abdeckt.
- d) Klicken Sie auf die Schaltfläche **Set Up Active Directory** und dann auf **Download Agent**.
- e) Installieren Sie den Okta AD Agent auf einem Windows-Server, indem Sie den Anweisungen unter [Install the Okta Active Directory agent](#) folgen.

**Hinweis:**

Stellen Sie sicher, dass die unter [Active Directory integration prerequisites](#) aufgeführten Anforderungen erfüllt werden, bevor Sie den Agent installieren.

2. Richten Sie die integrierte Windows-Authentifizierung (IWA) ein:

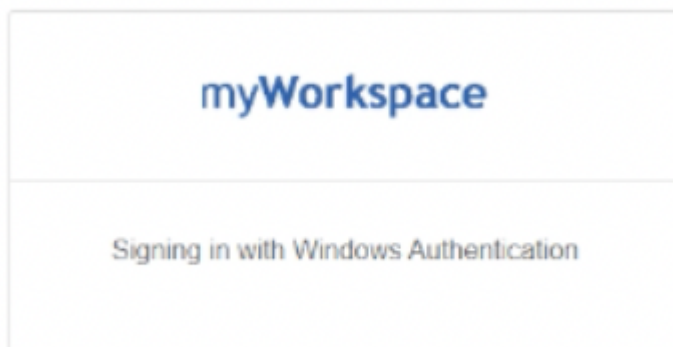
- a) Klicken Sie im Okta Admin-Portal auf **Security** und dann auf **Delegated Authentication**.
- b) Scrollen Sie auf der nun angezeigten Seite nach unten zum Teil **On-prem Desktop SSO** und klicken Sie auf **Download Agent**.
- c) Richten Sie die **Routingregeln** für IWA ein. Weitere Informationen finden Sie unter [Configure Identity Provider routing rules](#).

3. Starten Sie das Okta-Kundenportal.

**Hinweis:**

- Wenn Okta IWA Agent installiert und aktiviert ist, können Sie sich von einem Gerät in der Windows-Domäne aus anmelden. Diese Konfiguration überspringt auch die Anmeldung, leitet Sie zur IWA-Anmeldeseite weiter und übergibt die Benutzeranmeldedaten.





- Weitere Informationen zur Problembehandlung finden Sie unter [Install and configure the Okta IWA Web agent for Desktop single sign-on](#).

4. Melden Sie sich auf <https://citrix.cloud.com> bei Citrix Cloud an und aktivieren Sie Okta als IdP. Weitere Informationen finden Sie in der Citrix Tech Zone-Dokumentation unter [Tech Insight: Authentication - Okta](#).

**Hinweis:**

Sie können sich über die Citrix Workspace-App oder den Browser anmelden. Beide bieten die Passthrough-Erfahrung gemäß Tech Zone-Dokumentation.

5. Um SSO für virtuelle Apps und Desktops zu erreichen, können Sie entweder FAS bereitstellen oder die Citrix Workspace-App konfigurieren.

**Hinweis:**

Ohne FAS werden Sie aufgefordert, den AD-Benutzernamen und das Kennwort einzugeben. Weitere Informationen finden Sie unter [Aktivieren von Single Sign-On für Workspaces mit dem Citrix Verbundauthentifizierungsdienst \(FAS\)](#).

Wenn Sie FAS nicht verwenden, [konfigurieren Sie die Citrix Workspace-App für die Unterstützung von SSO](#).

## HDX

April 22, 2024

In diesem Abschnitt wird Folgendes beschrieben:

- [Grafik und Display](#)
- [Optimierung für Microsoft Teams](#)
- [HDX-Transport](#)

- [Browserinhaltsumleitung](#)
- [Bidirektionale Inhaltsumleitung](#)
- [Referenz für ICA-Einstellungen](#)

## Grafik und Display

April 22, 2024

### Multimonitorunterstützung

Sie können maximal acht Monitore mit der Citrix Workspace-App für Windows verwenden.

Jeder Monitor in einer Multimonitorumgebung hat eine eigene, vom Hersteller festgelegte Auflösung. Monitore können in Sitzungen verschiedene Auflösungen und Ausrichtungen haben.

Sitzungen können auf zwei Arten auf mehrere Monitore übergreifend ausgeführt werden:

- Vollbildmodus: Mehrere Monitore werden in der Sitzung angezeigt; Anwendungen werden genauso wie beim lokalen Desktop an Monitore angedockt.

**Citrix Virtual Apps and Desktops und Citrix DaaS:** Sie können das Desktop Viewer-Fenster über eine beliebige rechteckige Untergruppe von Monitoren ausdehnen, wenn Sie die Größe des Fensters über einen Monitorbereich hinweg ändern und auf **Maximieren** klicken.

- Im Fenstermodus mit nur einem Monitorbild für die Sitzung werden Anwendungen nicht an einzelne Monitore angedockt.

**Citrix Virtual Apps and Desktops und Citrix DaaS:** Wenn ein Desktop in derselben Zuordnung (früher Desktopgruppe) dann gestartet wird, wird die Fenstereinstellung gespeichert, und der Desktop wird auf denselben Monitoren angezeigt. Mehrere virtuelle Desktops können auf einem Gerät angezeigt werden, wenn die Monitoranordnung rechteckig ist. Wenn der primäre Monitor auf dem Gerät von der Sitzung mit virtuellen Apps und Desktops verwendet wird, wird er zum primären Monitor in der Sitzung. Sonst wird der zahlenmäßig niedrigste Monitor in der Sitzung zum primären Monitor.

Für die Multimonitorunterstützung müssen Sie Folgendes sicherstellen:

- Das Benutzergerät ist für die Unterstützung von mehreren Monitoren konfiguriert.
- Das Betriebssystem kann jeden Monitor erkennen. Um auf Windows-Plattformen zu überprüfen, ob diese Erkennung erfolgt, gehen Sie zu **Einstellungen > System**, klicken Sie auf **Anzeige** und bestätigen Sie, dass jeder Monitor separat angezeigt wird.
- Nach dem Erkennen der Monitore:

- **Citrix Virtual Desktops:** Konfigurieren Sie das Grafikspeicherlimit mit der Citrix Maschinenrichtlinieneinstellung **Anzeigespeicherlimit**.
- **Citrix Virtual Apps:** Je nach installierter Citrix Virtual Apps-Serverversion:
  - \* Konfigurieren Sie das Limit für den Grafikspeicher mit der Citrix Computerrichtlinieneinstellung **Anzeigespeicherlimit**.
  - \* Wählen Sie die Farm in der Citrix Verwaltungskonsole für den Citrix Virtual Apps-Server aus und wählen Sie im Aufgabenbereich Folgendes:
    - **Servereigenschaften ändern > Alle Eigenschaften ändern > Serverstandard > HDX Broadcast > Anzeige** oder
    - **Servereigenschaften ändern > Alle Eigenschaften ändern > Serverstandard > ICA > Anzeige**.
  - \* Legen Sie dann den maximalen Grafikspeicher pro Sitzung fest.

Prüfen Sie, ob die Einstellung (in Kilobyte) hoch genug ist, damit ausreichend Grafikspeicher bereitgestellt wird. Ist der Wert zu niedrig, wird die veröffentlichte Ressource auf einen Teilbereich der Monitore beschränkt, der in die angegebene Größe passt.

#### **Verwenden von Citrix Virtual Desktops auf zwei Monitoren:**

1. Wählen Sie den Desktop Viewer aus und klicken Sie auf den Pfeil nach unten.
2. Wählen Sie **Fenster**.
3. Ziehen Sie den Bildschirm von Citrix Virtual Desktops zwischen die beiden Monitore. Stellen Sie sicher, dass etwa die Hälfte des Bildschirms in jedem Monitor angezeigt wird.
4. Wählen Sie auf der Symbolleiste des Citrix Virtual Desktops die Option **Vollbild** aus.

Der Bildschirm ist nun auf beide Monitore erweitert.

Informationen zum Berechnen der Größe des Grafikspeichers in Sitzungen für Citrix Virtual Apps and Desktops und Citrix DaaS finden Sie im Knowledge Center-Artikel [CTX115637](#).

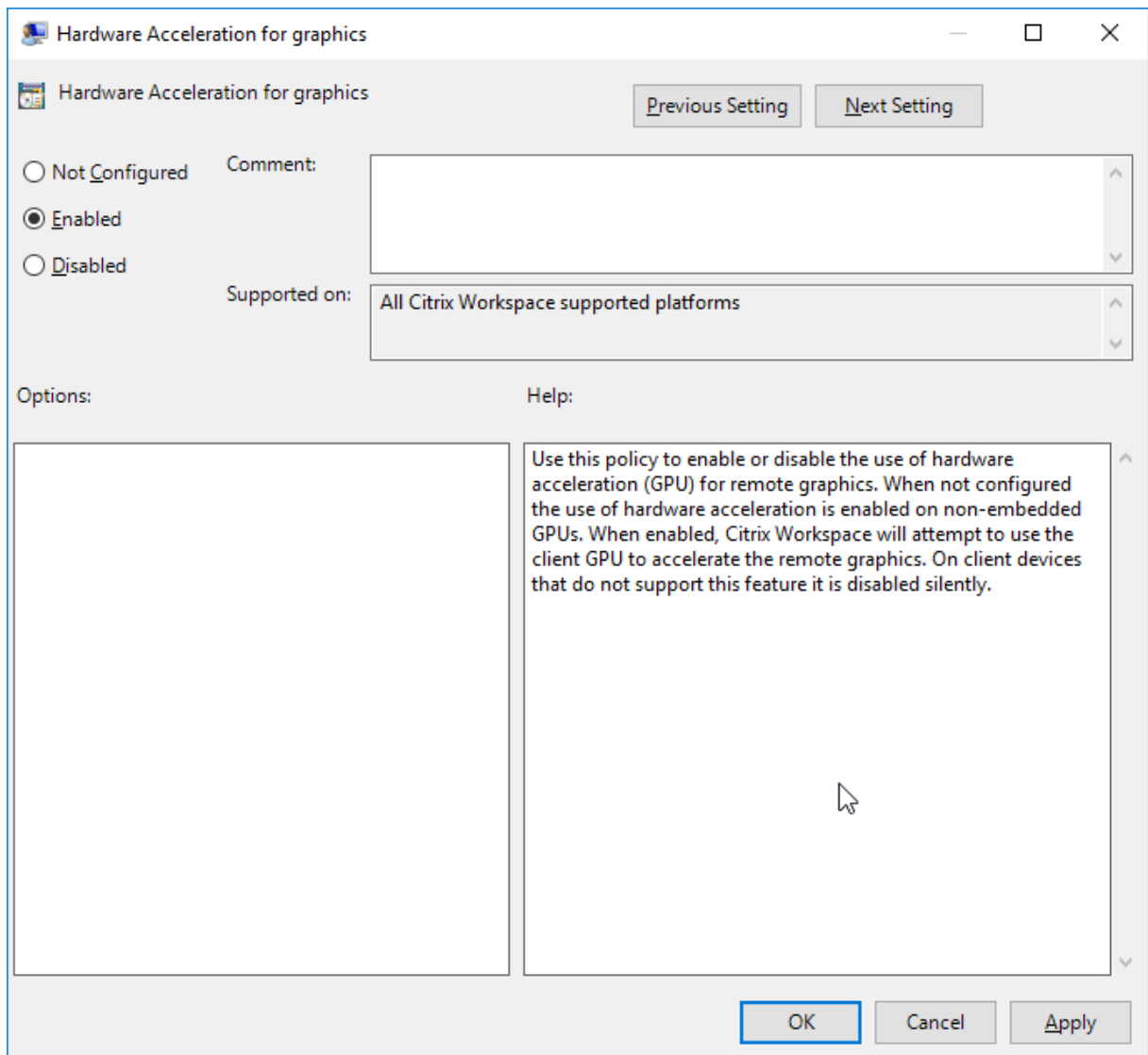
#### **Hardwaredecodierung**

Wenn Sie die Citrix Workspace-App (mit HDX Engine 14.4) verwenden, kann die GPU für H.264-Decodierung verwendet werden, wenn sie auf dem Client verfügbar ist. Die für GPU-Decodierung verwendete API-Ebene ist DirectX Video Acceleration.

#### **Aktivieren der Hardwaredecodierung mit der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App:**

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.

2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie **Hardwarebeschleunigung für Grafiken**.
4. Wählen Sie **Aktiviert** und klicken Sie auf **Übernehmen** und anschließend auf **OK**.



Anhand der folgenden Registrierungseinträge prüfen Sie, ob die Richtlinie eingerichtet ist und die Hardwarebeschleunigung in einer aktiven ICA-Sitzung verwendet wird:

Registrierungspfad: `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`.

#### Tipp

Der Wert für **Graphics\_GfxRender\_Decoder** und **Graphics\_GfxRender\_Renderer** muss 2 sein. Wenn der Wert 1 ist, wird auf der CPU basierende Decodierung verwendet.

Wenn Sie das Hardwaredecodierungsfeature verwenden, berücksichtigen Sie folgende Einschränkungen:

- Wenn der Client zwei GPUs hat und wenn einer der Bildschirme auf der zweiten GPU aktiv ist, wird CPU-Decodierung verwendet.
- Verwenden Sie keine Hardwaredecodierung auf dem Windows-Gerät des Benutzers, wenn Sie eine Verbindung mit einem Citrix Virtual Apps-Server herstellen, der unter Windows Server 2008 R2 ausgeführt wird. Ist die Hardwaredecodierung aktiviert, treten Probleme auf, wie geringe Leistung beim Markieren von Text und Flackern.

## Virtuelles Anzeigelayout

Mit diesem Feature definieren Sie ein virtuelles Bildschirmlayout für den Remotedesktop. Außerdem können Sie einen einzelnen Clientmonitor virtuell in bis zu acht Bildschirme auf dem Remotedesktop aufteilen. Sie können die virtuellen Bildschirme auf der Registerkarte **Bildschirmlayout** im Desktop Viewer konfigurieren. Dort können Sie horizontale oder vertikale Linien ziehen, um den Bildschirm in virtuelle Bildschirme zu unterteilen. Der Bildschirm wird entsprechend den angegebenen Prozentsätzen der Auflösung des Clientbildschirms aufgeteilt.

Sie können für die virtuellen Bildschirme eine DPI festlegen, die für die DPI-Skalierung bzw. DPI-Anpassung verwendet wird. Ändern Sie nach dem Anwenden eines virtuellen Bildschirmlayouts die Größe der Sitzung oder stellen Sie erneut eine Verbindung her.

Die Konfiguration gilt nur für Desktopsitzungen mit einem Bildschirm im Vollbildmodus. Sie hat keine Auswirkungen auf veröffentlichte Anwendungen. Diese Konfiguration gilt für alle nachfolgenden Verbindungen von diesem Client.

Ab Citrix Workspace-App für Windows 2106 wird das virtuelle Anzeigelayout auch für Desktopsitzungen mit mehreren Bildschirmen im Vollbildmodus unterstützt. Das virtuelle Anzeigelayout ist standardmäßig aktiviert. In einem Szenario mit mehreren Bildschirmen wird das gleiche virtuelle Anzeigelayout auf alle Sitzungsmonitore angewendet, sofern nicht mehr als acht virtuelle Anzeigen vorhanden sind. Wird dieses Limit überschritten, wird das virtuelle Anzeigelayout ignoriert und auf keinen Sitzungsbildschirm angewendet.

Die Verbesserung für die Multimonitoranzeige kann durch Festlegen des folgenden Registrierungsschlüssels deaktiviert werden:

- `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`

Name: **SplitAllMonitors**

Typ: DWORD

Werte:

1 - Aktiviert

0 - Deaktiviert

## **DPI-Skalierung**

Die Citrix Workspace-App ist DPI-fähig und unterstützt die Anpassung der Bildschirmauflösung und der DPI-Skalierungseinstellungen auf dem Windows-Client an die Sitzung mit virtuellen Apps und Desktops.

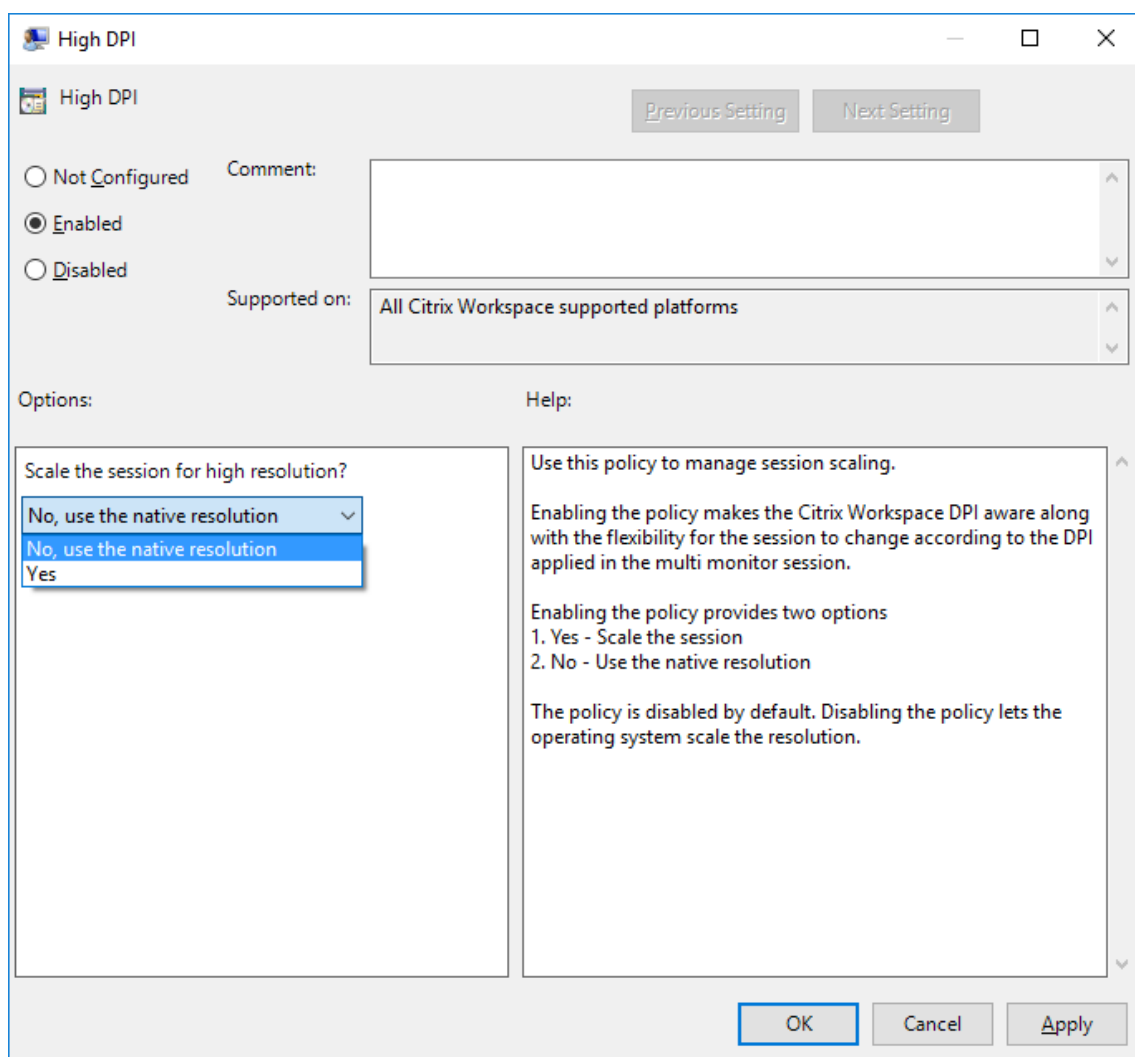
Die DPI-Skalierung wird hauptsächlich mit großen und hochauflösenden Monitoren verwendet, um Anwendungen, Text, Bilder und andere grafische Elemente in einer Größe anzuzeigen, die bequem angezeigt werden kann.

Dieses Feature ist standardmäßig aktiviert und wird für alle Anwendungsfälle empfohlen. Administratoren können die DPI-Skalierung jedoch bei Bedarf weiterhin mithilfe der administrativen GPO-Vorlage (Konfiguration pro Maschine) konfigurieren.

DPI-Skalierung mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren:

### **DPI-Skalierung mit der administrativen Gruppenrichtlinienobjektvorlage konfigurieren:**

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > DPI**
3. Wählen Sie die Richtlinie **Hoher DPI-Wert** aus.



4. Wählen Sie eine der folgenden Optionen:
  - a) Ja - Gibt an, dass ein hoher DPI-Wert in einer Sitzung angewendet wird.
  - b) Nein, native Auflösung verwenden - Gibt an, dass die Auflösung vom Betriebssystem festgelegt wird.
5. Klicken Sie auf **Anwenden** und auf **OK**.
6. Führen Sie an der Befehlszeile den Befehl `gpupdate /force` aus, um die Änderungen anzuwenden.

#### Konfiguration von DPI-Skalierung über die grafische Benutzeroberfläche:

1. Klicken Sie mit der rechten Maustaste im Infobereich auf das Citrix Workspace-App-Symbol.
2. Wählen Sie **Erweiterte Einstellungen** und klicken Sie auf **Hoher DPI-Wert**.
3. Wählen Sie eine der folgenden Optionen:
  - a) **Ja** - Gibt an, dass ein hoher DPI-Wert in einer Sitzung angewendet wird.

- b) **Nein, native Auflösung verwenden** - Gibt an, dass die Citrix Workspace-App den DPI-Wert auf dem VDA erkennt und ihn anwendet.
  - c) **Betriebssystem die Auflösung skalieren lassen** – Standardmäßig ist diese Option ausgewählt. Damit kann Windows die DPI-Skalierung verarbeiten. Diese Option bedeutet auch, dass die Richtlinie “Hoher DPI-Wert” deaktiviert ist.
4. Klicken Sie auf **Speichern**.
  5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

#### HINWEIS:

##### Zusätzliche Hinweise:

- Für den DPI-Abgleich ist Citrix Virtual Apps and Desktops Version 1912 LTSR oder höher erforderlich.
- Die Einstellung **Nein, native Auflösung verwenden** (DPI-Abgleich) wird in den meisten Fällen empfohlen.
- Die Standardeinstellung **Betriebssystem die Auflösung skalieren lassen** deaktiviert die DPI-Erkennung in der Citrix Workspace-App. Dieser Modus kann zu verschwommenen Grafiken führen, wenn die DPI-Skalierung des Windows-Clients auf etwas anderes als 100% eingestellt ist. Dieser Modus unterstützt nicht mehrere Monitore mit unterschiedlichen DPI-Skalierungen.
- Die Option **Ja** führt dazu, dass die Citrix Workspace-App das Sitzungsfenster hochskaliert, sodass es der auf dem Windows-Client konfigurierten DPI-Skalierung entspricht. Dies ist eine Legacy-Funktion, die nur für Verbindungen zu älteren XenApp- und XenDesktop-Umgebungen empfohlen wird, wenn auf dem Client DPI-Skalierungen über 100% erforderlich sind. Dieser Modus kann zu verschwommenen Grafiken führen.

Informationen zur Behandlung von Problemen im Zusammenhang mit der DPI-Skalierung finden Sie im Knowledge Center-Artikel [CTX230017](#).

### Automatische Auswahl des Videocodecs

Die Citrix Workspace-App für Windows erkennt jetzt automatisch den am besten zu verwendenen Videocodec. Während der Installation der Citrix Workspace-App für Windows werden die Decodierungsfunktionen des Endpunkts evaluiert. Basierend auf diesen Informationen wählt die Citrix Workspace-App für Windows beim Start der Sitzung den besten Codec für die Verwendung mit dem VDA aus. Die Videocodecs werden in der folgenden Reihenfolge ausgewertet:

1. AV1
2. H.265
3. H.264



Diese Funktion ist verfügbar, wenn die Richtlinie **Videocodec zur Komprimierung verwenden** auf eine der folgenden Einstellungen gesetzt ist:

- **Verwenden, wenn bevorzugt**
- **Für den gesamten Bildschirm**
- **Für aktive Änderungsbereiche**

Weitere Informationen zur Richtlinie **Videocodec zur Komprimierung verwenden** finden Sie unter [Videocodec zur Komprimierung verwenden](#).

Die automatische Auswahl gilt nur für YUV 4:2:0 -Varianten dieser Codecs. YUV 4:2:0 verwendet weniger Bandbreite und beeinträchtigt die Qualität. Wenn die Richtlinieneinstellung **Bildqualität** auf **Zu verlustfrei verbessern** oder **Immer verlustfrei** gesetzt ist und wenn die Richtlinie **Visuell verlustfreie Komprimierung zulassen** auf **aktiviert** gesetzt ist, wird die automatische Auswahl des Videocodecs deaktiviert und stattdessen YUV 4:4:4 H.264 oder H.265 verwendet.

Weitere Informationen zu diesen Richtlinien finden Sie unter:

- [Bildqualität](#)
- [Visuell verlustfreie Komprimierung zulassen](#)

**Hinweis:**

YUV 4:2:0 ist ein Chroma-Subsampling und eine Farbkomprimierungstechnik, die den Gesamtbandbreitenverbrauch senkt.

Beim Herstellen einer Verbindung zu einer Ressource testet die Citrix Workspace-App die Fähigkeit des Endpunkts, H.265 und AV1 zu dekodieren und die Funktionen in der Registrierung zu speichern. Danach wählt die Citrix Workspace-App automatisch den besten zu verwendenden Videocodec aus und handelt diesen Codec mit dem VDA aus. Wenn sowohl der VDA als auch der Client H.265 und AV1 verwenden können, wird AV1 als Videocodec ausgewählt. Wenn AV1 weder auf dem VDA noch auf dem Client verfügbar ist, wird H.265 ausgewählt. Wenn H.265 auch auf keinem von beiden verfügbar ist, verwendet die Sitzung H.264 als Videocodec.

Dieses Feature ist standardmäßig aktiviert.

Um die automatische Auswahl des Videocodecs zu deaktivieren, setzen Sie **DisableDecoderCaps** wie folgt:

1. Öffnen Sie den Registrierungs-Editor, indem Sie den Befehl `regedit` ausführen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine`.

Oder

Navigieren Sie zu `HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Graphics Engine`

3. Erstellen Sie einen DWORD-Schlüssel mit dem Namen **DisableDecoderCaps** und legen Sie seinen Wert auf 1 fest.

Wenn der Wert von **DisableDecoderCaps** in HKEY\_LOCAL\_MACHINE oder HKEY\_CURRENT\_USER auf 1 gesetzt ist, wird die automatische Auswahl des Videocodecs nicht verwendet.

## H.265-Videocodierung

Die Citrix Workspace-App unterstützt die Verwendung des H.265-Videocodecs für die Hardwarebeschleunigung von Remote-Grafiken und -Videos. Der H.265-Videocodec muss auf dem VDA und in der Citrix Workspace-App unterstützt und aktiviert sein. Wenn die GPU auf dem Endpunkt H.265-Decodierung über die DXVA-Schnittstelle nicht unterstützt, wird die Einstellung der Richtlinie "H265-Decodierung für Grafiken" ignoriert und die Sitzung greift auf den H.264-Videocodec zurück.

### Voraussetzungen:

1. VDA 7.16 oder höher.
2. Aktivieren Sie auf dem VDA die Richtlinie **Optimierung für 3D-Grafikworkload**.
3. Aktivieren Sie auf dem VDA die Richtlinie **Hardwarecodierung für Videocodec verwenden**.

Client-GPU, die H.265-Decodierung unterstützt:

- GPUs der NVIDIA Pascal-Generation oder höher
- Intel-GPU der 6. Generation oder höher
- AMD Generation GCN3 oder höher

### Hinweis:

Für diese Funktion gelten weitere VDA-Anforderungen wie die folgenden:

- GPU der NVIDIA-Maxwell-Generation oder höher
- Intel-GPU der 6. Generation oder höher
- GPU der AMD Raven Generation oder höher

Dieses Feature wird mit der Einführung des Features **Automatische Auswahl des Videocodecs** automatisch aktiviert.

Dieses Verhalten kann geändert werden, indem die H.265-Decodierung explizit mit dem clientseitigen Registrierungsschlüssel **EnableH265** gesteuert wird.

### H.265-Videocodierung mit dem Registrierungs-Editor konfigurieren:

H.265-Videocodierung in einem nicht in eine Domäne eingebundenen Netzwerk auf einem 32-Bit-Betriebssystem aktivieren:

1. Öffnen Sie den Registrierungs-Editor, indem Sie den Befehl `regedit` ausführen.

2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine`.
3. Erstellen Sie einen DWORD-Schlüssel mit dem Namen **EnableH265** und legen Sie seinen Wert auf 1 fest.

H.265-Videocodierung in einem nicht in eine Domäne eingebundenen Netzwerk auf einem 64-Bit-Betriebssystem aktivieren:

1. Öffnen Sie den Registrierungs-Editor, indem Sie den Befehl `regedit` ausführen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Erstellen Sie einen DWORD-Schlüssel mit dem Namen **EnableH265** und legen Sie seinen Wert auf 1 fest.
4. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Das Vorhandensein von **EnableH265** deaktiviert die automatische Erkennung. Wenn Sie **EnableH265** auf 0 setzen, wird die H.265-Decodierung deaktiviert. Daher verwendet die Sitzung nicht den H.265-Videocodec, auch wenn er auf dem VDA konfiguriert ist.

Wenn **EnableH265** auf 1 gesetzt ist, versucht die Citrix Workspace-App für Windows, die H.265-Decodierung zu verwenden. Wenn die H.265-Decodierung fehlschlägt, greifen Client und Server auf die H.264-Codierung zurück.

Die Verwendung von H.265 kann auch aktiviert werden, indem die Citrix Workspace-App mithilfe der administrativen Vorlage für das Citrix Gruppenrichtlinienobjekt (GPO) so konfiguriert wird, dass die H.265-Videocodierung verwendet wird:

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 >> Benutzererfahrung**.
3. Wählen Sie die Richtlinie H265-Decodierung für Grafiken.
4. Wählen Sie **Aktiviert**.
5. Klicken Sie auf **Anwenden** und auf **OK**.
6. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

#### Hinweis:

- Wenn die Richtlinie "Hardwarebeschleunigung für Grafiken" in der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App deaktiviert ist, werden die Einstellungen der Richtlinie H.265-Decodierung für Grafiken ignoriert. Das Feature wird dann nicht angewendet und es wird wieder der H.264-Videocodec verwendet.
- Die Grafikstatusanzeige und der Citrix HDX-Monitor können verwendet werden, um die Ver-

wendung des Videocodecs zu überprüfen.

## AV1

Die Citrix Workspace-App unterstützt die Verwendung des AV1-Videocodecs für die Hardwarebeschleunigung von Remote-Grafiken und -Videos. Der Videocodec AV1 muss sowohl auf dem VDA als auch auf der Citrix Workspace-App unterstützt und aktiviert werden.

### Die Voraussetzungen für AV1 sind wie folgt:

- VDA 2308 oder höher.
- Citrix Workspace-App für Windows 2305 oder höher
- Aktivieren Sie auf dem VDA (standardmäßig) die Richtlinie **Hardwarecodierung für Videocodec verwenden**.
- Für die Citrix Workspace-App für Windows gelten die folgenden Client-Hardwareanforderungen für AV1:
  - NVIDIA Ampere oder höher
  - Intel 11th Gen / Arc oder neuer
  - AMD Radeon RX 6000 / Radeon Pro W6000 Serie (RDNA2) oder höher

### Hinweis:

Für AV1 gelten weitere VDA-Anforderungen, z. B. die folgenden:

- GPU der NVIDIA Lovelace-Generation oder höher (z. B. L4/L40)
- GPU der Intel Arc-Generation oder höher

Dieses Feature wird mit der Einführung des Features **Automatische Auswahl des Videocodecs** automatisch aktiviert.

Dieses Verhalten kann geändert werden, indem die AV1-Decodierung explizit mit dem clientseitigen Registrierungsschlüssel **EnableAV1** gesteuert wird.

### AV1-Videocodierung mit dem Registrierungs-Editor konfigurieren::

AV1-Videocodierung in einem nicht in eine Domäne eingebundenen Netzwerk auf einem 32-Bit-Betriebssystem aktivieren:

1. Öffnen Sie den Registrierungs-Editor, indem Sie den Befehl `regedit` ausführen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine`.
3. Erstellen Sie einen DWORD-Schlüssel mit dem Namen **EnableAV1** und legen Sie seinen Wert auf 1 fest.
4. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

AV1-Videocodierung in einem nicht in eine Domäne eingebundenen Netzwerk auf einem 64-Bit-Betriebssystem aktivieren:

1. Öffnen Sie den Registrierungs-Editor, indem Sie den Befehl `regedit` ausführen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Erstellen Sie einen DWORD-Schlüssel mit dem Namen **EnableAV1** und legen Sie seinen Wert auf 1 fest.
4. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Das Vorhandensein von **EnableAV1** deaktiviert die automatische Erkennung. Wenn **EnableAV1** auf 0 gesetzt ist, wird die AV1-Dekodierung deaktiviert. Daher verwendet die Sitzung nicht den AV1-Videocodec.

Wenn **EnableAV1** auf 1 gesetzt ist, versucht die Citrix Workspace-App für Windows, die AV1-Decodierung zu verwenden. Wenn die AV1-Decodierung fehlschlägt, greifen Client und Server auf die H.264-Codierung zurück.

**Hinweis:**

Wenn die Richtlinie "Hardwarebeschleunigung für Grafiken" in der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App deaktiviert ist, werden die Einstellungen der Richtlinie AV1-Decodierung für Grafiken ignoriert. Das Feature wird dann nicht angewendet und es wird wieder der H.264-Videocodec verwendet.

Die Grafikstatusanzeige und der Citrix HDX-Monitor können verwendet werden, um die Verwendung des Videocodecs zu überprüfen.

## Optimierung für Microsoft Teams

April 22, 2024

### Unterstützung für die Wiedergabe kurzer Töne in optimiertem Microsoft Teams hinzugefügt

Bisher wurden bei aktiviertem sekundären Ruftönen kurze Signaltöne oder Benachrichtigungen wiederholt wiedergegeben: zum Beispiel der Ton, wenn ein Gast der Microsoft Teams-Besprechung beiträgt. Das Problem ließ sich nur umgehen, indem man Microsoft Teams beendete und neu startete. Dies beeinträchtigte die Benutzererfahrung.

Citrix Workspace-App unterstützt die Wiedergabe der kurzen Töne nach Wunsch. Diese Unterstützung aktiviert auch die sekundäre Ruftfunktion.

**Voraussetzungen:**

Installieren Sie die neueste Version von Microsoft Teams.

**Verbessertes Erlebnis bei optimierten Microsoft Teams-Videokonferenzen**

Die Simulcast-Unterstützung ist standardmäßig für optimierte Microsoft Teams-Videokonferenzen aktiviert. Dadurch werden die Qualität und das Erlebnis bei Videokonferenzen an verschiedenen Endpunkten verbessert, indem die bestgeeignete Auflösung für alle Anrufer gewählt wird.

Dank der Verbesserung kann jeder Benutzer mehrere Videostreams in unterschiedlichen Auflösungen (z. B. 720p, 360p usw.), abhängig von verschiedenen Faktoren wie Endpunktfähigkeit, Netzwerkbedingungen usw. bereitstellen. Der empfangende Endpunkt fordert dann die maximale Auflösung an, die er verarbeiten kann. So ist für jeden Benutzer das optimale Videoerlebnis gewährleistet.

**Hintergrundunschärfe und -effekte für Microsoft Teams-Optimierung mit HDX**

Die Citrix Workspace-App für Windows unterstützt jetzt Hintergrundunschärfe und -effekte für die Microsoft Teams-Optimierung mit HDX.

Sie können den Hintergrund weichzeichnen oder durch ein benutzerdefiniertes Bild ersetzen, damit zur Vermeidung von Ablenkung die Konzentration auf die Silhouette (Körper und Gesicht) erleichtert wird. Das Feature kann bei persönlichen Anrufen und Telefonkonferenzen verwendet werden.

Sie können die folgenden Optionen für Hintergrundunschärfe und -effekte auswählen:

- Kein Hintergrundeffekt
- Wählen Sie "Hintergrundunschärfe"
- Wählen Sie "Hintergrundbild"

**Hinweis:**

Dieses Feature ist jetzt in die Benutzeroberfläche und die Schaltflächen von Microsoft Teams integriert. Unterstützung für mehrere Fenster ist eine Voraussetzung, die ein VDA-Update auf 2112 oder höher erfordert. Weitere Informationen finden Sie unter Meetings und Chat mit mehreren Fenstern.

**Einschränkungen:**

- Von Benutzern definierte Hintergrundersetzung wird nicht unterstützt.

- Der Hintergrundeffekt bleibt zwischen den Sitzungen nicht bestehen. Wenn Sie Microsoft Teams schließen und neu starten oder der VDA erneut verbunden wird, wird der Hintergrundeffekt auf "Aus" zurückgesetzt.
- Nachdem die ICA-Sitzung wieder verbunden wurde, ist der Effekt deaktiviert. Die Benutzeroberfläche von Microsoft Teams zeigt jedoch durch ein Häkchen, dass der vorherige Effekt immer noch aktiviert ist. Citrix und Microsoft arbeiten zusammen daran, dieses Problem zu lösen.
- Das Gerät muss mit dem Internet verbunden sein, während das Hintergrundbild ersetzt wird.

#### Hinweis:

Dieses Feature ist erst nach Veröffentlichung eines zukünftigen Microsoft Teams-Updates verfügbar. Wenn das Update von Microsoft veröffentlicht wurde, finden Sie in [CTX253754](#) und unter [Microsoft 365-Roadmap](#) Informationen über das Dokumentationsupdate und die Ankündigung.

## Akustische Echounterdrückung

Die Echounterdrückung in `HdxRtcEngine.exe` kann deaktiviert werden, um Probleme mit der Audioleistung oder der Kompatibilität mit Peripheriegeräten zu beheben, die über integrierte AEC-Funktionen verfügen.

Navigieren Sie zum Registrierungspfad `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`, und erstellen Sie folgenden Schlüssel:

Name: EnableAEC

Typ: REG\_DWORD

Data: 0

(0 deaktiviert AEC. 1 aktiviert AEC. Ohne `Regkey` wird AEC in `HdxRtcEngine` standardmäßig aktiviert, unabhängig von den Hardwarefunktionen des Peripheriegeräts.)

## Erweiterungen für die Microsoft Teams-Optimierung

- Die Version von WebRTC, die für optimiertes Microsoft Teams verwendet wird, wurde auf Version M98 aktualisiert.
- **Aktualisiertes Verhalten bei der Auswahl von Audiogeräten für optimiertes Microsoft Teams:** Änderungen an den Standardaudiogeräten, die Sie in den Soundeinstellungen auf dem Endpunkt vornehmen, werden vom optimierten Microsoft Teams im Citrix VDI in der Auswahl der aktuellen Audiogeräte übernommen.

1 However, **if** you make an explicit device selection in Microsoft Teams, your selection takes precedence and does not follow the endpoint defaults. Your selection is persistent until you clear the Microsoft Teams cache.

Informationen zu Features, die Teil von Versionen mit erreichtem End of Life (EOL) sind, finden Sie in der [Legacy-Dokumentation](#).

## HDX-Transport

April 22, 2024

### Adaptiver HDX-Durchsatz

Der adaptive HDX-Durchsatz passt den Spitzendurchsatz einer ICA-Sitzung über die Ausgabepuffer intelligent an. Die Anzahl der Ausgabepuffer ist anfangs auf einen hohen Wert eingestellt. Der hohe Wert ermöglicht es insbesondere in Netzwerken mit hoher Latenz, Daten schneller und effizienter an den Client zu übertragen.

Bessere Interaktivität, schnellere Dateiübertragungen, flüssigere Videowiedergabe sowie höhere Framerate und Auflösung sorgen für eine bessere Benutzererfahrung.

Die Sitzungsinteraktivität wird ständig gemessen, um festzustellen, ob Datenströme innerhalb der ICA-Sitzung die Interaktivität beeinträchtigen. Ist dies der Fall, wird der Durchsatz verringert, um die Beeinträchtigungen durch den großen Datenstrom zu verringern und die Interaktivität wiederherzustellen.

Das Feature wird nur in der Citrix Workspace-App für Windows ab Version 1811 unterstützt.

#### **Wichtig:**

Der adaptive HDX-Durchsatz ändert die Ausgabepuffer durch Übertragung des Mechanismus vom Client auf den VDA. Das Anpassen der Anzahl der Ausgabepuffer auf dem Client, wie es im Knowledge Center-Artikel [CTX125027](#) erläutert wurde, hat daher keine Wirkung.

### Adaptiver Transport

Adaptiver Transport ist ein Verfahren in Citrix Virtual Apps and Desktops und Citrix DaaS, mit dem Enlightened Data Transport (EDT) als Transportprotokoll für ICA-Verbindungen verwendet werden kann. Weitere Informationen finden Sie unter [Adaptiver Transport](#) in der Citrix Virtual Apps and Desktops-Dokumentation.



## Verlusttoleranzmodus für Audio

Die Citrix Workspace-App verwendet den verlusttoleranten Modus für die Audioumleitung. Das Feature verbessert das Echtzeit-Streaming bei Verbindungen über ein Netzwerk mit Paketverlust und hoher Latenz.

Sie müssen VDA-Version 2311 oder höher verwenden. Dieses Feature ist standardmäßig in der Citrix Workspace-App für Windows aktiviert. Es ist jedoch auf dem VDA deaktiviert.

Um den verlusttoleranten Modus zu aktivieren, konfigurieren Sie den folgenden Registrierungswert und starten Sie die Maschine dann neu.

### Multisitzungs-OS-VDA:

- Schlüssel: HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- Wertname: EdtUnreliableAllowed
- Werttyp: DWORD
- Wertdaten: 1

### Workstation-VDA:

- Schlüssel: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Audio
- Wertname: EdtUnreliableAllowed
- Werttyp: DWORD
- Wertdaten: 1

## Browserinhaltsumleitung

April 22, 2024

Die Umleitung des Browserinhalts verhindert die VDA-seitige Wiedergabe von Webseiten auf einer Positivliste. Dabei wird von der Citrix Workspace-App clientseitig die Instanz einer entsprechenden Renderingengine erzeugt, die den HTTP- und HTTPS-Inhalt von der URL abrufen.

Die Umleitung von Browserinhalten unterstützt den Google Chrome-Browser. Mit der Browserinhaltsumleitung wird der Inhalt eines Webbrowsers an ein Clientgerät umgeleitet und ein entsprechender Browser erstellt, der in die Citrix Workspace-App eingebettet ist. Dadurch werden Netzwerklast, Seitenverarbeitung und Grafikwiedergabe an den Endpunkt abgeladen. Dies verbessert die Benutzererfahrung beim Anzeigen komplexer Webseiten, insbesondere solcher mit HTML5 oder WebRTC-Videos.

- Cookies sind in den Sitzungen persistent: Wenn Sie einen Browser beenden und neu starten, werden Sie nicht aufgefordert, Ihre Anmeldeinformationen erneut einzugeben.

- Browser berücksichtigen nun die auf dem lokalen System eingestellte Sprache.

Weitere Informationen finden Sie unter [Umleitung des Browserinhalts](#).

#### **Wichtig:**

- Die Browserinhaltsumleitung kann für 2402 LTSR über die Befehlszeile aktiviert werden
- Es ist standardmäßig für alle aktuellen Versionen der Citrix Workspace-App für Windows aktiviert.
- Die Browserinhaltsumleitung wird für die Versionen LTSR 1912 und 2203.1 der Citrix Workspace-App nicht unterstützt.

Um die Browserinhaltsumleitung auf dem VDA zu aktivieren, achten Sie darauf, dass die folgenden Richtlinien in Citrix Web Studio aktiviert sind:

- [Browserinhaltsumleitung](#)
- [ACL-Konfiguration für die Browserinhaltsumleitung](#)
- [Authentifizierungssites für Browserinhaltsumleitung](#)

## **Speicherpfad für temporäre Daten für Browserinhaltsumleitungs-Overlay konfigurieren**

Sie können den Pfad des Speichers für temporäre Daten für CEF-basierte Browser (Chromium Embedded Framework) konfigurieren. Sie können den Pfad auf dem VDA oder dem Client wie folgt konfigurieren:

#### **Auf dem VDA:**

1. Öffnen Sie den Registrierungs-Editor, indem Sie den Befehl `regedit` ausführen.
2. Navigieren Sie zum Registrierungspfad `HKEY_LOCAL_MACHINE\Software\Citrix\DXMediaStream\ClientConfigurations\WindowsCef`.
3. Erstellen Sie den String-Eintrag **BCRProfilePath** und setzen Sie seinen Wert auf "folder" für CEF-basierte BCRtmp-Dateien. Beispiel:

```
"BCRProfilePath"="C:\\tmp\\AlternateBcrProfilePath"
```

4. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

#### **Auf dem Client:**

1. Öffnen Sie den Registrierungs-Editor, indem Sie den Befehl `regedit` ausführen.
2. Navigieren Sie zum Registrierungspfad `HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream`.

3. Erstellen Sie einen Registrierungswert mit den folgenden Attributen:

- Name des Registrierungsschlüssels: `BCRProfilePath`
- Registrierungswert: Zeichenfolge `<folder for CEF based BCRtmp files>`

4. Starten Sie die Citrix Workspace-App neu, um die Änderungen zu übernehmen.

#### **Hinweis:**

Die Version des Chromium Embedded Framework (CEF) ist auf Version 117 aktualisiert. Dieses Versionsupgrade hilft, Sicherheitslücken zu schließen.

#### **Einschränkungen:**

Für die Browserinhaltsumleitung gelten die folgenden Einschränkungen:

- Webanwendungen, die Popup-Fenster oder die Persistenz von Sitzungscookies erfordern, werden nicht unterstützt.
- Microsoft Internet Explorer wird nicht unterstützt.
- Anwendungen, die vom Google-Authentifizierungsdienst abhängig sind (z. B. Google Meet), sind derzeit blockiert.
- Das Erweiterungs-Plug-In ist derzeit nicht offiziell auf Microsoft Edge veröffentlicht. Es gibt jedoch einen Workaround.
- Die HTML5-Videoumleitungsrichtlinie muss deaktiviert sein, wenn die Browserinhaltsumleitung verwendet wird.
- Benutzer können von Sitzungen aufgrund von unzuverlässigen Netzwerken, stark variierender Netzwerklatenz oder Bereichseinschränkungen von drahtlosen Geräten getrennt werden. Die Browserinhaltsumleitung verfügt für solche Szenarien nicht über ausreichende Fallback- oder Berichtsmechanismen.
- Über das Overlay heruntergeladene Dateien werden lokal gespeichert (auf der Clientmaschine des Endbenutzers).

#### **Verbesserte Leistung bei der Browserinhaltsumleitung**

Bisher verwendete die Browserinhaltsumleitung den clientseitigen Datenträgercache und die zwischengespeicherten Informationen wurden bei einem Upgrade nicht gelöscht. Diese Einstellung führte im Laufe der Zeit zu einer höheren Speicherplatznutzung und zu einem inkonsistenten Verhalten, wenn eine Seite mit der Browserinhaltsumleitung umgeleitet wurde.

Um dieses Problem zu beheben, verwendet BCR einen In-Memory-Cache. Diese Verbesserung hilft, die Leistung der Browserinhaltsumleitung zu verbessern.

Das Feature ist in der Standardeinstellung deaktiviert. Sie können diese Funktion auf dem VDA oder dem Client wie folgt aktivieren:

#### **Auf dem VDA:**

1. Öffnen Sie den Registrierungs-Editor, indem Sie den Befehl `regedit` ausführen.
2. Navigieren Sie zum Registrierungspfad `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXMediaStream\ClientConfigurations\WindowsCef`.
3. Erstellen Sie einen `DWORD`-Schlüssel mit dem Namen `BCRStoreCEFCacheInMemory` und setzen Sie seinen Wert auf 1.

Wenn der Wert von `BCRStoreCEFCacheInMemory` auf 0 gesetzt ist, verwendet die Browserinhaltsleitung Speicherplatz auf dem Client.

#### **Auf dem Client:**

1. Öffnen Sie den Registrierungs-Editor, indem Sie den Befehl `regedit` ausführen.
2. Navigieren Sie zum Registrierungspfad `HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream`.
3. Erstellen Sie einen `DWORD`-Schlüssel mit dem Namen `BCRStoreCEFCacheInMemory` und setzen Sie seinen Wert auf 1.

Wenn der Wert von `BCRStoreCEFCacheInMemory` auf 0 gesetzt ist, verwendet die Browserinhaltsleitung Speicherplatz auf dem Client.

#### **Hinweis:**

- Wenn `BCRStoreCEFCacheInMemory` sowohl auf dem Client als auch auf dem VDA festgelegt ist, hat die Einstellung auf dem Client Vorrang.
- Wenn sowohl `BCRProfilePath` als auch `BCRStoreCEFCacheInMemory` gesetzt sind, hat die Konfiguration `BCRProfilePath` Vorrang und die Konfiguration `BCRStoreCEFCacheInMemory` wird ignoriert.

#### **Einschränkung:**

Die Größenbeschränkung für den In-Memory-Cache ist auf 10 MB festgelegt.

## **Bidirektionale Inhaltsumleitung**

April 22, 2024

Die bidirektionale Inhaltsumleitung ermöglicht das Aktivieren und Deaktivieren der Client-zu-Host- und der Host-zu-Client-URL-Umleitung. Serverrichtlinien werden in Studio festgelegt und Clientrichtlinien werden in der administrativen Gruppenrichtlinienobjektvorlage der Citrix Workspace-App festgelegt.

Citrix bietet Host-zu-Client-Umleitung und lokalen App-Zugriff für die Client-zu-URL-Umleitung. Wir empfehlen jedoch, dass Sie die bidirektionale Inhaltsumleitung für domänenverbundene Windows-Clients verwenden.

Sie können die bidirektionale Inhaltsumleitung auf folgende Weise aktivieren:

1. Administrative Gruppenrichtlinienobjektvorlage
2. Registrierungs-Editor

**Hinweis:**

- Die bidirektionale Inhaltsumleitung funktioniert nicht in einer Sitzung, in der **Lokaler App-Zugriff** aktiviert ist.
- Die bidirektionale Inhaltsumleitung muss auf dem Server und dem Client aktiviert sein. Wenn sie auf dem Server oder auf dem Client deaktiviert ist, ist die Funktion deaktiviert.
- Wenn Sie URLs einschließen, können Sie eine URL angeben oder eine durch Semikolon getrennte Liste von URLs. Sie können ein Sternchen (\*) als Platzhalter verwenden.

**Aktivieren der bidirektionalen Inhaltsumleitung mit der administrativen Gruppenrichtlinienobjektvorlage:**

Verwenden Sie die Konfiguration mit der administrativen Gruppenrichtlinienobjektvorlage nur für die Erstinstallation der Citrix Workspace-App für Windows.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen** > **Klassische administrative Vorlagen (ADM)** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzererfahrung**.
3. Wählen Sie die Richtlinie **Bidirektionale Inhaltsumleitung**.

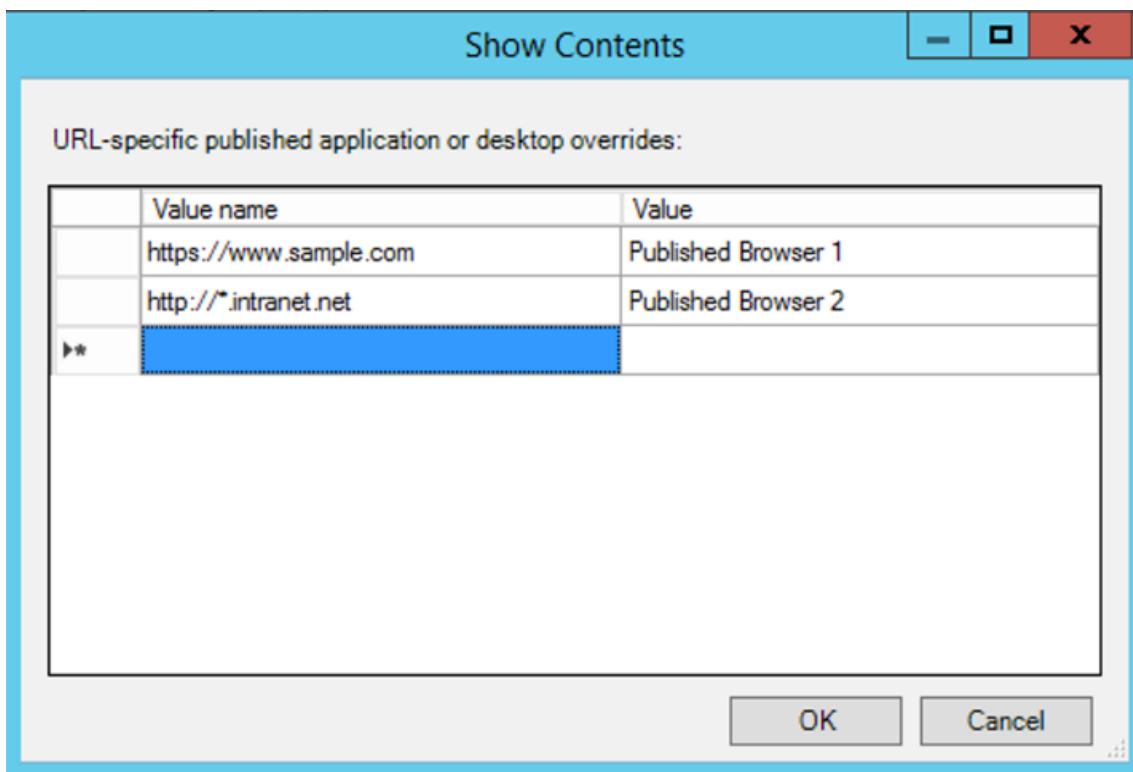
1. Geben Sie im Feld **Veröffentlichte Anwendungen oder Desktops** den Namen der Ressource ein, die zum Starten der umgeleiteten URL verwendet wird.

**Hinweis:**

Wenn Sie URLs einschließen, geben Sie eine URL oder eine durch Semikola getrennte Liste der URLs an. Sie können ein Sternchen (\*) als Platzhalter verwenden.

2. Wählen Sie unter **Veröffentlicht als** die Option **Anwendung** oder **Desktop** aus.
3. Geben Sie im Feld **Für Umleitung an VDA zulässige URLs** die URL ein, die umgeleitet werden soll. Trennen Sie die Listeneinträge durch Semikola voneinander.

4. Wählen Sie **URL-spezifische Außerkraftsetzungen für veröffentlichte Anwendungen oder Desktops aktivieren?**, wenn für eine URL eine Außerkraftsetzung gelten soll.
5. Klicken Sie auf **Anzeigen**, um eine Liste anzuzeigen, in der der Wertname mit einer der URLs im Feld **Für Umleitung an VDA zulässige URLs** übereinstimmen muss. Der Wert muss mit dem Namen einer veröffentlichten Anwendung übereinstimmen.



6. Geben Sie im Feld **Für Umleitung an Client zulässige URLs** die URL ein, die vom Server an den Client umgeleitet werden soll. Trennen Sie die Listeneinträge durch Semikola voneinander.

**Hinweis:**

Wenn Sie URLs einschließen, geben Sie eine URL oder eine durch Semikola getrennte Liste der URLs an. Sie können ein Sternchen (\*) als Platzhalter verwenden.

7. Klicken Sie auf **Anwenden** und auf **OK**.
8. Führen Sie an der Befehlszeile den Befehl `gpupdate /force` aus.

**Aktivieren der bidirektionalen Inhaltsumleitung mit der Registrierung:**

Zum Aktivieren der bidirektionalen Inhaltsumleitung führen Sie den Befehl `redirector.exe /RegIE` auf dem Citrix Workspace-App-Client im Installationsordner der Citrix Workspace-App aus (C:\Program Files (x86)\Citrix\ICA Client).

**Wichtig:**

- Stellen Sie sicher, dass die Umleitungsregel keine Schleifenkonfiguration ergibt. Eine Schleifenkonfiguration entsteht zum Beispiel, wenn VDA-Regeln so festgelegt sind, dass eine URL wie [https://www.my\\\_\\\_company.com](https://www.my\_\_company.com) an den Client und an den VDA umgeleitet wird.
- Die URL-Umleitung unterstützt nur explizite URLs, also URLs, die in der Adressleiste des Browsers angezeigt werden oder die mit der browserinternen Suchfunktion gefunden wurden (je nach Browser).
- Wenn zwei Anwendungen mit demselben Anzeigenamen mehrere StoreFront-Konten verwenden, wird der Anzeigename im primären StoreFront-Konto für den Start der Anwendung oder einer Desktopsitzung verwendet.
- Ein neues Browserfenster wird nur geöffnet, wenn eine URL zum Client umgeleitet wird. Wenn eine URL zum VDA umgeleitet wird, und der Browser bereits geöffnet ist, wird die umgeleitete URL auf einer neuen Registerkarte geöffnet.
- Eingebettete Links in Dateien wie Dokumente, E-Mails, PDFs werden unterstützt.
- Stellen Sie sicher, dass auf einer Maschine nur eine der Serverdateitypzuordnungen existiert und dass die Richtlinien für die Hostinhaltsumleitung aktiviert sind. Citrix empfiehlt, entweder die Serverdateitypzuordnung oder das URL-Umleitungsfeature zu deaktivieren, damit die URL-Umleitung ordnungsgemäß funktioniert.
- Klicken Sie im Internet Explorer auf **Einstellungen > Internetoptionen > Erweitert** und wählen Sie im Abschnitt **Browsen** die Option **Browsererweiterungen von Drittanbietern aktivieren** aus.

**Einschränkung:**

Kein Fallbackmechanismus ist vorhanden, wenn die Umleitung aufgrund von Problemen mit dem Sitzungsstart fehlschlägt.

**Bidirektionale URL-Unterstützung mit Chromium-basierten Browsern**

Die bidirektionale Inhaltsumleitung ermöglicht es Ihnen, URLs für die Umleitung vom Client zum Server und vom Server zum Client mithilfe von Richtlinien auf Server und Client zu konfigurieren.

Serverrichtlinien werden auf dem Delivery Controller festgelegt und Clientrichtlinien in der Citrix Workspace-App. Die Richtlinien werden mit der administrativen Gruppenrichtlinienobjektvorlage festgelegt.

Ab Version 2106 wird die bidirektionale URL-Umleitung für Google Chrome und Microsoft Edge unterstützt.

**Voraussetzungen:**



- Citrix Virtual Apps and Desktops Version 2106 oder höher.
- Erweiterung für die Browserumleitung Version 5.0.

Um den Google Chrome-Browser für die bidirektionale URL-Umleitung zu registrieren, führen Sie den folgenden Befehl im Installationsordner der Citrix Workspace-App aus:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /  
verbose
```

**Hinweis:**

Wenn Sie diese Befehle für Chrome-Browser verwenden, wird die [Erweiterung für die bidirektionale Inhaltsumleitung](#) automatisch aus dem Chrome Web Store installiert.

Um die Registrierung des Google Chrome-Browsers für die bidirektionale URL-Umleitung aufzuheben, führen Sie den folgenden Befehl im Installationsordner der Citrix Workspace-App aus:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome /  
verbose
```

**Hinweis:**

Wenn beim Zugriff auf die Seite “Browsererweiterungen” die folgende Fehlermeldung angezeigt wird, ignorieren Sie die Meldung:

```
WebSocket connection to wss://... failed.
```

Informationen zum Konfigurieren der URL-Umleitung in der Citrix Workspace-App finden Sie unter [Bidirektionale Inhaltsumleitung](#).

Weitere Informationen zur Browserinhaltsumleitung finden Sie unter [Browserinhaltsumleitung](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

**Abblenden des Desktop Viewer-Fensters verhindern:**

Wenn Sie mehrere Desktop Viewer-Fenster verwenden, sind die nicht aktiven Desktops in der Standardeinstellung abgeblendet. Wenn Benutzer mehrere Desktops gleichzeitig anzeigen möchten, können die Informationen auf den Desktops unlesbar sein. Sie können das Standardverhalten deaktivieren und das Abblenden des **Desktop Viewer**-Fensters durch Bearbeiten der Registrierung verhindern.

**Achtung**

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Machen Sie auf jeden Fall eine

Sicherungskopie der Registrierung, bevor Sie sie bearbeiten.

- Erstellen Sie auf dem Benutzergerät einen REG\_DWORD-Eintrag mit dem Namen **DisableDimming** in einem der folgenden Registrierungsschlüssel, abhängig davon, ob Sie ein Abblenden für den aktuellen Benutzer des Geräts oder für das Gerät selbst einstellen möchten. Ein Eintrag ist bereits vorhanden, wenn Desktop Viewer auf dem Gerät verwendet wurde:
  - HKEY\_CURRENT\_USER\Software\Citrix\XenDesktop\DesktopViewer
  - HKEY\_LOCAL\_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

Sie können das Abblenden steuern oder auch eine lokale Richtlinie festlegen, indem Sie denselben REG\_WORD-Eintrag in einem der folgenden Schlüssel erstellen:

- HKEY\_CURRENT\_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

Überprüfen Sie vor der Verwendung dieser Schlüssel, ob der Administrator von Citrix Virtual Apps and Desktops und Citrix DaaS eine Richtlinie für dieses Feature festgelegt hat.

Stellen Sie den Eintrag auf einen Wert ungleich Null ein, z. B. 1 oder true.

Wenn keine Einträge angegeben sind, oder der Eintrag auf 0 gesetzt ist, wird das **Desktop Viewer**-Fenster abgeblendet. Bei Angabe mehrerer Einträge wird die folgende Priorität verwendet. Der erste Eintrag und Wert in der Liste legen fest, ob das Fenster abgeblendet wird:

1. HKEY\_CURRENT\_USER\Software\Policies\Citrix\...
2. HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\...
3. HKEY\_CURRENT\_USER\Software\Citrix\...
4. HKEY\_LOCAL\_MACHINE\Software\Citrix\...

## Referenz für ICA-Einstellungen

April 22, 2024

Die Referenzdatei für ICA-Einstellungen enthält Registrierungseinstellungen und Listen der ICA-Dateieinstellungen, mit denen Administratoren das Verhalten der Citrix Workspace-App anpassen können. Sie können die Referenz für ICA-Einstellungen auch zur Problembehandlung bei unerwartetem Verhalten der App verwenden.

[Referenz für ICA-Einstellungen \(PDF-Download\)](#)

## Geräte

April 22, 2024

In diesem Abschnitt wird Folgendes beschrieben:

- [Maus](#)
- [Tastatur](#)
- [Drucken](#)
- [USB](#)
- [Clientlaufwerkzuordnung](#)
- [Mikrofon](#)

## Maus

April 22, 2024

### Relative Maus

Das Feature für die relative Mausfunktion bestimmt, wie weit sich die Maus seit dem letzten Frame innerhalb eines Fensters oder Bildschirms bewegt hat.

Die relative Maus verwendet das Pixeldelta zwischen den Mausbewegungen. Wenn Sie beispielsweise die Richtung der Kamera mit den Steuerelementen der Maus ändern, ist die Funktion effizient. Außerdem verbergen Apps den Mauszeiger häufig, da die Position des Cursors relativ zu den Bildschirmkoordinaten beim Bearbeiten eines 3D-Objekts oder einer Szene nicht relevant ist.

Durch die Unterstützung für relative Mausbewegungen wird die Mausposition auf relative statt auf absolute Weise interpretiert. Diese Interpretation ist für Anwendungen erforderlich, die relative Mausgabe statt absoluter Eingabe erfordern.

Sie können das Feature sowohl pro Benutzer als auch pro Sitzung konfigurieren, wodurch die Verfügbarkeit des Features genauer gesteuert werden kann.

#### Hinweis

Dieses Feature kann nur in einer veröffentlichten Desktopsitzung angewendet werden.

Wenn Sie das Feature mit dem Registrierungs-Editor oder der Datei default.ica konfigurieren, kann die Einstellung auch nach dem Beendigung der Sitzung fortbestehen.

## Konfigurieren der relativen Mausfunktion mit dem Registrierungs-Editor

Um das Feature zu konfigurieren, aktivieren Sie die folgenden Registrierungsschlüssel und starten Sie dann die Sitzung neu, damit die Änderungen wirksam werden:

### So stellen Sie das Feature pro Sitzung zur Verfügung:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse

### So stellen Sie das Feature pro Benutzer zur Verfügung:

HKEY\_CURRENT\_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse

- Name: RelativeMouse
- Typ: REG\_SZ
- Wert: True

#### Hinweis:

- Die im Registrierungs-Editor festgelegten Werte haben Vorrang vor den in der ICA-Datei festgelegten Einstellungen.
- Die in HKEY\_LOCAL\_MACHINE und HKEY\_CURRENT\_USER festgelegten Werte müssen identisch sein. Unterschiedliche Werte können Konflikte verursachen.

## Konfigurieren der relativen Mausfunktion mit der Datei default.ica

1. Öffnen Sie die Datei default.ica, die normalerweise in `C:\inetpub\wwwroot\Citrix\\conf\default.ica` ist, wobei "sitename" der Name der Site ist, der bei der Erstellung angegeben wurde. Bei StoreFront-Kunden ist die Datei default.ica normalerweise unter `C:\inetpub\wwwroot\Citrix\\App_Data\default.ica`, wobei storename der Name des Stores ist, der bei der Erstellung angegeben wurde.
2. Fügen Sie im Abschnitt WFClient den Schlüssel RelativeMouse hinzu. Legen Sie als Wert dieselbe Konfiguration wie für das JSON-Objekt fest.
3. Legen Sie den Wert wie gewünscht fest:
  - true –Aktivieren der relativen Maus
  - false –Deaktivieren der relativen Maus
4. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

#### Hinweis:

Die im Registrierungs-Editor festgelegten Werte haben Vorrang vor den in der ICA-Datei festgelegten Einstellungen.

## Aktivieren der relativen Mausfunktion über den Desktop Viewer

1. Melden Sie sich bei der Citrix Workspace-App an.
2. Starten Sie eine veröffentlichte Desktopsitzung.
3. Klicken Sie auf der Desktop Viewer-Symbolleiste auf **Einstellungen**.  
Das Fenster "Citrix Workspace-Einstellungen" wird angezeigt.
4. Wählen Sie **Verbindungen**.
5. Aktivieren Sie unter **Relative Mauseinstellungen** die Option **Relative Maus verwenden**.
6. Klicken Sie auf **Anwenden** und auf **OK**.

### Hinweis:

Beim Konfigurieren der relativen Maus mit dem Desktop Viewer wird das Feature nur pro Sitzung angewendet.

## Tastatur

April 22, 2024

## Tastenkombinationen

Sie können Tastenkombinationen konfigurieren, die die Citrix Workspace-App als Sonderfunktionen interpretiert. Wenn die Richtlinie für Tastenkombinationen aktiviert ist, können Sie Zuordnungen von Citrix Tastenkombinationen, das Verhalten von Windows-Tastenkombinationen und das Tastaturlayout für Sitzungen festlegen.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Benutzererfahrung**.
3. Wählen Sie die Richtlinie Tastenkombinationen.
4. Wählen Sie **Aktiviert** und die gewünschten Optionen.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

### **Citrix Workspace-App-Unterstützung für Symbole in 32-Bit-Farben:**

Die Citrix Workspace-App unterstützt Symbole in 32-Bit-High Color. Um Anwendungen im Seamless-Modus darzustellen, wird die Farbtiefe automatisch ausgewählt für:

- Anwendungen im Dialogfeld **Connection Center**,
- das Startmenü und
- die Taskleiste.

#### **Achtung**

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Um eine bevorzugte Farbtiefe zu definieren, können Sie unter `HKEY\LOCAL_MACHINE\SOFTWARE Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences` als Registrierungsschlüssel die Zeichenfolge `TWIDesiredIconColor` hinzufügen und den gewünschten Wert festlegen. Die möglichen Werte für die Farbtiefe von Symbolen sind 4, 8, 16, 24 und 32 Bits pro Pixel. Benutzer können eine geringere Farbtiefe für die Symbole wählen, wenn die Netzwerkverbindung langsam ist.

### **Speicherort für Anwendungsverknüpfungen über die Befehlszeile anpassen**

Über die Integration in das Startmenü und den Nur-Desktopverknüpfungsmodus können Sie Verknüpfungen für veröffentlichte Anwendungen im **Windows-Startmenü** oder auf dem Windows-Desktop platzieren. Benutzer müssen Anwendungen nicht über die Citrix Workspace-Benutzeroberfläche abonnieren. Die Integration in das Startmenü und die Verwaltung von Desktopverknüpfungen bieten eine nahtlose Desktopperfahrung für Benutzergruppen. Dies gilt auch für Benutzer, die einen gleichförmigen Zugriff auf einen bestimmten Anwendungssatz benötigen.

Das Flag heißt **SelfServiceMode** und ist standardmäßig auf `True` festgelegt. Wenn der Administrator das Flag **SelfServiceMode** auf `False` festlegt, können Sie nicht auf die Self-Service-Benutzeroberfläche zugreifen. Der Zugriff auf abonnierte Apps ist stattdessen über das Startmenü und über Desktopverknüpfungen möglich. Dies wird als "Nur-Verknüpfungsmodus" bezeichnet.

Benutzer und Administratoren können das Einrichten von Verknüpfungen über mehrere Registrierungseinstellungen anpassen.

## Arbeiten mit Verknüpfungen

- Benutzer können Apps nicht entfernen. Alle Apps sind verbindlich, wenn das Flag **SelfService-Mode** auf "false" festgelegt ist (= Nur-Verknüpfungsmodus). Wenn Sie ein Verknüpfungssymbol vom Desktop entfernen, wird das Symbol wieder angezeigt, sobald der Benutzer über das Citrix Workspace-App-Symbol im Infobereich die Option **Aktualisieren** auswählt.
- Benutzer können nur einen Store konfigurieren. Die Optionen "Konto" und "Einstellungen" sind nicht verfügbar, damit der Benutzer keine weiteren Stores konfiguriert. Der Administrator kann einem Benutzer besondere Privilegien zum Hinzufügen mehrerer Konten erteilen, indem er die Gruppenrichtlinienobjektvorlage verwendet. Administratoren können auch spezielle Berechtigungen bereitstellen, indem sie manuell den Registrierungsschlüssel "HideEditStoresDialog" auf der Clientmaschine hinzufügen. Wenn der Administrator einem Benutzer dieses Privileg erteilt, steht diesem die Option "Einstellungen" im Infobereich zur Verfügung, mit der er Konten hinzufügen und entfernen kann.
- Benutzer können Apps nicht über die **Windows-Systemsteuerung** entfernen.
- Sie können Desktopverknüpfungen über eine anpassbare Registrierungseinstellung hinzufügen. Desktopverknüpfungen werden nicht standardmäßig hinzugefügt. Starten Sie nach dem Bearbeiten der Registrierungseinstellungen die Citrix Workspace-App neu.
- Verknüpfungen werden im Startmenü standardmäßig mit einem Kategoriepfad erstellt: UseCategoryAsStartMenuPath.

### Hinweis:

In Windows 10 ist die Erstellung von verschachtelten Ordnern im Startmenü nicht zulässig. Anwendungen können im Stammordner angezeigt werden, aber nicht in den Unterordnern der Kategorie, die mit Citrix Virtual Apps definiert sind.

- Sie können während der Installation das Flag [/DESKTOPDIR="Dir\_name"] hinzufügen, um alle Verknüpfungen in einem Ordner zusammenzufassen. CategoryPath wird für Desktopverknüpfungen unterstützt.
- Die automatische Neuinstallation geänderter Apps ist ein Feature, das über den Registrierungsschlüssel `AutoReInstallModifiedApps` aktiviert werden kann. Wenn `AutoReInstallModifiedApps` aktiviert ist, werden alle auf dem Server durchgeführten Änderungen an Attributen veröffentlichter Anwendungen und Desktops auf der Clientmaschine angezeigt. Wenn der Schlüssel `AutoReInstallModifiedApps` deaktiviert ist, werden Apps und Desktopattribute nicht aktualisiert. Außerdem werden Verknüpfungen beim Aktualisieren nicht wiederhergestellt, wenn sie auf dem Client gelöscht werden. Standardmäßig ist `AutoReInstallModifiedApps` aktiviert.

## Anpassen des Speicherorts für Anwendungsverknüpfungen über den Registrierungs-Editor

**Hinweis:**

- Standardmäßig verwenden Registrierungsschlüssel das Format **Zeichenfolge**.
- Ändern Sie die Registrierungsschlüssel, bevor Sie einen Store konfigurieren. Wenn Sie oder ein Benutzer die Registrierungsschlüssel anpassen möchten, müssen Sie oder der Benutzer folgende Schritte ausführen:
  1. Setzen Sie die Citrix Workspace-App zurück.
  2. Konfigurieren Sie die Registrierungsschlüssel.
  3. Konfigurieren Sie dann den Store neu.

**Wiederverbindung über Workspace Control verwalten**

Mit Workspace Control folgen Anwendungen dem Benutzer, wenn er das Gerät wechselt. Beispielsweise können Krankenhausärzte mit Workspace Control von einer Arbeitsstation zu einer anderen wechseln, ohne ihre Anwendungen auf jedem einzelnen Gerät neu starten zu müssen. In der Citrix Workspace-App können Sie Workspace Control auf Clientgeräten durch Ändern der Registrierung verwalten. Für domänengebundene Clientgeräte können Sie für Workspace Control auch die Gruppenrichtlinie verwenden.

**Achtung:**

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Erstellen Sie **WSCReconnectModeUser** und ändern Sie den vorhandenen Registrierungsschlüssel **WSCReconnectMode** im Masterdesktopimage oder auf dem Citrix Virtual Apps-Server. Der veröffentlichte Desktop kann das Verhalten der Citrix Workspace-App ändern.

WSCReconnectMode-Schlüsseleinstellungen für die Citrix Workspace-App:

- 0 = keine Wiederverbindung mit vorhandenen Sitzungen
- 1 = Wiederverbindung bei Anwendungsstart
- 2 = Wiederverbindung bei Anwendungsaktualisierung
- 3 = Wiederverbindung bei Anwendungsstart oder Anwendungsaktualisierung
- 4 = Wiederverbindung beim Öffnen der Citrix Workspace-Benutzeroberfläche
- 8 = Wiederverbindung beim Anmelden an Windows
- 11 = Kombination von 3 und 8



**Workspace Control deaktivieren** Erstellen Sie den folgenden Schlüssel, um Workspace Control zu deaktivieren:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 Bit)

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Dazzle (32 Bit)

Name: **WSCReconnectModeUser**

Typ: REG\_SZ

Wertdaten: 0

Ändern Sie den folgenden Schlüssel vom Standardwert 3 auf 0

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 Bit)

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Dazzle (32 Bit)

Name: **WSCReconnectMode**

Typ: REG\_SZ

Wertdaten: 0

**Hinweis:**

Wenn Sie keinen Schlüssel erstellen möchten, können Sie auch den Schlüssel **WSCReconnectAll** auf "false" festlegen.

### Registrierungsschlüssel für 32-Bit-Maschinen

**Registrierungsschlüssel: WSCSupported Wert: True**

**Schlüsselpfad:**

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Citrix\Dazzle

**Registrierungsschlüssel: WSCReconnectAll Wert: True**

**Schlüsselpfad:**

- 1 - `HKEY\_CURRENT\_USER\Software\Citrix\Dazzle`
- 2 - `HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties`
- 3 - `HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\Dazzle`
- 4 - `HKEY\_LOCAL\_MACHINE\Software\Citrix\Dazzle`

**Registrierungsschlüssel: WSCReconnectMode Wert: 3**

**Schlüsselpfad:**

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Citrix\Dazzle

**Registrierungsschlüssel: WSCReconnectModeUser Wert:** Die Registrierung wird während der Installation nicht erstellt.

**Schlüsselpfad:**

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Citrix\Dazzle

**Registrierungsschlüssel für 64-Bit-Maschinen:**

**Registrierungsschlüssel: WSCSupported Wert: True**

**Schlüsselpfad:**

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

**Registrierungsschlüssel: WSCReconnectAll Wert: True**

**Schlüsselpfad:**

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

**Registrierungsschlüssel: WSCReconnectMode Wert: 3**

**Schlüsselpfad:**

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
  primaryStoreID +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

**Registrierungsschlüssel: WSCReconnectModeUser** Wert: Die Registrierung wird während der Installation nicht erstellt.

**Schlüsselpfad:**

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
  +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

## Tastaturlayout und Sprachenleiste

### Tastaturlayout

**Hinweis:**

Sie können die über das Citrix Workspace-App-Symbol im Infobereich verfügbare Seite “Erweiterte Einstellungen” ganz oder teilweise ausblenden. Weitere Informationen finden Sie unter [Erweiterte Einstellungen](#).

Die Tastaturlayoutsynchronisierung ermöglicht es Ihnen, zwischen bevorzugten Tastaturlayouts auf dem Clientgerät zu wechseln. Das Feature ist in der Standardeinstellung deaktiviert. Die Tastaturlayoutsynchronisierung ermöglicht das automatische Synchronisieren des Clienttastaturlayouts mit einer Sitzung mit virtuellen Apps und Desktops.

### Konfigurieren der Tastaturlayoutsynchronisierung mit der administrativen GPO-Vorlage:

**Hinweis:**

Die GPO-Konfiguration hat Vorrang vor der StoreFront- bzw. GUI-Konfiguration.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** oder **Benutzerkonfiguration** zu **Administrative Vorlagen > Administrative Vorlage (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung**.

3. Wählen Sie die Richtlinie **Tastatureinstellungen**.

4. Wählen Sie **Aktiviert** und wählen Sie eine der folgenden Optionen:

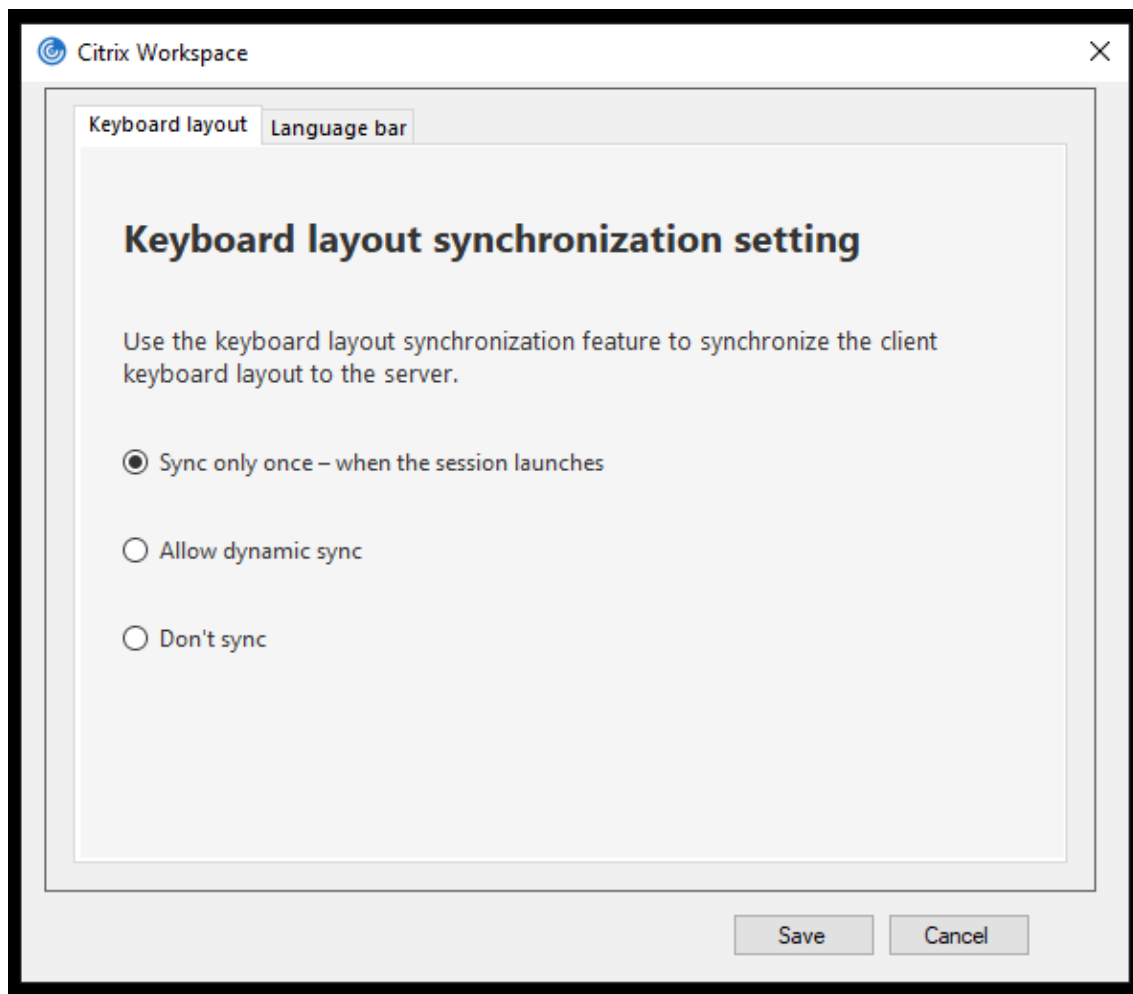
- **Dynamische Synchronisierung zulassen** - Wählen Sie im Dropdownmenü **Ja** oder **Nein**. Diese Option synchronisiert das Clienttastaturlayout mit dem Server, wenn Sie das Clienttastaturlayout ändern. Wenn diese Option ausgewählt ist, wird auch der Client-IME für ostasiatische Sprachen aktiviert.  
Wenn Sie für diese Option **Ja** auswählen, werden die folgenden beiden Optionen überschrieben.
- **Synchronisierung beim Sitzungsstart** - Wählen Sie im Dropdownmenü eine der folgenden Optionen:
  - **Nur einmal beim Sitzungsstart synchronisieren** - Synchronisiert das Clienttastaturlayout beim Sitzungsstart mit dem Server. Änderungen, die Sie während der Sitzung am Clienttastaturlayout vornehmen, werden nicht sofort wirksam. Melden Sie sich ab und wieder an, um die Änderungen zu übernehmen.
  - **Nicht synchronisieren** - Der Client verwendet das auf dem Server vorhandene Tastaturlayout.

5. Wählen Sie **Übernehmen** und **OK**.

### Konfigurieren der Tastaturlayoutsynchronisierung über die grafische Benutzeroberfläche:

1. Klicken Sie auf das Infobereichsymbol der Citrix Workspace-App und wählen Sie **Erweiterte Einstellungen > Tastatur und Sprachenleiste**.

Das Dialogfeld **Tastatur und Sprachenleiste** wird angezeigt.



2. Wählen Sie eine der folgenden Optionen:

- **Nur einmal beim Sitzungsstart synchronisieren** - Gibt an, dass das Tastaturlayout nur einmal beim Sitzungsstart mit dem VDA synchronisiert wird.
- **Dynamische Synchronisierung zulassen** - Synchronisiert das Tastaturlayout dynamisch mit dem VDA, wenn die Clienttastatur in einer Sitzung geändert wird.
- **Nicht synchronisieren** - Der Client verwendet das auf dem Server vorhandene Tastaturlayout.

3. Klicken Sie auf **Speichern**.

### Konfigurieren der Tastaturlayoutsynchronisierung mit der Befehlszeilenschnittstelle (CLI):

Führen Sie den folgenden Befehl im Installationsordner der Citrix Workspace-App für Windows aus.

Der Installationsordner der Citrix Workspace-App ist in der Regel in `C:\Program files (x86)\Citrix\ICA Client`.

- Zum Aktivieren: `wfica32.exe /localime:on`
- Zum Deaktivieren: `wfica32.exe /localime:off`

Beim Verwenden der Clienttastaturlayoutoption wird der Client-IME (Eingabemethoden-Editor) aktiviert. Wenn Benutzer, die Japanisch, Chinesisch oder Koreanisch verwenden, den Server-IME bevorzugen, müssen sie die Clienttastaturlayoutoption durch Auswahl von **Nein** oder über den Befehl `wfica32.exe /localime:off` deaktivieren. Wenn sie eine Verbindung mit der nächsten Sitzung herstellen, wird das Tastaturlayout des Remoteservers wiederhergestellt.

Gelegentlich wird der Wechsel des Clienttastaturlayouts nicht in einer aktiven Sitzung wirksam. Sie beheben das Problem, indem Sie sich von der Citrix Workspace-App ab- und dann wieder anmelden.

**Tastaturlayoutsynchronisierung mit der Befehlszeilenschnittstelle (CLI) konfigurieren** Die folgenden neuen Befehle wurden eingeführt, um die Tastaturlayoutsynchronisierung über die Befehlszeilenschnittstelle zu konfigurieren:

---

Befehle	Beschreibung
<code>wfica32.exe /kbdsyncmode:once</code>	Legt den Tastatursynchronisierungsmodus auf "Nur einmal synchronisieren" fest.
<code>wfica32.exe /kbdsyncmode:dynamic</code>	Legt den Tastatursynchronisierungsmodus auf "Dynamische Synchronisierung" fest.
<code>wfica32.exe /kbdsyncmode:no</code>	Legt den Tastatursynchronisierungsmodus auf "Nicht synchronisieren" fest.

---

Führen Sie den obigen Befehl im Installationsordner der Citrix Workspace-App für Windows aus.

Der Installationsordner der Citrix Workspace-App ist in der Regel in `C:\Programme (x86)\Citrix\ICA Client`.

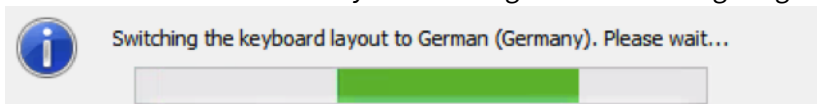
### Konfigurieren der Tastatursynchronisierung auf Windows VDA

#### Hinweis:

Das folgende Verfahren gilt nur für Windows Server 2016 und höher. Unter Windows Server 2012 R2 und früher ist die Tastatursynchronisierung standardmäßig aktiviert.

1. Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Erstellen Sie den DWORD-Eintrag `DisableKeyboardSync` und legen Sie seinen Wert auf 0 fest.  
1 deaktiviert die Synchronisierung des Tastaturlayouts.
3. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

Nachdem Sie das Tastaturlayout für den VDA und für die Citrix Workspace-App aktiviert haben, wird beim Wechsel von Tastaturlayouts das folgende Fenster angezeigt.



Dieses Fenster zeigt an, dass das Tastaturlayout in der Sitzung auf das Clienttastaturlayout umgestellt wird.

### Konfigurieren der Tastatursynchronisierung auf Linux VDA

Starten Sie die Eingabeaufforderung, und führen Sie folgenden Befehl aus:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar"-v "SyncKeyboardLayout"-d "0x00000001"
```

Starten Sie den VDA neu, damit die Änderungen wirksam werden.

Weitere Informationen zur Tastaturlayoutsynchronisierung auf Linux VDA finden Sie unter [Dynamische Tastaturlayoutsynchronisierung](#).

### Ausblenden der Benachrichtigung beim Tastaturlayoutwechsel:

Durch die Benachrichtigung beim Wechseln des Tastaturlayouts erfahren Sie, dass die VDA-Sitzung das Tastaturlayout ändert. Der Wechsel des Tastaturlayouts dauert ungefähr zwei Sekunden. Wenn Sie die Benachrichtigung ausblenden, warten Sie einige Zeit, bevor Sie mit der Eingabe beginnen, um die Eingabe falscher Zeichen zu vermeiden.

#### Warnung

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

### **Ausblenden der Benachrichtigung beim Tastaturlayoutwechsel mit dem Registrierungs-Editor:**

1. Starten Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Erstellen Sie einen neuen Zeichenfolgenwertschlüssel mit dem Namen **HideNotificationWindow**.
3. Legen Sie den DWORD-Wert auf **1** fest.
4. Klicken Sie auf **OK**.
5. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

### **Einschränkungen:**

- Für Remoteanwendungen, die mit erhöhten Rechten ausgeführt werden (z. B. wenn Sie mit der rechten Maustaste auf ein Anwendungssymbol klicken und “Als Administrator ausführen” wählen), kann keine Tastaturlayoutsynchronisierung erfolgen. Als Workaround ändern Sie das Tastaturlayout manuell auf der Serverseite (VDA) oder deaktivieren Sie die Benutzerkontensteuerung (UAC).
- Wenn das Tastaturlayout auf dem Client auf ein Layout geändert wird, das vom Server nicht unterstützt wird, dann wird das Synchronisierungsfeature des Tastaturlayouts aus Sicherheitsgründen deaktiviert. Ein unbekanntes Tastaturlayout wird als mögliches Sicherheitsrisiko behandelt. Um das Feature für die Tastaturlayoutsynchronisierung wiederherzustellen, muss der Benutzer sich von der Sitzung abmelden und wieder anmelden.
- In einer RDP-Sitzung können Sie das Tastaturlayout nicht mit der Tastenkombination **Alt + Shift** ändern. Als Workaround können Sie das Tastaturlayout mit der Sprachenleiste in der RDP-Sitzung ändern.

### **Sprachenleiste**

Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Sitzungen angezeigt. Die Sprachenleiste wird in Sitzungen standardmäßig angezeigt.

#### **Hinweis:**

Das Feature ist in Sitzungen verfügbar, die unter einem VDA der Version 7.17 und höher ausgeführt werden.

### **Konfigurieren der Sprachenleiste über die administrative GPO-Vorlage:**

Remotesprachenleiste ein- und ausblenden: Auf der Sprachenleiste wird die bevorzugte Eingabesprache von Anwendungssitzungen angezeigt.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.

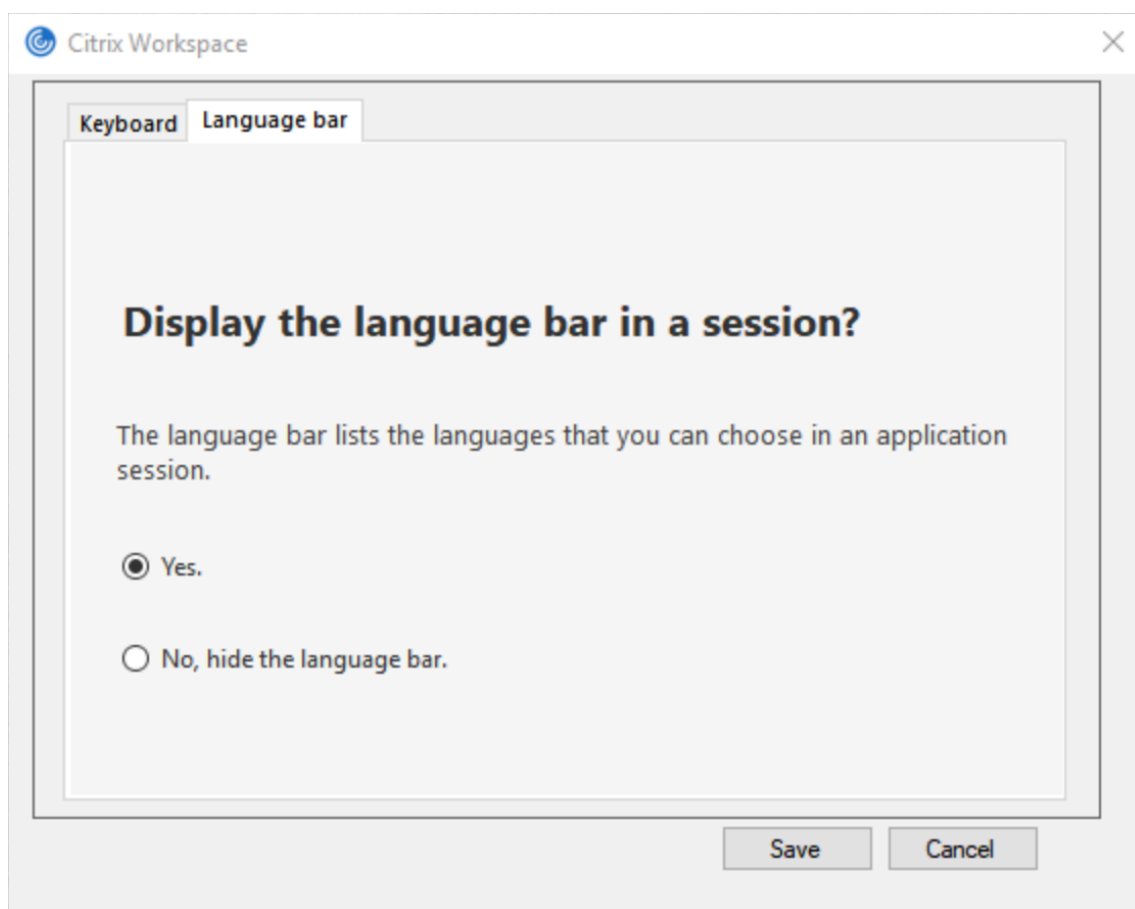


2. Navigieren Sie unter dem Knoten **Computerkonfiguration** oder **Benutzerkonfiguration** zu **Administrative Vorlagen > Administrative Vorlage (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung**.
3. Wählen Sie die Richtlinie **Sprachenleiste** aus.
4. Wählen Sie **Aktiviert** und wählen Sie eine der folgenden Optionen:
  - Ja – Gibt an, dass die Sprachenleiste in einer Anwendungssitzung angezeigt wird.
  - Nein, Sprachenleiste ausblenden - Gibt an, dass die Sprachenleiste in einer Anwendungssitzung ausgeblendet ist.
5. Klicken Sie auf **Anwenden** und auf **OK**.

#### **Konfigurieren der Sprachenleiste über die grafische Benutzeroberfläche:**

1. Klicken Sie im Infobereich mit der rechten Maustaste auf das Symbol der Citrix Workspace-App und wählen Sie **Erweiterte Einstellungen**.
2. Wählen Sie **Tastatur und Sprachenleiste**.
3. Wählen Sie die Registerkarte **Sprachenleiste**.
4. Wählen Sie eine der folgenden Optionen:
  - a) Ja —Zeigt an, dass die Sprachleiste in einer Sitzung angezeigt wird.
  - b) Nein, Sprachenleiste ausblenden – Zeigt an, dass die Sprachenleiste in einer Sitzung ausgeblendet ist.
5. Klicken Sie auf **Speichern**.

Die Änderungen werden sofort wirksam.



**Hinweis:**

- Sie können die Einstellungen in einer aktiven Sitzung ändern.
- Die Remotesprachenleiste wird in Sitzungen mit nur einer Eingabesprache nicht angezeigt.

**Ausblenden der Registerkarte “Sprachenleiste” von der Seite “Erweiterte Einstellungen”:**

Sie können die Registerkarte “Sprachenleiste” von der Seite **Erweiterte Einstellungen** über die Registrierung ausblenden.

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`.
3. Erstellen Sie den DWORD-Wertschlüssel **ToggleOffLanguageBarFeature** und legen Sie ihn auf **1** fest, um die Option für die Sprachenleiste auf der Seite “Erweiterte Einstellungen” auszublenden.

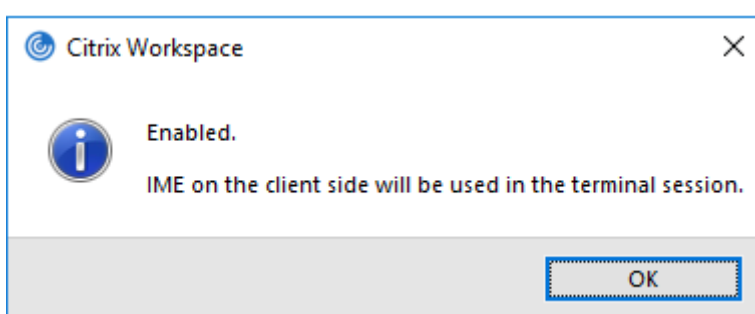
**Generischer Client-IME (Eingabemethoden-Editor)**

**Hinweis:**

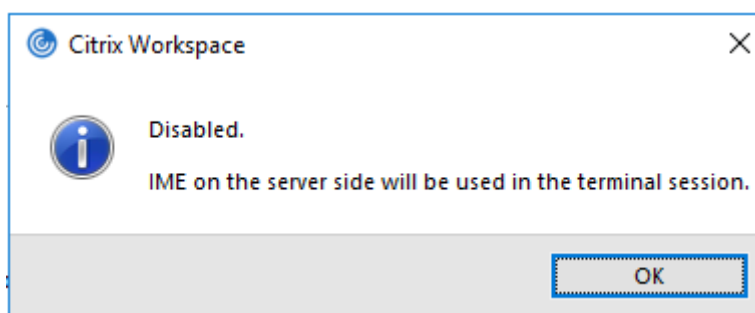
Wenn Sie mit dem Betriebssystem Windows 10 Version 2004 arbeiten, können bestimmte technische Probleme auftreten, wenn Sie das IME-Feature in einer Sitzung verwenden. Diese Probleme treten aufgrund eines Drittanbieterproblems auf. Weitere Informationen finden Sie im [Microsoft-Supportartikel](#).

**Konfigurieren eines generischen Client-IME über die Befehlszeilenschnittstelle:**

- Führen Sie den Befehl `wfica32.exe /localime:on` im Citrix Workspace-App-Installationsordner `C:\Program Files (x86)\Citrix\ICA Client` aus, um den generischen Client-IME zu aktivieren.



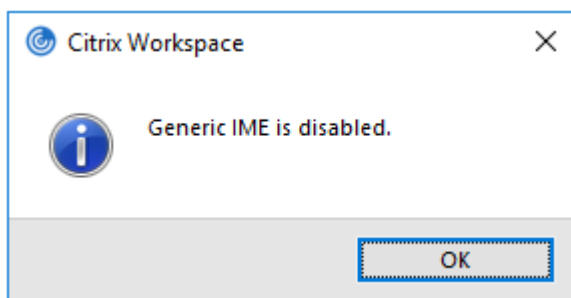
- Führen Sie den Befehl `wfica32.exe /localime:off` im Citrix Workspace-App-Installationsordner `C:\Program Files (x86)\Citrix\ICA Client` aus, um den generischen Client-IME zu deaktivieren.



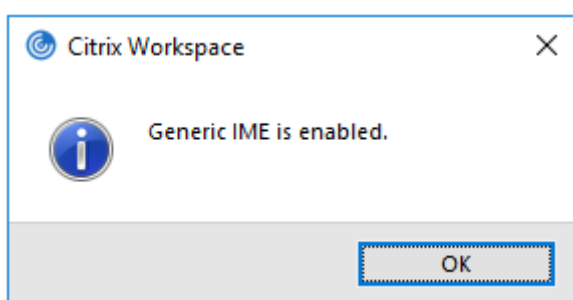
**Hinweis:**

Sie können mit der Befehlszeilenoption `wfica32.exe /localime:on` den generischen Client-IME und die Tastaturlayoutsynchronisierung aktivieren.

- Führen Sie den Befehl `wfica32.exe /localgenericime:off` im Citrix Workspace-App-Installationsordner `C:\Program Files (x86)\Citrix\ICA Client` aus, um den generischen Client-IME zu deaktivieren. Dieser Befehl hat keine Auswirkungen auf die Einstellungen für die Tastaturlayoutsynchronisierung.



Wenn Sie den generischen Client-IME über die Befehlszeilenschnittstelle deaktiviert haben, können Sie das Feature durch Ausführen des Befehls `wfica32.exe /localgenericime:on` wieder aktivieren.



### **Ein-/Ausschalten:**

Die Citrix Workspace-App unterstützt das Ein- und Ausschalten dieses Features. Sie können das Feature durch Ausführen des Befehls `wfica32.exe /localgenericime:on` ein- und ausschalten. Die Einstellungen für die Tastaturlayoutsynchronisierung haben jedoch Vorrang vor der Ein-/Ausschaltfunktion. Wenn die Layoutsynchronisierungseinstellung auf **Aus** gesetzt ist, wird durch Umschalten kein generischer Client-IME aktiviert.

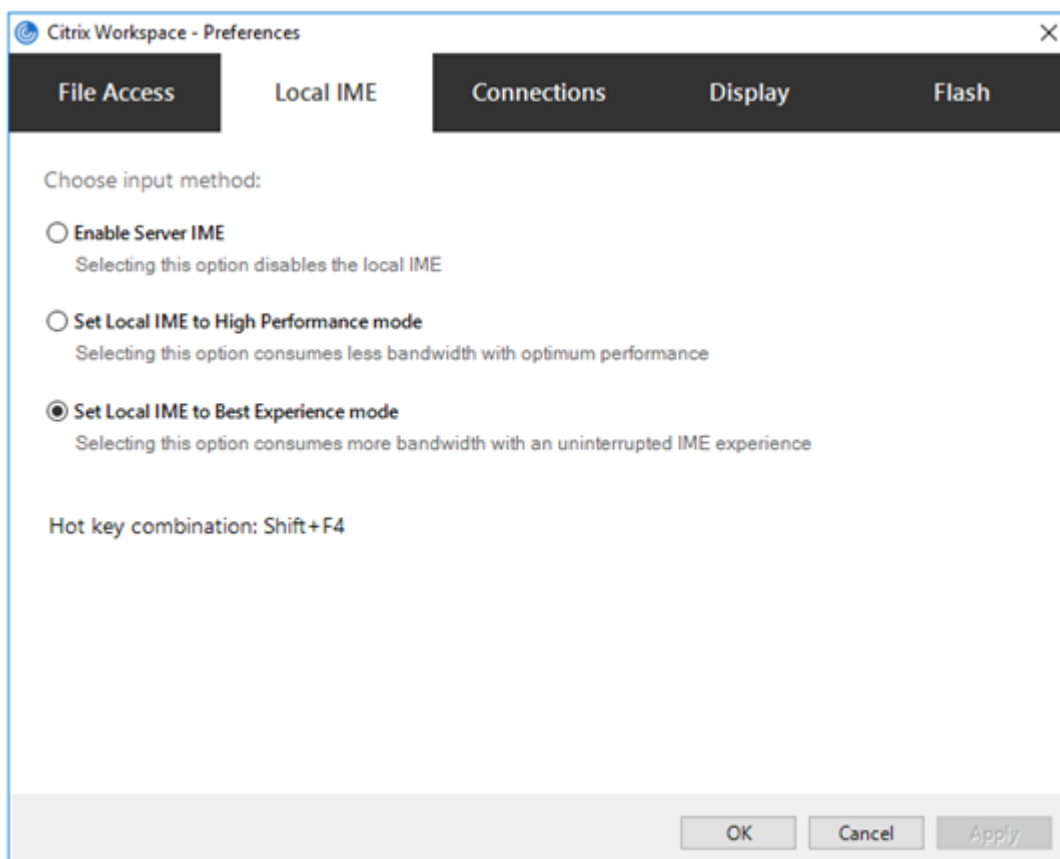
### **Konfigurieren eines generischen Client-IME über die grafische Benutzeroberfläche:**

Der generische Client-IME erfordert VDA-Version 7.13 oder höher.

Das generische Client-IME-Feature kann durch Aktivieren der Tastaturlayoutsynchronisierung aktiviert werden. Weitere Informationen finden Sie unter [Tastaturlayoutsynchronisierung](#).

Die Citrix Workspace-App ermöglicht das Konfigurieren verschiedener Optionen für den generischen Client-IME. Entsprechend Ihrer Anforderungen und der Nutzung können Sie eine der Optionen auswählen.

1. Klicken Sie mit der rechten Maustaste auf das Citrix Workspace-App-Symbol im Infobereich und wählen Sie **Connection Center**.
2. Wählen Sie **Einstellungen** und **Lokaler IME**.



Für die verschiedenen IME-Modi sind die folgenden Optionen verfügbar:

1. **Server-IME aktivieren** –Deaktiviert den lokalen IME und nur die auf dem Server festgelegten Sprachen können verwendet werden.
2. **Lokalen IME auf Hochleistungsmodus einstellen** –Verwendet den lokalen IME mit beschränkter Bandbreite. Diese Option schränkt die Funktionalität des Kandidatenfensters ein.
3. **Lokalen IME-Modus für beste Erfahrung einstellen** –Verwendet den lokalen IME mit optimaler Benutzerfreundlichkeit. Diese Option verbraucht hohe Bandbreite. Diese Option ist standardmäßig ausgewählt, wenn der generische Client-IME aktiviert ist.

Die Änderungen werden nur in der aktuellen Sitzung angewendet.

#### **Tastenkombinationen mit einem Registrierungs-Editor konfigurieren:**

Wenn der generische Client-IME aktiviert ist, können Sie mit der Tastenkombination **Umschalt+F4** verschiedene IME-Modi auswählen. Die verschiedenen Optionen für die IME-Modi werden oben rechts in der Sitzung angezeigt.

Standardmäßig ist die Tastenkombination für den generischen Client-IME deaktiviert.

Navigieren Sie im Registrierungs-Editor zu `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Key`.

Wählen Sie **AllowHotKey** und ändern Sie den Standardwert in 1.

Mit der Tastenkombination **Umschalt+F4** können Sie verschiedene IME-Modi in einer Sitzung auswählen.

Die verschiedenen IME-Modi werden rechts oben in der Sitzung angezeigt, während Sie die Optionen mit der Tastenkombination durchlaufen.



#### **Einschränkungen:**

- Der generische Client-IME unterstützt keine UWP-Apps (Universelle Windows-Plattform-Anwendungen) wie Suchbenutzeroberfläche und Edge-Browser des Windows 10-Betriebssystems. Verwenden Sie als Workaround den Server-IME.
- Der generische Client-IME wird für Internet Explorer Version 11 im **geschützten Modus** nicht unterstützt. Als Workaround können Sie den geschützten Modus unter **Internetoptionen** deaktivieren. Klicken Sie zum Deaktivieren auf **Sicherheit** und deaktivieren Sie das Kontrollkästchen **Geschützten Modus aktivieren**.

#### **Synchronisierung mehrerer Tastaturen beim Sitzungsstart**

Bisher wurde nur die aktive Tastatur auf dem Client mit dem VDA synchronisiert, nachdem die Sitzung im Vollbildmodus gestartet wurde. Wenn Sie in diesem Szenario **Nur einmal beim Sitzungsstart synchronisieren** in Ihrer Citrix Workspace-App konfiguriert hatten und Sie zu einer anderen Tastatur wechseln mussten, war es nötig, die Tastatur manuell auf Ihrem Remotedesktop zu installieren. Wenn Sie **Dynamische Synchronisierung zulassen** in Ihrer Citrix Workspace-App konfiguriert hatten, mussten Sie auch in den Fenstermodus wechseln, die Tastatur auf Ihrem Client ändern und dann zurück in den Vollbildmodus wechseln.

Alle verfügbaren Tastaturen auf dem Client mit dem VDA synchronisiert, nachdem die Sitzung im Vollbildmodus gestartet wurde. Sie können die erforderliche Tastatur aus der Liste der installierten oder verfügbaren Tastaturen auf dem Client auswählen, nachdem die Sitzung im Vollbildmodus gestartet wurde.

Das Feature **Mehrere Tastaturen beim Sitzungsstart synchronisieren** ist auf dem VDA standardmäßig aktiviert und in der Citrix Workspace-App standardmäßig deaktiviert.

## Voraussetzungen

### In Citrix Workspace-App für Windows:

Aktivieren Sie die Tastaturlayouteinstellung **Nur einmal synchronisieren – wenn die Sitzung beginnt**. Weitere Informationen finden Sie unter in der Dokumentation zum [Tastaturlayout](#).

### Auf dem VDA:

Aktivieren Sie die folgenden VDA-Richtlinien:

- Unicode-Tastaturlayoutzuordnung. Weitere Informationen finden Sie unter [Unicode-Tastaturlayoutzuordnung aktivieren](#) oder [Tastatur- und Eingabemethoden-Editor \(IME\)](#)
- Client-Tastaturlayoutsynchronisierung und Verbesserung des IME: Weitere Informationen finden Sie unter [Tastatur und Eingabemethoden-Editor \(IME\)](#)

### Citrix Workspace-App konfigurieren:

Diese Funktion ist nur auf virtuellen Desktops verfügbar. Das Feature ist in der Standardeinstellung deaktiviert. Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Navigieren Sie zum Abschnitt [Virtual Channels\Keyboard] der Datei **All\_Regions.ini**.
2. Fügen Sie einen booleschen Registrierungsschlüssel `SyncKbdLayoutList` to `HKEY_CURRENT_USER\SOFTWARE\Citrix\Ica Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard` hinzu.
3. Legen Sie den Wert auf 1 fest.

### VDA-Konfiguration:

Die Funktion **Mehrere Tastaturen beim Sitzungsstart synchronisieren** ist auf dem VDA standardmäßig aktiviert.

Um diese Funktion zu deaktivieren, aktualisieren Sie die VDA-Registrierung wie folgt:

1. Öffnen Sie den Registrierungs-Editor und navigieren Sie zu `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Erstellen Sie den DWORD-Eintrag `DisableKbdLayoutList` und setzen Sie seinen Wert auf 0. Wenn Sie den Wert auf 1 setzen, wird die Funktion **Mehrere Tastaturen beim Sitzungsstart synchronisieren** deaktiviert.
3. Starten Sie die Sitzung neu, damit die Änderungen wirksam werden.

## Drucken

April 22, 2024

### Drucker

Überschreiben der Druckereinstellungen auf dem Benutzergerät

1. Klicken Sie im Menü **Drucken**, das in einer Anwendung auf dem Benutzergerät zur Verfügung steht, auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Clienteneinstellungen** auf “Erweiterte Optimierungen” und ändern Sie die Optionen “Bildkomprimierung” und “Bild- und Schriftartcaching”.

### Steuerung der Bildschirmtastatur

Damit über Windows-Tablets der Touchzugriff auf virtuelle Anwendungen und Desktops möglich ist, zeigt die Citrix Workspace-App in folgenden Situationen automatisch die Bildschirmtastatur an:

- wenn Sie ein Texteingabefeld aktivieren und
- wenn das Gerät im Zelt- oder Tabletmodus ist.

Auf einigen Geräten und unter bestimmten Umständen kann die Citrix Workspace-App den Geräte-  
modus nicht präzise erkennen. Die Bildschirmtastatur wird möglicherweise auch angezeigt, wenn sie  
nicht benötigt wird.

Um auf einem konvertierbaren Gerät keine Bildschirmtastatur anzuzeigen:

- Erstellen Sie in `HKEY\\_CURRENT\\_USER\\SOFTWARE\\Citrix\\ICA Client  
\\Engine\\Configuration\\Advanced\\Modules\\MobileReceiver` den  
REG\_DWORD-Wert `DisableKeyboardPopup`.
- Legen Sie den Wert auf 1 fest.

#### Hinweis:

Erstellen Sie den Wert auf einer 64-Bit-Maschine in `HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Citrix\\ICA  
Client\\Engine\\Configuration\\Advanced\\Modules\\MobileReceiver`.

Die Tasten können auf folgende 3 Modi festgelegt werden:

- **Automatisch:** `AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0`
- **Immer anzeigen** (Bildschirmtastatur): `AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0`
- **Nie anzeigen** (Bildschirmtastatur): `AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1`



## PDF-Druck

Die Citrix Workspace-App für Windows unterstützt den PDF-Druck in einer Sitzung. Der universelle PDF-Druckertreiber von Citrix ermöglicht das Drucken von Dokumenten aus gehosteten Anwendungen und Desktops, die unter Citrix Virtual Apps and Desktops und Citrix DaaS ausgeführt werden.

Wenn Sie im Dialogfeld **Drucken** die Option **Citrix PDF-Drucker** auswählen, wird die Datei vom Treiber in das PDF-Format konvertiert und auf das lokale Gerät übertragen. Die PDF-Datei wird dann mit dem standardmäßigen PDF-Viewer zur Ansicht geöffnet und kann auf einem lokal angeschlossenen Drucker ausgedruckt werden.

Citrix empfiehlt den Google Chrome-Browser oder Adobe Acrobat Reader zur Anzeige von PDF-Dateien.

Sie können den PDF-Druck in Citrix mit Citrix Studio auf dem Delivery Controller aktivieren.

### Voraussetzungen:

- Citrix Virtual Apps and Desktops Version 7 1808 oder höher
- Auf Ihrem Computer muss mindestens ein PDF-Viewer installiert sein.

### Aktivieren der PDF-Druckfunktion:

1. Verwenden Sie auf dem Delivery Controller das Citrix Studio, und wählen Sie im linken Bereich den Knoten **Richtlinie**. Sie können entweder eine Richtlinie erstellen oder eine vorhandene Richtlinie bearbeiten.
2. Legen Sie die Richtlinie **Universellen PDF-Drucker automatisch erstellen** auf "Aktiviert" fest.

Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

### Einschränkung:

- Das Anzeigen und Drucken von PDF-Dateien wird im Microsoft Edge-Browser nicht unterstützt.

## Erweiterter Tabletmodus in Windows 10 mit Windows Continuum

Windows Continuum ist ein Windows 10-Feature, das sich an die Art und Weise der Verwendung des Clientgeräts anpasst. Die Citrix Workspace-App für Windows unterstützt Windows Continuum, einschließlich der dynamischen Änderung von Modi.

Bei Geräten mit Touchscreen startet der Windows 10-VDA im Tabletmodus, wenn keine Tastatur oder Maus angeschlossen ist. Ist eine Tastatur und/oder Maus angeschlossen, startet er im Desktopmodus. Durch das Anschließen oder Trennen eines Eingabegeräts an beliebigen Clientgeräten oder am Bildschirm eines 2-in-1-Geräts (z. B. Surface Pro) wird zwischen Tablet- und Desktopmodus umgeschaltet. Weitere Informationen finden Sie unter [Tabletmodus für Geräte mit Touchscreen](#) in der Dokumentation von Citrix Virtual Apps and Desktops.

Auf Clientgeräten mit Touchscreen erkennt der Windows 10-VDA das Vorhandensein einer Tastatur oder einer Maus, wenn Sie eine Verbindung zu einer Sitzung herstellen oder wiederherstellen. Er erkennt auch, wenn Sie während der Sitzung eine Tastatur oder eine Maus anschließen oder entfernen. Dieses Feature ist standardmäßig auf dem VDA aktiviert. Um das Feature zu deaktivieren, ändern Sie mit Citrix Studio die Richtlinie **Tabletmodus ein/aus**.

Der Tabletmodus bietet eine für Touchscreens besser geeignete Benutzeroberfläche:

- Die Schaltflächen sind etwas größer.
- Die **Startseite** und alle gestarteten Apps werden im Vollbildmodus geöffnet.
- Die Taskleiste enthält eine Schaltfläche "Zurück".
- Die Taskleiste enthält keine Symbole.

Der Desktopmodus ist die klassische Benutzeroberfläche, bei der die Interaktion wie bei einem PC mit Tastatur und Maus erfolgt.

**Hinweis:**

Workspace für Web unterstützt Windows Continuum nicht.

## USB

April 22, 2024

### USB-Unterstützung

Mit der USB-Unterstützung können Sie mit zahlreichen USB-Geräten interagieren, wenn sie mit Citrix Virtual Apps and Desktops und Citrix DaaS verbunden sind. Sie können USB-Geräte an die Geräte anschließen und mit Remoting der Geräte stehen sie auf dem virtuellen Desktop zur Verfügung. Zu den USB-Geräten, die für Remoting verfügbar sind, gehören Flashlaufwerke, Smartphones, PDAs, Drucker, Scanner, MP3 Player, Sicherheitsgeräte und Tablets. Benutzer von Desktop Viewer können mit einer Einstellung auf der Symbolleiste steuern, ob USB-Geräte für Citrix Virtual Apps and Desktops und Citrix DaaS verfügbar sind.

Isochrone Features in USB-Geräten wie Webcams, Mikrofonen, Lautsprechern und Headsets werden in typischen LAN-Umgebungen mit geringer Latenz oder hoher Geschwindigkeit unterstützt. In solchen Umgebungen können diese Geräte mit Programmpaketen wie Microsoft Office Communicator und Skype verwendet werden.

Die folgenden Gerätetypen werden direkt in Sitzungen mit virtuellen Apps und Desktops unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards

USB-Spezialgeräte (beispielsweise Bloomberg-Tastaturen und 3D-Maus) können für die USB-Unterstützung konfiguriert werden. Weitere Informationen zur Konfiguration von Bloomberg-Tastaturen finden Sie unter [Konfigurieren von Bloomberg-Tastaturen](#).

Weitere Informationen zur Konfiguration von Richtlinienregeln für andere USB-Spezialgeräte finden Sie im Knowledge Center-Artikel [CTX122615](#).

In der Standardeinstellung werden bestimmte Typen von USB-Geräten nicht für Remoting über Citrix Virtual Apps and Desktops und Citrix DaaS unterstützt. Beispielsweise könnte ein Benutzer eine Netzwerkkarte über internes USB mit der Systemplatine verbunden haben. Remoting wäre bei einem solchen Gerät nicht angebracht. Die folgenden USB-Gerätetypen werden standardmäßig nicht in Sitzungen mit virtuellen Apps und Desktops unterstützt:

- Bluetooth-Dongle
- Integrierte Netzwerkkarte
- USB-Hubs
- USB-Grafikadapter

Remoting ist möglich für USB-Geräte, die mit einem Hub verbunden sind, jedoch nicht für den Hub selbst.

Die folgenden USB-Gerätetypen werden standardmäßig nicht in einer Sitzung mit virtuellen Apps unterstützt:

- Bluetooth-Dongle
- Integrierte Netzwerkkarte
- USB-Hubs
- USB-Grafikadapter
- Audiogeräte
- Massenspeichergeräte

### **Funktionsweise der USB-Unterstützung:**

Wenn ein Benutzer ein USB-Gerät anschließt, wird es mit der USB-Richtlinie überprüft, und wenn das Gerät zulässig ist, erfolgt ein Remoting zum virtuellen Desktop. Wenn das Gerät von der Standardrichtlinie abgelehnt wird, steht es nur auf dem lokalen Desktop zur Verfügung.

Wenn ein Benutzer ein USB-Gerät anschließt, wird eine Meldung über den Anschluss eines neuen Geräts angezeigt. Der Benutzer kann die Geräte, für die ein Remoting zum virtuellen Desktop erfolgen soll, bei jeder Verbindung auswählen. Der Benutzer kann die USB-Unterstützung auch so konfigurieren, dass für alle USB-Geräte, die vor oder während einer Sitzung angeschlossen werden, automatisch ein Remoting zu dem virtuellen Desktop erfolgt, der den Fokus hat.

## In der Standardeinstellung zulässige USB-Geräteklassen

Verschiedene Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln zugelassen.

Auch wenn sie in dieser Liste sind, stehen manche Klassen nur nach zusätzlicher Konfiguration für das Remoting in Sitzungen mit virtuellen Apps und Desktops zur Verfügung. Folgende USB-Geräteklassen sind möglich.

- **Audio (Geräteklasse 01):** Umfasst Audioeingabegeräte (Mikrofone), Audioausgabegeräte und MIDI-Controller. Moderne Audiogeräte verwenden im Allgemeinen isochrone Transfers, die von XenDesktop 4 oder höher unterstützt werden. Audio (Geräteklasse 01) ist für virtuelle Apps nicht relevant, da Geräte dieser Klasse für das Remoting in virtuelle Apps mit USB-Unterstützung nicht verfügbar sind.

### Hinweis:

Für manche Spezialgeräte (z. B. VOIP-Telefone) ist eine zusätzliche Konfiguration erforderlich. Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX123015](#).

- **PID (Physical Interface Devices) (Geräteklasse 05):** Diese Geräte ähneln HIDs (Human Interface Devices), bieten jedoch im Allgemeinen Eingabe oder Feedback in Echtzeit, hierzu gehören u. a. Force-Feedback-Joysticks, Bewegungsplattformen und Force-Feedback-Endoskelette.
- **Bilder (Geräteklasse 06):** Hierzu gehören digitale Kameras und Scanner. Digitale Kameras unterstützen oft die Bilderklasse, in der Bilder mit den Protokollen PTP (Picture Transfer Protocol) oder MTP (Media Transfer Protocol) zu einem Computer oder zu einem anderen Peripheriegerät übertragen werden. Kameras können auch als Massenspeichergeräte angezeigt werden. Eine Kamera kann möglicherweise auch über die Setupmenüs der Kamera für beide Klassen konfiguriert werden.

### Hinweis:

Wird eine Kamera als Massenspeichergerät angezeigt, wird die Clientlaufwerkzuordnung verwendet und die USB-Unterstützung wird nicht benötigt.

- **Drucker (Geräteklasse 07):** Die meisten Drucker gehören zu dieser Klasse, obwohl einige herstellerspezifische Protokolle (Klasse ff) verwenden. Multifunktionsdrucker haben ggf. einen internen Hub oder sind Composite-Geräte. In beiden Fällen verwendet das Druckerelement meistens die Druckerklasse und das Scanner- oder Faxelement verwendet eine andere Klasse, z. B. Bilder.

Drucker funktionieren normalerweise ohne USB-Unterstützung.

### Hinweis

Für diese Klasse von Geräten (vor allem Drucker mit Scanfunktion) ist eine zusätzliche Konfiguration erforderlich. Anweisungen finden Sie im Knowledge Center-Artikel [CTX123015](#).

- **Massenspeicher (Geräteklasse 08):** Die gängigsten Massenspeichergeräte sind USB-Flashlaufwerke sowie über USB angeschlossene Festplatten, CD- bzw. DVD-Laufwerke und SD/MMC-Kartenleser. Außerdem gibt es zahlreiche Geräte mit einem internen Speicher, der auch eine Massenspeicherschnittstelle darstellt, u. a. Media Player, digitale Kameras und Mobiltelefone. Massenspeicher (Geräteklasse 08) ist für virtuelle Apps nicht relevant, da Geräte dieser Klasse für das Remoting in virtuelle Apps mit USB-Unterstützung nicht verfügbar sind. Bekannte Unterklassen:

- 01: Begrenzte Flashlaufwerke
- 02: Normalerweise CD- bzw. DVD-Geräte (ATAPI/MMC-2)
- 03: Normalerweise Bandgeräte (QIC-157)
- 04: Normalerweise Diskettenlaufwerke (UFI)
- 05: Normalerweise Diskettenlaufwerke (SFF-8070i)
- 06: Die meisten Massenspeichergeräte verwenden diese SCSI-Variante

Der Zugriff auf Massenspeichergeräte erfolgt oft über die Clientlaufwerkzuordnung und USB-Unterstützung wird daher nicht benötigt.

- **Content Security (Geräteklasse 0d):** Content-Security-Geräte erzwingen Inhaltsschutz normalerweise für die Lizenzierung oder das Management digitaler Rechte. Dongles gehören zu dieser Klasse.
- **Video (Geräteklasse 0e):** Die Videoklasse umfasst Geräte, mit denen Videos und videobezogenes Material verwendet werden. Dies können Webcams, digitale Camcorder, analoge Videokonverter und einige Fernsehuner sein, aber auch einige digitale Kameras, die Videostreaming unterstützen.

### Wichtig

Die meisten Videostreaminggeräte verwenden isochrone Transfers, die von XenDesktop 4 oder höher unterstützt werden. Für manche Videogeräte (z. B. Webcams mit Bewegungserkennung) ist eine zusätzliche Konfiguration erforderlich. Anweisungen finden Sie im Knowledge Center-Artikel [CTX123015](#).

- **Personal Healthcare (Geräteklasse 0f):** Hierzu gehören Geräte zur persönlichen Gesundheitspflege, u. a. Blutdruckmessgeräte, Herzfrequenzmessgeräte, Schrittzähler, Geräte zur Medikamenteneinnahmeüberwachung und Spirometer.
- **Anwendungs- und herstellerspezifisch (Geräteklassen fe und ff):** Bei vielen Geräten werden herstellerspezifische oder nicht USB-Konsortium-konforme Protokolle verwendet. Diese

Geräte werden normalerweise als herstellerspezifisch (Klasse ff) ausgezeichnet.

### **In der Standardeinstellung nicht zugelassene USB-Geräteklassen**

Die folgenden Klassen von USB-Geräten werden von den USB-Standardrichtlinienregeln nicht zugelassen:

- Kommunikation und CDC-Steuerung (Geräteklasse 02 und 0a): Die USB-Standardrichtlinie lässt diese Geräte nicht zu, da ein solches Gerät möglicherweise selbst die Verbindung zum virtuellen Desktop bereitstellt.
- HID (Human Interface Devices, Geräteklasse 03): Umfasst viele Eingabe- und Ausgabegeräte. Typische HIDs sind Tastaturen, Mäuse, Zeigegeräte, Grafiktablets, Sensoren, Game Controller, Tasten und Steuerfunktionen.

Die Unterklasse 01 wird "Boot Interface"-Klasse genannt und für Tastaturen und Maus verwendet.

USB-Tastaturen (Klasse 03, Unterklasse 01, Protokoll 1) oder USB-Mäuse (Klasse 03, Unterklasse 01, Protokoll 2) werden von der USB-Standardrichtlinie nicht zugelassen. Begründung: Die meisten Tastaturen und Mäuse können auch ohne USB-Unterstützung genutzt werden. Sie werden zudem sowohl lokal als auch remote bei Verbindungen mit einem virtuellen Desktop verwendet.

- USB-Hubs (Geräteklasse 09): Mit USB-Hubs können zusätzliche Geräte am lokalen Computer angeschlossen werden. Auf diese Geräte muss nicht remote zugegriffen werden.
- Smartcard (Geräteklasse 0b): Zu Smartcardlesegeräten gehören berührungslose und Smartcard-Berührungslesegeräte sowie USB-Token mit einem eingebetteten smartcardäquivalenten Chip.

Der Zugriff auf Smartcardlesegeräte erfolgt nicht mit Smartcard-Remoting und erfordert keine USB-Unterstützung.

- Kabellose Controller (Geräteklasse e0): Einige dieser Geräte stellen u. U. wichtigen Netzwerkzugang bereit oder schließen wichtige Peripheriegeräte an, z. B. Bluetooth-Tastaturen oder -Mäuse.

Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit der USB-Unterstützung gegeben werden sollte.

- **Verschiedene Netzwerkgeräte (Geräteklasse ef, Unterklasse 04):** Einige dieser Geräte sind u. U. unabdingbar für den Netzwerkzugang. Die USB-Standardrichtlinie lässt diese Geräte nicht zu. Es kann jedoch Geräte geben, denen Zugriff mit der USB-Unterstützung gegeben werden sollte.

## Für Remoting verfügbare USB-Geräteliste aktualisieren

Bearbeiten Sie die Vorlagendatei für Citrix Workspace für Windows, um die USB-Geräte zu aktualisieren, die für das Remoting zu Desktops verfügbar sind. Mit diesem Update können Sie Citrix Workspace für Windows über eine Gruppenrichtlinie ändern. Die Datei ist in folgendem Installationsordner:

```
\C:\Program Files\Citrix\ICA Client\Configuration\en
```

Sie können auch die Registrierung auf jedem Benutzergerät ändern und den folgenden Registrierungsschlüssel hinzufügen:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name="DeviceRules"Wert=
```

### Wichtig

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.

Die Standardregeln für das Produkt sind an folgendem Speicherort gespeichert:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name="DeviceRules"Value=
```

Ändern Sie nicht die Produktstandardregeln.

Weitere Informationen zu den Richtlinieneinstellungen für USB-Geräte finden Sie unter [Einstellungen der Richtlinie "USB-Geräte"](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

## Umleitung von USB-Verbundgeräten

USB 2.1 und höher unterstützt USB-Verbundgeräte, bei denen mehrere untergeordnete Geräte sich eine Verbindung mit demselben USB-Bus teilen. Die Geräte teilen sich Konfigurationsraum und Busverbindung, und zur Identifizierung jedes untergeordneten Geräts wird eine eindeutige Schnittstellenzahl 00-ff verwendet. Diese Geräte sind auch nicht identisch mit einem USB-Hub, der einen neuen USB-Bus zum Anschluss anderer USB-Geräte mit jeweils eigener Adresse bereitstellt.

Auf dem Clientendpunkt gefundene Verbundgeräte können wie folgt an den virtuellen Host weitergeleitet werden:

- als einzelnes USB-Verbundgerät oder

- als Gruppe unabhängiger untergeordneter Geräte (aufgeteilte Geräte)

Wenn ein USB-Verbundgerät weitergeleitet wird, steht das gesamte Gerät dem Endpunkt nicht mehr zur Verfügung. Durch das Weiterleiten wird auch die lokale Nutzung des Geräts für alle Anwendungen auf dem Endpunkt blockiert –auch für den Citrix Workspace-Client, der für eine optimierte HDX-Remoteerfahrung erforderlich ist.

Verwenden Sie gegebenenfalls ein USB-Headset mit Audiogerät und HID-Taste für Stummschaltung und Lautstärkeregelung. Wenn das gesamte Gerät über einen generischen USB-Kanal weitergeleitet wird, kann es nicht mehr über den optimierten HDX-Audiokanal umgeleitet werden. Die Audioqualität ist jedoch am besten, wenn Audiodaten über den optimierten HDX-Audiokanal und nicht mit hostseitigen Audiotreibern über generisches USB-Remoting gesendet werden. Dieses Verhalten liegt an der “geschwätzigen”Natur der USB-Audioprotokolle.

Weitere Probleme treten auf, wenn Systemtastatur oder Zeigegerät zu einem Verbundgerät gehören, in dem auch Funktionen integriert sind, die für Remotesitzungen erforderlich sind. Wird ein komplettes Verbundgerät weitergeleitet, funktionieren Systemtastatur oder Maus am Endpunkt nur noch innerhalb der Remotedesktopsitzung oder -anwendung.

Zum Beheben dieser Probleme empfiehlt Citrix, das Verbundgerät per Splitting aufzuteilen und nur die untergeordneten Schnittstellen weiterzuleiten, die einen generischen USB-Kanal verwenden. Die übrigen untergeordneten Geräte können dadurch weiterhin von Anwendungen auf dem Clientendpunkt verwendet werden, einschließlich der Citrix Workspace-App, die ein optimiertes HDX-Erlebnis bietet. Gleichzeitig werden nur die erforderlichen Geräte weitergeleitet und der Remotesitzung zur Verfügung gestellt.

### **Geräteregeln:**

Wie auch USB-Standardgeräte werden die Verbundgeräte von Geräteregeln, die in der Richtlinie oder der Citrix Workspace-App auf dem Clientendpunkt konfiguriert sind, für die Weiterleitung ausgewählt. Die Citrix Workspace-App entscheidet dann anhand dieser Regeln, welche USB-Geräte an die Remotesitzung weitergeleitet werden dürfen.

Jede Regel besteht aus einem Aktionsschlüsselwort (Allow, Connect oder Deny), einem Doppelpunkt (:), und null oder mehr Filterparametern, die den tatsächlichen Geräten am USB-Subsystem des Endpunkts entsprechen. Diese Filterparameter entsprechen den Metadaten des USB-Gerätedeskriptors, die von jedem USB-Gerät zur Identifizierung verwendet werden.

Geräteregeln sind als Klartext angegeben, mit einer Regel pro Zeile und einem optionalen Kommentar nach dem #-Zeichen. Regeln werden von oben nach unten (in absteigender Prioritätsreihenfolge) zugeordnet. Die erste Regel, die dem Gerät oder der untergeordneten Schnittstelle entspricht, wird angewendet. Nachfolgende Regeln, die dasselbe Gerät oder dieselbe Schnittstelle auswählen, werden ignoriert.

Beispiele für Geräteregeln:



- ALLOW: vid=046D pid=0102 # Bestimmtes Gerät gemäß vid/pid zulassen
- ALLOW: vid=0505 class=03 subclass=01 # Jede pid für Anbieter 0505 zulassen, wenn subclass=01
- DENY: vid=0850 pid=040C # Bestimmtes Gerät (und alle untergeordneten Geräte) ablehnen
- DENY: class=03 subclass=01 prot=01 # Jedes Gerät ablehnen, dass allen Filtern entspricht
- CONNECT: vid=0911 pid=0C1C # Bestimmtes Gerät zulassen und automatisch verbinden
- ALLOW: vid=0286 pid=0101 split=01 # Dieses Gerät aufteilen und alle Schnittstellen zulassen
- ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # Aufteilen und nur zwei Schnittstellen zulassen
- CONNECT: vid=1050 pid=0407 split=01 intf=02 # Aufteilen und Schnittstelle 2 automatisch verbinden
- DENY: vid=1050 pid=0407 split=1 intf=03 # Remoting von Schnittstelle 03 verhindern

Sie können einen der folgenden Filterparameter verwenden, um Regeln auf die erkannten Geräte anzuwenden:

Filterparameter	Beschreibung
vid=xxxx	Hersteller-ID des USB-Geräts (vierstelliger Hexadezimalcode)
pid=xxxx	Produkt-ID des USB-Geräts (vierstelliger Hexadezimalcode)
rel=xxxx	Release-ID des USB-Geräts (vierstelliger Hexadezimalcode)
class=xx	Klassencode des USB-Geräts (zweistelliger Hexadezimalcode)
subclass=xx	Unterklassencode des USB-Geräts (zweistelliger Hexadezimalcode)
prot=xx	Protokollcode des USB-Geräts (zweistelliger Hexadezimalcode)
split=1 (oder split=0)	Aufteilen (oder Nichtaufteilen) eines Verbundgeräts
intf=xx[,xx,xx,...]	Auswahl einer bestimmten Gruppe untergeordneter Schnittstellen eines Verbundgeräts (durch Kommas getrennte Liste mit zweistelligen Hexadezimalcodes)

Mit den ersten sechs Parametern werden die USB-Geräte ausgewählt, auf die die Regel angewendet werden soll. Wenn kein Parameter definiert ist, wird die Regel einem Gerät mit einem BELIEBIGEN Wert für diesen Parameter zugeordnet.

Das USB Implementers Forum (USB-IF) bietet unter [Defined Class Codes](#) eine Liste definierter Klassen-, Unterklassen- und Protokollwerte. USB-IF bietet außerdem eine Liste registrierter Hersteller-IDs.

Hersteller-, Produkt-, Release- und Schnittstellen-ID eines Geräts finden Sie auch in der Windows-Geräteverwaltung oder mithilfe kostenloser Tools wie USBTreeView.

Die letzten beiden Parameter gelten (sofern vorhanden) nur für USB-Verbundgeräte. Der `split`-Parameter legt fest, ob ein Verbundgerät als aufgeteiltes Gerät oder als einzelnes Verbundgerät weitergeleitet werden soll.

- `Split=1` zeigt an, dass die ausgewählten untergeordneten Schnittstellen eines Verbundgeräts als aufgeteilte Geräte weiterzuleiten sind.
- `Split=0` zeigt an, dass das Verbundgerät nicht aufgeteilt werden darf.

#### **Hinweis:**

Ist der `split`-Parameter nicht vorhanden, wird dies als `Split=0` interpretiert.

Der `intf`-Parameter wählt die untergeordneten Schnittstellen des Verbundgeräts aus, auf die eine Aktion anzuwenden ist. Ist der Parameter nicht vorhanden, wird die Aktion auf alle Schnittstellen des Verbundgeräts angewendet.

Das folgende Headset ist ein USB-Verbundgerät mit drei Schnittstellen:

- Schnittstelle 0: Geräteendpunkte der Audioklasse
- Schnittstelle 3: Geräteendpunkte der HID-Klasse (Tasten für Lautstärkeregelung und Stumm-schaltung)
- Schnittstelle 5: Schnittstelle für Verwaltung/Aktualisierung

Folgende Regeln werden für diese Gerätetypen empfohlen:

- CONNECT: `vid=047F pid=C039 split=1 intf=03` # Eingabegerät zulassen und automatisch verbinden
- DENY: `vid=047F pid=C039 split=1 intf=00` # Audioendpunkte ablehnen
- ALLOW: `vid=047F pid=C039 split=1 intf=05` # Verwaltungsschnittstelle zulassen aber nicht automatisch verbinden

#### **Aktivieren der Richtlinie für Geräteregele:**

Die Citrix Workspace-App für Windows enthält mehrere Standardgeräteregele, mit denen unerwünschte Geräteklassen herausgefiltert werden und eine vom Kunden häufig verwendete Klasse zugelassen wird.

Sie finden diese Standardgeräteregele in der Systemregistrierung für:

- `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\GenericUSB` (32-Bit-Windows) oder
- `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\ICA Client\GenericUSB` (64 Bit Windows), im Wert der mehrteiligen Zeichenfolge **DeviceRules**.

In der Citrix Workspace-App für Windows können Sie diese Standardregeln jedoch mit der Richtlinie **USB-Geräteregeln** überschreiben.

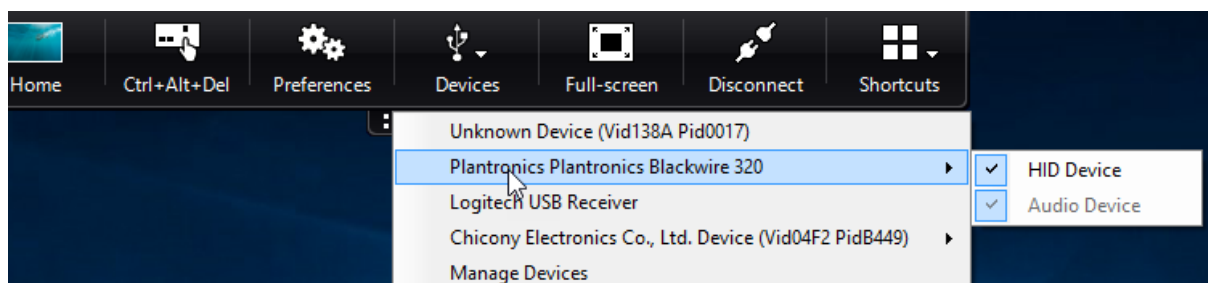
Aktivieren der Richtlinie für Geräteregele für die Citrix Workspace-App für Windows:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Remoting von Clientgeräten** > **Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **USB-Geräteregeln**.
4. Wählen Sie **Aktiviert**.
5. Fügen Sie im Textfeld **USB-Geräteregeln** die gewünschten USB-Geräteregeln ein (oder bearbeiten Sie sie direkt).
6. Klicken Sie auf **Anwenden** und auf **OK**.

Citrix empfiehlt, die voreingestellten Standardregeln auf dem Client vor dem Erstellen dieser Richtlinie zu sichern, indem Sie die Originalregeln kopieren und dann neue Regeln einfügen, um das Verhalten nach Wunsch zu ändern.

### USB-Geräte anschließen:

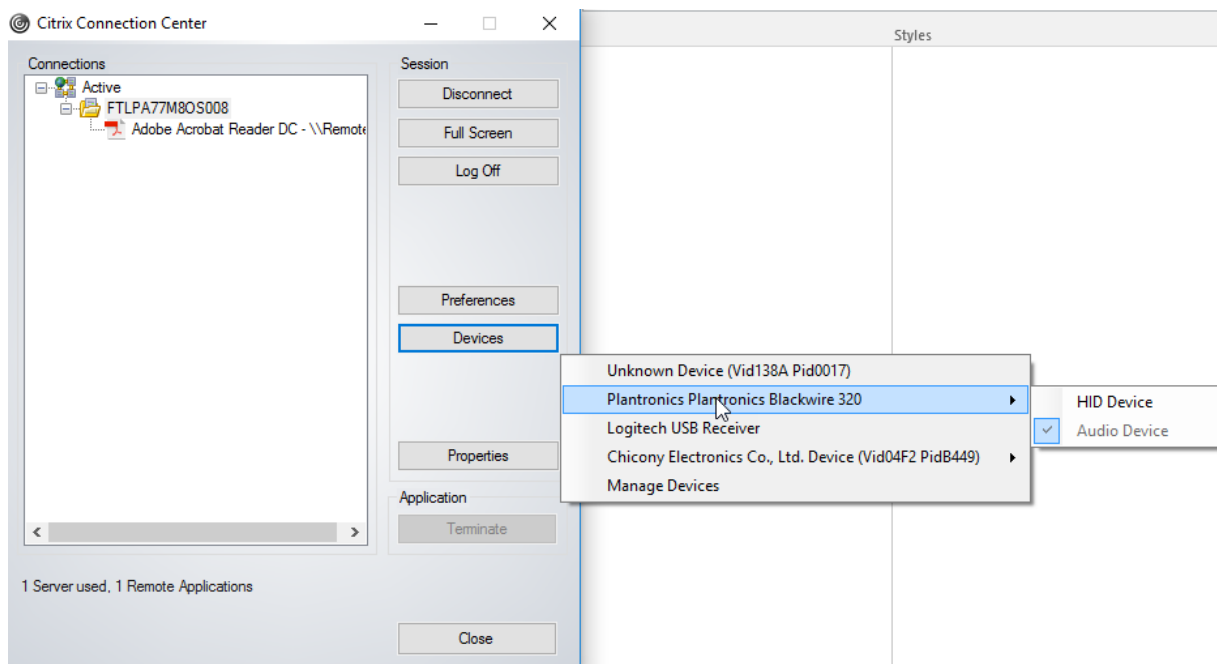
In einer Desktopsitzung werden per Splitting aufgeteilte USB-Geräte im Desktop Viewer unter **Geräte** angezeigt. Darüber hinaus werden aufgeteilte USB-Geräte unter **Einstellungen** > **Geräte** angezeigt.



#### Hinweis:

Das Schlüsselwort CONNECT aktiviert das automatische Verbinden eines USB-Geräts. Wenn Sie das Schlüsselwort CONNECT jedoch beim Aufteilen eines USB-Verbundgeräts für die generische USB-Umleitung nicht verwenden, müssen Sie das Gerät im Desktop Viewer oder Connection Center manuell auswählen, um ein zugelassenes Gerät zu verbinden.

In einer Anwendungssitzung werden per Splitting aufgeteilte USB-Geräte im **Connection Center** angezeigt.



### Automatisches Verbinden einer Schnittstelle:

Das Schlüsselwort CONNECT, das in der Citrix Workspace-App für Windows 2109 eingeführt wurde, ermöglicht das automatische Umleiten von USB-Geräten. Die CONNECT-Regel kann die ALLOW-Regel ersetzen, wenn der Administrator zulässt, dass ein Gerät oder ausgewählte Schnittstellen sich automatisch in der Sitzung verbinden.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von gpedit.msc.
2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Remoting von Clientgeräten** > **Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **USB-Geräteregeln**.
4. Wählen Sie **Aktiviert**.

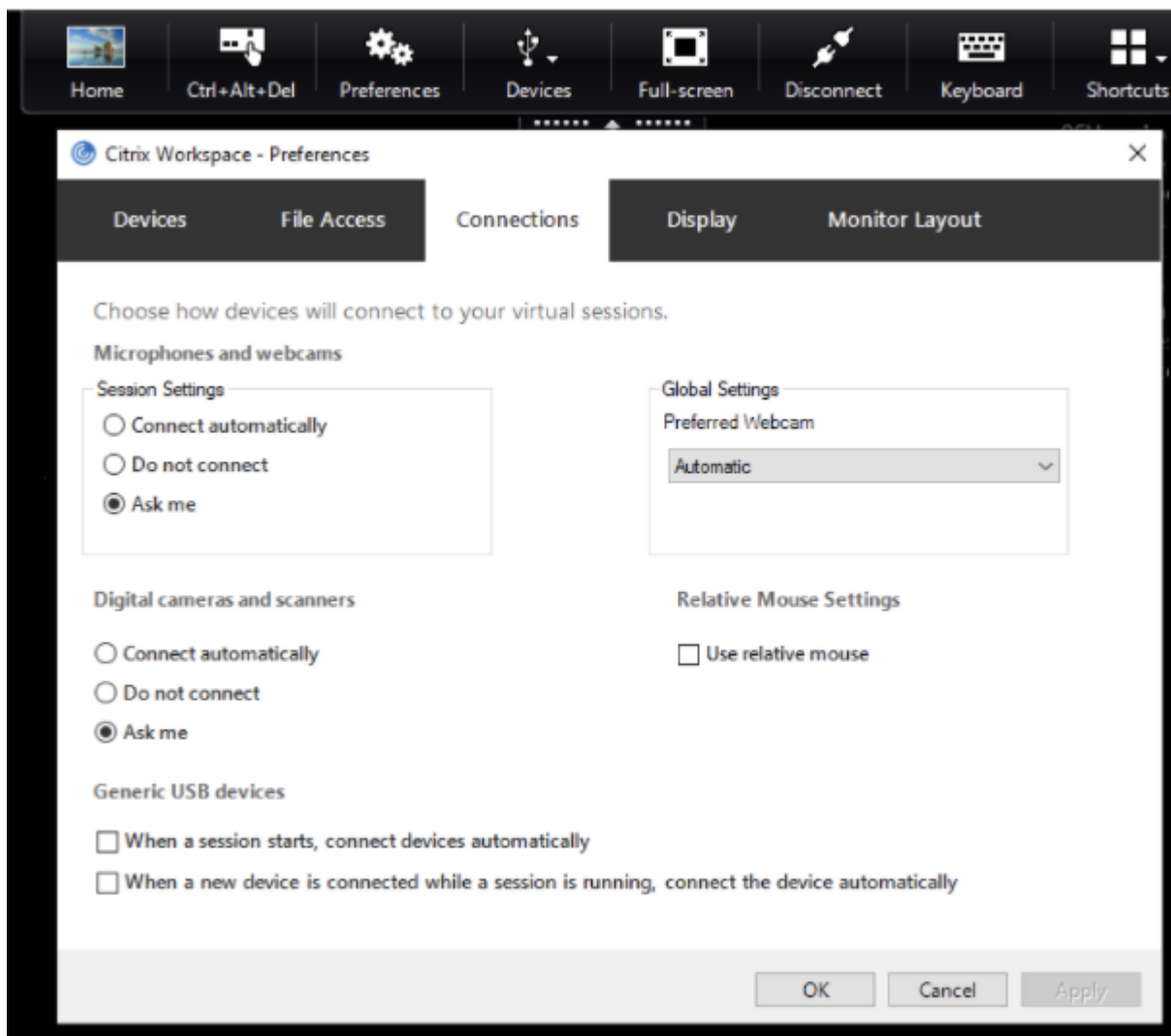
5. Fügen Sie im Textfeld **USB-Geräteregeln** das USB-Gerät hinzu, für das Sie das automatische Verbinden aktivieren möchten.

Beispiel: CONNECT: vid=047F pid=C039 split=01 intf=00.03 ermöglicht das Aufteilen eines Verbundgeräts, das automatische Verbinden der Schnittstellen 00 und 03 und die Beschränkung anderer Schnittstellen dieses Geräts.

6. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.

### Einstellungen für die automatische Verbindung von USB-Geräten ändern:

Die Citrix Workspace-App verbindet mit CONNECT-Aktion gekennzeichnete USB-Geräte automatisch gemäß den Einstellungen, die für die aktuelle Desktopressource festgelegt sind. Sie können die Einstellungen in der Symbolleiste des **Desktop Viewer** ändern, wie in der folgenden Abbildung dargestellt.



Mit den beiden Kontrollkästchen unten im Fenster legen Sie fest, ob Geräte sich automatisch verbinden oder auf eine manuelle Verbindung in der Sitzung warten müssen. Diese Einstellungen sind nicht standardmäßig aktiviert. Sie können die Einstellungen ändern, falls generische USB-Geräte automatisch verbunden werden müssen.

Ein Administrator kann die Benutzereinstellungen auch überschreiben, indem er die entsprechenden Richtlinien über die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App bereitstellt. Maschinen- und Benutzerrichtlinien finden Sie unter **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Remoting von Clientgeräten > Generisches USB-Remoting**. Die entsprechenden Richtlinien sind als “Vorhandene USB-Geräte” bzw. “Neue USB-Geräte” gekennzeichnet.

### Ändern der Standardeinstellung für aufgeteilte Geräte:

Standardmäßig werden Verbundgeräte von der Citrix Workspace-App für Windows nur dann aufgeteilt, wenn sie in den Geräteregelein explizit mit *Split=1* gekennzeichnet sind. Dieses Standardverhalten lässt sich jedoch ändern, um alle Verbundgeräte aufzuteilen, die nicht mit *Split=0* in einer zugeordneten Geräteregelein gekennzeichnet sind.

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Benutzerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Remoting von Clientgeräten** > **Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **SplitDevices** (Geräte teilen).
4. Wählen Sie **Aktiviert**.
5. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.

#### Hinweis:

Citrix empfiehlt, aufzuteilende Geräte oder Schnittstellen über explizite Geräteregelein festzulegen, anstatt die Standardeinstellung zu ändern. Diese Einstellung wird in einem zukünftigen Release ausgemustert.

### Einschränkung:

- Citrix empfiehlt, Schnittstellen für eine Webcam nicht per Splitting aufzuteilen. Als Workaround können Sie das Gerät über die generische USB-Umleitung an ein einzelnes Gerät weiterleiten. Verwenden Sie zur Leistungsverbesserung den optimierten virtuellen Kanal.
- Manchmal werden USB-Verbundgeräte möglicherweise nicht automatisch aufgeteilt, obwohl eine korrekte Geräteumleitungsregel festgelegt ist, um das Gerät aufzuteilen. Das Problem tritt auf, weil sich das Gerät im Energiesparmodus befindet. In diesen Fällen ist das untergeordnete Gerät, das in den Energiesparmodus wechselt, möglicherweise nicht in der Geräteliste enthalten. Sie können folgende Problemumgehungen verwenden, um dieses Problem zu lösen:
  - Trennen Sie die Sitzung, schließen Sie das USB-Gerät an und stellen Sie erneut eine Verbindung zur Sitzung her.
  - Trennen Sie das USB-Gerät und schließen Sie es wieder an. Diese Aktion führt dazu, dass das Gerät den Energiesparmodus verlässt. [HDX-34143]

### Bloomberg-Tastaturen

Die Citrix Workspace-App unterstützt die Verwendung einer Bloomberg-Tastatur in Sitzungen mit virtuellen Apps und Desktops. Die erforderlichen Komponenten werden mit dem Plug-In installiert.

Sie können das Feature für Bloomberg-Tastaturen zusammen mit der Citrix Workspace-App für Windows installieren oder über die Registrierung aktivieren.

Im Vergleich zu Standardtastaturen bieten Bloomberg-Tastaturen andere Funktionen, mit denen Benutzer auf Finanzmarktdaten zugreifen und Transaktionen durchführen können.

Die Bloomberg-Tastatur besteht aus mehreren USB-Geräten, die in einem Gehäuse zusammengefasst sind:

- Tastatur
- Fingerabdruckleser
- Audiogerät
- USB-Hub zum Anschluss all dieser Geräte an das System
- HID-Tasten für das Audiogerät, z. B. zum Stummschalten und zur Lautstärkeregelung

Zusätzlich zu den Standardfunktionen dieser Geräte unterstützt das Audiogerät diverse Tasten und Tastatur-LEDs und eine Steuerung der Tastatur.

Um die Spezialfunktionen in einer Sitzung zu verwenden, müssen Sie das Audiogerät als USB-Gerät umleiten. Dadurch wird das Audiogerät für die Sitzung verfügbar, es kann jedoch nicht mehr lokal verwendet werden. Die Spezialfunktionen können zudem nur von einer Sitzung und nicht von mehreren Sitzungen gemeinsam genutzt werden.

Mehrere Sitzungen mit Bloomberg-Tastaturen sind nicht empfehlenswert. Die Tastatur funktioniert nur in Einzelsitzungen.

### **Konfigurieren der Bloomberg-Tastatur 5:**

Ab Version 2109 der Citrix Workspace-App für Windows wird ein neues CONNECT-Schlüsselwort eingeführt, das die automatische Verbindung von USB-Geräten beim Sitzungsstart und Anschließen von Geräten ermöglicht. Das Schlüsselwort CONNECT kann anstelle des Schlüsselworts ALLOW verwendet werden, wenn ein Benutzer ein USB-Gerät oder eine Schnittstelle automatisch verbinden möchte.

#### **Hinweis:**

Mit der Einführung der Geräteumleitungsregeln Version 2 in Studio in Citrix Virtual Apps and Desktops muss die Bloomberg 5-Tastatur nicht über clientseitige Gruppenrichtlinien in der Citrix Workspace-App für Windows konfiguriert werden. Weitere Informationen finden Sie unter [Regeln für die Client-USB-Geräteumleitung \(Version 2\)](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Für Versionen vor Version 2212 der Citrix Workspace-App für Windows wird im folgenden Beispiel gezeigt, wie das CONNECT-Schlüsselwort zu verwenden ist:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.

2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace > Remoting von Clientgeräten > Generisches USB-Remoting**.
3. Wählen Sie die Richtlinie **SplitDevices** (Geräte teilen).
4. Wählen Sie **Aktiviert**.
5. Fügen Sie im Textfeld **USB-Geräteregeln** die folgenden Regeln hinzu, falls sie noch nicht vorhanden sind.
  - CONNECT: vid=1188 pid=A101 # Biometrisches Bloomberg-Modul 5
  - DENY: vid=1188 pid=A001 split=01 intf=00 # Primäre Bloomberg-Tastatur 5
  - CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg-Tastatur 5 - Eingabegerät
  - DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg-Tastatur 5 - Audiokanal
  - CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg-Tastatur 5 - Audio-Eingabegerät

**Hinweis:**

Zeilenumbruch oder Semikolon können verwendet werden, um Regeln zu trennen, sodass ein- oder mehrzeilige Registrierungswerte gelesen werden können.

6. Klicken Sie auf **Übernehmen** und auf **OK**, um die Richtlinie zu speichern.
7. Wählen Sie im Fenster **Einstellungen** die Registerkarte **Verbindungen** und aktivieren Sie ein oder beide Kontrollkästchen, um Geräte automatisch zu verbinden. Das Fenster **Einstellungen** kann über die Desktopsymbolleiste oder den Verbindungsmanager geöffnet werden.

Mit diesem Verfahren wird die Bloomberg-Tastatur 5 einsatzbereit. Mit den DENY-Regeln in der Schrittfolge erzwingen Sie, dass die primäre Tastatur und der Audiokanal nicht über generisches USB, sondern über einen optimierten Kanal umgeleitet werden. Mit den CONNECT-Regeln aktivieren Sie die automatische Umleitung des Fingerabdruckmoduls, von Sondertasten auf der Tastatur und von Tasten zur Audiosteuerung.

**Konfigurieren der Bloomberg-Tastatur 4 oder 3:**

**Achtung**

Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Erstellen Sie auf jeden Fall ein Backup der Registrierung, bevor Sie sie bearbeiten.



1. Gehen Sie zu folgendem Schlüssel in der Registrierung:

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

2. Führen Sie einen der folgenden Schritte aus:

- Zum Aktivieren dieses Features müssen Sie den Eintrag mit Typ DWORD und dem Namen **EnableBloombergHID** auf den Wert 1 setzen.
- Zum Deaktivieren dieses Features setzen Sie den Wert auf 0.

Unterstützung für die Bloomberg-Tastatur 3 ist im Online-Plug-In für Windows ab Version 11.2 verfügbar.

Unterstützung für die Bloomberg-Tastatur 4 ist für Windows Receiver 4.8 und höher verfügbar.

#### **Prüfung auf aktivierte Unterstützung für Bloomberg-Tastaturen:**

- Um festzustellen, ob die Bloomberg-Tastaturunterstützung im Online-Plug-In aktiviert ist, prüfen Sie, ob die Bloomberg-Tastaturgeräte im Desktop Viewer angezeigt werden. Wenn der Desktop Viewer nicht verwendet wird, können Sie die Registrierung auf der Maschine überprüfen, auf der das Online-Plug-In ausgeführt wird.
- Bei nicht aktivierter Unterstützung für Bloomberg-Tastaturen wird Folgendes im Desktop Viewer angezeigt:
  - zwei Geräte für die Bloomberg-Tastatur 3, angezeigt als **Bloomberg Fingerprint Scanner** und **Bloomberg Keyboard Audio**.
  - ein Gerät mit Richtlinienumleitung für die Bloomberg-Tastatur 4. Dieses Gerät wird als **Bloomberg LP Keyboard 2013** angezeigt.
- Bei aktivierter Unterstützung für Bloomberg-Tastaturen werden zwei Geräte im Desktop Viewer angezeigt. Ein Gerät wird wie zuvor als **Bloomberg Fingerprint Scanner** angezeigt und ein Gerät als **Bloomberg Keyboard Features**.
- Bei nicht installiertem Treiber für den Bloomberg-Fingerabdruckscanner wird der zugehörige Eintrag möglicherweise nicht im Desktop Viewer angezeigt. Fehlt der Eintrag, steht der Bloomberg-Fingerabdruckscanner möglicherweise nicht für die Umleitung zur Verfügung. Sie können weiterhin den Namen des anderen Bloomberg-Geräts suchen, falls die Unterstützung für Bloomberg-Tastaturen aktiviert ist.
- Sie können auch anhand des Werts in der Registrierung überprüfen, ob die Unterstützung aktiviert ist:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB\EnableBloombergHID`

Ist der Wert nicht vorhanden oder auf 0 (null) gesetzt, werden Bloomberg-Tastaturen nicht unterstützt. Wird der Wert 1 angezeigt, ist die Unterstützung aktiviert.

## Aktivieren der Unterstützung für Bloomberg-Tastaturen:

### Hinweis:

Mit Citrix Receiver für Windows 4.8 wurde Unterstützung für zusammengesetzte Geräte über die Richtlinie **Geräte teilen** eingeführt. Für die Bloomberg-Tastatur 4 müssen Sie jedoch anstelle der Richtlinie das Bloomberg-Tastaturfeature verwenden.

Die Unterstützung der Bloomberg-Tastatur ändert die Art und Weise, wie bestimmte USB-Geräte zu einer Sitzung umgeleitet werden. Diese Unterstützung ist nicht standardmäßig aktiviert.

- Um die Unterstützung während der Installation zu aktivieren, legen Sie an der Befehlszeile der Installation die Eigenschaft **ENABLE\_HID\_REDIRECTION** auf den Wert "TRUE" fest. Beispiel:

```
CitrixOnlinePluginFull.exe /silent  
ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"  
ENABLE_SSON="no"INSTALLDIR="c:\test"  
ENABLE_DYNAMIC_CLIENT_NAME="Yes"  
DEFAULT_NDSCONTEXT="Context1,Context2"  
SERVER_LOCATION="http://testserver.net"ENABLE_HID_REDIRECTION="TRUE"
```

- Um die Unterstützung nach der Installation des Online-Plug-Ins zu aktivieren, bearbeiten Sie die Windows-Registrierung auf dem System, auf dem das Online-Plug-In ausgeführt wird:
  1. Öffnen Sie den Registrierungs-Editor.
  2. Navigieren Sie zu folgendem Schlüssel:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
  3. Wenn der Wert **EnableBloombergHID** vorhanden ist, ändern Sie den Wert zu 1.
  4. Wenn der Wert **EnableBloombergHID** nicht vorhanden ist, erstellen Sie einen DWORD-Wert namens EnableBloombergHID und geben Sie als Wert 1 an.

## Deaktivieren der Unterstützung für die Bloomberg-Tastatur:

Sie können die Unterstützung für die Bloomberg-Tastatur im Online-Plug-In wie folgt deaktivieren:

1. Öffnen Sie den Registrierungs-Editor auf dem System, auf dem das Online-Plug-In ausgeführt wird.
2. Navigieren Sie zu folgendem Schlüssel:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
3. Wenn der Wert **EnableBloombergHID** vorhanden ist, ändern Sie den Wert zu 0 (null).

Wenn der Wert **EnableBloombergHID** nicht vorhanden ist, ist die Unterstützung für die Bloomberg-Tastatur nicht aktiviert. In diesem Fall müssen Sie keine Registrierungswerte ändern.

### **Bloomberg-Tastaturen ohne aktivierte Unterstützung verwenden:**

- Sie können die Tastatur auch bei nicht aktivierter Bloomberg-Tastaturunterstützung im Online-Plug-In verwenden. Sie können dann jedoch nicht die Spezialfunktionen für mehrere Sitzungen freigeben und benötigen unter Umständen mehr Netzwerkbandbreite für Audiodaten.
- Die Standardtasten von Bloomberg-Tastaturen stehen wie bei jeder anderen Tastatur zur Verfügung. Sie müssen keine besondere Aktion ergreifen.
- Zur Verwendung der Bloomberg-Spezialtasten müssen Sie das Audiogerät der Bloomberg-Tastatur in die Sitzung umleiten. Wenn Sie den Desktop Viewer verwenden, werden der Herstellername und der Geräte name der USB-Geräte sowie **Bloomberg Keyboard Audio** für das Audiogerät der Bloomberg-Tastatur angezeigt.
- Um den Fingerabdruckleser zu verwenden, müssen Sie das Gerät zu “Bloomberg Fingerprint Scanner” umleiten. Wenn die Treiber für den Fingerabdruckleser nicht lokal installiert sind, zeigt das Gerät nur an:
  - ob das Online-Plug-In eine automatische Verbindung von Geräte erlaubt, oder
  - dass der Benutzer auswählen kann, ob Geräte verbunden werden sollen.

Wenn die Bloomberg-Tastatur vor dem Einrichten der Sitzung verbunden ist und die Treiber für den Fingerabdruckleser nicht lokal vorhanden sind, wird der Fingerabdruckleser nicht angezeigt und kann in der Sitzung nicht verwendet werden.

#### **Hinweis:**

Bei Verwendung von Bloomberg 3 kann der Fingerabdruckleser von einer einzelnen Sitzung oder dem lokalen System verwendet, aber nicht freigegeben werden. Bloomberg 4 darf nicht umgeleitet werden.

### **Bloomberg-Tastaturen nach dem Aktivieren der Unterstützung verwenden:**

- Wenn Sie die Unterstützung für Bloomberg-Tastaturen im Online-Plug-In aktivieren, können Sie die Spezialtastenfunktionen in mehreren Sitzungen verwenden. Außerdem ist weniger Netzwerkbandbreite für Audiodaten erforderlich.
- Bei aktivierter Unterstützung der Bloomberg-Tastatur kann das Audiogerät der Bloomberg-Tastatur nicht umgeleitet werden. Stattdessen wird ein neues Gerät zur Verfügung gestellt. Wenn Sie den Desktop Viewer verwenden, wird dieses Gerät als “Bloomberg Keyboard Features” angezeigt. Durch Umleiten dieses Geräts werden die Bloomberg-Spezialtasten in der Sitzung verfügbar.

Das Aktivieren der Unterstützung der Bloomberg-Tastatur wirkt sich nur auf die Bloomberg-Spezialtasten und das Audiogerät aus. Die Standardtasten und der Fingerabdruckleser werden wie bei nicht aktivierter Unterstützung verwendet.

## HDX Plug-n-Play-USB-Geräteumleitung

Die HDX Plug-n-Play USB-Geräteumleitung ermöglicht die dynamische Umleitung von Mediengeräten zum Server. Mediengeräte können Kameras, Scanner, Mediaplayer und POS-Geräte sein. Sie oder der Benutzer können die Umleitung auf einige oder alle Geräte beschränken. Bearbeiten Sie die Richtlinien auf dem Server oder wenden Sie Gruppenrichtlinien auf dem Benutzergerät an, um die Einstellungen für die Umleitung zu konfigurieren. Weitere Informationen finden Sie unter [Überlegungen zu USB und Clientlaufwerk](#) in der Citrix Virtual Apps and Desktops-Dokumentation.

### Wichtig:

Wenn Sie die USB-Geräteumleitung für Plug & Play-Geräte in einer Serverrichtlinie verbieten, kann der Benutzer diese Richtlinieneinstellung nicht außer Kraft setzen.

Ein Benutzer kann Berechtigungen in der Citrix Workspace-App festlegen, um die Geräteumleitung immer oder nie zuzulassen, oder bei jedem angeschlossenen Gerät benachrichtigt werden. Diese Einstellung wirkt sich nur auf Geräte aus, die eingesteckt werden, nach dem der Benutzer die Einstellung geändert hat.

## Zuordnen eines COM-Ports für Clients zu einem Server-COM-Port

Mit der Client-COM-Portzuordnung können Geräte, die an COM-Ports des Benutzergeräts angeschlossen sind, in Sitzungen verwendet werden. Diese Zuordnungen können in gleicher Weise wie andere Netzwerkzuordnungen verwendet werden.

Sie können Client-COM-Ports von der Befehlszeile aus zuordnen. Sie können auch die Client-COM-Portzuordnung vom Remotedesktop-Konfigurationstool (Terminaldienste) oder mit Richtlinien steuern. Informationen zu Richtlinien finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

### Wichtig:

Die Zuordnung von COM-Ports ist nicht mit TAPI kompatibel.

1. Aktivieren Sie für Citrix Virtual Apps and Desktops-Bereitstellungen die Richtlinieneinstellung "Client-COM-Portumleitung".
2. Melden Sie sich bei der Citrix Workspace-App an.
3. Geben Sie an der Eingabeaufforderung Folgendes ein:

```
net use comx: \\client\comz:
```

Wobei:

- x ist die Nummer des COM-Ports auf dem Server (Ports 1 bis 9 stehen für die Zuordnung zur Verfügung).

- z ist die Nummer des Client-COM-Ports, den Sie zuordnen möchten.

4. Geben Sie zur Bestätigung des Vorgangs

```
net use
```

Die Eingabeaufforderung enthält zugeordnete Laufwerke, LPT-Ports und zugeordnete COM-Ports.

Installieren Sie das Gerät für den zugeordneten Namen, um diesen COM-Port in einem virtuellen Desktop oder einer Anwendung zu verwenden. Wenn Sie beispielsweise den Port COM1 auf dem Client dem Port COM5 auf dem Server zuordnen, installieren Sie das COM-Portgerät in der Sitzung auf COM5. Verwenden Sie diesen zugeordneten COM-Port dann wie einen COM-Port auf dem Benutzergerät.

## USB-Audio konfigurieren

### Hinweis:

- Wenn Sie die Citrix Workspace-App für Windows zum ersten Mal installieren oder aktualisieren, fügen Sie dem lokalen Gruppenrichtlinienobjekt die neuesten Vorlagendateien hinzu. Weitere Informationen über das Hinzufügen von Vorlagendateien zum lokalen Gruppenrichtlinienobjekt finden Sie unter [Administrative Gruppenrichtlinienobjektvorlage](#). Bei einem Upgrade bleiben die vorhandenen Einstellungen erhalten, während die neuesten Dateien importiert werden.
- Dieses Feature ist nur für Citrix Virtual Apps-Server verfügbar.

### USB-Audiogeräte konfigurieren:

1. Öffnen Sie die administrative Gruppenrichtlinienobjektvorlage der Citrix Workspace-App durch Ausführen von `gpedit.msc`.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen > Klassische administrative Vorlagen (ADM) > Citrix Komponenten > Citrix Workspace > Benutzererfahrung** und wählen Sie **Audio über generische USB-Umleitung**.
3. Bearbeiten Sie die Einstellungen.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Öffnen Sie eine Eingabeaufforderung im Administratormodus.
6. Führen Sie den folgenden Befehl aus  
`gpupdate /force`.

## Massenspeichergeräte

Nur bei Massenspeichergeräten ist der Remotezugriff neben USB-Unterstützung auch durch Clientlaufwerkzuordnung verfügbar. Sie können dies in der Citrix Workspace-App für Windows über die

Richtlinie **Remoting von Clientgeräten > Clientlaufwerkzuordnung** konfigurieren. Wenn Sie diese Richtlinie anwenden, werden die Laufwerke auf dem Benutzergerät automatisch den Laufwerksbuchstaben auf dem virtuellen Desktop zugeordnet, wenn Benutzer sich anmelden. Die Laufwerke werden als freigegebene Ordner mit zugeordneten Laufwerksbuchstaben angezeigt.

Die Hauptunterschiede zwischen den beiden Typen der Remotingrichtlinie sind:

Feature	Clientlaufwerkzuordnung	USB-Unterstützung
Diese Option ist in der Standardeinstellung aktiviert.	Ja	Nein
Konfigurierbare Leserechte	Ja	Nein
Sicheres Entfernen des Geräts in einer Sitzung	Nein	Ja, wenn der Benutzer im Infobereich auf Hardware sicher entfernen klickt.

Wenn Sie die Richtlinien für die generische USB-Umleitung und die Clientlaufwerkzuordnung aktivieren und vor dem Sitzungsstart ein Massenspeichergerät anschließen, wird es zuerst mit der Clientlaufwerkzuordnung umgeleitet, bevor eine Umleitung mit USB-Unterstützung erwogen wird. Wenn das Gerät nach dem Sitzungsstart angeschlossen wird, wird die Umleitung mit der USB-Unterstützung vor der Clientlaufwerkzuordnung erwogen.

## Clientlaufwerkzuordnung

April 22, 2024

Die Clientlaufwerkzuordnung unterstützt die Datenübertragung zwischen Host und Client als Stream. Die Dateiübertragung passt sich an veränderliche Netzwerkdurchsatzbedingungen an. Dabei wird außerdem jede verfügbare zusätzliche Bandbreite genutzt, um die Datenübertragungsrate zu erhöhen.

Standardmäßig ist dieses Feature aktiviert.

Um das Feature zu deaktivieren, legen Sie den folgenden Registrierungsschlüssel fest und starten Sie den Server neu:

Pfad: `HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters`  
 Name: `DisableFullStreamWrite`  
 Typ: `REG_DWORD`  
 Wert:

0x01 = deaktiviert,

0 oder Wert löschen = aktiviert

Die Citrix Workspace-App für Windows unterstützt die Gerätezuordnung auf Benutzergeräten, sodass sie in einer Sitzung zur Verfügung stehen. Benutzer haben folgende Möglichkeiten:

- Zugreifen auf lokale Laufwerke, Drucker und COM-Ports
- Ausschneiden und Einfügen zwischen der Sitzung und der lokalen Windows-Zwischenablage
- Wiedergeben von Audiodateien (Systemklänge und WAV-Dateien), die in der Sitzung abgespielt werden

Während der Anmeldung informiert die Citrix Workspace-App den Server über die verfügbaren Clientlaufwerke, COM- und LPT-Ports. Standardmäßig werden Clientlaufwerke Serverlaufwerksbuchstaben zugeordnet. Für Clientdrucker werden Druckerwarteschlangen erstellt, sodass die Clientdrucker direkt mit der Sitzung verbunden zu sein scheinen. Diese Zuordnungen stehen nur dem aktuellen Benutzer während der aktuellen Sitzung zur Verfügung. Sie werden bei der Abmeldung des Benutzers gelöscht und bei seiner nächsten Anmeldung neu erstellt.

Mit den Einstellungen der Richtlinie für die Umleitung können Sie Benutzergeräte zuordnen, die nicht automatisch bei der Anmeldung zugeordnet werden. Weitere Informationen finden Sie in der Dokumentation zu Citrix Virtual Apps and Desktops.

## Deaktivieren von Benutzergerätozuordnungen

Sie können die Benutzergerätozuordnung einschließlich Optionen für Laufwerke, Drucker und Ports mit dem **Windows-Servermanager** einstellen. Weitere Informationen über verfügbare Optionen finden Sie in der Dokumentation zu den Remotedesktopdiensten.

## Umleiten von Clientordnern

Durch die Clientordnerumleitung ändert sich der Zugriff auf clientseitige Dateien bei der hostseitigen Sitzung. Wenn auf dem Server nur die Clientlaufwerkzuordnung aktiviert ist, werden die clientseitigen vollständigen Volumes den Sitzungen automatisch als UNC-Link (Universal Naming Convention) zugeordnet. Wenn Sie die Clientordnerumleitung auf dem Server aktivieren und der Benutzer sie auf dem Benutzergerät konfiguriert, wird der Teil des vom lokalen Benutzer angegebenen lokalen Volumes umgeleitet.

Nur die vom Benutzer angegebenen Ordner (und nicht das komplette Dateisystem auf dem Benutzergerät) werden als UNC-Links in den Sitzungen angezeigt. Wenn Sie UNC-Links durch die Registrierung deaktivieren, werden Clientordner als zugeordnete Laufwerke in der Sitzung angezeigt. Weitere Informationen, u. a. zur Konfiguration der Umleitung von Clientordnern für Benutzergeräte, finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

## Zuordnen von Clientlaufwerken zu serverseitigen Laufwerksbuchstaben

Durch die Clientlaufwerkzuordnung werden Laufwerksbuchstaben auf der Hostseite auf Laufwerke umgeleitet, die auf dem Benutzergerät vorhanden sind. Beispiel: In einer Citrix Benutzersitzung kann das Laufwerk H dem Laufwerk C auf dem Benutzergerät, auf dem die Citrix Workspace-App für Windows ausgeführt wird, zugeordnet werden.

Die Clientlaufwerkzuordnung ist in die Standardfunktionen von Citrix zur Geräteumleitung integriert. Im Dateimanager, Windows Explorer und in den Anwendungen werden diese Zuordnungen genauso wie andere Netzwerkzuordnungen angezeigt.

Der Server, auf dem virtuelle Desktops und Anwendungen ausgeführt werden, kann während der Installation so konfiguriert werden, dass Clientlaufwerke automatisch einem festgelegten Satz von Laufwerksbuchstaben zugeordnet werden. In der Standardinstallation werden Laufwerksbuchstaben angefangen mit V und dann absteigend Clientlaufwerksbuchstaben zugeordnet. Ein Laufwerksbuchstabe wird jeder Festplatte und jedem CD-ROM-Laufwerk zugeordnet. (Diskettenlaufwerken werden die vorhandenen Laufwerksbuchstaben zugewiesen.) Diese Methode ergibt die folgenden Laufwerkzuordnungen in einer Sitzung:

Clientlaufwerksbuchstabe	Zugriff vom Server möglich als
A	A
B	B
C	V
D	U

Der Server kann so konfiguriert werden, dass zwischen den Laufwerksbuchstaben des Servers und des Clients keine Konflikte entstehen. Dazu werden die Laufwerksbuchstaben des Servers in höhere Laufwerksbuchstaben geändert.

Im folgenden Beispiel werden die Serverlaufwerke C und D in M und N geändert, sodass Clientgeräte direkt auf ihre Laufwerke C und D zugreifen können. Diese Methode führt zu den folgenden Laufwerkzuordnungen in einer Sitzung:

Clientlaufwerksbuchstabe	Zugriff vom Server möglich als
A	A
B	B
C	C
D	D



Der Laufwerksbuchstabe, durch den das Serverlaufwerk C ersetzt wird, wird während des Setups festgelegt. Alle anderen Festplatten- und CD-Laufwerksbuchstaben werden durch aufeinander folgende Laufwerksbuchstaben ersetzt (zum Beispiel: C > M, D > N, E > O). Bei diesen Laufwerksbuchstaben darf es keine Konflikte mit bereits existierenden Laufwerkszuordnungen im Netzwerk geben. Wenn Sie das Netzlaufwerk einem bereits vorhandenen Laufwerksbuchstaben eines Servers zuordnen, ist die Netzlaufwerkzuordnung ungültig.

Beim Verbinden eines Benutzergeräts mit einem Server werden die Clientzuordnungen wiederhergestellt, sofern die automatische Clientgerätszuordnung nicht deaktiviert ist. Die Clientlaufwerkzuordnung ist standardmäßig aktiviert. Sie können die Einstellungen mit dem Konfigurationstool der Remotedesktopdienste (Terminaldienste) ändern. Außerdem können Sie mit Richtlinien genauer steuern, wie die Clientgerätszuordnung angewendet wird. Weitere Informationen zu Richtlinien finden Sie in der Citrix Virtual Apps and Desktops-Dokumentation.

## Mikrofon

April 22, 2024

Die Citrix Workspace-App unterstützt die mehrfache clientseitige Mikrofoneingabe. Sie können lokal installierte Mikrofone für Folgendes verwenden:

- Echtzeitaktivitäten, wie Softphone-Anrufe und Webkonferenzen
- Gehostete Aufzeichnungsanwendungen, z. B. Diktierprogramme
- Video- und Audio-Aufzeichnungen

Benutzer der Citrix Workspace-App können in Connection Center auswählen, ob am Gerät angeschlossene Mikrofone verwendet werden sollen. Benutzer von Citrix Virtual Apps and Desktops und Citrix DaaS können außerdem ihre Mikrofone und Webcams im Citrix Virtual Apps and Desktops sowie und Citrix DaaS-Viewer unter “Einstellungen” deaktivieren.

## Gruppenrichtlinie

April 22, 2024

### Administrative Gruppenrichtlinienobjektvorlage

Wir empfehlen die administrative Gruppenrichtlinienobjektvorlage zum Konfigurieren von Regeln für Folgendes:

- Netzwerkrouting
- Proxyserver
- Konfiguration vertrauenswürdiger Server
- Benutzerrouting
- Remote-Benutzergeräte
- Benutzererfahrung

Sie können die Vorlagendateien `receiver.admx` / `receiver.adml` für Domänenrichtlinien und lokale Computerrichtlinien verwenden. Importieren Sie die Vorlagendatei für Domänenrichtlinien mit der Gruppenrichtlinien-Verwaltungskonsole. Der Import ist nützlich, wenn Sie Citrix Workspace-App-Einstellungen auf mehrere verschiedene Benutzergeräte im Unternehmen anwenden möchten. Wenn Sie nur ein einziges Benutzergerät ändern möchten, importieren Sie die Vorlagendatei mit dem lokalen Gruppenrichtlinien-Editor auf dem Gerät.

Citrix empfiehlt die Verwendung der administrativen Gruppenrichtlinienobjektvorlage von Windows für die Konfiguration der Citrix Workspace-App.

Im Installationsverzeichnis befinden sich die Dateien `CitrixBase.admx` und `CitrixBase.adml` sowie administrative Vorlagendateien (`receiver.adml` oder `receiver.admx` 'receiver.adml').

**Hinweis:**

Die ADMX- und ADML-Dateien sind für die Verwendung mit der in der [Kompatibilitätsmatrix](#) genannten [Windows-Version](#) vorgesehen.

Wird die Citrix Workspace-App mit dem VDA installiert, sind die ADMX/ADML-Dateien normalerweise im Verzeichnis `\<installation directory>\Online Plugin\Configuration`.

Wird die Citrix Workspace-App ohne den VDA installiert, sind die ADMX/ADML-Dateien normalerweise im folgenden Verzeichnis zu finden.

- Für 64 Bit: `C:\Program Files (x86)\Citrix\ICA Client\Configuration directory`
- Für (32 Bit): `C:\Program Files\Citrix\ICA Client\\Configuration directory`

In der folgenden Tabelle finden Sie Informationen zu den Vorlagendateien der Citrix Workspace-App und deren Speicherorten.

**Hinweis:**

Citrix empfiehlt, dass Sie die GPO-Vorlagendateien verwenden, die mit der aktuellen Version der Citrix Workspace-App bereitgestellt werden.

Dateityp	Dateispeicherort
receiver.adm	\\ICA Client\\Configuration
receiver.admx	\\ICA Client\\Configuration
receiver.adml	\\ICA Client\\Configuration\\[MUIculture]
CitrixBase.admx	\\ICA Client\\Configuration
CitrixBase.adml	\\ICA Client\\Configuration\\[MUIculture]

**Hinweis:**

- Wenn CitrixBase.admx\\adml nicht dem lokalen Gruppenrichtlinienobjekt hinzugefügt wird, geht möglicherweise die Richtlinie **ICA-Dateisignierung aktivieren** verloren.
- Fügen Sie beim Upgrade der Citrix Workspace-App dem lokalen Gruppenrichtlinienobjekt die neuesten Vorlagendateien hinzu. Frühere Einstellungen werden nach dem Import beibehalten. Weitere Informationen finden Sie im folgenden Verfahren:

**Hinzufügen der receiver.admx/adml-Vorlagendateien zum lokalen Gruppenrichtlinienobjekt:**

Sie können ADM-Vorlagendateien zum Konfigurieren von lokalen und domänenbasierten Gruppenrichtlinienobjekten verwenden. Weitere Informationen zum Verwalten von ADMX-Dateien finden Sie in [diesem Microsoft MSDN-Artikel](#).

Kopieren Sie nach der Installation der Citrix Workspace-App die folgenden Vorlagendateien:

Dateityp	Kopieren von	Kopieren nach
receiver.admx	Installation Directory\\ICA Client\\ Configuration\\ receiver.admx	%systemroot%\ policyDefinitions
CitrixBase.admx	Installation Directory\\ICA Client\\ Configuration\\ CitrixBase.admx	%systemroot%\ policyDefinitions

---

Dateityp	Kopieren von	Kopieren nach
receiver.adml	Installation Directory\ICA Client\ Configuration\ MUIculture]receiver. adml	%systemroot%\ policyDefinitions\ MUIculture]
CitrixBase.adml	Installation Directory\ICA Client\ Configuration\ MUIculture]\ CitrixBase.adml	%systemroot%\ policyDefinitions\ MUIculture]

---

**Hinweis:**

Fügen Sie die Dateien CitrixBase.admx/CitrixBase.adml dem Ordner `\PolicyDefinitions` hinzu, um die Vorlagendateien unter **Administrative Vorlagen > Citrix Komponenten > Citrix Workspace** anzuzeigen.

## Sitzungserfahrung

April 22, 2024

### Dauer des Anwendungsstarts

Verwenden Sie das Sitzungsvorabstartfeature, um den Anwendungsstart in Zeiten mit normalem oder hohem Netzwerkverkehr zu verkürzen und die Benutzererfahrung dadurch zu verbessern. Mit dem Vorabstartfeature kann eine Vorabstartsession erstellt werden. Eine Vorabstartsession wird erstellt, wenn ein Benutzer sich an der Citrix Workspace-App anmeldet oder zu einem geplanten Zeitpunkt (wenn der Benutzer bereits angemeldet ist).

Die Vorabstartsession verkürzt die Startzeit der ersten Anwendung. Wenn ein Benutzer eine neue Kon-  
toverbindung in der Citrix Workspace-App für Windows hinzufügt, findet der Sitzungsvorabstart erst  
in der nächsten Sitzung statt. Die Standardanwendung `ctxprelaunch.exe` wird in der Sitzung ausge-  
führt, ist jedoch für Sie unsichtbar.

Weitere Informationen finden Sie in den Anleitungen zum Vorabstart von Sitzungen und zum Sitzungsfortbestehen unter [Verwalten von Bereitstellungsgruppen](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

Der Sitzungsvorabstart ist standardmäßig deaktiviert. Geben Sie zum Aktivieren des Vorabstarts von Sitzungen den Parameter `ENABLEPRELAUNCH=true` an der Workspace-Befehlszeile an oder legen Sie den Registrierungsschlüssel `EnablePreLaunch` auf "true" fest. Die Standardeinstellung "Null" bedeutet, dass der Vorabstart deaktiviert ist.

**Hinweis:**

Wenn der Client zur Unterstützung der Domänen-Passthrough-Authentifizierung (SSON) konfiguriert wurde, ist Vorabstart automatisch aktiviert. Wenn Sie die Domänen-Passthrough-Authentifizierung (SSON) ohne Vorabstart verwenden möchten, legen Sie den Registrierungsschlüssel `EnablePreLaunch` auf "false" fest.

Die Registrierungsverzeichnisse sind:

- `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle`
- `HKEY_CURRENT_USER\Software\Citrix\Dazzle`

Es gibt zwei Arten von Vorabstart:

- **Just-In-Time-Vorabstart:** Der Vorabstart wird direkt nach dem Authentifizieren der Anmeldeinformationen des Benutzers gestartet, unabhängig davon, ob es sich um eine Zeit mit hohem Netzwerkverkehr handelt. Diese Option wird normalerweise für Zeiten mit normalen Datenverkehr verwendet. Ein Benutzer kann den Just-In-Time-Vorabstart durch einen Neustart der Citrix Workspace-App auslösen.
- **Geplanter Vorabstart:** Der Vorabstart wird nach einem Zeitplan gestartet. Ein geplanter Vorabstart startet nur, wenn das Benutzergerät bereits ausgeführt wird und authentifiziert wurde. Wenn diese beiden Bedingungen zur geplanten Vorabstartzeit nicht erfüllt sind, wird keine Sitzung gestartet. Um Netzwerk- und Serverlast zu teilen, wird die geplante Sitzung innerhalb eines Zeitfensters gestartet. Ist der Vorabstart beispielsweise für 13:45 geplant, erfolgt der Sitzungsstart irgendwann zwischen 13:15 und 13:45. Normalerweise für Zeiten mit normalen Datenverkehr verwendet.

Die Konfiguration des Vorabstarts auf einem Citrix Virtual Apps-Server umfasst Folgendes:

- Erstellen, Bearbeiten oder Löschen von Vorabstartanwendungen
- Aktualisieren der Benutzerrichtlinien, die die Vorabstartanwendung steuern.

Sie können das Vorabstartfeature nicht mit der Datei `receiver.admx` anpassen. Sie können die Vorabstartkonfiguration jedoch ändern, indem Sie die Registrierungswerte ändern. Dies kann während oder nach der Installation der Citrix Workspace-App für Windows erfolgen.

- Die HKEY\_LOCAL\_MACHINE-Werte werden während der Clientinstallation geschrieben.
- Mit den HKEY\_CURRENT\_USER-Werten können Sie verschiedenen Benutzern auf derselben Maschine unterschiedliche Einstellungen bereitstellen. Die Benutzer können die HKEY\_CURRENT\_USER-Werte ohne Administratorrechte ändern. Sie können Skripts bereitstellen, mit denen Benutzer die Werte ändern können.

#### **Registrierungswerte für HKEY\_LOCAL\_MACHINE:**

Für 64-Bit-Windows-Betriebssysteme: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\PreLaunch`

Für 32-Bit-Windows-Betriebssysteme: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\PreLaunch`

Name: **UserOverride**

Typ: REG\_DWORD

Werte:

0 - Wert unter HKEY\_LOCAL\_MACHINE verwenden, selbst wenn unter HKEY\_CURRENT\_USER Werte vorhanden sind.

1 - Werte unter HKEY\_CURRENT\_USER verwenden, wenn vorhanden; sonst die Werte unter HKEY\_LOCAL\_MACHINE verwenden.

Name: **State**

Typ: REG\_DWORD

Werte:

0 - Vorabstart deaktivieren.

1 - Just-In-Time-Vorabstart aktivieren. (Der Vorabstart beginnt, nachdem die Anmeldeinformationen des Benutzers authentifiziert wurden.)

2 - Einen geplanten Vorabstart aktivieren. (Der Vorabstart beginnt zu der für "Schedule" konfigurierten Zeit.)

Name: **Schedule**

Typ: REG\_DWORD

Wert:

Uhrzeit (24-Stunden-Format) und Wochentage für geplante Vorabstarts werden im folgenden Format angegeben:

---

HH:MM	Mo:Di:Mi:Do:Fr:Sa:So, wobei HH und MM Stunden und Minuten sind. Mo:Di:Mi:Do:Fr:Sa:So sind die Wochentage. Um beispielsweise den geplanten Vorabstart montags, mittwochs und freitags um 13:45 zu aktivieren, stellen Sie Folgendes ein: Schedule=13:45	1:0:1:0:1:0:0. Die Sitzung startet dann zwischen 13:15 und 13:45 Uhr.
-------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------

---

### Registrierungswerte für HKEY\_CURRENT\_USER:

HKEY\_CURRENT\_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

Die Schlüssel **State** und **Schedule** haben dieselben Werte wie für HKEY\_LOCAL\_MACHINE.

### Desktop Viewer

Jedes Unternehmen kann andere Anforderungen haben. Die Wünsche und Anforderungen bezüglich des Benutzerzugriffs auf virtuelle Desktops können sich zudem im Laufe der Zeit ändern. Wie Benutzer das Verbinden mit virtuellen Desktops erleben und inwiefern sie Verbindungen selbst konfigurieren können, wird beim Einrichten der Citrix Workspace-App für Windows festgelegt.

Verwenden Sie **Desktop Viewer**, wenn Benutzer mit dem virtuellen Desktop interagieren müssen. Bei einem virtuellen Desktop kann es sich um einen veröffentlichten virtuellen Desktop, einen freigegebenen Desktop oder einen dedizierten Desktop handeln. In diesem Zugriffsszenario kann der Benutzer über die **Desktop Viewer**-Symbolleiste einen virtuellen Desktop in einem Fenster öffnen und den Desktop im lokalen Desktop ziehen und skalieren. Benutzer können Einstellungen festlegen und mit mehreren Desktops über mehrere Citrix Virtual Apps and Desktops- und Citrix DaaS-Verbindungen auf demselben Benutzergerät arbeiten.

#### Hinweis:

Verwenden Sie die Citrix Workspace-App, um die Bildschirmauflösung auf virtuellen Desktops zu ändern. Die Bildschirmauflösung kann nicht in der Windows-Systemsteuerung geändert werden.

### Tastatureingabe in Desktop Viewer

In Desktop Viewer-Sitzungen wird die **Windows-Logo-Taste+L** an den lokalen Computer gesendet.

Strg+Alt+Entf wird an den lokalen Computer gesendet.

Tastatureingaben, die Microsoft-Eingabehilfen wie die Einrastfunktion, die Anschlagverzögerung und Umschalttasten aktivieren, werden normalerweise an den lokalen Computer gesendet.

Als Eingabehilfe von Desktop Viewer werden die Schaltflächen der **Desktop Viewer**-Symbolleiste in einem Pop-up-Fenster angezeigt, wenn Sie Strg+Alt+Entf drücken.

Strg+Esc wird an den virtuellen Remotedesktop gesendet.

**Hinweis:**

Wenn Desktop Viewer maximiert ist, können Sie mit Alt+Tab standardmäßig zwischen Fenstern in der Sitzung wechseln. Wenn Desktop Viewer in einem Fenster angezeigt wird, wechseln Sie mit Alt+Tab zwischen Fenstern außerhalb der Sitzung.

Citrix hat bestimmte Tastenkombinationen entwickelt. Beispiele für Tastenkombinationen: Mit Strg+F1 reproduzieren Sie Strg+Alt+Entf und mit Umschalt+F2 wechseln Sie Anwendungen vom Vollbild- in den Fenstermodus und umgekehrt.

**Hinweis:**

Sie können Tastenkombinationen nicht mit virtuellen Desktops verwenden, die in Desktop Viewer angezeigt werden (d. h. in Sitzungen mit virtuellen Apps und Desktops). Sie können sie aber mit veröffentlichten Anwendungen verwenden (d. h. in Sitzungen mit virtuellen Apps).

## Timeout der Statusanzeige

Sie können die Zeit ändern, die die Statusanzeige beim Start einer Sitzung durch einen Benutzer angezeigt wird.

Sie ändern den Timeoutzeitraum mit den folgenden Schritten:

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu folgendem Pfad:
  - Auf 64-Bit-Systemen: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\Engine`
  - Auf 32-Bit-Systemen: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\`
3. Erstellen Sie einen Registrierungsschlüssel wie im Folgenden beschrieben:
  - Typ: REG\_DWORD
  - Name: `SI_INACTIVE_MS`
  - Wert: 4, wenn die Statusanzeige früher ausgeblendet werden soll.



Wenn Sie diesen Schlüssel konfigurieren, wird der Statusindikator möglicherweise häufig angezeigt und ausgeblendet. Dieses Verhalten entspricht dem Design. Sie können den Statusindikator wie folgt unterdrücken:

1. Öffnen Sie den Registrierungs-Editor.
2. Navigieren Sie zu folgendem Pfad:
  - Auf 64-Bit-Systemen: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\`
  - Auf 32-Bit-Systemen: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\`
3. Erstellen Sie einen Registrierungsschlüssel wie im Folgenden beschrieben:
  - Typ: `REG_DWORD`
  - Name: `NotificationDelay`
  - Wert: Beliebiger Wert in Millisekunden (zum Beispiel 120000)

### Verbesserte Wiederverbindung für virtuelle Apps und Desktops

Citrix Workspace 2302 bietet eine Verbesserung beim Wiederherstellen von getrennten Verbindungen zu virtuellen Apps und Desktops.

Beim Aktualisieren der getrennten Citrix Workspace-App oder dem Start neuer virtueller Apps oder Desktops innerhalb von Workspace Control durch die Citrix Workspace-App wird folgende Eingabeaufforderung angezeigt:

## Restore session?

You have one or more apps/desktops running from the previous session in Citrix Workspace app. Would you like to restore them?

Remember my preference

Restore

Cancel

Diese Aufforderung wird nur angezeigt, wenn **show reconnection prompt to reconnect sessions** im Global App Configuration Service auf “true” gesetzt ist.

Klicken Sie auf **Wiederherstellen**, um die Verbindung wiederherzustellen und neue und getrennte virtuelle Apps und Desktops zu öffnen. Klicken Sie auf **Abbrechen**, wenn Sie nur neu ausgewählte Apps und Desktops starten möchten.

Wählen Sie **Einstellung speichern**, um die gewählte Einstellung bei der nächsten Anmeldung zu verwenden.

Die zuvor erwähnte neue Eingabeaufforderung **Sitzung wiederherstellen?** erscheint nur, wenn Folgendes gilt:

- Der Benutzer versucht, eine App zu starten, die zu einem Workspace Store gehört,
- für das Feature “Workspace Control” sind keine Administratorrichtlinien oder App-Konfigurationseinstellungen konfiguriert,
- auf dem Client sind die Standardeinstellungen für die Wiederverbindung über Workspace Control festgelegt.

#### **Hinweis:**

Die Einstellungen unter **Wiederverbindungsoptionen** haben Vorrang vor den Einstellungen, die im Dialogfeld festgelegt sind. Weitere Informationen finden Sie unter [Optionen zum Wiederverbinden über das Dialogfeld “Erweiterte Einstellungen” konfigurieren](#).

## **Nachhaltigkeitsinitiative der Citrix Workspace-App**

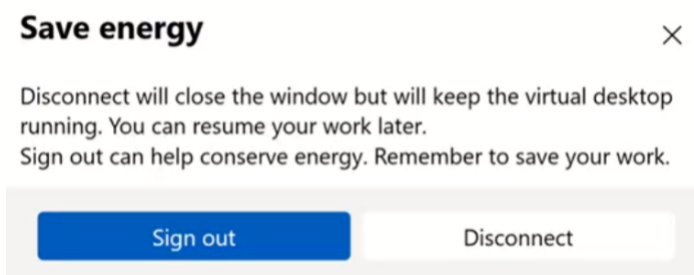
### **Für den nativen Start**

Wenn dieses Feature aktiviert ist, wird eine Aufforderung zum Abmelden von der Desktop-Sitzung angezeigt, wenn ein Benutzer einen virtuellen Desktop schließt. Das Feature kann zur Energieeinsparung beitragen, sofern Windows-Betriebssystemrichtlinien verwendet werden, die VMs herunterfahren, wenn keine Benutzer angemeldet sind.

Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Gehen Sie zu Citrix Studio.
2. Klicken Sie im linken Navigationsbereich auf **Bereitstellungsgruppen**.
3. Wählen Sie im Abschnitt **Bereitstellungsgruppe** den erforderlichen VDA aus.
4. Klicken Sie auf das Symbol **Bearbeiten**. Die Seite **Bereitstellungsgruppe bearbeiten** wird angezeigt.
5. Klicken Sie im linken Navigationsbereich auf **Desktops**.

6. Wählen Sie den VDA aus, zu dem Sie die Schlüsselwörter hinzufügen müssen.
7. Klicken Sie auf **Bearbeiten**. Die Seite **Desktop bearbeiten** wird angezeigt.
8. Legen Sie das Schlüsselwort `LogoffOnClose` im Feld **Beschreibung** auf **true** fest.
9. Klicken Sie auf **OK**. Das folgende Dialogfeld wird angezeigt, wenn Sie den virtuellen Desktop schließen:



**Text von “Energie sparen”-Anzeige ändern** Sie können den Text auf dem Bildschirm **Energie sparen** ändern.

1. Folgen Sie den Schritten 1–8 im vorherigen Abschnitt.
2. Legen Sie das Schlüsselwort `PromptMessage` im Feld **Beschreibung** auf den gewünschten Text fest.

**Beispiel:**

```
1 KEYWORDS:LogoffOnClose=true PromptMessage="Do you want to Log off?"  
2 <!--NeedCopy-->
```

## Edit Desktop

Display name:

Description:  
  
The name and description are shown in Citrix Workspace app.

Restrict launches to machines with tag:

Allow everyone with access to this delivery group to use a desktop

Restrict desktop use:  

Allow list ?

You have not yet added any users or groups.

Enable desktop  
Clear this check box to disable delivery of this desktop.

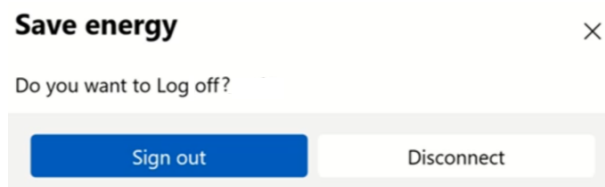
Session roaming  
When enabled, if the user launches this desktop and then moves to another device, the same session is used, and applications are available on both devices. When disabled, the session no longer roams between devices.

Die Schlüsselwörter werden standardmäßig für neue Desktopmaschinen zugewiesen, die der Gruppe zugewiesen sind. Für vorhandene Desktopmaschinen müssen Sie die folgenden Powershell-Befehle ausführen, damit die Änderungen wirksam werden:

```
1 $dg = Get-BrokerDesktopGroup -Name '<group name>' -Property 'Name', 'Uid'
2
3 $apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid
4           -Property 'Description' )
5 Get-BrokerMachine -DesktopGroupUid $dg.Uid -IsAssigned $true | Set
6           -BrokerMachine -Description $apr[0].Description
7 <!--NeedCopy-->
```

Mit diesem PowerShell-Skript ist es möglich, mehrere Zuweisungsrichtlinienregeln für eine einzelne Bereitstellungsgruppe zu verwenden. Mit Citrix Studio können Sie auch mehrere Zuweisungsrichtlinienregeln konfigurieren, jede mit einem eindeutigen Beschreibungswert und einem möglichen Satz unterschiedlicher Schlüsselwörter.

3. Klicken Sie auf **OK**. Das folgende Dialogfeld wird angezeigt, wenn Sie den virtuellen Desktop schließen.

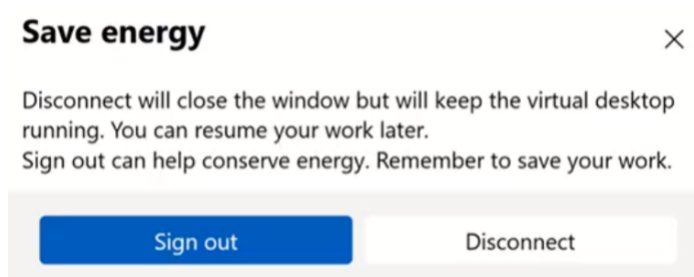


### Für den Start der Hybrid Cloud

Ab Version 2402 der Citrix Workspace-App ist diese Funktion für hybride Starts in der Cloud verfügbar. Sobald dieses Feature aktiviert ist, wird eine Aufforderung zum Abmelden von der Desktop-Sitzung angezeigt, wenn ein Benutzer einen virtuellen Desktop schließt. Das Feature trägt zur Energieeinsparung bei, sofern Windows-Betriebssystemrichtlinien verwendet werden, die VMs herunterfahren, wenn keine Benutzer angemeldet sind.

Führen Sie folgende Schritte aus, um das Feature zu aktivieren:

1. Gehen Sie zu Citrix Studio.
2. Klicken Sie im linken Navigationsbereich auf **Bereitstellungsgruppen**.
3. Wählen Sie im Abschnitt **Bereitstellungsgruppe** den erforderlichen VDA aus.
4. Klicken Sie auf das Symbol **Bearbeiten**. Die Seite **Bereitstellungsgruppe bearbeiten** wird angezeigt.
5. Klicken Sie im linken Navigationsbereich auf **Desktops**.
6. Wählen Sie den VDA aus, zu dem Sie die Schlüsselwörter hinzufügen müssen.
7. Klicken Sie auf **Bearbeiten**. Die Seite **Desktop bearbeiten** wird angezeigt.
8. Legen Sie das Schlüsselwort `ICA-LogOffOnClose` im Feld **Beschreibung** auf **true** fest.
9. Klicken Sie auf **OK**. Das folgende Dialogfeld wird angezeigt, wenn Sie den virtuellen Desktop schließen:



## Text von “Energie sparen”-Anzeige ändern

Sie können den Text auf dem Bildschirm **Energie sparen** ändern.

1. Folgen Sie den Schritten 1–8 im vorherigen Abschnitt.
2. Legen Sie das Schlüsselwort `ICA-PromptMessage` im Feld **Beschreibung** auf den gewünschten Text fest.

### Hinweis:

Im Feld “Beschreibung” sind maximal 200 Zeichen zulässig.

### Beispiel:

```
1 KEYWORDS:ICA-LogOffOnClose=true="Do you want to Log off?"
2 <!--NeedCopy-->
```

Die Schlüsselwörter werden standardmäßig für neue Desktopmaschinen zugewiesen, die der Gruppe zugewiesen sind. Für vorhandene Desktopmaschinen müssen Sie die folgenden Powershell-Befehle ausführen, damit die Änderungen wirksam werden:

```
1 $dg = Get-BrokerDesktopGroup -Name '<group name>' -Property 'Name'
   , 'Uid'
2
3 $apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid
   -Property 'Description' )
4
5 Get-BrokerMachine -DesktopGroupUid $dg.Uid -IsAssigned $true | Set
   -BrokerMachine -Description $apr[0].Description
6 <!--NeedCopy-->
```

Mit diesem PowerShell-Skript ist es möglich, mehrere Zuweisungsrichtlinienregeln für eine einzelne Bereitstellungsgruppe zu verwenden. Mit Citrix Studio können Sie auch mehrere Zuweisungsrichtlinienregeln konfigurieren, jede mit einem eindeutigen Beschreibungswert und einem möglichen Satz unterschiedlicher Schlüsselwörter.

3. Klicken Sie auf **OK**. Das folgende Dialogfeld wird angezeigt, wenn Sie den virtuellen Desktop schließen.



## Citrix Workspace-App Desktop Lock

April 22, 2024

Sie können Citrix Workspace-App Desktop Lock verwenden, wenn Sie nicht mit dem lokalen Desktop arbeiten müssen. Sie können den Desktop Viewer verwenden (wenn aktiviert), jedoch sind auf der Symbolleiste nur die folgenden Optionen verfügbar:

- Strg+Alt+Entf
- Einstellungen
- Geräte
- Trennen:

Die Citrix Workspace-App für Windows mit Desktop Lock funktioniert auf in Domänen eingebundenen Maschinen mit aktiviertem Single Sign-On und konfigurierbarem Store. PNA-Sites werden nicht unterstützt. Vorherige Versionen von Desktop Lock werden beim Upgrade auf Citrix Receiver für Windows 4.2 oder höher nicht unterstützt.

### Hinweis:

Bei Verwendung der Citrix Workspace-App für Windows mit Desktop Lock wird der Benutzer bei dem ersten Desktop in der alphabetischen Liste aller für ihn verfügbaren Desktops angemeldet. Derzeit gibt es keine Möglichkeit der Auswahl des Desktops, bei dem der Benutzer sich anmelden muss. Außerdem unterstützt das Feature nur Desktops und keine Apps.

Installieren Sie die Citrix Workspace-App für Windows mit dem Flag `/includeSSON`. Konfigurieren Sie Single Sign-On und den Store mit der ADM/ADMX-Datei oder über die Befehlszeilenoption. Weitere Informationen finden Sie unter [Installation](#).

Installieren Sie dann Citrix Workspace-App Desktop Lock als Administrator mit dem Installationspaket `CitrixWorkspaceDesktopLock.msi`, das auf der [Citrix Downloadseite](#) verfügbar ist.

## Systemanforderungen

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. Weitere Informationen finden Sie auf der [Microsoft-Downloadseite](#).

- Unterstützung für Windows 10 (einschließlich Anniversary Update) und Windows 11.
- Verbindung mit StoreFront nur über native Protokolle.
- In Domänen eingebundene Endpunkte:
- Benutzergeräte müssen mit einem LAN oder WAN verbunden sein.

## Lokaler App-Zugriff

### Wichtig

Das Aktivieren des lokalen App-Zugriffs kann den lokalen Desktopzugriff zulassen, es sei denn, es wurde eine vollständige Sperrung über die Gruppenrichtlinienobjektvorlage oder eine ähnliche Richtlinie angewendet. Weitere Informationen finden Sie unter [Konfigurieren von lokalem App-Zugriff und URL-Umleitung](#) in der Dokumentation zu Citrix Virtual Apps and Desktops.

## Arbeiten mit Citrix Workspace-App Desktop Lock

- Citrix Workspace-App Desktop Lock kann mit den folgenden Features der Citrix Workspace-App verwendet werden:
  - 3Dpro, Flash, USB, HDX Insight, Microsoft Lync 2013-Plug-In und lokaler App-Zugriff.
  - Nur Domänen-, Smartcard- oder zweistufige Authentifizierung.
- Trennen der Citrix Workspace-App Desktop Lock-Sitzung führt zur Abmeldung des Endgeräts.
- Flash-Umleitung ist unter Windows 8 und höher deaktiviert. Flash-Umleitung ist unter Windows 7 aktiviert.
- Desktop Viewer ist für Citrix Workspace-App Desktop Lock ohne die Eigenschaften “Home”, “Restore”, “Maximize” und “Display” optimiert.
- Strg+Alt+Entf ist auf der Desktop Viewer-Symbolleiste verfügbar.
- Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben. Eine Ausnahme bildet Windows+L.
- Strg+F1 löst Strg+Alt+Entf aus, wenn Sie die Verbindung oder Desktop Viewer für Desktopverbindungen deaktivieren.
- Ein lokales Benutzerprofil wird auf dem Endgerät erstellt, wenn sich der Benutzer am System anmeldet. Das Profil wird auf dem Endgerät beibehalten, auch wenn sich der Benutzer abmeldet, basierend auf den Konfigurationen der Profilverwaltung.

### Hinweis:

Wenn Desktop Lock installiert ist und `LiveInDesktopDisconnectOnLock` am Registrierungspfad `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` oder `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` auf **False** festgelegt ist, wird die aktive Sitzung getrennt, wenn der Endpunkt aus dem Ruhezustand oder Standbymodus reaktiviert



wird.

## Installieren von Citrix Workspace-App Desktop Lock

Mit diesen Schritten installieren Sie die Citrix Workspace-App für Windows so, dass virtuelle Desktops mit Citrix Workspace-App Desktop Lock angezeigt werden. Informationen zu Bereitstellungen, die Smartcards verwenden, finden Sie unter [Smartcard](#).

1. Melden Sie sich mit einem lokalen Administratorkonto an.
2. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus:

Beispiel:

```
1 CitrixWorkspaceApp.exe
2 /includeSSON
3 STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
4 <!--NeedCopy--> discovery;on;Desktop Store"
```

Der Befehl ist in der Citrix Workspace-App und im Ordner **Plug-Ins > Windows > Citrix Workspace-App** auf dem Installationsmedium verfügbar. Weitere Informationen zu den Befehlen finden Sie in der Installationsdokumentation zur Citrix Workspace-App unter [Installation](#).

3. Doppelklicken Sie im selben Ordner auf dem Installationsmedium auf [CitrixWorkspaceDesktopLock.msi](#). Der Assistent "Desktop Lock" wird angezeigt. Folgen Sie den Anweisungen.
4. Wenn die Installation abgeschlossen ist, starten Sie das Benutzergerät neu. Wenn Sie Zugriffsrechte für einen Desktop haben und sich als Domänenbenutzer anmelden, wird das neu gestartete Gerät mit Citrix Workspace-App Desktop Lock angezeigt.

Sie können die Verwaltung des Benutzergeräts nach der Installation ermöglichen. Das für die Installation von [CitrixWorkspaceDesktopLock.msi](#) verwendete Konto wird dazu bei der Ersatz-Shell ausgeschlossen. Wenn das Konto später gelöscht wird, können Sie sich nicht bei dem Gerät anmelden und es verwalten.

Verwenden Sie zum Installieren von Citrix Workspace Desktop Lock **ohne Benutzereingriff** folgenden Befehl:

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

## Konfigurieren von Citrix Workspace-App Desktop Lock

Wenn Sie sich als Nicht-Administrator angemeldet haben, startet Desktop Lock automatisch eine zugewiesene Desktopsitzung.

Verhindern Sie mit Active Directory-Richtlinien, dass Benutzer virtuelle Desktops in den Ruhezustand versetzen.

Verwenden Sie das Administratorkonto zum Konfigurieren von Citrix Workspace-App Desktop Lock, das Sie für die Installation verwendet haben.

- Überprüfen Sie, ob die Dateien receiver.admx (oder receiver.adml) und receiver\_usb.admx (.adml) in die Gruppenrichtlinie geladen wurden (wo die Richtlinien unter “Computerkonfiguration” bzw. **Benutzerkonfiguration > Administrative Vorlagen > Klassische administrative Vorlagen (ADMX) > Citrix Komponenten** angezeigt werden). Die ADMX-Dateien sind in %Programme%\Citrix\ICA Client\Configuration\.
- USB-Einstellungen: Wenn ein Benutzer ein USB-Gerät anschließt, erfolgt ein automatisches Remoting des Geräts zum virtuellen Desktop. Es ist kein Benutzereingriff erforderlich. Der virtuelle Desktop steuert das USB-Gerät und zeigt es auf der Benutzeroberfläche an.
  - Aktivieren Sie die USB-Richtlinienregel.
  - Aktivieren und konfigurieren Sie unter **Citrix Workspace-App > Remoting von Clientgeräten > Generisches USB-Remoting** die Richtlinien “Vorhandene USB-Geräte” und “Neue USB-Geräte”.
- Laufwerkzuordnung: Aktivieren und konfigurieren Sie unter **Citrix Workspace-App > Remoting von Clientgeräten** die Richtlinie “Clientlaufwerkzuordnung”.
- Mikrofon: Aktivieren und konfigurieren Sie unter **Citrix Workspace-App > Remoting von Clientgeräten** die Richtlinie “Clientmikrofon”.

## Konfigurieren von Smartcards für die Verwendung mit Windows Desktop Lock

1. Konfigurieren Sie StoreFront.
  - a) Konfigurieren Sie den XML-Dienst zur Verwendung der DNS-Adressauflösung für Kerberos-Unterstützung.
  - b) Konfigurieren Sie StoreFront-Sites für HTTPS-Zugriff, erstellen Sie ein Serverzertifikat, das von Ihrer Domänenzertifizierungsstelle signiert wurde und fügen Sie HTTPS-Bindung zur Standardwebsite hinzu.
  - c) Stellen Sie sicher, dass Passthrough-Authentifizierung mit Smartcard aktiviert ist (standardmäßig aktiviert).
  - d) Aktivieren Sie Kerberos.
  - e) Aktivieren Sie Kerberos und Passthrough-Authentifizierung mit Smartcard.
  - f) Aktivieren Sie den anonymen Zugriff auf die IIS-Standardwebsite und verwenden Sie die integrierte Windows-Authentifizierung.
  - g) Stellen Sie sicher, dass für die IIS-Standardwebsite kein SSL erforderlich ist, und dass Clientzertifikate ignoriert werden.

2. Verwenden Sie die Gruppenrichtlinien-Verwaltungskontrolle zum Konfigurieren lokaler Computerrichtlinien auf dem Benutzergerät.
  - a) Importieren Sie die Vorlage Receiver.admx aus %Programme%\Citrix\ICA Client\Configuration\.
  - b) Erweitern Sie **Administrative Vorlagen > Klassische administrative Vorlagen (ADMX) > Citrix Komponenten > Citrix Workspace > Benutzerauthentifizierung**.
  - c) Aktivieren Sie "Smartcardauthentifizierung".
  - d) Aktivieren Sie "Lokaler Benutzername und Kennwort".
3. Konfigurieren Sie das Benutzergerät vor der Installation von Citrix Workspace-App Desktop Lock.
  - a) Fügen Sie die URL für den Delivery Controller in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites" hinzu.
  - b) Fügen Sie die URL für die erste Bereitstellungsgruppe in der Windows Internet Explorer-Liste "Vertrauenswürdige Sites" hinzu. Fügen Sie die URL im Format "desktop://delivery-group-name" hinzu.
  - c) Aktivieren Sie Internet Explorer für die automatische Anmeldung für vertrauenswürdige Sites.

Wenn Citrix Workspace-App Desktop Lock auf dem Benutzergerät installiert ist, wird eine konsistente Richtlinie für das Entfernen der Smartcard zwingend angewendet. Wird die Richtlinie für das Entfernen der Smartcard beispielsweise für den Desktop auf "Abmelden erzwingen" festgelegt, muss der Benutzer sich vom Benutzergerät abmelden, unabhängig davon, wie die Richtlinie dort eingestellt ist. Desktop Lock stellt sicher, dass das Benutzergerät sich nicht in einem inkonsistenten Zustand befindet. Dies gilt nur für Benutzergeräte mit Citrix Workspace-App Desktop Lock.

## Entfernen von Desktop Lock

Stellen Sie sicher, dass beide der folgenden Komponenten entfernt werden:

1. Melden Sie sich mit demselben lokalen Administratorkonto an, das bei der Installation und Konfiguration von Citrix Workspace-App Desktop Lock verwendet wurde.
2. Gehen Sie mit der Windows-Funktion zum Entfernen oder Ändern von Programmen wie folgt vor:
  - Entfernen Sie Citrix Workspace-App Desktop Lock.
  - Entfernen Sie die Citrix Workspace-App für Windows.

## Weitergeben von Windows-Tastenkombinationen an die Remotesitzung

Die meisten Windows-Tastenkombinationen werden an die Remotesitzung weitergegeben. In diesem Abschnitt finden Sie einige der gebräuchlichsten Tastenkombinationen.

## Windows

- Win+D - Minimieren aller Fenster auf dem Desktop.
- Alt+Tab - Wechseln des aktiven Fensters.
- Strg+Alt+Entf - über Strg+F1 und die Desktop Viewer-Symbolleiste.
- Alt+Umschalt+Tab
- Windows+Tab
- Windows+Umschalt+Tab
- Windows+Alle Zeichentasten

## Windows 8

- Win+C - Charms öffnen.
- Win+Q - Charm "Suche".
- Win+H - Charm "Teilen".
- Win+K - Charm "Geräte".
- Win+I - Charm "Einstellungen".
- Win+Q - Apps durchsuchen.
- Win+W - Einstellungen durchsuchen.
- Win+F - Dateien durchsuchen.

## Windows 8 Apps

- Win+Z - App-Optionen anzeigen.
- Win+. - App links andocken.
- Win+Umschalt+. - App rechts andocken.
- Strg+Tab - Zum App-Verlauf wechseln.
- Alt+F4 - App schließen.

## Desktop

- Win+D - Desktop öffnen.
- Win+, - Desktop kurz anzeigen.
- Win+B - Zurück zum Desktop.

## Sonstiges

- Win+U - Center für erleichterte Bedienung öffnen.
- Strg+Esc - Startbildschirm.

- Win+Eingabetaste - Windows Sprachausgabe öffnen.
- Win+X - Menü für Systemprogrammeinstellungen öffnen.
- Win+Druck - Bildschirmfoto erstellen und unter "Bilder" speichern.
- Win+Tab - Liste zum Wechseln öffnen.
- Win+T - Vorschau offener Fenster in Taskleiste anzeigen.

## Software Development Kit (SDK) und API

April 22, 2024

### Certificate Identity Declaration SDK

Mit dem Certificate Identity Declaration (CID) SDK können Entwickler ein Plug-In erstellen. Mit diesem Plug-In kann die Citrix Workspace-App sich mithilfe des auf der Clientmaschine installierten Zertifikats beim StoreFront-Server authentifizieren. CID deklariert die Smartcard-Identität des Benutzers an einem StoreFront-Server, ohne anhand der Smartcard eine Authentifizierung durchzuführen.

Die neueste Version der [Zertifikatidentitätsdeklaration für Citrix Workspace für Windows](#) ist **2212**.

Weitere Informationen finden Sie unter [Certificate Identity Declaration SDK for Citrix Workspace app for Windows](#).

### Citrix Common Connection Manager SDK

Das Common Connection Manager (CCM) SDK stellt eine Reihe nativer APIs bereit, mit denen Sie programmgesteuert interagieren und grundlegende Vorgänge ausführen können. Das SDK erfordert keinen separaten Download, da es Teil des Installationspakets der Citrix Workspace-App für Windows ist.

#### Hinweis:

Bei einigen APIs, die mit dem Start in Zusammenhang stehen, muss die ICA-Datei den Startvorgang für Sitzungen mit virtuellen Apps und Desktops initiieren.

Die CCM SDK-Funktionen umfassen Folgende:

- Sitzungsstart
  - Ermöglicht das Starten von Anwendungen und Desktops mit der generierten ICA-Datei.
- Session disconnect

- Ähnlich wie das Trennen der Verbindung über Connection Center. Die Trennung kann für alle Sitzungen oder für einen bestimmten Benutzer erfolgen.
- Session logoff
  - Ähnlich wie die Abmeldung über Connection Center. Die Abmeldung kann für alle Sitzungen oder für einen bestimmten Benutzer erfolgen.
- Sitzungsinformationen
  - Bietet verschiedene Methoden zum Abrufen von Verbindungsinformationen zu den gestarteten Sitzungen. Dazu gehören Desktopsitzung, Anwendungssitzung und invertierte Seamless-Anwendungssitzung.

Weitere Informationen über die Dokumentation zum SDK finden Sie unter [Programmers guide to Citrix CCM SDK](#).

## Citrix Virtual Channel SDK

Das Citrix Virtual Channel Software Development Kit (SDK) bietet Unterstützung für das Schreiben von serverseitigen Anwendungen und clientseitigen Treibern für weitere virtuelle Kanäle, die das ICA-Protokoll verwenden. Die serverseitigen virtuellen Kanal Anwendungen sind auf Citrix Virtual Apps and Desktops-Servern. Wenn Sie virtuelle Treiber für andere Clientplattformen schreiben möchten, wenden Sie sich an den technischen Support von Citrix.

Das Virtual Channel SDK bietet Folgendes:

- Die Citrix Virtual Driver Application Programming Interface (VD-API) wird mit dem virtuellen Kanal im Citrix Server API SDK (WF-API SDK) verwendet, um neue virtuelle Kanäle zu erstellen. Die von der VD-API bereitgestellte Unterstützung für virtuelle Kanäle macht das Schreiben der eigenen virtuellen Kanäle einfacher.
- Die Windows Monitoring API, die die visuelle Darstellung verbessert und Unterstützung für Anwendungen von Drittanbietern bietet, die in ICA integriert sind.
- Funktionierender Quellcode für Beispielprogramme für virtuelle Kanäle, die Programmiermethoden demonstrieren.
- Das Virtual Channel SDK erfordert, dass das WF-API SDK die serverseitige Komponente des virtuellen Kanals schreibt.

Die neueste Version für [Virtual Channel SDK für Windows](#) ist **2302**.

Weitere Informationen finden Sie unter [Citrix Virtual Channel SDK for Citrix Workspace app for Windows](#).

## Fast Connect 3 Credential Insertion API

Die Fast Connect 3 Credential Insertion API bietet eine Schnittstelle zum Bereitstellen von Benutzeranmeldeinformationen für das Single Sign-On (SSO)-Feature. Dieses Feature ist in der Citrix Workspace-App für Windows Version 4.2 und höher verfügbar. Mit dieser API können Citrix Partner Authentifizierungs- und SSO-Produkte bereitstellen, die StoreFront verwenden, um Benutzer an virtuellen Anwendungen oder Desktops anzumelden und die Verbindungen zu diesen Sitzungen auch wieder zu trennen.

Die neueste Version der [Fast Connect API für Citrix Workspace für Windows](#) ist **2212**.

Weitere Informationen finden Sie unter [Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows](#).

## Skripts für die Bereitstellung von Citrix Workspace für Windows

Dies sind Beispielskripts zum Bereitstellen und Konfigurieren der Citrix Workspace-App.

Die neueste Version für [Skripts für die Bereitstellung von Citrix Workspace für Windows](#) ist **2212**.

## Storebrowse

April 22, 2024

### Hinweis:

Dieser Artikel gilt nur für On-Premises-Bereitstellungen von Citrix Workspace. Informationen zu Cloud-Bereitstellungen finden Sie in der Dokumentation zu [Storebrowse für Workspace](#).

**Storebrowse** ist ein Befehlszeilenhilfsprogramm zur Interaktion zwischen Client und Server. Es wird zur Authentifizierung aller Operationen innerhalb von StoreFront und mit Citrix Gateway verwendet.

Mit **Storebrowse** können Administratoren folgende Vorgänge automatisieren:

- Hinzufügen von Stores.
- Auflisten der veröffentlichten Apps und Desktops eines konfigurierten Stores
- Manuelles Erstellen einer ICA-Datei unter Auswahl von beliebigen virtuellen Apps und Desktops
- Generieren einer ICA-Datei mit der **Storebrowse**-Befehlszeile
- Starten der veröffentlichten Anwendung

Das **Storebrowse**-Hilfsprogramm ist Teil der **Authmanager**-Komponente. Nach abgeschlossener Installation der Citrix Workspace-App ist das **Storebrowse**-Hilfsprogramm im **AuthManager**-Installationsordner.

Um sicherzustellen, dass **Storebrowse** gemeinsam mit der **Authmanager**-Komponente installiert wurde, überprüfen Sie den folgenden Registrierungspfad:

**Bei Installation der Citrix Workspace-App durch Administratoren:**

---

Auf 32-Bit-Maschinen [HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\AuthManager\Inst

Auf 64-Bit-Maschinen [HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\A

---

**Bei Installation der Citrix Workspace-App durch Benutzer (Nicht-Administratoren):**

---

Auf 32-Bit-Maschinen [HKEY\_CURRENT\_USER\SOFTWARE\Citrix\AuthManager\Inst

Auf 64-Bit-Maschinen [HKEY\_CURRENT\_USER\SOFTWARE\WOW6432Node\Citrix\A

---

## Anforderungen

- Citrix Workspace-App Version 1808 für Windows oder höher
- Mindestens 530 MB freier Festplattenspeicher
- 2 GB RAM

## Compatibility Matrix

Das **Storebrowse**-Hilfsprogramm ist mit folgenden Betriebssystemen kompatibel:

---

Betriebssystem

---

Windows 10 (32-Bit- und 64-Bit-Edition)

Windows Server 2022

Windows Server 2016

Windows Server 2008 R2, 64-Bit-Edition

Windows Server 2008 R2, 64-Bit-Edition

---



## Verbindungen

Das **Storebrowse**-Hilfsprogramm unterstützt folgende Verbindungsarten:

- HTTP-Store
- HTTPS-Store
- Citrix Gateway 11.0 und höher

### Hinweis:

In einem HTTP-Store akzeptiert das **Storebrowse**-Hilfsprogramm nicht die Eingabe der Anmeldeinformationen über die Befehlszeile.

## Authentifizierungsmethoden

**StoreFront-Server** StoreFront unterstützt verschiedene Authentifizierungsmethoden für den Zugriff auf Stores, es werden jedoch nicht alle empfohlen. Aus Sicherheitsgründen sind einige Authentifizierungsmethoden standardmäßig deaktiviert, wenn Sie einen Store erstellen.

- **Benutzername und Kennwort:** Geben Sie die Anmeldeinformationen zur Authentifizierung des Zugriffs auf Stores ein. Die explizite Authentifizierung ist standardmäßig aktiviert, wenn Sie den ersten Store erstellen.
- **Domänen-Passthrough:** Nach der Authentifizierung bei den Windows-Computern, die der Domäne angehören, werden Sie automatisch an Stores angemeldet. Um diese Option zu verwenden, aktivieren Sie die Passthrough-Authentifizierung bei der Installation der Citrix Workspace-App. Weitere Informationen zu Domänen-Passthrough finden Sie unter [Konfigurieren von Passthrough-Authentifizierung](#).
- **HTTP Basic:** Diese Methode wird von Kundenintegrationen und Webportalen von Drittanbietern verwendet, wobei über eine externe Benutzeroberfläche ein domänenqualifizierter Benutzername und ein Kennwort erfasst werden. StoreFront verwendet die Basic-Authentifizierungsfunktion in IIS, um die Anmeldeinformationen an den StoreFront-Server zu übermitteln. StoreFront verwendet dann entweder die [Domänendienste](#) oder die [Broker-XML-Dienstauthentifizierung](#), um die Anmeldeinformationen zu überprüfen und die Gruppeninformationen abzurufen. Informationen zum Aktivieren der HTTP-Basic-Authentifizierung finden Sie unter [HTTP Basic](#) in der Dokumentation unter [Authentifizierungsmethoden verwalten](#).

Das **Storebrowse**-Hilfsprogramm unterstützt folgende Authentifizierungsmethoden:

- Verwendung des [AuthManager](#), der in das **Storebrowse**-Hilfsprogramm integriert ist. Hinweis: Aktivieren Sie die HTTP Basic-Authentifizierungsmethode in StoreFront, während Sie mit **Storebrowse** arbeiten. Diese Methode gilt, wenn der Benutzer die Anmeldeinformationen über die **Storebrowse**-Befehle bereitstellt.

- Verwendung des [Authmanager](#), der in der Citrix Workspace-App für Windows enthalten ist. Sie können diese Methode verwenden, wenn Sie die Domänen-Passthrough-Authentifizierung verwenden. Weitere Informationen finden Sie unter [Domänen-Passthrough-Authentifizierung](#).

## Starten eines veröffentlichten Desktops oder einer veröffentlichten Anwendung

Sie können Ressourcen jetzt direkt aus dem Store starten, ohne eine ICA-Datei verwenden zu müssen.

### Hinweis:

Sie können SaaS-Apps oder [veröffentlichte Inhalte](#) nicht mit Storebrowse-Befehlen öffnen.

## Verwendung von Befehlen

Der folgende Abschnitt enthält detaillierte Informationen zu den Befehlen, die Sie im **Storebrowse**-Hilfsprogramm verwenden können.

### Store hinzufügen

`-a, --addstore`

### Beschreibung:

Fügt einen neuen Store hinzu. Gibt die vollständige URL des Stores zurück. Wenn die Rückgabe fehlschlägt, wird ein Fehler gemeldet.

### Hinweis:

Das **Storebrowse**-Hilfsprogramm unterstützt Konfigurationen mit mehreren Stores.

### Befehlsbeispiel in StoreFront:

Befehl:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of Storefront*
```

Beispiel:

```
'\storebrowse.exe -U {Username} -P {Password} -D {Domain} -a https://my.firstexamplestore.net'
```

### Befehlsbeispiel in Citrix Gateway:

Befehl:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of CitrixGateway*
```

Beispiel:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a < https://mysecondexample.com>
```

## Hilfe

```
/?
```

### Beschreibung:

Bietet Details zur Verwendung des **Storebrowse**-Hilfsprogramms.

### Store auflisten

```
(-l), --liststore
```

### Beschreibung:

Listet die Stores auf, die vom Benutzer hinzugefügt wurden.

### Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -l
```

### Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -l
```

### Enumeration

```
(-M 0x2000 -E)
```

### Beschreibung:

Enumeriert die Ressourcen.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0 x2000 -E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0 x2000 -E <https://my.secondexample.net>
```

## Schnellstart

`-q, --quicklaunch`

### Beschreibung:

Erstellt die ICA-Datei für veröffentlichte Apps und Desktops mit dem **Storebrowse**-Hilfsprogramm. Die `quicklaunch`-Option erfordert die Eingabe einer Start-URL und der Store-URL. Die Start-URL kann entweder der StoreFront-Server oder die Citrix Gateway-URL sein. Die ICA-Datei wird im Verzeichnis `%LocalAppData%\Citrix\Storebrowse\cache` erstellt.

Sie können die Start-URL für alle veröffentlichten Apps und Desktops mit folgendem Befehl abrufen:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

Eine typische Start-URL lautet wie folgt:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_published_apps_and_desktops } <https://my.firstexamplestore.net/Citrix/Store/resources/v2/Q2hJk0lmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_published_apps_and_desktops } <https://my.secondexamplestore.com>
```

## Start

`-L, --launch`

### Beschreibung:

Erstellt die erforderliche ICA-Datei für veröffentlichte Apps und Desktops mit dem **Storebrowse**-Hilfsprogramm. Die Startoption erfordert die Eingabe des Ressourcennamens und der Store-URL. Der Name kann entweder der StoreFront-Server oder die Citrix Gateway-URL sein. Die ICA-Datei wird im Verzeichnis `%LocalAppData%\Citrix\Storebrowse\cache` erstellt.

Mit dem folgenden Befehl rufen Sie den Anzeigenamen der veröffentlichten Apps und Desktops ab:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

Dieser Befehl führt zu folgender Ausgabe:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/
/Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

Der in der vorherigen Ausgabe fett gedruckte Name wird als Eingabeparameter für die Startoption verwendet.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L
“{ Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery>
```

Befehlsbeispiel in Citrix Gateway:

```
<.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L {
Resource_Name } https://my.secondexamplestore.com>
```

## Sitzungsstart

`-S, --sessionlaunch`

### Beschreibung:

Mit diesem Befehl können Sie einen Store hinzufügen sowie die veröffentlichten Ressourcen überprüfen und starten. Diese Option übernimmt die folgenden Parameter:

- Benutzername
- Kennwort
- Domäne
- Name der zu startenden Ressource
- Store-URL

Wenn Benutzer keine Anmeldeinformationen angeben, werden sie von `AuthManager` zur Eingabe der Anmeldeinformationen aufgefordert. Anschließend wird die Ressource gestartet.

Sie können den Namen der Ressource von veröffentlichten Apps und Desktops mit folgendem Befehl abrufen:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

Dieser Befehl führt zu folgender Ausgabe:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/
/Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

Der in der vorherigen Ausgabe fett gedruckte Name wird als Eingabeparameter für die Option `-S` verwendet.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S “  
{ Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/  
Store/discovery >
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S {  
Friendly_Resource_Name } <https://my.secondexamplestore.com>
```

### Dateiordner

`-f, --filefolder`

#### Beschreibung:

Generiert die ICA-Datei im benutzerdefinierten Pfad für die veröffentlichten Apps und Desktops.

Die Startoption erfordert die Eingabe eines Ordnersnamens und des Ressourcennamens sowie der Store-URL. Die Store-URL kann entweder der StoreFront-Server oder die Citrix Gateway-URL sein.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -f “C:\Temp\Launch.ica” -L “Resource_Name” { Store }
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -f “C:\Temp\Launch.ica” -L “Resource_Name” { NSG_URL  
}
```

### Trace-Authentifizierung

`-t, --traceauthentication`

#### Beschreibung:

Generiert Protokolle für die `AuthManager`-Komponente. Protokolle werden nur erstellt, wenn **Storebrowse** einen integrierten `AuthManager` verwendet. Protokolle werden im Verzeichnis `localappdata%\Citrix\Storebrowse\logs` erstellt.

#### Hinweis:

Diese Option darf nicht der letzte Parameter in der Befehlszeile des Benutzers sein.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a { StoreURL }
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a { NSG_URL }
```

## Store löschen

`-d, --deletestore`

### Beschreibung:

Löscht den vorhandenen StoreFront- oder Citrix Gateway-Store.

Befehlsbeispiel in StoreFront:

```
.\storebrowse.exe -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

Befehlsbeispiel in Citrix Gateway:

```
.\storebrowse.exe -d https://my.secondexamplestore.com
```

## Status des Storebrowse-Befehls verfolgen

Sie können den Ausführungsstatus eines Storebrowse-Befehls in einer Datei verfolgen. Um den Erfolgsstatus zu verfolgen, geben Sie für den Befehl `-f launch` einen eindeutigen Dateinamen an. Dieser Befehl generiert eine Datei mit dem von Ihnen angegebenen Namen. Der Fehlerstatus ist in der Datei `ica.error` vorhanden, die automatisch erstellt wird.

### Hinweis:

Stellen Sie sicher, dass Sie dem Dateinamen mit dem Befehl `-f launch` die Erweiterung `.ica` hinzufügen. Andernfalls wird die Datei nicht generiert.

Die Dateien zum Verfolgen von Erfolg und Fehler befinden sich beide in `%LOCALAPPDATA%\citrix\selfservice\cache` und Sie können diese Dateien nach Bedarf überwachen.

Diese Erweiterung ist standardmäßig aktiviert.

Beispiel für die Verwendung des Startbefehls mit Option `-f`:

```
1 -launch -f <uniqueFileName.ica> "launchcommandline"  
2 For example:
```

```
3 SelfService.exe storebrowse -launch -f uniqueFileName.ica -s store0-5
  c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-
  e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/
  Citrix/Store/resources/v2/
  YTLh0GUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkJzM5Lk5vdGVwYWQ-/launch/
  ica" -cmdline
4
5 <!--NeedCopy-->
```

## Unterstützung von Single Sign-On mit Citrix Gateway

Mit Single Sign-On können Sie sich bei einer Domäne authentifizieren und das von dieser Domäne bereitgestellte Citrix Virtual Apps and Desktops und Citrix DaaS (ehemals Citrix Virtual Apps and Desktops Service) verwenden. Sie können sich anmelden, ohne sich für jede App oder jeden Desktop neu authentifizieren zu müssen. Wenn Sie einen Store hinzufügen, werden Ihre Anmeldeinformationen zusammen mit den Citrix Virtual Apps and Desktops und Citrix DaaS und den Startmenüeinstellungen an den Citrix Gateway-Server übergeben.

Dieses Feature wird ab Citrix Gateway Version 11 unterstützt.

### Voraussetzungen:

Informationen zu den Voraussetzungen für die Konfiguration von Single Sign-On für Citrix Gateway finden Sie unter [Konfigurieren von Domänen-Passthrough-Authentifizierung](#).

Das Single Sign-On-Feature mit Citrix Gateway kann über die administrative Gruppenrichtlinienobjektvorlage aktiviert werden.

1. Öffnen Sie die administrative GPO-Vorlage von Citrix Workspace-App, indem Sie gpedit.msc ausführen.
2. Navigieren Sie unter dem Knoten **Computerkonfiguration** zu **Administrative Vorlagen** > **Citrix Komponenten** > **Citrix Workspace** > **Benutzerauthentifizierung** > **Single Sign-On für Citrix Gateway**.
3. Verwenden Sie die Umschaltoptionen, um Single Sign-On ein- oder auszuschalten.
4. Klicken Sie auf **Anwenden** und auf **OK**.
5. Starten Sie die Citrix Workspace-App-Sitzung neu, um die Änderungen zu übernehmen.

### Einschränkungen:

- Zur Eingabe von Anmeldeinformationen mit dem **Storebrowse**-Hilfsprogramm muss auf dem StoreFront-Server die **HTTP Basic-Authentifizierung** aktiviert sein.
- Wenn Sie mit dem Hilfsprogramm eine Verbindung zum HTTP-Store herstellen, um die veröffentlichten virtuellen Apps und Desktops zu prüfen oder zu starten, wird die Eingabe der Anmeldeinformationen über die Befehlszeilenoption nicht unterstützt. Verwenden Sie als



Workaround das externe **AuthManager**-Modul, wenn Sie keine Anmeldeinformationen über die Befehlszeile bereitstellen.

- Das **Storebrowse**-Hilfsprogramm unterstützt derzeit nur ein einzelnes, Store-konfiguriertes Citrix Gateway auf dem StoreFront-Server.
- Die Funktion "Credential Injection" im **Storebrowse**-Hilfsprogramm funktioniert nur, wenn Citrix Gateway mit einstufiger Authentifizierung konfiguriert ist.
- Für die Befehlszeilenoptionen **Username** (-U), **Password** (-P) und **Domain** (-D) im **Storebrowse**-Hilfsprogramm wird die Groß- und Kleinschreibung beachtet und es dürfen nur Großbuchstaben verwendet werden.

Um Single Sign-On für Anwendungen von Drittanbietern zu aktivieren, die ICOSDK verwenden, erstellen Sie die folgende Registrierung:

- Registrierungsschlüssel: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Registrierungswert: vollständiger Pfad der Drittanbieteranwendungen
- Registrierungstyp: `reg_multi_sz`

Beispiel:

- Registrierungsschlüssel: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Registrierungswert: `C:\temp1\abc.exe;C:\temp2\xyz.exe`
- Registrierungstyp: `reg_multi_sz`

#### Hinweis:

- Sie können mehrere Anwendungen von Drittanbietern bereitstellen, indem Sie sie durch Semikolons trennen.
- Dieses Feature wird ab Version 2107 unterstützt.

## Storebrowse für Workspace

April 23, 2024

Die Citrix Workspace-App für Windows bietet **Storebrowse**-Unterstützung für Self-Service und On-Premises-Bereitstellung der Citrix Workspace-App. Außerdem ermöglicht sie Benutzern von **Storebrowse** den Zugriff auf Cloud- und Workspace-Features.

#### Hinweis:

- Dieser Artikel gilt nur für Cloud-Bereitstellungen von Citrix Workspace. Informationen zu On-Premises-Bereitstellungen finden Sie in der [Storebrowse-Dokumentation](#).
- Dieses Feature bietet **Storebrowse**-Unterstützung nur mit Single Sign-On.
- Die unter [Systemanforderungen und Kompatibilität](#) genannten Voraussetzungen müssen erfüllt sein, damit Benutzer das Feature nutzen können.
- Sie können SaaS-Apps oder [veröffentlichte Inhalte](#) nicht mit Storebrowse-Befehlen öffnen.

## Verwendung von Befehlen

Der folgende Abschnitt enthält detaillierte Informationen zu den Befehlen, die Sie im **Storebrowse**-Hilfsprogramm verwenden können.

#### Hinweis:

- Dieses Feature unterstützt auch andere Befehle des Self-Service-Plug-Ins, wie unter [CTX200337](#) beschrieben.
- Sie können die folgenden Befehle über die Eingabeaufforderung ausführen.
- **-a "discoveryurl"**: Fügt einen Store über die Befehlszeile hinzu. Es wird keine Authentifizierungsaufforderung angezeigt, wenn SSO aktiviert ist. Beispielsweise verbinden AAD-Domänen Geräte, bei denen die Authentifizierung über Webview erfolgt. Auf anderen Geräten wird die Authentifizierungsaufforderung angezeigt.
  - Beispiel:`SelfService.exe storebrowse -a "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
- **-d "discoveryurl"**: Löscht den Store.
  - Beispiel:`SelfService.exe storebrowse -d "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
- **-e "discoveryurl"**: Exportiert die Ressourcendetails im JSON-Format. Mit diesem Befehl wird die Datei `ressource.json` am Standardspeicherort `%LOCALAPPDATA%\citrix\selfservice` gespeichert. Die Citrix Workspace-App muss aktiviert sein, um diesen Befehl ausführen zu können, und der Benutzer muss angemeldet sein.
  - Beispiel:`SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

Sie können auch einen eigenen Pfad angeben, wenn Sie `ressource.json` nicht am Standardspeicherort speichern möchten.

- Beispiel: `.\SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"C:\Users\>\Documents\Fiddler2"`. Dadurch wird die Datei `ressource.json` unter `C:\Users\\Documents\Fiddler2` gespeichert.
- `-q "FriendlyName"discoveryurl"`: Verwenden Sie diesen Befehl für einen Schnellstart der angegebenen Ressource.
  - Beispiel:`SelfService.exe storebrowse -q "Excel 2016"https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

- `-launch "launchcommandline"`: Starten von Ressourcen mit "launchcommandline" aus `resource.json`.

**Hinweis:**

- Kopieren Sie die "launchcommandline" aus der Datei `resource.json`.
- Entfernen Sie `/` aus der in der Datei `resource.json` angegebenen "launchcommandline", bevor Sie den Befehl ausführen.

- Beispiel:`SelfService.exe storebrowse -launch -s store0-5c3ec017-CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-e33d0695df39 .Notepad -ica "https://cwawiniwstest.cloudburrito.com/Citrix/Store/resources/v2/YTlh0GUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkJm5Lk5-/launch/ica"-cmdline`

Nach dem Ausführen von `-launch "launchcommandline"` wird die ICA-Datei im Verzeichnis `%LOCALAPPDATA%\citrix\selfservice\cache` gespeichert. Doppelklicken Sie auf die ica-Datei, um die Ressource zu starten.

- `-liststore`: Listet die Stores auf, die in SSP hinzugefügt wurden. Die Storeliste enthält die `storeId` und die Discovery-URL für jeden Store.
  - Beispiel:`SelfService.exe storebrowse -liststore`

**Hinweis:**

Die Citrix Workspace-App muss aktiviert sein, um den Befehl `-liststore` ausführen zu können.

Der Befehl `Selfservice.exe storebrowse -liststore` speichert die Datei `store-details.json` unter `AppData\Local\Citrix\SelfService`.

## Problembehandlung

April 22, 2024

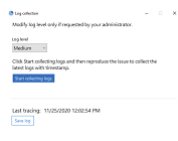
### Protokollsammlung

Protokollsammlung vereinfacht das Sammeln von Protokollen für die Citrix Workspace-App. Die Protokolle helfen Citrix bei der Problembehandlung und erleichtern bei komplizierten Problemen den Support. Dieses Feature ist in der Citrix Workspace-App für Windows Version 2012 und höher verfügbar.

Sie können Protokolle über die GUI sammeln.

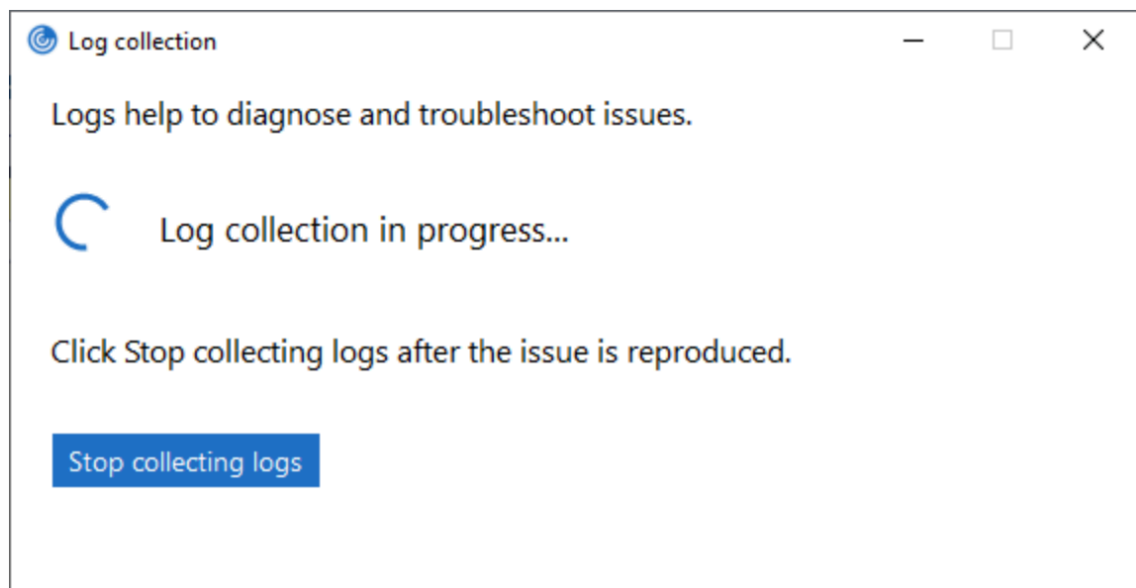
#### Protokolle sammeln:

1. Klicken Sie im Infobereich mit der rechten Maustaste auf das Citrix Workspace-App-Symbol und wählen Sie **Erweiterte Einstellungen**.
2. Wählen Sie **Protokollsammlung**.  
Das Dialogfeld “Protokollsammlung” wird angezeigt.



3. Wählen Sie eine der folgenden Protokollebenen aus:
  - Niedrig
  - Medium
  - Ausführlich
4. Klicken Sie auf **Protokollsammlung starten**, um das Problem zu reproduzieren und die neuesten Protokolle zu sammeln.

Der Protokollsammelungsprozess wird gestartet.



5. Klicken Sie auf **Protokollsammlung stoppen**, wenn Sie das Problem reproduziert haben.
6. Klicken Sie auf **Protokoll speichern**, um die Protokolle an einem gewünschten Ort zu speichern.

## In Protokollen erfasste Daten

### Hardware

- Informationen zu angeschlossenen Monitoren
- Speicherinformationen
- Netzwerkadapter
- Prozessor
- Direct X-Diagnoseinformationen

### Software

- Citrix Workspace-App
- Betriebssysteminformationen (Version, Service Pack und Architektur)
- Internet Explorer-Version
- Standardbrowser
- ActiveX Flash-Version
- NPAPI Flash-Version

### Registrierung

- HKEY\_LOCAL\_MACHINE\Software\Citrix\AuthManager

- HKEY\_LOCAL\_MACHINE\Software\Citrix\CitrixCAB
- HKEY\_LOCAL\_MACHINE\Software\Citrix\Dazzle
- HKEY\_LOCAL\_MACHINE\Software\Citrix\ICA Client
- HKEY\_LOCAL\_MACHINE\Software\Citrix\Install
- HKEY\_LOCAL\_MACHINE\Software\Citrix\InstallDetect
- HKEY\_LOCAL\_MACHINE\Software\Citrix\PluginPackages
- HKEY\_LOCAL\_MACHINE\Software\Citrix\Receiver
- HKEY\_LOCAL\_MACHINE\Software\Citrix\ReceiverInside
- HKEY\_LOCAL\_MACHINE\Software\Citrix\XenDesktop
- HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\NetworkProvider\Order
- HKEY\_CURRENT\_USER\Software\Citrix\AuthManager
- HKEY\_CURRENT\_USER\Software\Citrix\CitrixCAB
- HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- HKEY\_CURRENT\_USER\Software\Citrix\ICA Client
- HKEY\_CURRENT\_USER\Software\Citrix\Install
- HKEY\_CURRENT\_USER\Software\Citrix\InstallDetect
- HKEY\_CURRENT\_USER\Software\Citrix\PluginPackages
- HKEY\_CURRENT\_USER\Software\Citrix\Receiver
- HKEY\_CURRENT\_USER\Software\Citrix\ReceiverInside
- HKEY\_CURRENT\_USER\Software\Citrix\XenDesktop
- HKEY\_CURRENT\_USER\Software\Policies\Citrix
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains

### **Ereignisprotokolle**

- Anwendungsereignisprotokoll
- Systemereignisprotokoll

### **Ablaufverfolgung**

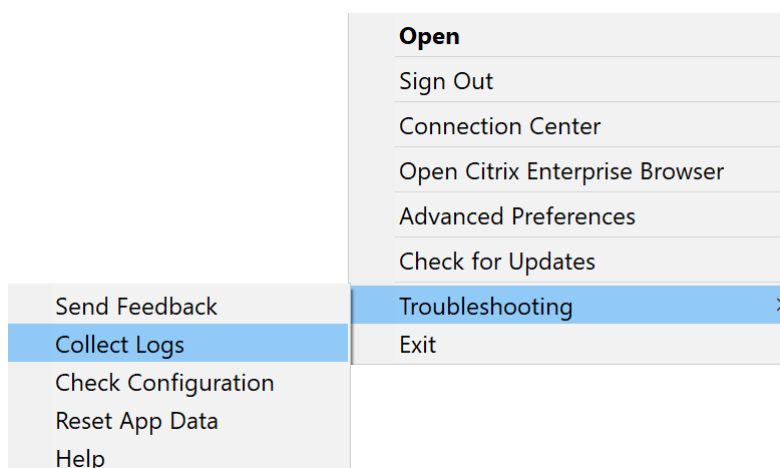
- HDX
- Receiver-Shell, Authentifizierungsmanager und Self-Service-Plug-In
- Installationsprotokolle
- Always-On-Protokolle

## Option “**Problembehandlung**” zu Taskleiste der Citrix Workspace-App hinzugefügt

Die Option **Problembehandlung** wurde eingeführt, um die Benutzererfahrung zu verbessern und die Problembehandlung zu vereinfachen. Sie können auf der Taskleiste unten rechts mit der rechten Maustaste auf das Symbol der Citrix Workspace-App klicken und dann **Problembehandlung** auswählen, um darauf zuzugreifen.

Verfügbare Optionen:

- Feedback senden
- Protokolle sammeln
- Konfiguration überprüfen
- App-Daten zurücksetzen
- Hilfe

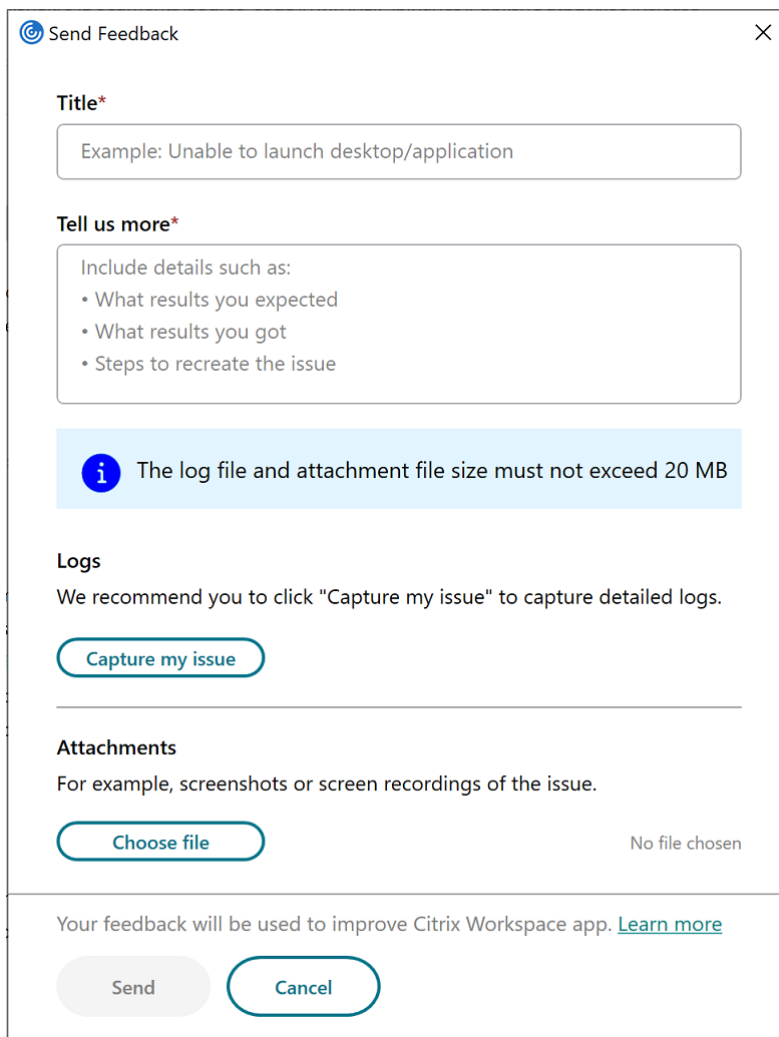


## Feedback zur Citrix Workspace-App senden

Mit der Option **Feedback senden** können Sie Citrix über Probleme bei der Verwendung der Citrix Workspace-App informieren und Verbesserungsvorschläge für die App einsenden.

Sie können Feedback wie folgt einreichen:

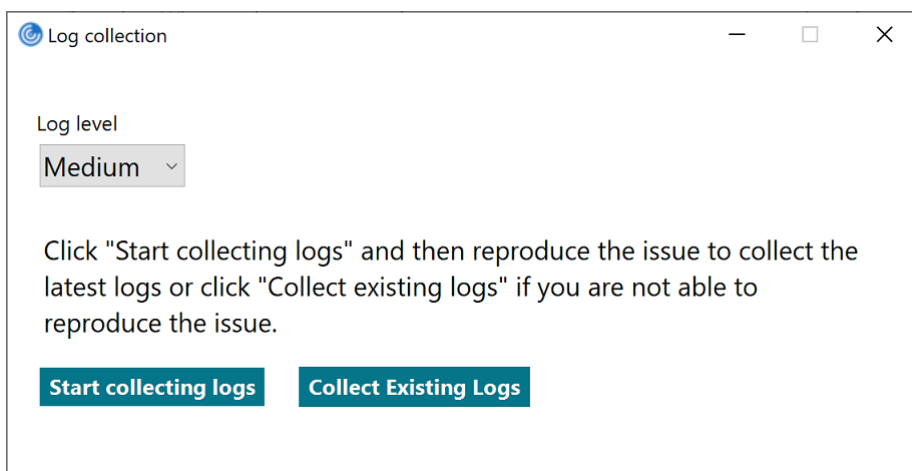
1. Klicken Sie mit der rechten Maustaste auf das Citrix Workspace-App-Symbol im Infobereich und wählen Sie **Problembehandlung > Feedback senden**. Die Seite **Feedback senden** wird angezeigt.



The image shows a 'Send Feedback' dialog box with the following sections:

- Title\***: A text input field containing the example text 'Example: Unable to launch desktop/application'.
- Tell us more\***: A text area containing the instruction 'Include details such as:' followed by a bulleted list: 'What results you expected', 'What results you got', and 'Steps to recreate the issue'.
- Information icon**: A blue circle with a white 'i' icon, followed by the text 'The log file and attachment file size must not exceed 20 MB'.
- Logs**: A section with the text 'We recommend you to click "Capture my issue" to capture detailed logs.' and a button labeled 'Capture my issue'.
- Attachments**: A section with the text 'For example, screenshots or screen recordings of the issue.' and a button labeled 'Choose file'. To the right of the button, it says 'No file chosen'.
- Footer**: A line of text stating 'Your feedback will be used to improve Citrix Workspace app. [Learn more](#)'.
- Buttons**: Two buttons at the bottom: 'Send' and 'Cancel'.

2. Geben Sie den **Titel** ein.
3. Geben Sie im Feld **Weitere Informationen** Informationen zu dem Problem ein.
4. Klicken Sie auf **Mein Problem aufzeichnen**. Die Seite **Protokollsammlung** wird angezeigt.

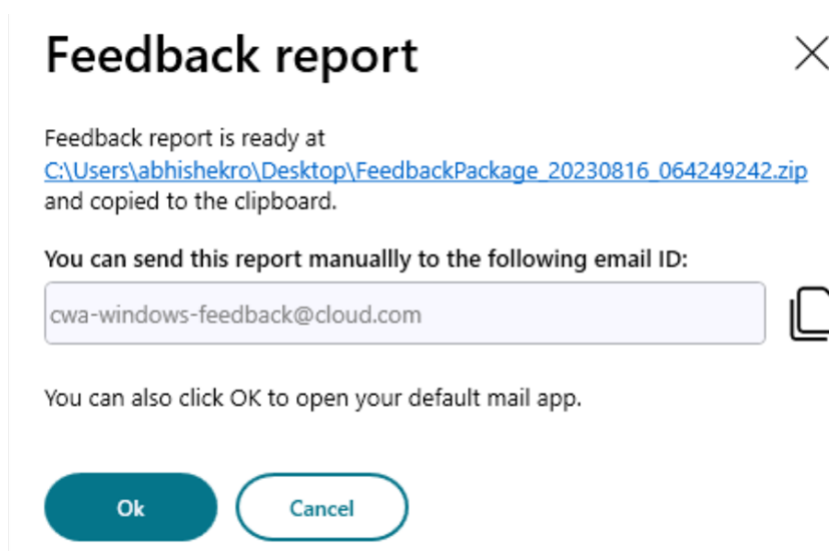


The image shows a 'Log collection' dialog box with the following elements:

- Log level**: A dropdown menu currently set to 'Medium'.
- Instructions**: Text stating 'Click "Start collecting logs" and then reproduce the issue to collect the latest logs or click "Collect existing logs" if you are not able to reproduce the issue.'
- Buttons**: Two buttons at the bottom: 'Start collecting logs' and 'Collect Existing Logs'.



- a) Klicken Sie auf **Protokollsammlung starten** und reproduzieren Sie das Problem, um die neuesten Protokolle zu sammeln.
  - b) Klicken Sie auf **Protokollsammlung stoppen**, wenn Sie das Problem reproduziert haben.  
Oder  
Klicken Sie auf **Vorhandene Protokolle sammeln**, wenn Sie das Problem nicht reproduzieren können.
  - c) Klicken Sie auf **Protokollsammlung stoppen**, wenn Sie das Problem reproduziert haben.
5. Vergewissern Sie sich, dass die Protokolldateien neben **Mein Problem aufzeichnen** angezeigt werden.
  6. Klicken Sie auf **Datei auswählen** und fügen Sie Anhänge hinzu, in denen das Problem beschrieben wird (Screenshots, Bildschirmaufzeichnungen usw.). Die maximal zulässige Dateigröße für alle Anlagen einschließlich der Protokolldatei beträgt 20 MB.
  7. Klicken Sie auf **Senden**. Die Seite **Feedbackbericht** wird angezeigt.



Die ZIP-Datei enthält die Protokolldateien, die Problembeschreibung in Form von Testdateien und die Anhänge.

8. Sie können den Feedbackbericht auf eine der folgenden Weisen an Citrix senden:
  - Klicken Sie auf **OK**, um die Standard-E-Mail-App Ihres Systems zu verwenden.

Oder

- Senden Sie den Bericht manuell an die angegebene E-Mail-Adresse.

**Hinweis:**

Stellen Sie sicher, dass die ZIP-Datei an die E-Mail angehängt ist.

## Einstellung von Features und Plattformen

April 22, 2024

Die Ankündigungen in diesem Artikel bieten Ihnen frühzeitige Informationen über Plattformen, Citrix Produkte und Features, die ausgemustert werden. Dies hilft Ihnen, rechtzeitig Geschäftsentscheidungen zu treffen.

Citrix überwacht die Nutzung von Features und Feedback, um den geeigneten Zeitpunkt für eine Außerbetriebnahme zu wählen. Diese Informationen unterliegen Änderungen in nachfolgenden Releases und enthalten ggf. nicht jedes veraltete Element.

Veraltete Elemente werden nicht sofort entfernt. Citrix setzt den Support in diesem Release fort, aber die Elemente werden in einem zukünftigen Release entfernt.

### Einstellung von Features und Plattformen - Tabelle

---

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Internet Explorer-basierte Browserinhaltsumleitung	2311.1	2311.1	Google Chrome-basierte Browserinhaltsumleitung
Unterstützung für das WebRTC SDP-Format (Plan B)	2309		Aktualisieren Sie die Citrix Workspace-App auf eine unterstützte Version.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Unterstützung für den Einzelfenstermodus in Optimierung für Microsoft Teams	2309		Aktualisieren Sie die Citrix Workspace-App auf eine Version, die den Mehrfenstermodus unterstützt. Weitere Informationen finden Sie unter <a href="#">Featurematrix und Versionsunterstützung</a> .
Switch / <code>includeappprotection</code>	2212	2212	Starten der Komponente "App Protection" mit / <code>startappprotection</code>
Unterstützung für benutzerdefinierte URLs für 301-Weiterleitungen	2210		URL-Migration von StoreFront zu Workspace
Unterstützung für Windows 8.1 und Windows Server 2012 R2	2204.1	2204.1	Verwenden Sie das im Abschnitt <a href="#">Systemanforderungen</a> angegebene unterstützte Betriebssystem.
Citrix Casting wird standardmäßig mit der Citrix Workspace-App installiert	2112.1	2205	Citrix Casting kann bei Bedarf mit der Citrix Workspace-App installiert werden. <b>Hinweis:</b> Citrix Casting wird nicht standardmäßig mit der Citrix Workspace-App installiert.

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Option <b>Alle Konten</b> im Menü nur für Workspace (Cloud)-Stores.	2112.1	2202	
Die Option <b>Kennwort speichern</b> im Anmeldebildschirm in Workspace-App (Cloud) Stores.	2008	2008	
Citrix Receiver für UWP (Universelle Windows-Plattform)	2006	2102	
Die Option zum Hinzufügen oder Entfernen von Beschreibungen für Stores im Dialogfeld <b>Konten hinzufügen oder entfernen</b> . Die Spalte <b>Beschreibung</b> ist veraltet.	2006.1		Sie können Storekontodetails hinzufügen oder entfernen, ohne eine Beschreibung hinzuzufügen.
Die Option zum Aktivieren oder Deaktivieren von Stores im Dialogfeld <b>Konten hinzufügen oder entfernen</b>	2006.1		
Unterstützung für Windows 7	2002	2006.1	Verwenden Sie das im Abschnitt <a href="#">Systemanforderungen</a> angegebene unterstützte Betriebssystem. <b>Hinweis:</b> Windows 7 wird in Version 2002 unterstützt.

---

Element	Einstellung der Unterstützung angekündigt	Entfernt in	Alternative
Switch <code>/rcu</code> im Installationsprogramm	1909		Verwenden Sie Switch <code>/forceinstall</code> statt <code>/rcu</code> .
On-Demand-Installation von Citrix Casting mit der Citrix Workspace-App	2112.1	2402	Ältere Version der Citrix Workspace-App verwenden

---



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).